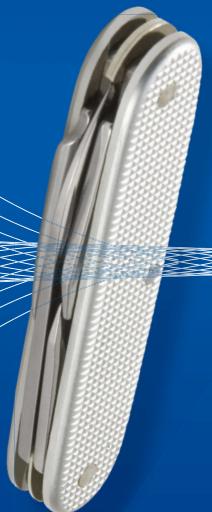




Windows Server® 2012

William R. Stanek



Guia de Bolso



O autor



WILLIAM R. STANEK (www.williamstanek.com) tem mais de 20 anos de experiência prática em programação e desenvolvimento avançados. É especialista em tecnologia, autor premiado e excelente instrutor. Ao longo dos anos, o seu aconselhamento prático ajudou milhares de programadores, desenvolvedores e engenheiros de redes no mundo todo.

William está envolvido com a comunidade da Internet comercial desde 1991. Seus principais conhecimentos e experiência em tecnologia são provenientes de mais de 11 anos de serviço militar. Tem grande experiência no desenvolvimento de tecnologias de servidor, criptografia e soluções para Internet. Escreveu diversos *white papers* técnicos e cursos de treinamento sobre uma ampla variedade de tópicos. Com frequência, atua como consultor e especialista no assunto.

William tem mestrado com distinção em sistemas de informação e bacharelado em Ciência da Computação, *magna cum laude*. Orgulha-se de ter servido na Guerra do Golfo como membro da tripulação de combate em um avião de guerra. Esteve no ar em várias missões no Iraque e recebeu nove medalhas por seu serviço durante a guerra, incluindo uma das mais altas condecorações da força aérea dos Estados Unidos, a Air Force Distinguished Flying Cross. Atualmente, mora no Noroeste Pacífico com a esposa e os filhos.

William redescobriu sua paixão por atividades ao ar livre recentemente. Quando não está escrevendo, pode ser encontrado escalando, pedalando, fazendo mochilão ou viajando com a família em busca de aventura!

Encontre o William no Twitter, em [@WilliamStanek](https://twitter.com/WilliamStanek), e no Facebook, em [www.facebook.com\William.Stanek.Author](https://facebook.com/William.Stanek.Author).



S786w

Stanek, William R.

Windows Server 2012 [recurso eletrônico] : guia de bolso / William R. Stanek ; tradução: Scientific Linguagem Ltda ; revisão técnica: Luciana Monteiro Michel. – Dados eletrônicos. – Porto Alegre : Bookman, 2014.

Editado também como livro impresso em 2014.
ISBN 978-85-8260-169-3

1. Informática. 2. Programa de computador. 3. Windows Server 2012. I. Título.

CDU 004.4(036)WINDOWS SERVER

William R. Stanek



Windows Server® 2012

Guia de Bolso

Tradução:

Scientific Linguagem Ltda.

Revisão Técnica:

Luciana Monteiro Michel
Profissional com certificações MCSA, MCSE, MCTS, MCITP, MCT
Instrutora da Alfamídia Prow – Educação Profissional

Versão impressa
desta obra: 2014



2014

Obra originalmente publicada sob o título *Windows Server® 2012 Pocket Consultant*,
de William R. Stanek.

ISBN 978-0-7356-6633-7

Edição original em inglês copyright©2012 de William R. Stanek

Tradução para a língua portuguesa Copyright © 2014, Bookman Companhia Editora Ltda., uma empresa do Grupo A Educação S.A. Tradução publicada e comercializada com permissão da O'Reilly Media, Inc., que detém ou controla todos os direitos de publicação e comercialização da mesma.

Gerente editorial: *Arysinha Jacques Affonso*

Colaboraram nesta edição:

Editora: *Mariana Belloli*

Capa: *Kaéle*, arte sobre capa original

Leitura final: *Bianca Basile*

Editoração eletrônica: *Techbooks*

Microsoft e todas as marcas listadas em <http://www.microsoft.com/about/legal/en/us/Intellectual-Property/Trademarks/EN-US.aspx> são marcas comerciais registradas do grupo de empresas da Microsoft. Outras marcas mencionadas aqui são marcas comerciais de seus respectivos proprietários.

Os exemplos de empresas, organizações, produtos, nomes de domínio, endereços de correio eletrônico, logotipo, pessoas, lugares ou eventos aqui apresentados são fictícios. Nenhuma associação com qualquer empresa, organização, produto, nome de domínio, endereço de correio eletrônico, logotipo, pessoa, lugar ou eventos reais foi proposital ou deve ser inferido.

Este livro expressa as visões e opiniões dos autores. As informações aqui contidas são fornecidas sem quaisquer garantias expressas, legais ou implícitas. Os autores, a Microsoft Corporation e seus revendedores ou distribuidores não poderão ser responsabilizados por qualquer dano causado, ou supostamente causado, direta ou indiretamente, por este livro.

Reservados todos os direitos de publicação, em língua portuguesa, à
BOOKMAN EDITORA LTDA., uma empresa do GRUPO A EDUCAÇÃO S.A.
Av. Jerônimo de Ornelas, 670 – Santana
90040-340 – Porto Alegre – RS
Fone: (51) 3027-7000 Fax: (51) 3027-7070

É proibida a duplicação ou reprodução deste volume, no todo ou em parte, sob quaisquer formas ou por quaisquer meios (eletrônico, mecânico, gravação, fotocópia, distribuição na Web e outros), sem permissão expressa da Editora.

Unidade São Paulo
Av. Embaixador Mamedo Soares, 10.735 – Pavilhão 5 – Cond. Espace Center
Vila Anastácio – 05095-035 – São Paulo – SP
Fone: (11) 3665-1100 Fax: (11) 3667-1333

SAC 0800 703-3444 – www.grupoa.com.br

IMPRESSO NO BRASIL
PRINTED IN BRAZIL

A minha esposa – que por muitos anos, ao longo de muitos livros, milhares de palavras e centenas de páginas esteve presente, oferecendo apoio e encorajamento e fazendo de cada lugar em que moramos um lar.

Aos meus filhos – por me ajudarem a enxergar o mundo de novas maneiras, por terem uma paciência excepcional e um amor sem limites e por fazerem de cada dia uma aventura.

A Karen, Martin, Lucinda, Juliana e vários outros que ajudaram de formas grandiosas ou singelas.

—WILLIAM R. STANEK

Sumário

Introdução

Para quem é este livro?xxvi
Como este livro está organizadoxxvii
Convenções usadas neste livro.....	.xxvii
Outros recursos.....	.xxviii
Suporte técnico.....	.xxix

PARTE I NOÇÕES BÁSICAS DA ADMINISTRAÇÃO DO WINDOWS SERVER 2012

Capítulo 1 Visão geral da administração do Windows Server 2012	3
Windows Server 2012 e Windows 8	3
Introdução ao Windows Server 2012	6
Opções de gerenciamento de energia	8
Ferramentas e protocolos de rede.....	11
Para entender as opções de rede	12
Como trabalhar com protocolos de rede.....	13
Controladores de domínio, servidores membros e serviços de domínio.....	14
Como trabalhar com o Active Directory.....	15
Como utilizar controladores de domínio somente leitura....	16
Como utilizar o Restartable Active Directory Domain Services.....	17
Serviços de resolução de nomes	18
Como utilizar o DNS	18
Como utilizar o Windows Internet Name Service.....	20
Como utilizar o Link-Local Multicast Name Resolution (LLMNR).....	22
Ferramentas frequentemente utilizadas.....	24
Windows PowerShell 3.0.....	24
Windows Remote Management	26

Capítulo 2	Gerenciamento de servidores com o Windows Server 2012	30
Funções de servidor, serviços de função e recursos para o Windows Server 2012	31	
Instalações de servidor completo, interface mínima e Server Core.....	39	
Navegação no Server Core.....	39	
Instalação do Windows Server 2012	42	
Instalação limpa	43	
Instalação de atualização	46	
Realização de tarefas administrativas adicionais durante a instalação	47	
Alteração da opção de instalação	54	
Gerenciamento de funções, serviços de função e recursos	56	
Realização de tarefas de configuração inicial	57	
Princípios básicos do Server Manager e binários	61	
Como gerenciar servidores remotamente	64	
Conexão e trabalho em servidores remotos	66	
Adição e remoção de funções, serviços de função e recursos.....	69	
Gerenciamento de propriedades do sistema	72	
A guia Computer Name	74	
A guia Hardware	74	
A guia Advanced	75	
A guia Remote	84	
Capítulo 3	Monitoramento de processos, serviços e eventos	85
Gerenciamento de aplicativos, processos e desempenho	85	
Task Manager	86	
Como visualizar e trabalhar com processos.....	86	
Administração de Processos.....	88	
Visualização de serviços do sistema	92	
Visualização e gerenciamento de desempenho do sistema	93	
Visualização e gerenciamento de sessões de usuário remoto	97	

Gerenciamento de serviços do sistema.....	98
Navegação por serviços no Server Manager.....	98
Navegação por serviços no Computer Management	100
Como iniciar, interromper e pausar serviços	101
Configuração de inicialização de serviço.....	101
Configuração de logon de serviço	102
Configuração de recuperação de serviço.....	104
Como desabilitar serviços desnecessários	105
Log e visualização de eventos	106
Acesso a eventos no Server Manager.....	107
Acesso a eventos no Event Viewer	108
Filtragem de logs de eventos.....	110
Configuração das opções de log de eventos.....	113
Limpeza de logs de eventos.....	114
Arquivamento de logs de eventos	114
Monitoramento de desempenho e atividade do servidor.....	116
Por que monitorar seu servidor?.....	116
Preparação para o monitoramento.....	117
Uso dos consoles de monitoramento.....	117
Escolha de contadores para monitoramento	120
Registro em log de desempenho	122
Visualização de relatórios de coletores de dados.....	126
Configuração de alertas de contadores de desempenho ..	127
Ajuste do desempenho do sistema	128
Monitoramento e ajuste do uso de memória	128
Monitoramento e ajuste do uso de processador	130
Monitoramento e ajuste de I/O de disco	131
Monitoramento e ajuste de largura de banda e conectividade de rede	132
Capítulo 4 Automatização de tarefas administrativas, políticas e procedimentos	133
Group Policies	135
Noções básicas sobre Group Policies	136
Em que ordem são aplicadas as políticas quando há várias políticas?	137

Quando as Group Policies são aplicadas?	137
Requisitos de Group Policy e compatibilidade de versões	138
Navegação pelas alterações em Group Policy	139
Gerenciamento de Group Policies locais.....	141
Objetos de Group Policy locais	141
Acesso às configurações de política local de nível superior	142
Configurações de objetos de Group Policy locais.....	143
Como acessar Group Policies locais específicas para usuários, para administradores e para não administradores	144
Gerenciamento de políticas de site, domínio e unidade organizacional	144
Como usar o Group Policy Management Console	146
Apresentação do editor de políticas.....	147
Uso de modelos administrativos para configurar políticas..	148
Criação e vinculação de GPOs	150
Criação e uso de GPOs de início	151
Delegação de privilégios para o gerenciamento de Group Policy	151
Bloqueio, modificação e desabilitação de políticas	153
Manutenção e solução de problemas de Group Policy	156
Atualização de Group Policy	156
Configuração do intervalo de atualização.....	157
Modelagem de Group Policy para fins de planejamento ..	159
Como copiar, colar e importar objetos de diretiva.....	162
Backup e restauração de objetos de diretiva.....	163
Como determinar as configurações e o status de atualização da Group Policy.....	164
Como desabilitar uma parte não usada da Group Policy ..	164
Alteração das preferências de processamento da política ..	165
Configuração da detecção de links lentos	165
Remoção de vínculos e exclusão de GPOs.....	168
Solução de problemas de Group Policy	169
Correção de Group Policy Objects padrão.....	170
Gerenciamento de usuários e computadores com Group Policy	171
Gerenciamento centralizado de pastas especiais	171
Gerenciamento de scripts de usuário e computador.....	176
Implantação de software com Group Policy	179

Registro automático de certificados de computador e usuário	184
Configuração do Automatic Updates na Group Policy	185
Capítulo 5 Como melhorar a segurança dos computadores	189
Utilização de modelos de segurança.....	189
Utilização dos snap-ins Security Templates e Security Configuration And Analysis	191
Como examinar e alterar configurações do modelo	191
Análise, exame e aplicação de modelos de segurança	199
Implantação de modelos de segurança em vários computadores	202
Utilização do Security Configuration Wizard.....	204
Criação de políticas de segurança.....	204
Edição de políticas de segurança.....	209
Aplicação de políticas de segurança.....	209
Reversão da última política de segurança aplicada	209
Implantação de uma política de segurança em vários computadores	210

PARTE II ADMINISTRAÇÃO DOS SERVIÇOS DE DIREtório DO WINDOWS SERVER 2012

Capítulo 6 Como utilizar o Active Directory	215
Noções básicas sobre o Active Directory	215
Active Directory e DNS	215
Implantação de RODC.....	217
Recursos do Active Directory para o Windows Server 2008 R2	218
Recursos do Active Directory para o Windows Server 2012.....	219
Como trabalhar com estruturas de domínio	221
Noções básicas sobre domínios.....	222
Noções básicas sobre floresta de domínio e árvore de domínios	223
Unidades Organizacionais	225
Noções básicas sobre sites e sub-redes	227

Como trabalhar com domínios do Active Directory	228
Como utilizar computadores com o Active Directory	228
Níveis funcionais de domínio.	229
A estrutura de diretório	235
O armazenamento de dados	236
Os catálogos globais	237
Cache de Associação de Grupo Universal	238
Replicação e o Active Directory	238
O Active Directory e o LDAP	240
Noções básicas sobre funções de mestre de operações	240
Como utilizar a Lixeira do Active Directory	242
Como preparar o esquema para a lixeira	242
Como recuperar objetos excluídos	243
Capítulo 7 Administração básica do Active Directory	247
Ferramentas para o gerenciamento do Active Directory	247
Ferramentas administrativas do Active Directory	247
Ferramentas de linha de comando do Active Directory	248
Ferramentas de suporte do Active Directory	249
Como utilizar o Active Directory Users And Computers	250
Active Directory Administrative Center e Windows PowerShell	254
Gerenciamento de contas de computador.	257
Criação de contas de computador para uma estação de trabalho ou servidor	257
Criação de contas de computador no Active Directory Administrative Center	258
Criação de contas de computador no Active Directory Users And Computers	259
Visualização e edição das propriedades da conta de computador	261
Como excluir, desabilitar e habilitar contas de computador.	262
Como redefinir contas de computador bloqueadas	262
Como mover contas de computador	264
Gerenciamento de computadores.	265
Como ingressar um computador a um domínio ou grupo de trabalho	265
Como usar o ingresso offline ao domínio	266

Gerenciamento de controladores de domínio, funções e catálogo	268
Como instalar e rebaixar controladores de domínio	268
Visualização e transferência de funções de domínio	271
Visualização e transferência da função mestre de nomeação de domínios	272
Visualização e transferência da função de mestre de esquema	273
Como transferir funções usando a linha de comando	274
Como capturar funções usando a linha de comando	274
Configuração de catálogos globais	278
Configuração de cache de associação de grupo universal ..	279
Gerenciamento de unidades organizacionais	279
Como criar unidades organizacionais	279
Visualização e edição de propriedades de unidade organizacional	280
Como renomear ou excluir unidades organizacionais	280
Como mover unidades organizacionais	280
Gerenciamento de sites	280
Criação de sites	281
Criação de sub-redes	282
Associação de controladores de domínio a sites	283
Configuração de links de site	283
Configuração de pontes de link de site	286
Manutenção do Active Directory	287
Como usar o ADSI Edit	287
Como examinar a topologia entre sites	289
Solução de problemas do Active Directory	290
Capítulo 8 Como criar contas de usuário e de grupo	293
Modelo de segurança do Windows Server	294
Protocolos de autenticação	294
Controles de acesso	295
Controles de acesso baseados em declarações	295
Políticas de acesso central	297
Diferenças entre contas de usuário e de grupo	299
Contas de usuário	299
Contas de grupo	300

Contas de usuário e grupos padrão.....	304
Contas de usuário internas.....	305
Contas de usuário predefinidas.....	305
Grupos internos e predefinidos.....	306
Grupos implícitos e identidades especiais	307
Capacidades de conta	307
Privilégios	308
Direitos de logon	310
Capacidades internas para grupos no Active Directory.....	311
Uso de contas de grupo padrão.....	313
Grupos usados por administradores.....	314
Grupos implícitos e identidades	315
Configuração e organização da conta de usuário.....	316
Políticas de nomeação de contas	317
Políticas de senha e conta.....	318
Configuração das políticas de conta	320
Configuração de políticas de senha	321
Configuração de política de bloqueio de conta	323
Configuração de políticas do Kerberos.....	324
Configuração das políticas de direitos do usuário	325
Direitos globais do usuário.....	326
Direitos locais do usuário	328
Como adicionar uma conta de usuário.....	328
Como criar contas de usuário de domínio.....	328
Como criar contas de usuário locais	332
Como adicionar uma conta de grupo	333
Como criar um grupo global	334
Como criar um grupo local e atribuir membros	335
Manipulação de associação de grupo.....	336
Gerenciamento de associação individual.....	337
Gerenciamento de várias associações a um grupo	338
Configuração do grupo primário para usuários e computadores	338
Implementação de contas gerenciadas.....	339
Como criar e usar as contas de serviço gerenciado	340

Configuração de serviços para o uso de contas de serviço gerenciado	342
Como remover contas de serviço gerenciado	342
Como mover contas de serviço gerenciado	343
Uso de contas virtuais	344
Capítulo 9 Gerenciamento de contas de usuário e de grupo	345
Gerenciamento das informações de contato do usuário	345
Configuração das informações de contato	345
Como pesquisar usuários e grupos no Active Directory	348
Configurações do ambiente do usuário	349
Variáveis de ambiente do sistema	350
Scripts de logon	351
Atribuição de pastas base	352
Configuração de opções e restrições de conta	353
Gerenciamento do horário de logon	353
Configuração de estações de trabalho com logon permitido	355
Configuração de privilégios de discagem e VPN	356
Configuração das opções de segurança da conta	358
Gerenciamento de perfis de usuário	359
Perfis locais, móveis e obrigatórios	360
Como usar o utilitário System para gerenciar perfis locais	363
Atualização de contas de usuário e de grupo	366
Como renomear contas de usuário e de grupo	367
Como copiar contas de usuário de domínio	369
Importação e exportação de contas	370
Exclusão de contas de usuário e de grupo	371
Alteração e redefinição de senhas	371
Como habilitar contas de usuário	372
Gerenciamento de várias contas de usuário	373
Configuração de perfis para várias contas	374
Definição do horário de logon para várias contas	375
Definição de estações de trabalho permitidas para logon para várias contas	376

Configuração de propriedades de logon, senha e data de validade para vários usuários.....	376
Solução de problemas de logon.....	376
Visualização e configuração de permissões no Active Directory	378

PARTE III ADMINISTRAÇÃO DE DADOS DO WINDOWS SERVER 2012

Capítulo 10 Gerenciamento de sistemas de arquivos e unidades	383
Gerenciamento da função File Services	383
Como adicionar unidades de disco rígido	387
Unidades físicas	387
Preparação de uma unidade física para uso	390
Utilização do Disk Management	392
Dispositivos de armazenamento removíveis	394
Instalação e verificação de uma nova unidade	396
O status da unidade.	397
Como trabalhar com discos básicos, dinâmicos e virtuais	399
Utilização dos discos básicos e dinâmicos	399
Considerações especiais para discos básicos e dinâmicos ..	400
Alteração dos tipos de unidade.....	400
Reativação de discos dinâmicos	402
Como reexaminar os discos	402
Como mover um disco dinâmico para um novo sistema ..	402
Gerenciamento de discos rígidos virtuais	404
Utilização de discos e partições básicos	404
Conceitos básicos de particionamento.....	404
Criação de partições e volumes simples.....	405
Formatação de partições	408
Compactação de unidades e dados.....	409
Compactação de unidades.....	410
Compactação de diretórios e arquivos.....	410
Como expandir unidades compactadas.....	411
Como expandir pastas e arquivos compactados.....	411

Criptografia de unidades e dados	411
Criptografia e o Encrypting File System.....	412
Criptografia de pastas e arquivos	413
Como trabalhar com arquivos e pastas criptografados.....	414
Configuração da política de recuperação	415
Descriptografia de arquivos e diretórios	416
Capítulo 11 Configuração de volumes e matrizes RAID	417
Como utilizar volumes e conjuntos de volumes	418
Noções básicas sobre volumes	418
Sobre conjuntos de volumes	420
Como criar volumes e conjuntos de volumes	422
Como excluir volumes e conjuntos de volumes	424
Gerenciamento de volumes	424
Como melhorar o desempenho e a tolerância a falhas com RAID	424
Implementação de RAID no Windows Server 2012	425
Implementação do RAID-0: Faixa de disco	426
Implementação do RAID-1: Espelhamento de disco	427
Implementação do RAID-5: Faixa de disco com paridade..	429
Gerenciamento de RAID e recuperação após falhas.....	430
Como quebrar um conjunto espelhado.....	430
Como resincronizar e reparar um conjunto espelhado	430
Como reparar um volume de sistema espelhado para habilitar inicialização	431
Como remover um conjunto espelhado	432
Como reparar um conjunto distribuído sem paridade	432
Como regenerar um conjunto distribuído com paridade....	432
Gerenciamento de armazenamento baseado em padrões	433
Introdução ao armazenamento baseado em padrões.....	433
Como trabalhar com o armazenamento baseado em padrões.....	434
Como criar pools de armazenamento e alocar espaço	436
Como criar espaços de armazenamento	437
Como criar um disco virtual em um espaço de armazenamento	438
Como criar um volume padrão	440

Gerenciamento de partições e unidades existentes	441
Como atribuir letras e caminhos de unidade	441
Como alterar ou excluir o rótulo de um volume.	442
Como excluir partições e unidades.	443
Como converter volumes FAT em NTFS.	443
Como redimensionar partições e volumes.	445
Como reparar erros e inconsistências de disco automaticamente.	447
Como analisar e otimizar discos	451
Capítulo 12 Compartilhamento de dados, segurança e auditoria	454
Como utilizar e habilitar o compartilhamento de arquivos	455
Configuração de compartilhamento de arquivos padrão	458
Visualização de compartilhamentos existentes.	458
Criação de pastas compartilhadas no Computer Management	460
Criação de pastas compartilhadas no Server Manager	463
Alteração das configurações de pasta compartilhada	465
Gerenciamento de permissões de compartilhamento	466
Permissões de compartilhamento variadas	466
Visualização e configuração de permissões de compartilhamento	467
Gerenciamento de compartilhamentos existentes	471
Os compartilhamentos especiais.	471
Conexão com compartilhamentos especiais	472
Visualização de sessões de usuário e computador.	473
Interrupção do compartilhamento de arquivos e pastas.	475
Configuração do compartilhamento NFS.	476
Utilização de cópias de sombra	478
As cópias de sombra	478
Criação de cópias de sombra.	479
Restauração de uma cópia de sombra	479
Reversão de um volume inteiro para uma cópia de sombra anterior	480
Exclusão de cópias de sombra	480
Como desabilitar cópias de sombra	481

Conexão com unidades de rede	481
Mapeamento de uma unidade de rede	481
Desconexão de uma unidade de rede	482
Gerenciamento, posse e herança de objetos	482
Objetos e gerenciadores de objetos	482
Posse e transferência de objetos	483
Herança de objeto	484
Permissões de arquivos e pastas.	485
As permissões de arquivos e pastas	486
Configuração de permissões básicas de arquivos e pastas ..	488
Configuração de permissões especiais em arquivos e pastas	490
Configuração de permissões baseadas em declarações.....	493
Auditoria de recursos do sistema.....	495
Configuração de políticas de auditoria	495
Auditoria de arquivos e pastas.....	497
Auditoria de registro	499
Auditoria de objetos do Active Directory.....	499
Utilização, configuração e gerenciamento de cotas de disco do NTFS	500
O que são cotas de disco NTFS e como elas são utilizadas ..	501
Configuração de políticas de cotas de disco NTFS.....	503
Habilitação de cotas de disco NTFS em volumes NTFS	505
Visualização de entradas de cota de disco.....	507
Criação de entradas de cota de disco.....	507
Exclusão de entradas de cota de disco.....	509
Exportação e importação de configurações de cotas de disco NTFS.....	509
Como desabilitar cotas de disco NTFS	510
Utilização, configuração e gerenciamento de cotas de disco do Resource Manager	511
Gerenciamento de modelos de cotas de disco.....	512
Criação de cotas de disco do Resource Manager.....	514
Capítulo 13 Backup e recuperação de dados	516
Como criar um plano de backup e recuperação	516
Elaboração de um plano de backup	516

Os tipos básicos de backup	518
Backup diferencial e backup incremental	519
Seleção de dispositivos e mídias de backup	519
Soluções comuns de backup	520
Compra e uso de mídia de backup.....	521
Seleção de um utilitário de backup.....	522
Backup de dados: fundamentos básicos.....	523
Instalação dos utilitários de backup e recuperação do Windows	523
Como iniciar os trabalhos com o Windows Server Backup ..	524
Como iniciar o trabalho com o utilitário de backup de linha de comando	526
Como trabalhar com os comandos do Wbadmin.....	528
Como usar comandos para fins gerais	528
Como utilizar comandos de gerenciamento de backup ..	529
Como utilizar comandos de gerenciamento de recuperação.....	530
Realização de backups do servidor	530
Configuração de backups agendados	532
Alteração ou interrupção de backups agendados	535
Criação e agendamento de backups com o Wbadmin ..	535
Execução de backups manuais.....	537
Como recuperar o servidor de falhas de hardware ou de inicialização	538
Como recuperar-se de um início com falhas.....	541
Como iniciar um servidor no modo de segurança.....	541
Backup e restauração do estado do sistema	543
Restauração do Active Directory	544
Restauração do sistema operacional e do sistema completo.....	544
Restauração de aplicativos, volumes que não são do sistema e arquivos e pastas	547
Gerenciamento de políticas de recuperação de criptografia.....	548
Noções básicas sobre certificados de criptografia e políticas de recuperação	548
Configuração da política de recuperação do EFS	550
Backup e restauração de dados criptografados e certificados ..	551
Backup de certificados de criptografia.....	551
Restauração de certificados de criptografia	552

PARTE IV ADMINISTRAÇÃO DE REDE DO WINDOWS SERVER 2012

Capítulo 14 Gerenciamento de redes TCP/IP	555
Como navegar por redes por meio do Windows Server 2012	555
Como gerenciar redes no Windows 8 e no Windows Server 2012	558
Como instalar redes TCP/IP.	561
Como configurar redes TCP/IP.	562
Como configurar endereços IP estáticos	562
Como configurar endereços IP dinâmicos e endereçamento IP alternativo	564
Como configurar múltiplos gateways.	565
Como configurar a rede para Hyper-V.	566
Como gerenciar conexões de rede	567
Como verificar o estado, velocidade e atividade das conexões de rede	567
Como habilitar e desabilitar conexões de rede.	568
Como renomear conexões de rede.	568
Capítulo 15 Como executar clientes e servidores DHCP	569
Introdução ao DHCP	569
Uso de endereçamento e configuração IPv4 dinâmico	569
Uso de endereçamento e configuração IPv6 dinâmico	571
Como verificar a atribuição de endereço IP.	574
Noções básicas sobre escopos.	574
Instalação de servidores DHCP.	575
Instalação de componentes DHCP	575
Como iniciar e usar o console DHCP	577
Como se conectar a servidores DHCP remotos.	578
Como iniciar e interromper um servidor DHCP	579
Como autorizar um servidor DHCP no Active Directory	579
Configuração de servidores DHCP.	580
Configuração das associações de servidor.	580
Atualização de estatísticas do DHCP.	580
Auditoria e solução de problemas do DHCP.	581
Integração do DHCP e do DNS	582

Integração do DHCP e da NAP	584
Como evitar conflitos de endereço IP.....	587
Como salvar e restaurar a configuração de DHCP	587
Gerenciamento dos escopos do DHCP	588
Criação e gerenciamento de superescopos.....	588
Criação e gerenciamento de escopos.....	589
Criação e gerenciamento de escopos de failover.....	598
Gerenciamento do pool de endereços, das concessões e das reservas	601
Visualização de estatísticas do escopo	601
Como habilitar e configurar a filtragem de endereços MAC	602
Configuração de um novo intervalo de exclusão.....	603
Reserva de endereços DHCP	604
Como modificar as propriedades de reservas.....	605
Como excluir concessões e reservas	606
Como fazer backup e restaurar o banco de dados do DHCP	606
Como fazer backup do banco de dados do DHCP.....	606
Como restaurar o banco de dados do DHCP a partir do backup	607
Como usar backup e restauração para mover um banco de dados do DHCP para um novo servidor.....	607
Como forçar o serviço DHCP Server a gerar o banco de dados do DHCP novamente	608
Como reconciliar concessões e reservas.....	608
Capítulo 16 Otimização do DNS	610
Introdução ao DNS.....	610
Integração do Active Directory com o DNS.....	611
Como habilitar o DNS na rede.....	612
Configuração de resolução de nomes em clientes DNS.....	615
Instalação de servidores DNS	616
Instalação e configuração do serviço DNS Server	617
Configuração de um servidor DNS primário.....	619
Configuração de um servidor DNS secundário.....	622
Configuração de nomes globais	624

Gerenciamento de servidores DNS	626
Como adicionar e remover servidores para gerenciamento	626
Como iniciar e interromper um servidor DNS	627
Utilização de DNSSEC e assinatura de zonas	627
Criação de domínios-filho dentro de zonas	629
Criação de domínios-filho em zonas separadas	630
Exclusão de um domínio ou de uma sub-rede	631
Gerenciamento de registros de DNS	631
Como adicionar registros de endereço e ponteiro	632
Como adicionar aliases para registros DNS com CNAME ..	633
Como adicionar servidores de email	633
Como adicionar servidores de nomes	634
Visualização e atualização de registros de DNS	635
Atualização de propriedades de zona e o registro SOA	636
Modificação do registro SOA	636
Permissão e restrição de transferências de zona	637
Notificação de alterações para secundários	639
Configuração do tipo de zona	640
Como habilitar e desabilitar as atualizações dinâmicas ..	640
Gerenciamento da configuração e da segurança do servidor DNS	640
Como habilitar e desabilitar endereços IP para um servidor DNS	641
Controle do acesso a servidores DNS fora da empresa ..	641
Como habilitar e desabilitar o log de eventos	643
Uso da depuração do registro em log para monitorar a atividade do DNS	643
Monitoramento de um servidor DNS	644

Introdução

Bem-vindo ao *Windows Server 2012 – Guia de Bolso*. Há muitos anos escrevo sobre várias tecnologias e produtos de servidor diferentes, mas o produto sobre o qual mais gosto de escrever é o Microsoft Windows Server. Para quem estiver fazendo a transição de uma versão anterior do Windows Server para o Windows Server 2012, já aviso de antemão que acredito que esta seja a atualização mais significativa no Windows Server desde a introdução do Windows 2000 Server. Embora as mudanças na interface de usuário (UI, user interface) sejam uma parte importante das revisões do sistema operacional, as mudanças mais profundas ficam abaixo da superfície, na arquitetura subjacente.

A boa nova é que o Windows Server 2012 foi construído sobre a mesma base de código do Microsoft Windows 8. Isso significa que você pode aplicar grande parte dos seus conhecimentos sobre Windows 8 ao Windows Server 2012, incluindo a forma como o Windows trabalha com interfaces do usuário baseadas em toque. Mesmo que você não instale o Windows Server 2012 em computadores com interfaces de usuário sensíveis ao toque, pode gerenciar o Windows Server 2012 a partir dos seus computadores com interfaces sensíveis ao toque. Se você for mesmo gerenciar dessa forma, entender a interface de usuário sensível ao toque, bem como as opções de interface revisadas, será crucial para o seu sucesso. É por isso que tanto a interface de usuário sensível ao de toque quanto as técnicas tradicionais de mouse e teclado são abordadas neste livro.

Ao trabalhar com computadores habilitados para interface de usuário sensível ao toque, podem-se manipular elementos na tela de formas que não eram possíveis anteriormente. Você pode inserir texto utilizando o teclado na tela e interagir com os elementos de tela das seguintes maneiras:

- **Tocar** Toque em um item com o dedo. Um toque ou toque duplo em elementos da tela normalmente equivalem a clicar ou clicar duas vezes no mouse.
- **Pressionar e manter pressionado** Pressione com o dedo e mantenha pressionado no mesmo local por alguns segundos. Pressionar e manter pressionados os elementos na tela normalmente equivale a um clique com o botão direito do mouse.
- **Passar o dedo para selecionar** Deslize um pouco um item na direção oposta àquela em que a página pode ser rolada. Isso seleciona os itens e ainda pode revelar comandos relacionados. Se a ação de pressionar e manter pressionado não exibir comandos e opções para um item, tente passar o dedo para selecionar.
- **Passar o dedo a partir da borda (deslizar a partir da borda)** Começando da borda da tela, passe o dedo ou deslize. Deslize a partir da borda direita para abrir a barra Charms (botões). Deslize a partir da borda esquerda para exibir os aplicativos abertos e alternar entre eles. Deslize a partir da borda superior ou inferior para exibir comandos do elemento ativo.
- **Pinçar** Toque em um item com dois ou mais dedos e depois aproxime os dedos em direção uns aos outros. Faça o gesto de pinçagem para ampliar o zoom ou exibir menos informações.
- **Ampliar** Toque em um item com dois ou mais dedos e depois afaste os dedos uns dos outros. Faça o gesto de ampliar para reduzir o zoom ou exibir mais informações.

Tendo escrito vários dos livros mais vendidos sobre Windows Server, pude trazer uma perspectiva exclusiva para este livro: aquele tipo de perspectiva que só é adquirida depois de trabalhar com tecnologias por muitos anos. Muito antes de existir um produto chamado Windows Server 2012, eu já trabalhava com a versão beta. A partir dessa fase inicial, a versão do Windows Server 2012 foi evoluindo até se tornar o produto final que está disponível atualmente.

Você deve ter reparado que existe uma grande quantidade de informações sobre o Windows Server 2012 disponível na web e em outros livros impressos. Podem ser encontrados tutoriais, sites de referências, grupos de discussão e outros para facilitar o uso do Windows Server 2012. A vantagem de ler este livro é que a maior parte das informações que você deve aprender sobre o Windows Server 2012 está organizada em um só lugar e apresentada de forma direta e ordenada. Este livro contém tudo de que você precisa para personalizar instalações, dominar configurações e manter servidores do Windows Server 2012.

Neste livro, ensino como os recursos funcionam, por que funcionam da forma que o fazem e como personalizá-los para atenderem às suas necessidades. Também ofereço exemplos específicos de como alguns recursos podem atender às suas necessidades e de como você pode usar outros recursos para solucionar problemas e resolver questões que possam surgir. Além disso, este livro oferece dicas, práticas recomendadas e exemplos de como otimizar o Windows Server 2012. O livro não irá apenas ensinar como configurar o Windows Server 2012 – ele ensinará como conseguir absorver todo o poder possível e aproveitar ao máximo os recursos e opções inclusas.

Ao contrário de outros livros sobre como administrar o Windows Server 2012, este livro não foca em um nível de conhecimento específico. Seja você um administrador iniciante ou um profissional experiente, muitos dos conceitos neste livro serão de grande valia, podendo ser aplicados às suas instalações do Windows Server 2012.

Para quem é este livro?

O *Windows Server 2012 – Guia de Bolso* abrange todas as edições do Windows Server 2012. O livro foi elaborado para os seguintes leitores:

- Administradores do sistema Windows
- Usuários avançados com algumas responsabilidades de administrador
- Administradores que estejam atualizando versões anteriores para o Windows Server 2012
- Administradores que estejam transferindo-se de outras plataformas

Para englobar o máximo possível de informações, parti do princípio de que você tenha habilidades básicas de sistemas de rede e um entendimento básico sobre o Windows Server. Com isso em mente, não dedico capítulos inteiros a explicações sobre a arquitetura do Windows Server, inicialização e desligamento do Windows Server ou por que usar o Windows Server. Entretanto, abordo a configuração de um servidor Windows, Group Policy (política de grupo), segurança, auditoria, backup de dados, recuperação do sistema e muito mais.

Também presumo que você esteja razoavelmente familiarizado com os comandos e procedimentos do Windows, bem como com a interface de usuário do Windows. Caso precise de alguma ajuda para aprender os fundamentos básicos do Windows, consulte fontes adicionais (muitas das quais estão disponíveis pela Microsoft Press).

Como este livro está organizado

Roma não foi feita em um dia e este livro também não foi pensado para ser lido em um dia, em uma semana ou até mesmo em um mês. O ideal seria que você lesse o livro no seu próprio ritmo, um pouco a cada dia, conforme você fosse trabalhando com todos os recursos que o Windows Server 2012 tem a oferecer. Este livro está organizado em 16 capítulos, organizados em uma ordem lógica que o conduzem das tarefas de planejamento e implantação às tarefas de configuração e manutenção.

A facilidade das referências é uma parte essencial deste guia prático. O livro possui um sumário completo e um índice extenso para localizar as respostas para os problemas rapidamente. Muitos outros recursos de referência rápida foram adicionados ao livro, incluindo procedimentos passo a passo, listas, tabelas com fatos rápidos e referências cruzadas.

Como é o caso de todos os guias de bolso, o *Windows Server 2012 – Guia de Bolso* foi criado para ser um recurso conciso e fácil de usar no gerenciamento de servidores Windows. Este é o guia de recursos em formato de leitura que você desejará ter na sua mesa de trabalho sempre, pois abrange tudo que é necessário à realização de tarefas administrativas centrais em servidores Windows. Como o objetivo é fornecer o máximo possível em um guia de bolso, não é preciso que você percorra centenas de páginas com informações irrelevantes para encontrar o que procura; você encontrará de maneira rápida exatamente o que é preciso para realizar o trabalho.

Resumindo: o livro é projetado para ser o recurso ao qual você recorre sempre que tiver dúvidas quanto à administração do Windows Server 2012. Para tanto, ele se foca em procedimentos administrativos diários, tarefas realizadas com frequência, exemplos documentados e opções que sejam representativas, ainda que não necessariamente inclusivas. Um dos meus objetivos é manter o conteúdo conciso o suficiente para que o livro se mantenha compacto e fácil de usar e, ao mesmo tempo, abrangente, com o máximo de informações possível.

Convenções usadas neste livro

Utilizei diversos elementos para ajudar a manter o texto limpo e fácil de acompanhar. Você encontrará listagens de códigos em fonte monoespacada. Quando eu solicitar que você insira um comando, o comando aparecerá em **negrito**. Quando eu introduzir e definir um novo termo ou utilizar um termo de código em um parágrafo de texto, ele será grafado em *italico*.

OBSERVAÇÃO A Group Policy agora inclui tanto políticas quanto preferências. Sob os nós Computer Configuration e User Configuration, você encontrará dois nós: Policies e Preferences. As configurações para políticas gerais estão listadas sob o nó Policies. As configurações para preferências gerais estão listadas sob o nó Preferences. Ao mencionar configurações sob o nó Policies, às vezes utilizo referências resumidas, como em User Configuration\Administrative Templates\Windows Components, às vezes utilizo referências completas, como quando específico que as políticas são encontradas em Administrative Templates abaixo de User Configuration sob o item Windows Components. Ambas as referências dizem que a configuração de política em questão está sob User Configuration e não em Computer Configuration e que ela pode ser encontrada sob Administrative Templates\Windows Components.

Outras convenções incluem:

- **Práticas recomendadas** Analisa a melhor técnica quando se trabalha com conceitos de configuração e manutenção avançados
- **Atenção** Alerta sobre problemas em potencial que você deve observar
- **Mais informações** Oferece mais informações sobre um assunto
- **Observação** Fornece detalhes adicionais sobre determinado ponto que precise ser destacado
- **Mundo real** Oferece conselhos retirados das experiências reais durante a discussão de tópicos avançados
- **Alerta de segurança** Sinaliza questões importantes de segurança
- **Dica** Oferece dicas úteis ou informações adicionais

Desejo sinceramente que o *Windows Server 2012 – Guia de Bolso* ofereça tudo de que você precisa para realizar as tarefas administrativas essenciais em servidores Windows da maneira mais rápida e eficiente possível. Fique à vontade para enviar sua opinião para williamstanek@aol.com. Siga-me no Twitter em @WilliamStanek e no Facebook em www.facebook.com/William.Stanek.Author.

Outros recursos

Não existe um formato mágico para aprender tudo que poderá ser necessário sobre o Windows Server 2012. Embora alguns livros sejam vendidos como guias completos, é simplesmente impossível que um só livro consiga conter tudo. Com isso em mente, espero que você utilize este livro da maneira como ele foi pensado: como um recurso conciso e fácil de usar. Ele abrange tudo de que você precisa para realizar tarefas administrativas centrais em servidores Windows, mas de forma alguma esgota o assunto.

O seu conhecimento atual será determinante no seu sucesso com este ou com qualquer outro livro ou recurso do Windows. Conforme você se depara com novos tópicos, dedique um tempo para ler e praticar o que aprendeu. Quando for preciso, busque mais informações para adquirir o *know-how* prático e o conhecimento necessários.

Recomendo que você visite o site da Microsoft dedicado ao Windows Server (microsoft.com/windowsserver/) e o site support.microsoft.com regularmente para se manter em dia com as últimas mudanças. Para ajudá-lo a aproveitar ao máximo este livro, você pode visitar o meu site: williamstanek.com/windows. O site contém informações sobre o Windows Server 2012 e atualizações do livro.

Suporte técnico*

Todos os esforços foram feitos para garantir a exatidão deste livro. Em caso de comentários, dúvidas, sugestões ou identificação de erros, você pode escrever diretamente para a Microsoft Press pelo endereço mspinput@microsoft.com ou acessar o link View/Submit Errata na página do livro em <http://microsoftpress.oreilly.com>.

* N. de E.: Comentários e sugestões relativos à edição brasileira desta obra podem ser enviados para secretariaeditorial@grupoa.com.br.

PARTE I

Noções básicas da administração do Windows Server 2012

CAPÍTULO 1	Visão geral da administração do Windows Server 2012	3
CAPÍTULO 2	Gerenciamento de servidores com o Windows Server 2012	30
CAPÍTULO 3	Monitoramento de processos, serviços e eventos	85
CAPÍTULO 4	Automatização de tarefas administrativas, políticas e procedimentos	133
CAPÍTULO 5	Como melhorar a segurança dos computadores	189

CAPÍTULO 1

Visão geral da administração do Windows Server 2012

- Windows Server 2012 e Windows 8 **3**
- Introdução ao Windows Server 2012 **6**
- Opções de gerenciamento de energia **8**
- Ferramentas e protocolos de rede **11**
- Controladores de domínio, servidores membros e serviços de domínio **14**
- Serviços de resolução de nomes **18**
- Ferramentas frequentemente utilizadas **24**

O Microsoft Windows Server 2012 é um sistema operacional de servidor poderoso, versátil e completo, elaborado a partir dos aperfeiçoamentos disponibilizados no Windows Server 2008 R2 pela Microsoft. O Windows Server 2012 e o Windows 8 compartilham alguns recursos porque fizeram parte de um mesmo projeto de desenvolvimento. Esses recursos têm uma base de códigos em comum e estão presentes em muitas áreas do sistema operacional, incluindo gerenciamento, segurança, rede e armazenamento. Por isso, é possível aplicar grande parte do conhecimento sobre o Windows 8 ao utilizar o Windows Server 2012.

Este capítulo faz uma introdução ao Windows Server 2012 e explora o modo como as modificações na arquitetura afetam a maneira de gerenciar e trabalhar com o Windows Server 2012. No decorrer deste capítulo e dos capítulos seguintes, você encontrará discussões sobre os diversos aprimoramentos e recursos de segurança. Essas discussões exploram todos os aspectos de segurança do computador, incluindo a segurança física, a segurança de informações e a segurança de rede. Embora o foco deste livro seja a administração do Windows Server 2012, as dicas e técnicas apresentadas podem auxiliar qualquer pessoa que preste suporte, desenvolva ou trabalhe com o sistema operacional Windows Server 2012.

Windows Server 2012 e Windows 8

Antes de implantar o Windows Server 2012, você deve planejar atentamente a arquitetura do servidor. Como parte do planejamento de implementação, é preciso considerar a configuração de software que será utilizada e modificar a configuração de hardware em cada servidor para adequá-la aos requisitos relacionados. Para mais flexibilidade nas implantações de servidores, é possível implantar servidores utilizando um destes três tipos de instalação:

- **Instalação com interface gráfica do usuário (GUI, graphical user interface)** Opção de instalação que fornece todas as funcionalidades; também cha-

mada de *instalação de servidor completo*. É possível configurar um servidor de forma a obter qualquer combinação permitida de funções, serviços de funções e recursos, além de uma interface de usuário completa ser fornecida para o gerenciamento do servidor. Essa opção de instalação oferece uma solução mais dinâmica e é recomendada para implantações do Windows Server 2012 em que a função de servidor possa mudar no decorrer do tempo.

- **Instalação Server Core** Opção de instalação mínima que fornece um subconjunto fixo de funções mas não inclui o Server Graphical Shell (Shell Gráfico de Servidor), o Microsoft Management Console (MMC, Console de Gerenciamento Microsoft) e o Desktop Experience. É possível configurar uma instalação Server Core com um conjunto limitado de funções. Uma interface de usuário limitada é fornecida para o gerenciamento do servidor, e grande parte do gerenciamento é realizada localmente em um prompt de comando ou remotamente por meio de ferramentas de gerenciamento. Essa opção de instalação é ideal para as situações nas quais deseja-se dedicar servidores a uma função de servidor específica ou a uma combinação de funções. Pelo fato de não haver funcionalidades adicionais instaladas, a sobrecarga causada por outros serviços é reduzida, por isso há mais recursos para a função ou funções dedicadas.
- **Instalação com interface mínima do servidor** Opção intermediária de instalação na qual é realizada uma instalação completa e, em seguida, o Server Graphical Shell é removido. Resta uma interface de usuário mínima, o Microsoft Management Console, o Server Manager (Gerenciador de Servidores) e um subconjunto do Control Panel (Painel de Controle) para gerenciamento local. Essa opção de instalação é ideal para situações nas quais você deseja controlar minuciosamente as tarefas que podem ser realizadas em um servidor, assim como as funções e os recursos instalados, mas nas quais ainda deseja a conveniência da interface gráfica.

Escolhe-se o tipo de instalação durante a instalação do sistema operacional. Diferentemente das versões anteriores do Windows Server, é possível alterar o tipo de instalação após a instalação de um servidor. Uma diferença-chave entre os tipos de instalação refere-se à presença das ferramentas gráficas de gerenciamento e do shell gráfico. Uma instalação Server Core não possui esses recursos; uma instalação de servidor completo possui os dois; e uma instalação com interface mínima possui apenas as ferramentas gráficas de gerenciamento.

MAIS INFORMAÇÕES Diversas funções e recursos de servidor requerem o shell gráfico, como a função Fax Server (Servidor de Fax), o Remote Desktop Session Host (Host de Sessão da Área de Trabalho Remota), o Windows Deployment Services (Serviços de Implantação do Windows) e a interface de usuário para Internet Printing (Impressão via Internet). Além desses casos, no Event Viewer (Visualizador de Eventos), o modo de exibição Details requer o shell gráfico, assim como a interface gráfica para o Windows Firewall.

Assim como o Windows 8, o Windows Server 2012 possui os seguintes recursos:

- **Modularização para independência de idiomas e geração de imagens de disco com independência de hardware** Cada componente do sistema operacional é projetado como um módulo independente que pode ser adicionado ou removido facilmente. Essa funcionalidade fornece a base para a configuração da arquitetura do Windows Server 2012. A Microsoft distribui o Windows Server

2012 através de imagens de disco no formato de arquivo de imagem do Windows (WIM), que utiliza compactação e armazenamento em instância única para reduzir significativamente o tamanho dos arquivos de imagem.

- **Ambientes de pré-instalação e de pré-inicialização** O Windows Preinstallation Environment 4.0 (Windows PE 4.0) substitui o MS-DOS como o ambiente de pré-instalação e fornece um ambiente de pré-inicialização para instalação, implantação, recuperação e solução de problemas. O ambiente de pré-instalação do Windows (Windows PE) fornece um ambiente de inicialização com um gerenciador que permite escolher o aplicativo a ser utilizado para carregar o sistema operacional. Em sistemas com múltiplos sistemas operacionais, o acesso aos sistemas operacionais anteriores ao Windows 7 ocorre no ambiente de inicialização, por meio da entrada para sistemas operacionais anteriores.
- **Controle de conta de usuário e elevação de privilégio** O User Account Control (UAC, Controle de Conta de Usuário) aumenta a segurança do computador através da separação entre contas de administrador e contas de usuário padrão. Com o UAC, todos os aplicativos são executados utilizando os privilégios de administrador ou de usuário padrão, e, por padrão, um prompt de segurança é mostrado toda vez que um aplicativo que requer privilégios de administrador for executado. A forma como o prompt de segurança trabalha depende das configurações da Group Policy (política de grupo). Se o logon for realizado utilizando a conta de Administrador interno, normalmente não serão mostrados prompts de elevação.

No Windows 8 e no Windows Server 2012, recursos com bases de código comuns possuem interfaces de gerenciamento idênticas. Na verdade, praticamente todos os utilitários do Control Panel disponíveis no Windows Server 2012 são idênticos ou muito parecidos com suas funções correspondentes no Windows 8. É claro, existem exceções em alguns casos devido a configurações padrão. Pelo fato de o Windows Server 2012 não utilizar índices de desempenho, os servidores do Windows não possuem avaliações do Windows Experience Index (Índice de Experiência do Windows). Pelo fato de o Windows Server 2012 não utilizar o modo Sleep ou modos relacionados, os servidores do Windows não possuem as funcionalidades suspender, hibernar e despertar. Pelo fato de não ser comum querer estender as opções de gerenciamento de energia no Windows Server, o Windows Server 2012 possui um conjunto limitado de opções de energia.

O Windows Server 2012 não inclui os aprimoramentos do Windows Aero, Windows Sidebar, gadgets do Windows ou qualquer outro aprimoramento de interface de usuário, pois o Windows Server 2012 foi projetado para fornecer desempenho ótimo das tarefas relacionadas ao servidor, não para possibilitar a personalização ampla da aparência da área de trabalho. Dito isso, quando estiver trabalhando com a instalação de servidor completo, é possível adicionar o recurso Desktop Experience e habilitar alguns recursos do Windows 8 no servidor.

O recurso Desktop Experience fornece a funcionalidade da área de trabalho do Windows ao servidor. Os recursos adicionados ao Windows incluem o Windows Media Player, temas de desktop, Vídeo para Windows (suporte AVI), Windows Defender, Limpeza de disco, Central de sincronização, Gravador de som, Mapa de caracteres e Ferramenta de captura. Embora esses recursos permitam que um servidor seja utilizado como um computador desktop, eles podem reduzir o desempenho geral do servidor.

Pelo fato de os recursos em comum entre o Windows 8 e o Windows Server 2012 terem tantas semelhanças, não abordarei as modificações de interface em relação às

versões anteriores de sistemas operacionais, nem discutirei como o UAC funciona, entre outras coisas. Uma cobertura abrangente desses recursos pode ser encontrada no *Windows 8 Administration Pocket Consultant* (Microsoft Press, 2012), o qual sugiro que você utilize em conjunto com este livro. Além dessa ampla cobertura de tarefas administrativas, o *Windows 8 Administration Pocket Consultant* aborda como personalizar o sistema operacional e o ambiente do Windows, como configurar dispositivos de hardware e de rede, como gerenciar o acesso dos usuários e as configurações gerais, como configurar computadores móveis, como utilizar gerenciamento remoto e assistência remota, como solucionar problemas do sistema e muito mais. Este livro, por outro lado, é totalmente voltado à administração de serviços de diretório, dados e rede.

Introdução ao Windows Server 2012

O sistema operacional Windows Server 2012 inclui várias edições diferentes. Todas as edições do Windows Server 2012 dão suporte a múltiplos núcleos em um processador. É importante destacar que, embora um edição possa dar suporte a apenas um processador de soquetes independentes (também chamado de *processador físico*), esse processador único pode ter até oito núcleos (também chamados de *processadores lógicos*).

O Windows Server 2012 é um sistema operacional disponível apenas em 64 bits. Neste livro, refiro-me aos sistemas de 64 bits projetados para a arquitetura x64 como sistemas de 64 bits. Como as diversas edições do servidor suportam os mesmos recursos e ferramentas de administração, você pode usar as técnicas discutidas neste livro independente da edição do Windows Server 2012 que estiver utilizando.

Quando instala o sistema Windows Server 2012, você configura o sistema de acordo com a função pretendida na rede, seguindo estas orientações:

- Os servidores geralmente são designados como parte de um grupo de trabalho ou de um domínio.
- Grupos de trabalho são associações de computadores nas quais cada computador é gerenciado separadamente.
- Domínios são conjuntos de computadores que podem ser gerenciados coletivamente através de controladores de domínio, que são funções do Windows Server 2012 que gerenciam o acesso à rede, ao banco de dados de diretório e a recursos compartilhados.

OBSERVAÇÃO Neste livro, *Windows Server 2012* e *família Windows Server 2012* referem-se a todas as edições do Windows Server 2012. As diversas edições do servidor suportam os mesmos recursos e ferramentas de administração.

Diferente do Windows Server 2008, o Windows Server 2012 utiliza uma tela inicial. Start (Iniciar) é uma janela, não um menu. Os programas podem ter seus blocos na tela Start (Tela Inicial). Ao clicar no bloco, o programa será executado. Geralmente, ao pressionar e manter pressionado ou clicar com o botão direito em um programa, um painel de opções será exibido. A barra Charms é um painel com as opções Start, Desktop e PC Settings. Com uma interface tátil, é possível exibir a barra Charms deslizando o toque a partir do canto direito da tela. Com um mouse e um teclado, é possível exibir a barra Charms movendo o ponteiro do mouse sobre o botão oculto no canto inferior direito ou no canto superior direito das telas Start, Desktop ou PC Settings; ou pressionando a tecla Windows+C.

Toque em ou clique em Search para exibir o painel Search. Qualquer texto digitado enquanto a tela Start estiver aberta será inserido na caixa Search no painel Search. A caixa Search pode focar em Apps, Settings ou Files. Quando focada em Apps, é possível utilizar Search para encontrar rapidamente programas instalados. Quando focada em Settings, é possível utilizar Search para encontrar rapidamente configurações e opções no Control Panel. Quando focada em Files, é possível utilizar Search para encontrar arquivos rapidamente.

Uma maneira de abrir um programa rapidamente é pressionar a tecla Windows, digitar o nome do programa e pressionar a tecla Enter. Esse atalho funcionará enquanto a caixa Search estiver focada em Apps (que é o padrão).

Ao pressionar a tecla Windows, você irá alternar entre a tela Start e a área de trabalho (ou, se estiver trabalhando com PC Settings, irá alternar entre Start e PC Settings). Em Start, há um bloco para o Desktop no qual você pode tocar ou clicar para exibir a área de trabalho. Também é possível exibir a área de trabalho pressionando a tecla Windows+D ou, para apenas olhar rapidamente a área de trabalho, pressione e mantenha pressionadas as teclas Windows+Vírgula. Em Start, o acesso ao Control Panel se dá tocando ou clicando no bloco do Control Panel. Na área de trabalho, o acesso ao Control Panel se dá pela barra Charms, tocando ou clicando em Settings, depois em Control Panel. Além dessa forma, já que o File Explorer está fixado à barra de tarefas da área de trabalho, por padrão é possível acessar o Control Panel a partir da área de trabalho seguindo estas etapas:

1. Abra o File Explorer tocando ou clicando no ícone da barra de tarefas.
2. Toque ou clique no botão de opção na extrema direita (seta para baixo) na lista de endereços.
3. Toque ou clique em Control Panel.

As telas Start e Desktop possuem um menu que pode ser exibido pressionando e mantendo pressionado ou clicando com o botão direito do mouse no canto inferior esquerdo da tela Start ou da área de trabalho. As opções do menu incluem Prompt de comando, Prompt de comando (Admin), Device Manager (Gerenciador de Dispositivos), Event Viewer (Visualizador de Eventos), System (Sistema) e Task Manager (Gerenciador de Tarefas). Em Start, o botão oculto no canto esquerdo da tela mostra uma miniatura da área de trabalho; ao tocar ou clicar nessa miniatura, a área de trabalho é aberta. Na área de trabalho, o botão oculto no canto esquerdo da tela mostra uma miniatura de Start; ao tocar ou clicar nessa miniatura, a tela Start é aberta. Ao pressionar e manter pressionada ou ao clicar com o botão direito do mouse na miniatura, um menu de atalho será exibido.

Agora, Shutdown e Restart são opções das configurações de Energia. Isso significa que, para desligar ou reiniciar um servidor, deve-se seguir estas etapas:

1. Exiba as opções de Start deslizando da extremidade direita da tela para a esquerda ou movendo o ponteiro do mouse para o canto superior direito ou inferior direito da tela.
2. Toque ou clique em Settings e depois em Power.
3. Toque ou clique em Shut Down ou Restart conforme o desejado.

Como alternativa, pressione o botão de energia físico do servidor para iniciar um desligamento ordenado que irá realizar o logoff e em seguida o desligamento efetivo. Se estiver utilizando o sistema em computador desktop e o computador tiver um bo-

tão para dormir, o botão dormir será desabilitado por padrão, assim como as opções de fechamento de tampa para computadores portáteis. Além disso, os servidores são configurados para desligar o vídeo após 10 minutos de inatividade.

O Windows 8 e o Windows Server 2012 suportam a especificação Advanced Configuration and Power Interface (ACPI, Interface de Energia e Configuração Avançada) 5.0. O Windows utiliza a ACPI para controlar as transições de estado de energia do sistema e dos dispositivos, alternando o estado dos dispositivos entre ativo com energia plena, com pouca energia e desligado, para reduzir o consumo de energia.

As configurações de energia para um computador dependem do plano de energia ativo. É possível acessar os planos de energia no Control Panel tocando ou clicando em System And Security (Sistema e Segurança) e depois em Power Options. O Windows Server 2012 inclui o utilitário Power Configuration (Powercfg.exe) para o gerenciamento das opções de energia via linha de comando. Em um prompt de comando, é possível visualizar os planos de energia selecionados digitando **powercfg /l**. O plano de energia ativo estará marcado com um asterisco.

O plano de energia ativo padrão do Windows Server 2012 é chamado de Balanced (Equilibrado). O plano Balanced é configurado para fazer o seguinte:

- Nunca desligar os discos rígidos (em oposição a desligar os discos rígidos após um período de tempo ocioso especificado)
- Desabilitar eventos cronometrados para acordar o computador (em oposição a habilitar eventos cronometrados para acordar o computador)
- Habilitar suspensão seletiva USB (em oposição a desabilitar suspensão seletiva)
- Utilizar economia de energia média para links PCI Express ociosos (em oposição à economia de energia máxima estar ligada ou desligada)
- Utilizar resfriamento ativo do sistema, no qual aumenta-se a velocidade do ventilador antes de reduzir a velocidade dos processadores (em oposição a utilizar resfriamento passivo do sistema, no qual reduz-se a velocidade dos processadores antes de aumentar a velocidade do ventilador)
- Utilizar estados mínimo e máximo de processadores se essa opção for possível (em oposição a utilizar um estado fixo)

OBSERVAÇÃO O consumo de energia é uma questão importante, especialmente à medida que organizações tentam tornar-se mais sustentáveis. Economizar energia também pode resultar numa economia de dinheiro para a empresa e, em alguns casos, pode permitir a instalação de mais servidores em seu centro de dados. Se, por exemplo, você instalar o Windows Server 2012 em um laptop (para teste ou para uso pessoal), suas configurações de energia serão um pouco diferentes e também haverá configurações para quando o laptop estiver se alimentando apenas da bateria.

Opções de gerenciamento de energia

Quando se está trabalhando com gerenciamento de energia, aspectos importantes incluem os seguintes:

- Modos de resfriamento
- Estados dos dispositivos
- Estados dos processadores

A ACPI define modos de resfriamento ativo e passivo. Esses modos de resfriamento são inversamente relacionados entre si:

- O resfriamento passivo reduz o desempenho do sistema, mas é mais silencioso porque há menos ruído do ventilador. Com o resfriamento passivo, o Windows diminui o consumo de energia para reduzir a temperatura de funcionamento do computador à custa do desempenho do sistema. Nesse modo, o Windows reduz a velocidade do processador a fim de resfriar o computador antes de aumentar a velocidade do ventilador, o que aumentaria o consumo de energia.
- O resfriamento ativo permite o desempenho máximo do sistema. Com o resfriamento ativo, o Windows aumenta o consumo de energia para reduzir a temperatura da máquina. Nesse modo, o Windows aumenta a velocidade do ventilador para resfriar o computador antes de tentar reduzir a velocidade do processador.

As políticas de energia incluem um limite máximo e mínimo para o estado do processador, chamados de *estado máximo do processador* e *estado mínimo do processador*, respectivamente. Esses estados são implementados através do uso de um recurso da ACPI 3.0 ou versões mais recentes, chamado de limitação do processador, que determina os estados de desempenho do processador atualmente disponíveis para serem utilizados pelo Windows. Ao configurar os valores máximo e mínimo, você define os limites para os estados de desempenho permitidos; também é possível utilizar o mesmo valor mínimo e máximo para forçar o sistema a permanecer em um estado de desempenho específico. O Windows reduz o consumo de energia limitando a velocidade do processador. Por exemplo, se o limite superior for 100% e o limite inferior for 5%, o Windows pode diminuir a potência do processador dentro desse intervalo conforme a carga de trabalho para reduzir o consumo de energia. Em um computador com um processador de 3GHz, o Windows ajustaria a frequência de funcionamento do processador entre 0,15GHz e 3,0GHz.

O recurso de limitação do processador e outros estados de desempenho relacionados foram introduzidos no Windows XP e não são novidade, mas essas implementações iniciais foram projetadas para computadores com processadores com soquetes independentes e não para computadores com processadores com núcleos. Como resultado, não são eficientes na redução do consumo de energia em computadores com processadores lógicos. O Windows 7 e versões posteriores de Windows reduzem o consumo de energia em computadores com processadores com núcleos múltiplos utilizando um recurso da ACPI 4.0 chamado de *suspensão de processador lógico* e atualizando os recursos de limitação do processador para trabalhar com núcleos do processador.

O recurso *suspensão de processador lógico* foi projetado para garantir que o Windows utilize o menor número possível de núcleos do processador em uma determinada carga de trabalho. O Windows alcança isso ao consolidar a carga de trabalho no menor número de núcleos possível e, ao mesmo tempo, suspendendo o uso dos núcleos inativos do processador. Conforme mais poder de processamento for necessário, o Windows ativa os núcleos inativos do processador. A funcionalidade para deixar o processador ocioso funciona juntamente com o gerenciamento dos estados de desempenho ao nível de núcleo.

A ACPI define os estados de desempenho do processador, também chamados de *p-states*, e estados de suspensão por ociosidade, também chamados de *c-states*. Estados de desempenho do processador incluem P0 (o processador/núcleo usa sua

capacidade máxima de desempenho e pode consumir o máximo de energia), P1 (o processador/núcleo é limitado abaixo do seu nível máximo e consome menos do que o máximo de energia) e Pn (em que o estado n é um número máximo dependente do processador, e em que o processador/núcleo está em seu nível mínimo e consome o mínimo de energia ao mesmo tempo que permanece em estado ativo).

Estados de suspensão por ociosidade incluem C0 (o processador/núcleo consegue executar instruções), C1 (o processador/núcleo tem a menor latência e permanece em um estado de energia sem realizar execuções), C2 (o processador/núcleo tem mais latência para aumentar a economia de energia em comparação ao estado C1) e C3 (o processador/núcleo tem a maior latência para aumentar a economia de energia em comparação aos estados C1 e C2).

MAIS INFORMAÇÕES A ACPI 4.0 foi finalizada em junho de 2009 e a ACPI 5.0 em dezembro de 2011. Computadores fabricados antes dessa época provavelmente não terão um firmware totalmente compatível, e você provavelmente terá que atualizar o firmware quando uma versão revisada compatível for disponibilizada. Em alguns casos, e especialmente com hardwares mais antigos, talvez não seja possível atualizar o firmware de um computador para torná-lo totalmente compatível com a ACPI 4.0 ou ACPI 5.0. Por exemplo, se estiver configurando as opções de energia e não houver as opções de estado mínimo e máximo do processador, o firmware do computador não é totalmente compatível com a ACPI 3.0 e provavelmente também não suportará por completo a ACPI 4.0 ou a ACPI 5.0. Ainda assim, verifique se há atualizações no site do fabricante do hardware.

Quanto aos processadores/núcleos, o Windows alterna entre qualquer p-state e a partir do estado C1 para o estado C0 quase instantaneamente (frações de milissegundos) e tende a não utilizar os estados de suspensão profundos, por isso não há necessidade de preocupar-se quanto ao impacto no desempenho ao diminuir a potência ou ativar processadores/núcleos. Os processadores/núcleos são disponibilizados quando tornam-se necessários. Dito isso, a forma mais fácil de limitar o gerenciamento de energia do processador é modificando o plano de energia ativo e definindo como 100% tanto o estado mínimo quanto o estado máximo do processador.

O recurso *suspensão de processador lógico* é utilizado para reduzir o consumo de energia por meio da remoção de um processador lógico da lista de processos sem afinidade com o processador do sistema operacional. No entanto, como processos com afinidade com o processador reduzem a eficácia desse recurso, é desejável um planejamento cuidadoso antes de estabelecer as configurações de afinidade com processador para aplicativos. O Windows System Resource Manager (Gerenciador de Recursos de Sistema do Windows) possibilita o gerenciamento dos recursos do processador através de metas de porcentagem de uso do processador e através de regras de afinidade com o processador. Ambas as técnicas reduzem a eficácia da suspensão de processadores lógicos.

O Windows economiza energia ao colocar ou retirar núcleos do processador dos p-states e c-states apropriados. Em um computador com quatro processadores lógicos, o Windows pode utilizar p-states de 0 a 5, em que P0 permite 100% de uso, P1 permite 90% de uso, P2 permite 80% de uso, P3 permite 70% de uso, P4 permite 60% de uso e P5 permite 50% de uso. Quando um computador está ativo, o processador lógico 0 provavelmente está ativo com um p-state entre 0 e 5 e os outros processadores provavelmente estão em um p-state adequado ou em um estado de suspensão. A Figura 1-1 mostra um exemplo. Aqui, o processador lógico 1 está rodando a 90%, o processador lógico 2 está rodando a 80%, o processador lógico 3 está rodando a 50% e o processador lógico 4 está em estado de suspensão.

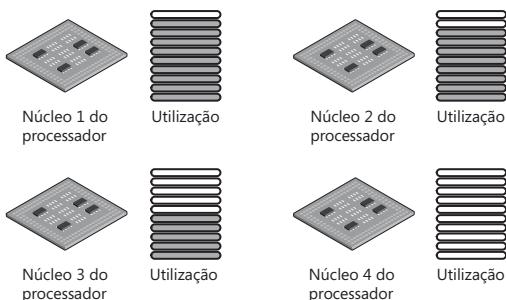


FIGURA 1-1 Para entender os estados de processador.

MUNDO REAL A ACPI 4.0 e a ACPI 5.0 definem quatro estados de energia globais. No G0, estado de funcionamento no qual o software é executado, o consumo de energia é o mais alto e a latência é a mais baixa. No G1, estado de suspensão, no qual o software não é executado, a latência varia com o estado de suspensão, e o consumo de energia é menor do que no estado G0. No G2 (também chamado de estado de suspensão S5), estado ocioso no qual o sistema operacional não é executado, a latência é longa e o consumo de energia é bem próximo de zero. No G3, estado ocioso mecânico, no qual o sistema operacional não é executado, a latência é longa e o consumo de energia é zero. Também há um estado global especial, conhecido como estado de suspensão não volátil S4, no qual o sistema operacional escreve todo o contexto do sistema em um arquivo de armazenamento não volátil, permitindo que o contexto do sistema seja salvo e restaurado.

Dentro do estado de suspensão global, o G1, há variações. O S1 é um estado de suspensão em que todo o contexto do sistema é mantido. O S2 é um estado de suspensão parecido com o S1, exceto que os contextos da CPU e do cache do sistema se perdem e o controle se dá após reiniciar o computador. O S3 é um estado de suspensão no qual todos os contextos da CPU, do cache e do chipset se perdem e o hardware mantém o contexto da memória e restaura alguns contextos das configurações da CPU e do cache L2. O S4 é um estado de suspensão no qual assume-se que o hardware tenha desligado todos os dispositivos a fim de reduzir ao máximo o consumo e que apenas o contexto da plataforma continua sendo mantido. O S5 é um estado de suspensão no qual assume-se que o hardware está em um estado ocioso, no qual nenhum contexto é mantido e uma inicialização completa é necessária quando o sistema é despertado.

Dispositivos também têm estados de energia. D0, o estado totalmente ligado, consome o maior nível de energia. O D1 e o D2 são estados intermediários que muitos dispositivos não utilizam. O D3hot é um estado de economia de energia, no qual o dispositivo é enumerado por software e pode, por opção, preservar o contexto do dispositivo. D3 é o estado desligado, no qual o contexto do dispositivo é perdido e o sistema operacional deve reinicializar o dispositivo para ligá-lo novamente.

Ferramentas e protocolos de rede

O Windows Server 2012 possui um pacote de ferramentas de rede que inclui o Network Explorer (Explorador de Rede), a Network And Sharing Center (Central de Rede e Compartilhamento) e o Network Diagnostics (Diagnóstico de Rede). A Figura 1-2 mostra a Network And Sharing Center.

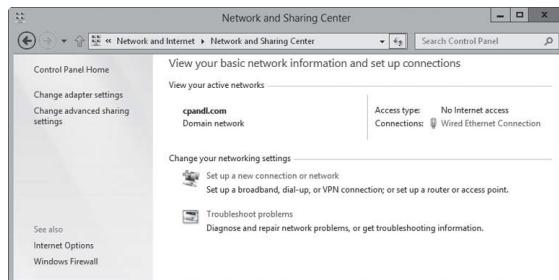


FIGURA 1-2 Network And Sharing Center fornece acesso rápido a opções de compartilhamento, descoberta e rede.

Para entender as opções de rede

As configurações de compartilhamento e descoberta na Network And Sharing Center controlam as configurações básicas de rede. Quando as configurações de descoberta estão ativadas e um servidor está conectado a uma rede, o servidor consegue ver os outros computadores e dispositivos da rede que estejam visíveis na rede. Quando as configurações de compartilhamento são ativadas ou desativadas, as várias opções de compartilhamento tornam-se permitidas ou restritas. Como será discutido no Capítulo 12, “Compartilhamento de dados, segurança e auditoria”, as opções de compartilhamento incluem compartilhamento de arquivos, compartilhamento de pasta pública, compartilhamento de impressora e compartilhamento protegido por senha.

No Windows 8 e no Windows Server 2012, as redes são identificadas como um dos seguintes tipos:

- **Domain (Domínio)** Uma rede na qual os computadores são conectados ao domínio corporativo do qual fazem parte.
- **Work (Trabalho)** Uma rede privada na qual os computadores são configurados como membros de um grupo de trabalho e não são conectados diretamente à Internet pública.
- **Home (Doméstica)** Uma rede privada na qual os computadores são configurados como membros de um grupo de doméstico e não são conectados diretamente à Internet pública.
- **Public (Pública)** Uma rede pública na qual os computadores são conectados à uma rede em um local público, como restaurantes ou aeroportos, e não à uma rede interna.

Esses tipos de rede estão organizados em três categorias: doméstica ou de trabalho, domínio e pública. Cada categoria de rede tem configurações de rede específicas. Como o computador salva configurações de compartilhamento e firewall separadamente para cada categoria de rede, é possível utilizar diferentes configurações de bloqueio e permissão para cada categoria de rede. Quando você se conecta a uma rede, vê uma caixa de diálogo que permite a especificação da categoria da rede. Se você selecionar Private e o computador determinar que está conectado ao domínio corporativo do qual faz parte, a categoria de rede é definida como rede de domínio.

Baseado na categoria de rede, o Windows Server define as configurações que ligam e desligam a opção da descoberta. O estado ligado (On, habilitado) significa que o computador pode descobrir outros computadores e dispositivos na rede e que outros computadores na rede podem descobrir o computador. O estado desligado (Off, desabilitado) significa que o computador não pode descobrir outros computadores e dispositivos na rede e que outros computadores na rede também não podem descobrir o computador.

É possível habilitar a opção da descoberta e o compartilhamento de arquivos utilizando tanto a janela Network quanto Advanced Sharing Settings na Network And Sharing Center. No entanto, a opção da descoberta e o compartilhamento de arquivos estão bloqueados por padrão na rede pública, o que aumenta a segurança ao impedir que computadores da rede pública descubram outros computadores e dispositivos naquela rede. Quando a opção da descoberta e o compartilhamento de arquivos estão desabilitados, os arquivos e impressoras que você compartilhou no computador não podem ser acessados a partir da rede. Além disso, alguns programas talvez não consigam acessar a rede.

Como trabalhar com protocolos de rede

Para permitir que um servidor acesse uma rede, você deve instalar uma rede TCP/IP e um adaptador de rede. O Windows Server utiliza TCP/IP como o protocolo padrão de rede de longa distância (WAN). Normalmente, a rede é instalada durante a instalação do sistema operacional. Você também pode instalar a rede TCP/IP a partir das propriedades da conexão de rede local.

Os protocolos TCP e IP possibilitam que os computadores comuniquem-se através de várias redes e através da Internet utilizando adaptadores de rede. O Windows 7 e as versões mais recentes do Windows possuem uma arquitetura com uma camada dupla de IP, no qual tanto o protocolo IP versão 4 (IPv4) quanto o protocolo IP versão 6 (IPv6) estão implementados e compartilham camadas de rede e transporte em comum. O IPv4 possui endereços de 32 bits e é a primeira versão de IP utilizada na maioria das redes, incluindo a Internet. O IPv6, por outro lado, possui endereços de 128 bits e é a versão mais atual de IP.

OBSERVAÇÃO Clientes do DirectAccess só enviam tráfego IPv6 através da conexão do DirectAccess para o servidor do DirectAccess. Graças ao apoio do NAT64 e do DNS64 em um servidor do DirectAccess no Windows Server 2012, clientes do DirectAccess agora podem iniciar comunicações com hosts que possuem só IPv4 na intranet corporativa. O NAT64 e o DNS64 operam em conjunto para converter o tráfego de conexão de entrada de um nó de IPv6 em um tráfego de IPv4. O NAT64 converte o tráfego de IPv6 de entrada em um tráfego de IPv4 e realiza uma conversão inversa para o tráfego de resposta. O DNS64 resolve o nome de um host somente IPv4 como um endereço IPv6 convertido.

MUNDO REAL O recurso TCP Chimney Offload foi introduzido com o Windows Vista e o Windows Server 2008. Esse recurso permite que o subsistema de rede descarregue o funcionamento de uma conexão TCP/IP do processador do computador para seu adaptador de rede, contanto que o adaptador de rede suporte o funcionamento de descarregamento TCP/IP. Tanto conexões TCP/IPv4 quanto conexões TCP/IPv6 podem ser descarregadas. Para o Windows 7 e versões mais recentes do Windows, conexões TCP são descarregadas, por padrão, em adaptadores de rede de 10 gigabits por segundo (Gbps), mas não são descarregadas, por padrão, em adaptadores de rede de 1 Gbps. Para descarregar conexões TCP em um adaptador de rede de 1 ou 10 Gbps, é preciso habilitar o descarregamento de TCP inserindo o comando seguinte em

um prompt de comandos com privilégios elevados: **netsh int tcp set global chimney=enabled**. É possível verificar o status do descarregamento de TCP digitando **netsh int tcp show global**. Embora o descarregamento de TCP opere com o Firewall do Windows, o descarregamento de TCP não será usado com o IPsec, o Hyper V (solução de virtualização da Microsoft), nem com o balanceamento da carga de rede ou com o serviço NAT (conversão de endereços de rede). Para verificar se o descarregamento de TCP está funcionando, digite **netstat -t** e confira o estado de descarregamento. O estado de descarregamento é listado como *offloaded* ou *inhost*.

O Windows também utiliza o receive-side scaling (RSS) e o NetDMA (acesso direto à memória de rede). É possível habilitar ou desabilitar o RSS digitando **netsh int tcp set global rss=enabled** ou **netsh int tcp set global rss=disabled**, respectivamente. Para verificar o status do RSS, digite **netsh int tcp show global**. É possível habilitar ou desabilitar o NetDMA definindo um valor DWord de 1 ou 0, respectivamente, abaixo da entrada de registro **EnableTCPA**. Essa entrada de registro encontra-se em **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters**.

Endereços IPv4 de 32 bits costumam ser expressos por quatro valores decimais separados, como 127.0.0.1 ou 192.168.10.52. Os quatro valores decimais são chamados de *octetos* porque cada um deles representa 8 bits do total de 32 bits. Com endereços IPv4 unicast padrão, uma parte variável do endereço IP representa o ID da rede e uma parte variável do endereço IP representa o ID do host. O endereço IPv4 de um host e o endereço MAC da máquina utilizado pelo adaptador de rede do host não têm correlação.

Endereços IPv6 de 128 bits são divididos em seis blocos de 16 bits delimitados por dois-pontos. Cada bloco de 16 bits é expresso de forma hexadecimal, como FEC0:0:02BC:FF:BECB:FE4F:961D. Com endereços IPv6 unicast padrão, os primeiros 64 bits representam o ID de rede e os últimos 64 bits representam a interface de rede. Como muitos blocos de endereço IPv6 são definidos por 0, um conjunto contíguo de blocos de 0 pode ser expresso por “::”, uma notação chamada de *notação de dois-pontos*. Se utilizarmos a notação de dois-pontos, os dois blocos 0 no endereço anterior podem ser compactados como FEC0::02BC:FF:BECB:FE4F:961D. Três ou mais blocos de 0 seriam compactados da mesma forma. Por exemplo, FFE8:0:0:0:0:0:1 torna-se FFE8::1.

Quando o hardware da rede é detectado durante a instalação do sistema operacional, o IPv4 e o IPv6 são habilitados por padrão; não é necessário instalar um componente em separado para habilitar o suporte ao IPv6. A arquitetura modificada de IP no Windows 7 e em versões mais recentes do Windows é chamada de *Next Generation TCP/IP stack*, e inclui muitos aprimoramentos que aperfeiçoam a forma como o IPv4 e o IPv6 são utilizados.

Controladores de domínio, servidores membros e serviços de domínio

Quando você instala o Windows Server 2012 em um novo sistema, pode configurar o servidor como servidor membro, controlador de domínio ou servidor autônomo. As diferenças entre esses tipos de servidores é de extrema importância. Servidores membros fazem parte de um domínio, mas não armazenam informações de diretório. Controladores de domínio diferenciam-se dos servidores membros porque armazenam informações de diretório e fornecem serviços de autenticação e de diretório ao domínio. Servidores autônomos não fazem parte de um domínio. Como os servidores autônomos possuem seu próprio banco de dados de usuário, autenticam solicitações de logon de forma independente.

Como trabalhar com o Active Directory

O Windows Server 2012 dá suporte a um modelo de replicação multimestre. Nesse modelo, qualquer controlador de domínio pode receber alterações de diretório e replicar essas alterações para outros controladores de domínio automaticamente. O Windows Server distribui um diretório de informações inteiro, chamado de um *repositório de dados*. Dentro de um repositório de dados há conjuntos de objetos que representam contas de computador, usuários e grupos, além de recursos compartilhados como servidores, arquivos e impressoras.

Domínios que utilizam Active Directory são chamados de *domínios do Active Directory*. Embora domínios do Active Directory funcionem com apenas um controlador de domínio, você pode e deve configurar múltiplos controladores de domínio no domínio. Dessa forma, se um controlador de domínio falhar, você pode contar que os outros controladores de domínio lidem com autenticação e outras tarefas críticas.

A Microsoft fez várias alterações no Active Directory na versão original do Windows Server 2008. Como resultado, a Microsoft realinhou a funcionalidade de diretório e criou uma família de serviços relacionados, incluindo os seguintes:

- **Active Directory Certificate Services (AD CS, Serviços de Certificados do Active Directory)** O AD CS fornece as funções necessárias para emitir e revogar certificados digitais para usuários, computadores clientes e servidores. O AD CS utiliza CAs (*certificate authorities*, autoridades de certificação), que são responsáveis por confirmar a identidade dos usuários e computadores e por emitir e validar certificados que confirmem essas identidades. Domínios podem ter CAs raiz corporativas, que são servidores de certificação da raiz da hierarquia de certificação para esses domínios e são os servidores de certificação mais confiáveis da empresa, e CAs subordinadas, que são membros de uma hierarquia de certificação corporativa específica. Grupos de trabalho somente podem possuir CAs raiz autônomas, que são servidores de certificação da raiz da hierarquia de certificação não corporativa, e CAs subordinadas autônomas, que são membros de uma hierarquia de certificação não corporativa específica.
- **Active Directory Domain Services (AD DS, Serviços de Domínio do Active Directory)** O AD DS fornece os serviços de diretório necessários para estabelecer um domínio, incluindo o repositório de dados que armazena informações sobre objetos na rede e as disponibiliza para os usuários. O AD DS utiliza controladores de domínio para gerenciar o acesso aos recursos de rede. Uma vez que os usuários fazem sua autenticação ao efetuar logon em um domínio, suas credenciais armazenadas podem ser utilizadas para acessar recursos da rede. Como o AD DS é a parte mais importante do Active Directory e é um requisito para aplicativos e tecnologias compatíveis com diretório, eu o chamo simplesmente de Active Directory em vez de Active Directory Domain Services ou AD DS.
- **Active Directory Federation Services (AD FS, Serviços de Federação do Active Directory)** O AD FS complementa os recursos de autenticação e gerenciamento de acesso do AD DS, estendendo-os para a World Wide Web. O AD FS utiliza agentes da Web para fornecer aos usuários acesso a aplicativos da web hospedados internamente e proxies para gerenciar o acesso para cliente. Uma vez que o AD FS estiver configurado, os usuários podem utilizar suas identidades digitais para autenticar-se na Web e acessar aplicativos da web hospedados internamente com um navegador da Web como o Internet Explorer.

- **Active Directory Lightweight Directory Services (AD LDS)** O AD LDS fornece um repositório de dados para aplicativos compatíveis com diretórios que não requerem AD DS e que não necessitam ser implantados em controladores de domínio. O AD LDS não funciona como um serviço do sistema operacional e pode ser utilizado tanto nos ambientes de domínios como nos de grupos de trabalho. Cada aplicativo que é executado em um servidor pode ter seu próprio repositório de dados implementado através do AD LDS.
- **Active Directory Rights Management Services (AD RMS)** O AD RMS fornece uma camada de proteção para as informações de uma empresa que podem ser estendidas além do ambiente da empresa, fazendo com que mensagens de email, documentos, páginas da Web e outros sejam protegidos de acessos não autorizados. O AD RMS utiliza um serviço de certificação para emitir certificados de direitos de conta que identificam os usuários, grupos e serviços confiáveis; um serviço de licenciamento que fornece acesso a informações protegidas a usuários, grupos e serviços autorizados; e um serviço de registro em log para monitorar e manter o serviço de gerenciamento de direitos. Uma vez que a confiança tenha sido estabelecida, os usuários com certificados de direitos da conta podem atribuir direitos a informações. Esses direitos controlam quais usuários podem acessar a informação e o que podem fazer com ela. Usuários com certificados de direitos da conta também podem acessar conteúdo protegido se o acesso tiver sido concedido a eles. A criptografia garante que o acesso a informações protegidas seja controlado tanto dentro como fora das empresas.

A Microsoft introduziu alterações adicionais com o Windows Server 2012. Essas alterações incluem um novo nível funcional de domínio, chamado de *nível funcional de domínio do Windows Server 2012*, e um novo nível funcional de floresta, chamado de *nível funcional de floresta do Windows Server 2012*. As diversas outras alterações são discutidas no Capítulo 6, "Como utilizar o Active Directory".

Como utilizar controladores de domínio somente leitura

O Windows Server 2008 e as versões mais recentes dão suporte a controladores de domínio somente leitura (RODC, Read-Only Domain Controllers) e a Restartable Active Directory Domain Services. Um RODC é um controlador de domínio adicional que hospeda uma réplica somente leitura do repositório de dados de um domínio do Active Directory. Os RODCs são ideais para as necessidades de filiais, onde a segurança física de um controlador de domínio não é garantida. Com exceção de senhas, os RODCs armazenam os mesmos objetos e atributos que os controladores de domínio graváveis armazenam. Esses objetos e atributos são replicados para RODCs através de replicação unidirecional a partir de um controlador de domínio gravável que age como um parceiro de replicação.

Como por padrão os RODCs não armazenam senhas nem credenciais além das utilizadas por sua própria conta de computador e na conta Krbtgt (Kerberos Target), os RODCs extraem as credenciais de usuário e de computador de um controlador de domínio gravável com o Windows Server 2008 ou versão mais recente. Se permitir através de uma política de replicação de senha aplicada a um controlador de domínio gravável, um RODC extrairá e armazenará em cache as credenciais conforme necessário até que essas credenciais mudem. Como apenas um subconjunto de credenciais fica armazenado em um RODC, isso limita o número de credenciais que podem ser comprometidas.

DICA Qualquer usuário de domínio pode ser definido como um administrador local de um RODC sem precisar conceder nenhum outro direito no domínio. Um RODC pode agir como um catálogo global mas não como um mestre de operações. Embora os RODCs possam extrair informações de controladores de domínio com o Windows Server 2003, podem extrair atualizações da partição do domínio somente de um controlador de domínio gravável com Windows Server 2008 ou versão mais recente no mesmo domínio.

Como utilizar o Restartable Active Directory Domain Services

O Restartable Active Directory Domain Services (Serviços de Domínio do Active Directory Reinicializáveis) é um recurso que permite a um administrador iniciar e parar o AD DS. No console Services, o serviço Active Directory Domain Services está disponível em controladores de domínio, permitindo que você pare e reinicie o AD DS com facilidade da mesma forma que faz com qualquer outro serviço que estiver sendo executado localmente no servidor. Enquanto o AD DS estiver pausado, é possível realizar tarefas de manutenção que, caso contrário, iriam requerer reiniciar o servidor, como desempenhar a desfragmentação offline do banco de dados do Active Directory, aplicar atualizações ao sistema operacional ou iniciar uma restauração autoritativa. Enquanto o AD DS estiver pausado em um servidor, outros controladores de domínio podem controlar as tarefas de autenticação e logon. Métodos de logon biométrico, credenciais armazenadas em cache e cartões inteligentes continuam tendo suporte. Se nenhum outro controlador de domínio estiver disponível e nenhum desses métodos de logon for aplicável, você ainda pode fazer o logon no servidor utilizando a conta e a senha do Directory Services Restore Mode.

Todos os controladores de domínio com Windows Server 2008 ou versões mais recentes suportam o Restartable Active Directory Domain Services, até mesmo RODCs. Se for administrador, você pode iniciar ou parar o AD DS usando a entrada Domain Controller no utilitário Services. Devido ao Restartable Active Directory Domain Services, controladores de domínio com Windows Server 2008 ou versões mais recentes têm três estados possíveis:

- **Active Directory Started** O Active Directory está iniciado e o controlador de domínio tem o mesmo estado de execução que um controlador de domínio com o Windows 2000 Server ou Windows Server 2003. Isso permite que o controlador de domínio forneça serviços de autenticação e logon para um domínio.
- **Active Directory Stopped** O Active Directory está pausado e o controlador de domínio não pode mais fornecer serviços de autenticação e logon para um domínio. Esse modo compartilha algumas características tanto de um servidor membro como de um controlador de domínio no Directory Services Restore Mode. Como ocorre com um servidor membro, o servidor conecta-se ao domínio. Os usuários podem efetuar logon interativamente utilizando métodos de logon biométrico, credenciais em cache e cartões inteligentes. Os usuários também podem efetuar logon na rede utilizando outro controlador de domínio para logon de domínio. Como ocorre no Directory Services Restore Mode, o banco de dados do Active Directory (Ntds.dit) no controlador de domínio local está offline. Isso significa que é possível realizar operações que necessitam que o AD DS esteja offline, como a desfragmentação do banco de dados e aplicação de atualizações de segurança, sem necessidade de reiniciar o controlador de domínio.
- **Directory Services Restore Mode** O Active Directory encontra-se em modo de restauração. O controlador de domínio possui o mesmo estado de restauração que um controlador de domínio com o Windows Server 2003. Esse modo permite

realizar uma restauração autoritativa ou não autoritativa do banco de dados do Active Directory.

Quando estiver trabalhando com o AD DS no estado Stopped, você deve lembrar que serviços dependentes também estão pausados quando o AD DS estiver pausado. Isso significa que o File Replication Service (FRS, Serviço de Replicação de Arquivos), o Kerberos Key Distribution Center (KDC, Centro de Distribuição de Chaves) e o Intersite Messaging (Mensagens entre Sites) são pausados antes do Active Directory ser pausado, e que mesmo quando estão sendo executados, esses serviços dependentes são reiniciados quando o Active Directory é reiniciado. Além disso, é possível reiniciar um controlador de domínio no Directory Services Restore Mode, mas não é possível iniciar um controlador de domínio com o Active Directory no estado Stopped. Para chegar ao estado Stopped, primeiramente é preciso iniciar o controlador de domínio normalmente para então parar o AD DS.

Serviços de resolução de nomes

Os sistemas operacionais Windows utilizam resolução de nomes para facilitar a comunicação com outros computadores em uma rede. A resolução de nomes associa os nomes dos computadores com os endereços IP numéricos utilizados para comunicações na rede. Assim, em vez de utilizar cadeias longas de dígitos, os usuários podem acessar um computador da rede utilizando um nome fácil.

Os atuais sistemas operacionais Windows suportam três sistemas de resolução de nomes:

- Domain Name System (DNS, Sistema de Nomes de Domínio)
- Windows Internet Name Service (WINS, Serviço de Cadastramento na Internet do Windows)
- Link-Local Multicast Name Resolution (LLMNR)

As seções que seguem analisam esses serviços.

Como utilizar o DNS

O DNS é o serviço de resolução de nomes que resolve nomes de computadores para endereços IP. Ao utilizar o DNS, o nome de host totalmente qualificado computer84.cpndl.com, por exemplo, pode ser resolvido para um endereço IP, permitindo que ele e os outros computadores se encontrem. O DNS opera na pilha de protocolo TCP/IP e pode ser integrado com o WINS, com o Dynamic Host Configuration Protocol (protocolo DHCP) e o AD DS. Como será discutido no Capítulo 15, “Como executar clientes e servidores DHCP”, o protocolo DHCP é utilizado para endereçamento de IP dinâmico e configuração TCP/IP.

O DNS organiza grupos de computadores em domínios. Esses domínios são organizados em estrutura hierárquica, que pode ser definida na Internet para redes públicas ou na empresa para redes privadas (também chamadas de *intranets* e *extranets*). Os vários níveis da hierarquia identificam computadores individuais, domínios organizacionais e domínios de primeiro nível (top-level). Para o nome do host totalmente qualificado computer84.cpndl.com, computer84 representa o nome do host para um computador individual, cpndl é o domínio organizacional e com é o domínio de primeiro nível.

Domínios de primeiro nível são a raiz da hierarquia DNS; eles também são chamados de *domínios-raiz*. Esses domínios são organizados geograficamente, por tipo de organização e por função. Domínios normais, como cpndl.com, também são chamados de *domínios-pai*. São chamados de domínios-pai porque são os pais de uma estrutura organizacional. Domínios-pai podem ser divididos em subdomínios que podem ser utilizados por grupos ou departamentos dentro de uma empresa.

Subdomínios são geralmente chamados de *domínios-filho*. Por exemplo, o nome de domínio totalmente qualificado (FQDN, fully qualified domain name) para um computador de um grupo de recursos humanos poderia ser jacob.hr.cpndl.com. Aqui, *jacob* é o nome do host, *hr* é o domínio-filho e *cpndl.com* é o domínio-pai.

Domínios do Active Directory utilizam o DNS para implementar sua estrutura de nomeação e hierarquia. O Active Directory e o DNS são quase totalmente integrados, tanto que é preciso instalar o DNS na rede antes de instalar os controladores de domínio utilizando o Active Directory. Durante a instalação do primeiro controlador de domínio em uma rede do Active Directory, você tem a oportunidade de instalar o DNS automaticamente se um servidor DNS não for encontrado na rede. Também pode especificar se deseja que o DNS e o Active Directory sejam totalmente integrados. Na maioria dos casos, é aconselhável responder afirmativamente a ambas as perguntas. Com a integração total, as informações do DNS são armazenadas diretamente no Active Directory. Isso permite que você aproveite as capacidades do Active Directory. A diferença entre integração parcial e total é muito importante:

- **Integração parcial** Com a integração parcial, o domínio utiliza o armazenamento de arquivo padrão. As informações do DNS são armazenadas em arquivos de texto com a extensão .dns, e a localização padrão desses arquivos é %SystemRoot%\System32\DNS. As atualizações para o DNS são controladas por um único servidor DNS autoritativo. Esse servidor é designado como o servidor DNS primário para um domínio específico ou área específicos dentro de um domínio chamado de *zona*. Clientes que utilizam atualizações dinâmicas do DNS através do DHCP devem estar configurados para utilizar o servidor DNS primário da zona. Se não estiverem, suas informações de DNS não serão atualizadas. Da mesma forma, atualizações dinâmicas através do DHCP não podem ocorrer se o servidor DNS primário estiver offline.
- **Integração total** Com a integração total, o domínio utiliza o armazenamento integrado com o diretório. As informações de DNS são armazenadas diretamente no Active Directory e ficam disponíveis através do contêiner para o objeto *dnsZone*. Como as informações fazem parte do Active Directory, qualquer controlador de domínio pode acessar os dados e uma abordagem multimestre pode ser utilizada para atualizações dinâmicas através do DHCP. Isso permite que qualquer controlador de domínio com o serviço DNS Server manipule as atualizações dinâmicas. Além disso, clientes que utilizam atualizações dinâmicas de DNS através do DHCP podem utilizar qualquer servidor DNS que faça parte da zona. Um benefício adicional da integração com o diretório é a habilidade de utilizar a segurança de diretório para controlar o acesso às informações de DNS.

Se observar a forma como as informações de DNS são replicadas pela rede, você verá mais vantagens na integração total com o Active Directory. Com a integração parcial, as informações de DNS são armazenadas e replicadas separadamente do Active Directory. Ter duas estruturas separadas reduz a eficácia tanto do DNS quanto do Active Directory e torna a administração mais complexa. Como o DNS é menos eficiente que

o Active Directory em replicar alterações, esse tipo de abordagem aumenta o tráfego da rede e a quantidade de tempo que leva para replicar as alterações de DNS pela rede.

Para habilitar o DNS na rede, é preciso configurar os clientes e servidores DNS. Quando você configura os clientes DNS, informa aos clientes os endereços IP dos servidores DNS da rede. Utilizando esses endereços, os clientes podem comunicar-se com os servidores DNS de qualquer parte da rede, mesmo que os servidores estejam em sub-redes diferentes.

Quando a rede utiliza o DHCP, é necessário configurar o DHCP para que trabalhe junto com o DNS. Para fazer isso, configure as opções de escopo DHCP 006 DNS Servers e 015 Domain Name como especificado em “Configuração das opções de escopo” no Capítulo 15. Além disso, se os computadores da rede precisarem ficar acessíveis a partir de outros domínios do Active Directory, é preciso criar registros para eles no DNS. Os registros no DNS são organizados em zonas; uma zona é, simplesmente, uma área de um domínio. Para configurar um servidor DNS, leia a explicação em “Configuração de um servidor DNS primário” no Capítulo 16, “Otimização do DNS”.

Quando você instala o Servidor DNS em um RODC, o RODC consegue extrair uma réplica somente leitura de todas as partições de diretório de aplicativo utilizadas pelo DNS, incluindo *ForestDNSZones* e *DomainDNSZones*. Então, os clientes podem consultar a resolução de nomes no RODC como consultariam em qualquer outro servidor DNS. No entanto, como no caso de atualizações do diretório, o servidor DNS em um RODC não suporta atualizações diretas. Isso significa que o RODC não registra um registro de recurso de servidor de nomes (NS, name server) em nenhuma zona integrada ao Active Directory que hospeda. Quando um cliente tenta atualizar seus registros de DNS contra um RODC, o servidor retorna uma referência a um servidor DNS que o cliente pode utilizar para atualização. O servidor DNS no RODC deve receber a atualização do registro do servidor DNS que recebeu os detalhes da atualização utilizando uma solicitação *replicate-single-object* (replicação de objeto único) que é executada em segundo plano.

O Windows 7 e versões mais recentes adicionaram suporte ao DNSSEC (Extensões de segurança DNS). O cliente DNS com esses sistemas operacionais pode enviar consultas que indiquem suporte ao DNSSEC, processar registros relacionados e determinar se um servidor DNS possui registros validados em seu nome. Nos servidores Windows, isso permite que os servidores DNS assinem zonas com segurança e hospedem zonas assinadas com DNSSEC. Também permite que servidores DNS processem registros relacionados e desempenhem validação e autenticação.

Como utilizar o Windows Internet Name Service

O WINS é um serviço que resolve nomes de computadores para endereços IP. Utilizando o WINS, o nome do computador COMPUTER84, por exemplo, pode ser resolvido para um endereço IP que permita a computadores em uma rede Microsoft encontrarem-se e trocarem informações. O WINS é necessário para dar suporte a sistemas anteriores ao Windows 2000 e a aplicativos mais抗igos que utilizam NetBIOS sobre TCP/IP, como os utilitários de linha de comando .NET. Se você não tiver aplicativos ou sistemas anteriores ao Windows 2000 na rede, não precisa utilizar o WINS.

O WINS funciona melhor em ambientes de cliente/servidor nos quais os clientes WINS enviam solicitações de resolução de nomes com rótulo único (host) para servidores WINS e os servidores WINS resolvem essas solicitações e respondem com o endereço IP equivalente. Quando todos os seus servidores DNS tiverem o Windows Ser-

ver 2008 ou uma versão mais recente, implantar uma zona de Nomes Globais (Global Names) cria registros globais estáticos, com rótulo único, sem depender do WINS. Isso permite que os usuários tenham acesso a hosts utilizando nomes de rótulo único em vez de FQDNs e remove a dependência ao WINS. Para transmitir informações e consultas WINS, os computadores utilizam o NetBIOS. O NetBIOS fornece uma interface de programação de aplicativo (API, application programming interface) que possibilita a comunicação entre os computadores de uma rede. Os aplicativos do NetBIOS dependem do WINS ou do arquivo LMHOSTS local para resolver nomes de computadores para endereços IP. Nas redes anteriores ao Windows 2000, o WINS era o principal serviço de resolução de nomes disponível. No Windows 2000 e em redes mais recentes, o DNS é o principal serviço de resolução de nomes e o WINS tem uma função diferente. Essa função serve para fazer com que sistemas anteriores ao Windows 2000 possam navegar por listas de recursos da rede e para permitir que o Windows 2000 e sistemas mais recentes localizem os recursos NetBIOS.

Para habilitar a resolução de nomes WINS na rede, é preciso configurar os clientes e servidores WINS. Quando você configura os clientes WINS, informa aos clientes os endereços IP dos servidores WINS da rede. Utilizando esses endereços, os clientes podem comunicar-se com os servidores WINS de qualquer parte da rede, mesmo que os servidores estejam em sub-redes diferentes. Os clientes WINS também podem comunicar-se utilizando um método de transmissão através do qual os clientes transmitem mensagens para outros computadores do mesmo segmento da rede local solicitando seus endereços IP. Pelo fato de essas mensagens serem transmitidas por difusão (broadcast), o servidor WINS não precisa ser utilizado. Qualquer cliente sem WINS que suporte esse tipo de transmissões de mensagem também poderá utilizar esse método para resolver nomes de computador para endereços IP.

Quando os clientes comunicam-se com servidores WINS, estabelecem sessões que têm estas três partes:

- **Registro de nome** Durante o registro de nome, o cliente dá ao servidor seu nome de computador e seu endereço IP e solicita que seja adicionado no banco de dados WINS. Se o nome de computador e endereço IP não estiverem em uso na rede, o servidor WINS aceita a solicitação e registra o cliente no banco de dados WINS.
- **Renovação de nome** O registro de nome não é permanente. Em vez disso, o cliente pode utilizar o nome por um período específico chamado de *concessão*. O cliente também recebe um prazo para renovar a concessão, esse prazo é chamado de intervalo de renovação. O cliente deve registrar-se novamente no servidor WINS durante o intervalo de renovação.
- **Liberação de nome** Se o cliente não puder renovar a concessão, o registro de nome é liberado, permitindo que outro sistema da rede utilize o nome de computador, endereço IP ou ambos. Os nomes também são liberados quando um cliente WINS é desligado.

Depois que um cliente estabelece um sessão com o servidor WINS, o cliente pode solicitar serviços de resolução de nome. O método utilizado para resolver nomes de computador para endereço IP depende de como a rede está configurada. Estes quatro métodos de resolução de nomes estão disponíveis:

- **B-node (difusão)** Utiliza mensagem de difusão para resolver nomes de computador para endereços IP. Computadores que necessitam resolver um nome

transmitem uma mensagem para cada host da rede local, solicitando o endereço IP para um nome de computador. Em uma rede grande com centenas ou milhares de computadores, essas mensagens de difusão podem usar largura de banda significativa da rede.

- **P-node (ponto a ponto)** Utiliza servidores WINS para resolver nomes de computador para endereços IP. Como explicado anteriormente, sessões de cliente têm três partes: registro de nome, renovação de nome e liberação de nome. Nesse modo, quando um cliente precisa resolver um nome de computador para um endereço IP, o cliente envia uma mensagem de consulta ao servidor e o servidor responde com uma resposta.
- **M-node (misto)** É uma combinação de B-node com P-node. Com o M-node, um cliente WINS primeiramente tenta utilizar o B-node para resolução de nomes. Se a tentativa falhar, o cliente tenta utilizar o P-node. Como o B-node é utilizado antes, esse método tem os mesmos problemas com uso da largura de banda da rede que o B-node.
- **H-node (híbrido)** Também é uma combinação de B-node com P-node. Com o H-node, um cliente WINS primeiramente tenta utilizar o P-node para resolução de nomes ponto a ponto. Se a tentativa falhar, o cliente tenta utilizar mensagem de difusão com o B-node. Como o primeiro método é o ponto a ponto, o H-node oferece o melhor desempenho na maioria das redes. O H-node também é o método padrão para resolução de nomes WINS.

Se servidores WINS estiverem disponíveis na rede, os clientes Windows utilizam o método P-node para resolução de nomes. Se não houver servidores WINS disponíveis na rede, os clientes Windows utilizam o método B-node para resolução de nomes. Computadores com Windows também podem utilizar o DNS e os arquivos locais LMHOSTS e HOSTS para resolver nomes de rede. O Capítulo 16 aborda como trabalhar com o DNS.

Quando você utiliza o DHCP para atribuir endereços IP dinamicamente, deve configurar o método de resolução de nomes para clientes DHCP. Para fazer isso, configure as opções de escopo DHCP para 046 WINS/NBT Node Type como especificado em “Configuração das opções de escopo” no Capítulo 15. O melhor método a utilizar é o H-node. Você obterá o melhor desempenho e terá tráfego de rede reduzido.

Como utilizar o Link-Local Multicast Name Resolution (LLMNR)

O LLMNR atende a uma necessidade por serviços ponto a ponto de resolução de nomes para dispositivos com um endereço IPv4, IPv6 ou ambos, permitindo que dispositivos IPv4 e IPv6 em uma única sub-rede sem um servidor WINS ou DNS resolvam o nome um do outro – um serviço que nem o WINS nem o DNS podem fornecer inteiramente. Embora o WINS possa fornecer serviços de resolução de nomes ponto a ponto e cliente/servidor para IPv4, ele não suporta endereços IPv6. O DNS, por outro lado, suporta endereços IPv4 e IPv6, mas depende dos servidores designados a fornecer serviços de resolução de nomes.

O Windows 7 e versões mais recentes dão suporte ao LLMNR. O LLMNR é projetado para clientes IPv4 e IPv6 em configurações nas quais outros sistemas de resolução de nomes não estão disponíveis, como em:

- Redes residenciais ou de escritórios pequenos
- Redes ad hoc
- Redes corporativas em que serviços DNS não estão disponíveis

O LLMNR é projetado para complementar o DNS habilitando resolução de nomes em situações nas quais a resolução de nomes DNS convencional não é possível. Embora o LLMNR possa substituir a necessidade pelo WINS nos casos em que o NetBIOS não é necessário, o LLMNR não é um substituto do DNS porque opera somente na sub-rede local. Como impede-se que o tráfego do LLMNR propague-se pelos roteadores, ele não tem como saturar a rede por acidente.

Como o WINS, utiliza-se o LLMNR para resolver um nome de host, como COMPUTER84, para um endereço IP. Por padrão, o LLMNR vem habilitado em todos os computadores com Windows 7 ou versões mais recentes, e esses computadores utilizam o LLMNR somente quando todas as tentativas de procurar por um nome de host através do DNS falham. Como resultado, a resolução de nomes funciona assim para o Windows 7 e versões mais recentes:

1. Um computador host envia uma consulta para seu servidor DNS configurado como primário. Se o computador host não receber uma resposta ou receber um erro, ele tenta cada servidor DNS configurado como alternativo por vez. Se o host não tiver um servidor DNS configurado ou não conseguir conectar-se a um servidor DNS sem erros, a resolução de nomes falha e passa para o LLMNR.
2. O computador host envia uma consulta multicast por meio do protocolo UDP (User Datagram Protocol) solicitando o endereço IP para o nome que está procurando. Essa consulta é restrita à sub-rede local (também chamada de *link local*).
3. Cada computador no link local que dê suporte ao LLMNR e que seja configurado para responder as consultas que chegam recebe a consulta e compara o nome ao seu próprio nome de host. Se o nome de host não for igual, o computador descarta a consulta. Se o nome de host for igual, o computador transmite uma mensagem unicast contendo o seu endereço IP para o host original.

Também é possível utilizar o LLMNR para mapeamento reverso. Com um mapeamento reverso, um computador envia uma consulta unicast para um endereço IP específico, solicitando o nome de host do computador de destino. Um computador com LLMNR habilitado que recebe a solicitação envia uma resposta unicast contendo seu nome de host para o host de origem.

Exige-se que computadores com LLMNR habilitado garantam que seus nomes sejam únicos na sub-rede local. Na maioria dos casos, um computador verifica se há exclusividade quando é iniciado, quando é retomado após um estado de suspensão e quando você altera as configurações da interface de rede. Se um computador ainda não tiver determinado que o nome é exclusivo, deve indicar essa condição quando responder a uma consulta de nome.

MUNDO REAL Por padrão, o LLMNR vem habilitado automaticamente em computadores com Windows 7 ou versões mais recentes. É possível desabilitar o LLMNR através das configurações de registro. Para desabilitar o LLMNR para todas as interfaces de rede, crie e defina com valor 0 o seguinte item no registro: HKLM/SYSTEM/CurrentControlSet/Services/Dnscache/Parameters/EnableMulticast.

Para desabilitar o LLMNR para interfaces de rede específicas, crie e defina com valor 0 para o item no registro: HKLM/SYSTEM/CurrentControlSet/Services/Tcpip/Parameters/Adapter-GUID/EnableMulticast.

Aqui, *AdapterGUID* é o identificador global exclusivo (GUID, global unique identifier) do adaptador de interface de rede para o qual você deseja desabilitar o LLMNR. É possível habilitar o LLMNR novamente a qualquer momento configurando para 1 esses valores de registro. Você também pode gerenciar o LLMNR usando Group Policy.

Ferramentas frequentemente utilizadas

Muitos utilitários estão disponíveis para administrar os sistemas Windows Server 2012. As ferramentas mais utilizadas incluem as seguintes:

- **Control Panel** Uma coleção de ferramentas para gerenciar a configuração do sistema. É possível organizar o Control Panel de diferentes formas de acordo com o modo de exibição que estiver utilizando. Um modo de exibição é simplesmente uma forma de organizar e representar opções. Altera-se o modo de exibição utilizando a lista View By. O modo Category é o padrão e fornece acesso a ferramentas por categorias, ferramentas e tarefas-chave. Os modos Large Icons e Small Icons são modos de exibição alternativos que listam cada ferramenta separadamente por nome.
- **Ferramentas administrativas gráficas** Ferramentas-chave para gerenciar os computadores da rede e seus recursos. É possível acessar essas ferramentas selecionando-as individualmente no grupo de programa Administrative Tools.
- **Assistentes administrativos** Ferramentas projetadas para automatizar tarefas administrativas-chave. É possível acessar muitos assistentes administrativos no Server Manager – o console de administração central do Windows Server 2012.
- **Utilitários de linha de comando** É possível iniciar a maioria dos utilitários usando o prompt de comando. Além desses utilitários, o Windows Server 2012 fornece outros que são úteis para trabalhar com os sistemas Windows Server 2012.

Para aprender como utilizar qualquer uma das ferramentas de linha de comando .NET, digite **NET HELP** em um prompt de comando seguido pelo nome do comando, como **NET HELP SHARE**. O Windows Server 2012 fornece, então, uma visão geral de como o comando é utilizado.

Windows PowerShell 3.0

Para mais flexibilidade nos scripts de sua linha de comando, o Windows PowerShell 3.0 é uma alternativa. O Windows PowerShell 3.0 é um comando shell completo que pode utilizar comandos internos (chamados de *cmdlets*), recursos de programação internos e utilitários de linha de comando padrão. Um console de comando e um ambiente gráfico estão disponíveis.

Embora o console do Windows PowerShell e o ambiente de criação de scripts gráfico estejam instalados por padrão, muitos outros recursos do PowerShell não vêm instalados por padrão. Dentre eles estão o mecanismo Windows PowerShell 2.0, que é fornecido para compatibilidade com versões anteriores de aplicativos host PowerShell, e o Windows PowerShell Access, que permite ao servidor agir como um gateway da web para gerenciar o servidor remotamente utilizando o PowerShell e um cliente web.

MUNDO REAL É possível instalar todos esses recursos adicionais do Windows PowerShell utilizando o assistente Add Roles And Features (Adicionar Funções e Recursos). Na área de trabalho, toque ou clique no botão Server Manager na barra de tarefas. Essa opção está inclusa por padrão. Em Server Manager, toque ou clique em Manage e depois em Add Roles And Features. Isso faz com que o assistente Add Roles And Features seja executado, com ele é possível adicionar recursos. Observe, no entanto, que com o Windows Server 2012, além de poder desabilitar uma função ou recurso, também é possível remover os binários necessários para tal função ou recurso. Os binários necessários para a instalação de funções e recursos são chamados de *payloads*.

O console do Windows PowerShell (PowerShell.exe) é um ambiente de 32 bits ou de 64 bits para trabalhar com o Windows PowerShell na linha de comando. Nas versões de 32 bits do Windows, você encontrará o PowerShell executável de 32 bits no diretório %SystemRoot%\System32\WindowsPowerShell\v1.0. Nas versões de 64 bits do Windows, você encontrará o PowerShell executável de 32 bits no diretório %SystemRoot%\SysWow64\WindowsPowerShell\v1.0 e o de 64 bits no diretório %SystemRoot%\System32\WindowsPowerShell\v1.0.

Na área de trabalho, é possível abrir o console do Windows PowerShell tocando ou clicando no botão PowerShell na barra de tarefas. Essa opção está inclusa por padrão. Em sistemas de 64 bits, a versão de 64 bits do PowerShell é iniciada por padrão. Se deseja utilizar o console do PowerShell de 32 bits em um sistema de 64 bits, é preciso selecionar a opção Windows PowerShell (x86).

Você pode iniciar o Windows PowerShell a partir de um prompt de comando do Windows (Cmd.exe) digitando o seguinte:

```
powershell
```

OBSERVAÇÃO O caminho do diretório para o Windows PowerShell deverá estar em seu caminho de comando (path) por padrão. Isso garante que você possa iniciar o Windows PowerShell a partir de um prompt de comando sem antes ter que mudar para o diretório relacionado.

Após iniciar o Windows PowerShell, você pode digitar o nome de um cmdlet no prompt e o cmdlet será executado de forma muito parecida com a de um comando de linha de comando. Também pode-se executar cmdlets em scripts. Cmdlets são nomeados utilizando pares de palavras (um verbo e um substantivo). O verbo indica o que o cmdlet faz no geral. O substantivo indica com o que especificamente o cmdlet trabalha. Por exemplo, o cmdlet Get-Variable recupera todas as variáveis de ambiente do Windows PowerShell e retorna seus valores, ou recupera uma variável de ambiente com nome específico e retorna seu valor. Os verbos comuns associados aos cmdlets são:

- **Get-** Pesquisa um objeto específico ou um subconjunto de um tipo de objeto, como um contador de desempenho específico ou todos os contadores de desempenho
- **Set-** Modifica as configurações específicas de um objeto
- **Enable-** Habilita uma opção ou um recurso
- **Disable-** Desabilita uma opção ou um recurso
- **New-** Cria uma nova instância de um item, como um novo evento ou serviço
- **Remove-** Remove uma instância de um item, como um evento ou log de evento

No prompt do Windows PowerShell, é possível obter uma lista completa de cmdlets digitando **get-help *-***. Para obter documentação de ajuda sobre um cmdlet específico, digite **get-help** seguido pelo nome do cmdlet, como em **get-help get-variable**.

Todos os cmdlets também possuem aliases configuráveis que agem como atalhos para a execução de um cmdlet. Para listar todos os aliases disponíveis, digite **get-item -path alias**: no prompt do Windows PowerShell. Você pode criar um alias que invoque qualquer comando utilizando o seguinte:

```
new-item -path alias:AliasName -value:FullCommandPath
```

Aqui, *AliasName* é o nome do alias a ser criado, e *FullCommandPath* é o caminho completo para o comando a ser executado, como

```
new-item -path alias:sm -value:c:\windows\system32\compmgmt\launcher.exe
```

Esse exemplo cria o alias *sm* para iniciar o Server Manager. Para utilizar esses alias, você deve simplesmente digitar **sm** e pressionar Enter quando estiver trabalhando com o Windows PowerShell.

MUNDO REAL De modo geral, tudo o que pode ser digitado em um prompt de comando também pode ser digitado no prompt do PowerShell. Isso é possível porque o PowerShell procura utilitários e comandos externos como parte de seu processamento normal. Contanto que o utilitário ou comando externo encontre-se em um diretório especificado pela variável de ambiente PATH, o utilitário ou comando será executado adequadamente. Entretanto, lembre-se de que a ordem de execução do PowerShell pode determinar se um comando é executado como esperado ou não. Para o PowerShell, a ordem de execução é 1) aliases alternativos internos ou definidos por perfil, 2) funções internas ou definidas por perfil, 3) palavras-chave de idiomas ou cmdlets, 4) scripts com a extensão .ps1, e 5) arquivos, utilitários e comandos externos. Assim, se qualquer elemento de 1 a 4 na ordem de execução tiver o mesmo nome que um comando, esse elemento será executado em vez do comando esperado.

Windows Remote Management

Os recursos de comunicação remota do Windows PowerShell são suportados pelo protocolo WS-Management e pelo serviço WinRM (Windows Remote Management) que implementa o WS-Management no Windows. Computadores com o Windows 7 e versões mais recentes, assim como o Windows Server 2008 R2 e versões mais recentes, incluem o WinRM 2.0 ou versão mais recente. Se quiser gerenciar um servidor do Windows a partir de uma estação de trabalho, é necessário ter certeza de que o WinRM 2.0 e o Windows PowerShell 3.0 estão instalados e de que o servidor possui um listener do WinRM habilitado. Uma extensão do IIS, instalável como um recurso do Windows chamado WinRM IIS Extension, permite que um servidor aja como um gateway da web para gerenciar o servidor remotamente utilizando o WinRM e um cliente web.

Como habilitar e utilizar o WinRM

É possível verificar a disponibilidade do WinRM 2.0 e configurar o Windows PowerShell para comunicação remota seguindo estas etapas:

1. Toque ou clique em Start; aponte para o Windows PowerShell. Inicie o Windows PowerShell como um administrador pressionando e segurando ou clicando com o botão direito do mouse no atalho para o Windows PowerShell e selecionando Run As Administrator.
2. Por padrão, o serviço WinRM vem configurado para inicialização manual. Deve-se alterar o tipo de inicialização para Automatic e iniciar o serviço em cada

computador com o qual deseja trabalhar. No prompt do Windows PowerShell, é possível verificar que o serviço WinRM está sendo executado, basta utilizar o seguinte comando:

```
get-service winrm
```

Como mostrado no exemplo a seguir, o valor da propriedade *Status* na saída deve ser *Running*:

Status	Name	DisplayName
Running	WinRM	Windows Remote Management

Se o serviço estiver pausado, digite o seguinte comando para iniciar o serviço e configurá-lo para iniciar automaticamente no futuro:

```
set-service -name winrm -startuptype automatic -status running
```

3. Para configurar o Windows PowerShell para utilização remota, digite o seguinte comando:

```
Enable-PSRemoting -force
```

É possível habilitar a utilização remota somente quando o computador estiver conectado a uma rede corporativa ou privada. Se seu computador estiver conectado a uma rede pública, é necessário desconectá-lo da rede pública e conectá-lo a uma rede corporativa ou privada para então realizar essa etapa. Se uma ou mais conexões do seu computador tiver o tipo de conexão Public Network mas estiver, na verdade, conectado a uma rede corporativa ou privada, é preciso alterar o tipo de conexão em Network And Sharing Center e então realizar essa etapa.

Em muitos casos, é possível trabalhar com computadores remotos em outros domínios. Entretanto, se o computador remoto não for um membro de domínio confiável, talvez o computador remoto não consiga autenticar as suas credenciais. Para habilitar a autenticação, é preciso adicionar o computador remoto à lista de hosts confiáveis para o computador local no WinRM. Para tanto, siga estas etapas:

```
winrm set winrm/config/client '@{TrustedHosts="RemoteComputer"}'
```

Aqui, *RemoteComputer* é o nome do computador remoto, como

```
winrm set winrm/config/client '@{TrustedHosts="CorpServer56"}'
```

Quando estiver trabalhando com computadores de um grupo de trabalho ou grupo doméstico, você deve utilizar HTTPS como transporte ou adicionar a máquina remota às configurações de TrustedHosts. Se não conseguir conectar-se a um host remoto, verifique se o serviço está sendo executado no host remoto e se ele está aceitando solicitações, para isso, execute o seguinte comando no host remoto:

```
winrm quickconfig
```

Esse comando analisa e configura o serviço WinRM. Se o serviço WinRM estiver configurado corretamente, você verá saídas parecidas com estas:

```
WinRM already is set up to receive requests on this machine.  
WinRM already is set up for remote management on this machine.
```

Se o serviço WinRM não estiver configurado corretamente, você verá erros e precisará responder afirmativamente para diversos prompts que permitem configurar o gerenciamento remoto automaticamente. Quando esse processo estiver concluído, o WinRM estará configurado corretamente.

Sempre que utilizar os recursos remotos do Windows PowerShell, inicie o Windows PowerShell como um administrador pressionando e segurando ou clicando com o botão direito do mouse no atalho do Windows PowerShell e selecionando Run As Administrator. Para iniciar o Windows PowerShell a partir de outro programa, como o prompt de comando, é preciso iniciar tal programa como um administrador.

Como configurar o WinRM

Quando você estiver trabalhando com um prompt de comando elevado como administrador, pode utilizar o utilitário de linha de comando WinRM para visualizar e gerenciar a configuração do gerenciamento remoto. Digite **winrm get winrm/config** para exibir informações detalhadas sobre a configuração do gerenciamento remoto.

Se analisar a listagem de configuração, perceberá que há uma hierarquia de informações. A base dessa hierarquia, o nível Config, é referenciado com o caminho `winrm/config`. Em seguida há subníveis para cliente, serviço e WinRS, referenciados por `winrm/config/client`, `winrm/config/service` e `winrm/config/winrs`. É possível alterar o valor da maioria dos parâmetros de configuração utilizando o seguinte comando:

```
winrm set ConfigPath @{ParameterName="Value"}
```

Aqui, *ConfigPath* é o caminho da configuração, *ParameterName* é o nome do parâmetro com o qual você deseja trabalhar, e *Value* define o valor para o parâmetro, como

```
winrm set winrm/config/winrs @{MaxShellsPerUser="10"}
```

Aqui, define-se o parâmetro *MaxShellsPerUser* dentro de `winrm/config/winrs`. Esse parâmetro controla o número máximo de conexões a um computador remoto que podem estarativas por um usuário. (Por padrão, cada usuário pode ter apenas cinco conexões ativas.) Lembre-se de que alguns dos parâmetros são somente leitura e não podem ser configurados dessa forma.

O WinRM requer pelo menos um ouvinte (listener) para indicar transportes e endereços IP que aceitem solicitações de gerenciamento. O transporte deve ser HTTP, HTTPS ou ambos. Com HTTP, as mensagens podem ser criptografadas utilizando criptografia NTLM ou Kerberos. Com HTTPS, utiliza-se o protocolo SSL (Secure Sockets Layer) na criptografia. É possível analisar os ouvintes configurados digitando **winrm enumerate winrm/config/listener**. Como mostrado na Listagem 1-1, esse comando exibe os detalhes da configuração dos ouvintes configurados.

LISTAGEM 1-1 Exemplo de configuração para ouvintes

Listener

```
Address = *
Transport = HTTP
Port = 80
Hostname
Enabled = true
URLPrefix = wsman
CertificateThumbprint
ListeningOn = 127.0.0.1, 192.168.1.225
```

Por padrão, seu computador está provavelmente configurado para ouvir qualquer endereço IP. Se esse for o caso, você não verá saída. Para limitar o WinRM para endereços IP específicos, o endereço de loopback local do computador (127.0.0.1) e endereços IPv4 e IPv6 atribuídos podem ser configurados explicitamente para ouvir. Você pode configurar um computador para que ouça solicitações de todos os endereços IP configurados através do HTTP digitando o seguinte:

```
winrm create winrm/config/listener?Address=*+Transport=HTTP
```

Você pode ouvir solicitações de todos os endereços IP configurados através do HTTPS digitando isto:

```
winrm create winrm/config/listener?Address=*+Transport=HTTPS
```

Aqui, o asterisco (*) indica todos os endereços IP configurados. Perceba que a propriedade *CertificateThumbprint* deve estar vazia para compartilhar a configuração SSL com outro serviço.

É possível habilitar ou desabilitar um ouvinte para um endereço IP específico digitando

```
winrm set winrm/config/listener?Address=IP:192.168.1.225+Transport=HTTP  
@{Enabled="true"}
```

ou

```
winrm set winrm/config/listener?Address=IP:192.168.1.225+Transport=HTTP  
@{Enabled="false"}
```

É possível habilitar ou desabilitar autenticação básica no cliente digitando

```
winrm set winrm/config/client/auth @{Basic="true"}
```

ou

```
winrm set winrm/config/client/auth @{Basic="false"}
```

Você pode habilitar ou desabilitar a autenticação do Windows usando o NTLM ou o Kerberos (conforme adequado) digitando

```
winrm set winrm/config/client @{TrustedHosts=<local>"}
```

ou

```
winrm set winrm/config/client @{TrustedHosts=""}
```

Além de gerenciar o WinRM na linha de comando, é possível gerenciar o serviço utilizando Group Policy (política de grupo). Como resultado, as configurações via Group Policy podem acabar sobrepondo qualquer configuração que você inserir.

CAPÍTULO 2

Gerenciamento de servidores com o Windows Server 2012

- Funções de servidor, serviços de função e recursos para o Windows Server 2012 **31**
- Instalações de servidor completo, interface mínima e Server Core **39**
- Instalação do Windows Server 2012 **42**
- Gerenciamento de funções, serviços de função e recursos **56**
- Gerenciamento de propriedades do sistema **72**

Os servidores são o coração de qualquer rede do Microsoft Windows e o gerenciamento desses recursos é uma das principais responsabilidades que você tem como administrador. O Windows Server 2012 vem com diversas ferramentas de gerenciamento integradas. A ferramenta que você utilizará para realizar tarefas de administração básicas do sistema chama-se Server Manager (Gerenciador do Servidor). O Server Manager oferece opções de instalação e configuração para o servidor local, bem como opções de gerenciamento de funções, recursos e configurações relacionadas em qualquer servidor da empresa que seja remotamente gerenciável. As tarefas em que o Server Manager pode ser utilizado incluem:

- Adição de servidores para gerenciamento remoto
- Inicialização de conexões remotas aos servidores
- Configuração do servidor local
- Gerenciamento de funções e recursos instalados
- Gerenciamento de volumes e compartilhamentos em servidores de arquivos
- Configuração de Network Interface Card (NIC) Teaming (Agrupamento de interfaces de rede)
- Visualização de eventos e alertas
- Reinicialização de servidores

O Server Manager é excelente para a administração geral do sistema, mas além dele é necessária uma ferramenta que ofereça um controle fino das configurações e propriedades do ambiente do sistema. É aí que aparece o utilitário System (Sistema). Você pode usar esse utilitário para:

- Alterar o nome de um computador
- Ajustar configurações de desempenho de aplicativos, memória virtual e registro
- Administrar variáveis de ambiente do sistema e do usuário
- Configurar opções de inicialização e recuperação do sistema

Funções de servidor, serviços de função e recursos para o Windows Server 2012

O Windows Server 2012 utiliza a mesma arquitetura de configuração que foi usada no Windows Server 2008 e no Windows Server 2008 Release 2 (R2). Para preparar os servidores durante a implantação, deve-se instalar e configurar os seguintes componentes:

- **Server roles (Funções de servidor)** Uma função de servidor é um conjunto relacionado de componentes de software que possibilita a um servidor desempenhar uma determinada função para usuários ou outros computadores em uma rede. Um computador pode ser dedicado à uma única função, como o Active Directory Domain Services (AD DS, Serviços de Domínio Active Directory), ou desempenhar múltiplas funções.
- **Role services (Serviços de função)** Um serviço de função é um componente de software que confere a funcionalidade à função de servidor. Cada função pode ter um ou mais serviços de função relacionados. Algumas funções de servidor, como o Domain Name Service (DNS, Serviço de Nomes de Domínio) ou o Dynamic Host Configuration Protocol (protocolo DHCP), possuem um só serviço de função. Assim, a instalação da função de servidor também instala o seu respectivo serviço de função. Outras funções possuem diversos serviços de função que podem ser instalados, como é o caso para Network Policy and Access Services (Serviços de Acesso e Política de Rede) e Active Directory Certificate Services (AD CS, Serviços de Certificados do Active Directory). Nessas funções de servidor, pode-se escolher quais serviços de função serão instalados.
- **Features (Recursos)** Um recurso é um componente de software que confere uma funcionalidade adicional. Recursos como Bitlocker Drive Encryption (Criptografia de Unidade de Disco BitLocker) e Windows Server Backup são instalados e removidos separados de funções e serviços de função. Um computador pode ter zero ou mais recursos instalados, dependendo da sua configuração.

Para configurar funções, serviços de função e recursos, utilize o Server Manager, um Microsoft Management Console (MMC, Console de Gerenciamento Microsoft). Algumas funções, serviços de função e recursos são dependentes de outras funções, serviços de função e recursos. Ao instalar funções, serviços de função e recursos, o Server Manager solicita que você instale outras funções, serviços de função e recursos necessários. Da mesma forma, se você tentar remover um componente necessário de uma função, serviço de função ou recurso instalado, o Server Manager dirá que não pode remover o componente a menos que você também remova as funções, serviços de função ou recursos dependentes.

Tendo em vista que a adição ou remoção de funções, serviços de função e recursos pode alterar requisitos de hardware, deve-se planejar com cuidado qualquer alteração nas configurações para determinar de que forma isso afetará o desempenho geral de um servidor. Embora o normal seja combinar funções complementares, fazer isso aumenta a carga de trabalho do servidor. Consequentemente, torna-se necessária a otimização do hardware do servidor. A Tabela 2-1 oferece uma visão geral das funções primárias e de serviços de função relacionados que se pode implantar em um servidor executando o Windows Server 2012.

TABELA 2-1 Funções primárias e serviços de função relacionados para o Windows Server 2012

FUNÇÃO	DESCRIÇÃO
Active Directory Certificate Services (AD CS)	Fornece funções necessárias para a emissão e a revogação de certificados digitais para usuários, computadores clientes e servidores. Inclui os seguintes serviços de função: Certification Authority (Autoridades de Certificação), Certification Authority Web Enrollment (Registro na Web de Autoridade de Certificação), Online Responder (Respondente Online), Network Device Enrollment Service (Serviço de Inscrição de Dispositivos de Rede), Certificate Enrollment Web Service (Serviço Web de Registro de Certificado) e Certificate Enrollment Policy Web Service (Serviço Web de Política de Registro de Certificado).
Active Directory Domain Services (AD DS)	Fornece funções necessárias para o armazenamento de informações sobre usuários, grupos, computadores e outros objetos na rede e disponibiliza essas informações aos usuários e computadores. Os controladores de domínio do Active Directory dão aos usuários e computadores acesso aos recursos de rede permitidos.
Active Directory Federation Services (AD FS)	Complementa os recursos de gerenciamento de autenticação e acesso AD DS, estendendo-os à World Wide Web. Inclui os seguintes serviços de função e subserviços: Federation Service (Serviço de Federação), Federation Service Proxy (Proxy do Serviço de Federação), AD FS Web Agents (Agentes da Web do AD FS), Claims-Aware Agent (Agente de reconhecimento de declaração do AD FS) e Windows Token-Based Agent (Agente baseado em token do Windows do AD FS).
Active Directory Lightweight Directory Services (AD LDS)	Fornece armazenamento de dados para aplicativos habilitados para serviços de diretório que não requerem AD DS e nem implantação em controladores de domínio. Não inclui serviços de função adicionais.
Active Directory Rights Management Services (AD RMS)	Oferece acesso controlado para proteger mensagens de email, documentos, páginas intranet e outros tipos de arquivos. Inclui os seguintes serviços de função: Active Directory Rights Management Server e Identify Federation Support (Suporte à Federação de Identidade).
Application Server	Permite que um servidor hospede aplicativos distribuídos construídos em ASP.NET, Enterprise Services e Microsoft .NET Framework 4.5. Inclui mais de uma dúzia de serviços de função.
DHCP Server	O DHCP oferece o gerenciamento centralizado de endereçamentos IP. Servidores DHCP podem atribuir endereços IP dinâmicos e configurações essenciais de TCP/IP aos outros computadores em uma rede. Não inclui serviços de função adicionais.
DNS Server	O DNS é um sistema de resolução de nomes que resolve nomes de computadores para endereços IP. Os servidores DNS são essenciais para a resolução de nomes nos domínios do Active Directory. Não inclui serviços de função adicionais.

FUNÇÃO	DESCRIÇÃO
Fax Server	Oferece gerenciamento centralizado sobre envio e recebimento de faxes na empresa. Um servidor de fax pode funcionar como gateway para o uso de fax e possibilitar o gerenciamento de recursos de fax (como tarefas e relatórios) e de dispositivos de fax no servidor ou na rede. Não inclui serviços de função adicionais.
File And Storage Services	Oferece serviços essenciais para gerenciar os arquivos e o armazenamento, além da maneira como são disponibilizados e replicados na rede. Diversas funções de servidor requerem algum tipo de serviço de arquivo. Inclui os seguintes serviços de função e subserviços: BranchCache for Network Files (BranchCache para Arquivos de Rede), Data Deduplication (Desduplicação de Dados), Distributed File System (DFS, Sistema de Arquivos Distribuído), DFS Namespaces, DFS Replication, File Server (Servidor de Arquivos), File Server Resource Manager (Gerenciador de Recursos de Servidor de Arquivos), Server for NFS, File Server VSS Agent Service (Serviço de Agente VSS de Servidor de Arquivos), iSCSI Target Server (Servidor de Destino iSCSI), iSCSI Target Storage Provider (Provedor de Armazenamento do Destino iSCSI) e Storage Services (Serviços de Armazenamento).
Hyper-V (solução de virtualização da Microsoft)	Fornece serviços para a criação e o gerenciamento de máquinas virtuais que emulam computadores físicos. As máquinas virtuais possuem ambientes de sistema operacional separados do servidor host.
Network Policy And Access Services (NPAS)	Fornece serviços essenciais ao gerenciamento de políticas de acesso à rede. Inclui os seguintes serviços de função: Network Policy Server (NPS, Servidor de Políticas de Rede), Health Registration Authority, (HRA, Autoridade de Registro de Integridade) e Host Credential Authorization Protocol (Protocolo HCAP).
Print And Document Services	Fornece serviços essenciais ao gerenciamento de impressoras e scanners em rede e drivers relacionados. Inclui os seguintes serviços de função: Print Server (Servidor de Impressão), LPD Service (Serviço LPD), Internet Printing (Impressão via Internet) e Distributed Scan Server.(Servidor de Digitalização Distribuída).
Remote Access	Fornece serviços para o gerenciamento de roteamento e acesso remoto às redes. Utilize esta função se precisar configurar Virtual Private Networks (VPN, Rede Virtual Privada), Network Address Translation (NAT, Conversão de Endereço de Rede) e outros serviços de roteamento. Inclui os seguintes serviços de função: DirectAccess e VPN (RAS) e Routing (Roteamento).
Remote Desktop Services	Fornece serviços que possibilitam aos usuários executarem aplicativos baseados em Windows instalados em um servidor remoto. Quando os usuários executam um aplicativo em um servidor de terminal, a execução e o processamento ocorrem no servidor e apenas os dados do aplicativo são transmitidos pela rede.

Continua

TABELA 2-1 Funções primárias e serviços de função relacionados para o Windows Server 2012 (*continuação*)

FUNÇÃO	DESCRIÇÃO
Volume Activation Services	Fornece serviços para a automação do gerenciamento de chaves de licença de volume e ativação de chaves de volume.
Web Server (IIS)	Utilizada para hospedar sites e aplicativos baseados na Web. Os sites hospedados em um servidor Web podem ter conteúdo estático ou dinâmico. É possível criar aplicativos Web hospedados em um servidor Web usando ASP.NET e .NET Framework 4.5. Ao implantar um servidor Web, você pode gerenciar a configuração do servidor através dos módulos e ferramentas de administração IIS 8. Inclui dezenas de serviços de função.
Windows Deployment Services (WDS)	Fornece serviços para a implantação de computadores Windows na empresa. Inclui os seguintes serviços de função: Deployment Server (Servidor de Implantação) e Transport Server (Servidor de Transporte).
Windows Server Update Services (WSUS)	Fornece serviços de atualização de produtos Microsoft, possibilitando que você distribua atualizações a partir de servidores designados.

A Tabela 2-2 oferece uma visão geral dos principais recursos que podem ser implantados em um servidor com Windows Server 2012. Ao contrário dos lançamentos anteriores do Windows, o Windows Server 2012 não instala automaticamente alguns recursos importantes do servidor. Por exemplo: você deve adicionar o Windows Server Backup para utilizar o backup integrado e restaurar recursos do sistema operacional.

TABELA 2-2 Principais recursos do Windows Server 2012

RECURSO	DESCRIÇÃO
Background Intelligent Transfer Service (BITS)	Fornece transferências inteligentes em segundo plano. Ao instalar este recurso, o servidor pode agir como um servidor BITS, podendo receber carregamentos de arquivos de clientes. Esse recurso não é necessário para realizar downloads para os clientes que utilizem BITS. Sub-recursos adicionais incluem IIS BITS Server Extension e BITS Compact Server.
BitLocker Drive Encryption	Fornece segurança baseada em hardware para a proteção de dados por meio da criptografia do volume completo, que impede a adulteração de discos enquanto o sistema operacional está offline. Os computadores que utilizam Trusted Platform Module (TPM) podem usar BitLocker Drive Encryption no modo Startup Key (chave de inicialização) ou no modo básico TPM-Only (somente TPM). Ambos os modos fornecem validação precoce da integridade.
BitLocker Network Unlock	Dá suporte aos protetores de chave baseados em rede que desbloqueiam automaticamente unidades de sistema operacional protegidos por BitLocker quando um computador membro de um domínio é reiniciado.

RECURSO	DESCRIÇÃO
BranchCache	Fornece os serviços necessários para as funcionalidades de cliente e servidor BranchCache. Inclui HTTP Protocol, Hosted Cache (Cache Hospedado) e serviços relacionados.
Client for NFS	Fornece funcionalidades para o acesso de arquivos em servidores NFS baseados em UNIX.
Data Center Bridging	Dá suporte ao conjunto de padrões IEEE para a melhoria de LANs e a garantia de alocação de largura de banda.
Enhanced Storage	Dá suporte aos Enhanced Storage Devices (Dispositivos de Armazenamento Avançado).
Failover Clustering	Fornece a funcionalidade de cluster, permitindo que múltiplos servidores trabalhem juntos para aumentar a disponibilidade de serviços e aplicativos. Muitos tipos de serviços podem ser instalados em um cluster, incluindo serviços de arquivo e impressão. Os servidores de mensagens e bases de dados são candidatos ideais para um cluster.
Group Policy Management	Instala o Group Policy Management Console (GPMC, Console de Gerenciamento de Group Policy), que possibilita a administração centralizada de Group Policy.
Ink and Handwriting Services	Oferece suporte ao reconhecimento de manuscrito e uso de caneta ou caneta stylus.
IP Address Management Server	Dá suporte ao gerenciamento central do espaço de endereços IP de uma empresa e servidores de infraestrutura relacionados.
Internet Printing Client	Confere funcionalidades que permitem aos clientes utilizarem HTTP para se conectar a impressoras em servidores de impressão via Web.
Internet Storage Naming Server (iSNS) Server Service	Fornece funções de gerenciamento e servidor para dispositivos Internet SCSI (iSCSI), permitindo que o servidor processe solicitações de registro, solicitações de cancelamento de registro e consultas de dispositivos iSNS.
LPR Port Monitor	Instala o Monitor de Porta LPR, habilitando a impressão para dispositivos anexados aos computadores baseados em UNIX.
Media Foundation	Fornece funcionalidades essenciais para o Windows Media Foundation.
Message Queuing	Oferece funções de gerenciamento e de servidor para o enfileiramento de mensagens distribuído. Também está disponível um conjunto de sub-recursos relacionados.
Multipath I/O (MPIO)	Confere a funcionalidade necessária ao uso de vários caminhos de dados para um dispositivo de armazenamento.
.NET Framework 4.5	Fornece APIs para o desenvolvimento de aplicativos. Os sub-recursos adicionais incluem .NET Framework 4.5, ASP .NET 4.5 e Windows Communication Foundation (WCF) Activation Components (Componentes de Ativação do WCF).

TABELA 2-2 Principais recursos do Windows Server 2012 (*continuação*)

RECURSO	DESCRIÇÃO
Network Load Balancing (NLB)	O NLB dá suporte a failover e balanceamento de carga para aplicativos e serviços baseados em IP, distribuindo as solicitações de aplicativos recebidas entre um grupo de servidores participantes. Servidores Web são candidatos ideais para o balanceamento de carga.
Peer Name Resolution Protocol (PNRP)	Fornece a funcionalidade Link-Local Multicast Name Resolution (LLMNR, Resolução de Nomes Multicast link-local) que permite serviços de resolução de nomes ponto a ponto. Ao instalar o recurso PNRP (Protocolo de Resolução de Nomes de Mesmo Nível), os aplicativos sendo executados no servidor podem usar o LLMNR para registrar e resolver nomes.
Quality Windows Audio Video Experience	Uma plataforma de rede para aplicativos de streaming de áudio e de vídeo (AV) em redes domésticas baseadas em IP.
RAS Connection Manager Administration Kit	Fornece a estrutura para a criação de perfis para a conexão a servidores e redes remotos.
Remote Assistance	Permite que um usuário remoto conecte-se ao servidor para fornecer ou receber Assistência Remota.
Remote Differential Compression (RDC)	Oferece suporte para compactação diferencial, determinando quais partes de um arquivo foram modificadas e replicando apenas as alterações.
Remote Server Administration Tools (RSAT)	Instala ferramentas de gerenciamento de funções e recursos que podem ser utilizadas para a administração remota de outros sistemas do Windows Server. São oferecidas opções para ferramentas individuais, podendo-se também instalar ferramentas por categoria e subcategoria.
Remote Procedure Call (RPC) over HTTP Proxy	Instala um proxy para a retransmissão de mensagens RPC de aplicativos clientes para o servidor por HTTP. O RPC sobre HTTP é uma alternativa para o acesso de clientes ao servidor por uma conexão VPN.
Simple TCP/IP Services	Instala serviços TCP/IP adicionais, incluindo Character Generator (CHARGEN, Gerador de Caracteres), Daytime, Discard, Echo e Quote of the Day (QUOTE, Frase do Dia).
Simple Mail Transfer Protocol (SMTP) Server	O SMTP é um protocolo de rede para o controle de transferência e roteamento de mensagens de email. Ao instalar esse recurso, o servidor pode agir como um servidor SMTP básico. Para uma solução mais completa, é necessária a instalação de um servidor de mensagens como o Microsoft Exchange Server.
Simple Network Management Protocol (SNMP) Services	O SNMP é um protocolo usado para simplificar o gerenciamento de redes TCP/IP. Se a sua rede possuir dispositivos compatíveis com o SNMP, ele pode ser utilizado para o gerenciamento centralizado da rede. O SNMP também pode ser usado no monitoramento de rede via software de gerenciamento de rede.

RECURSO	DESCRIÇÃO
Subsystem for UNIXBased Applications (SUA)	Oferece a funcionalidade para rodar programas e aplicativos baseados em UNIX. Pode-se fazer o download de utilitários de gerenciamento adicionais no site da Microsoft. (Preterido)
Telnet Client	Possibilita que um computador se conecte a um servidor Telnet remoto e execute aplicativos naquele servidor.
Telnet Server	Hospeda as sessões remotas de clientes Telnet. Quando o Telnet Server está sendo executado em um computador, os usuários podem se conectar ao servidor com um cliente Telnet a partir de um computador remoto.
User Interfaces And Infrastructure	Permite que você controle a experiência do usuário e as opções de infraestrutura com o Graphical Management Tools And Infrastructure (Ferramentas de Gerenciamento Gráfico e Infra-estrutura), Desktop Experience (Experiência Desktop) ou Server Graphical Shell.
Windows Biometric Framework (WBF)	Fornece as funcionalidades necessárias para o uso de dispositivos de impressão digital.
Windows Internal Database	Permite que o servidor utilize bancos de dados relacionais com funções e recursos do Windows que exijam um banco de dados interno, como: AD RMS, UDDI Services, WSUS, Windows SharePoint Services e Windows System Resource Manager (Gerenciador de Recursos de Sistema do Windows).
Windows PowerShell	Permite que você gerencie os recursos do Windows PowerShell do servidor. O Windows PowerShell 3.0 e o PowerShell ISE estão instalados por padrão.
Windows PowerShell Web Access	Possibilita que o servidor atue como um gateway de acesso via web para gerenciar remotamente os servidores com um navegador da Web.
Windows Process Activation Service	Oferece suporte para aplicativos distribuídos baseados na Web que utilizem protocolos HTTP ou não HTTP.
Windows Standards Based Storage Management	Oferece suporte para o gerenciamento de armazenamento baseado em padrões e inclui interfaces de gerenciamento e extensões para o WMI e o Windows PowerShell.
Windows Server Backup	Permite que você faça backup e restaure o sistema operacional, o estado do sistema e qualquer dado armazenado em um servidor.
Windows System Resource Manager (WSRM)	Permite que você gerencie o uso dos recursos por processador. (Preterido)
Windows TIFF IFilter	Concentra-se em documentos baseados em texto, ou seja: a busca é mais bem-sucedida para documentos que contenham texto claramente identificável (texto na cor preta sobre um plano de fundo branco, por exemplo).

Continua

TABELA 2-2 Principais recursos do Windows Server 2012 (*continuação*)

RECURSO	DESCRIÇÃO
WinRM IIS Extension	Oferece um modelo de hospedagem baseado em Serviços de Informações da Internet (IIS). A Extensão IIS do WinRM pode ser habilitada no nível do site da Web ou de um diretório virtual.
WINS Server	É um serviço de resolução de nomes que resolve nomes de computadores para endereços IP. A instalação desse recurso permite que o computador atue como um servidor WINS.
Wireless LAN Service	Possibilita que o servidor utilize conexões e perfis de redes sem fio.
WoW64 Support	Dá suporte ao WoW64, necessário em uma instalação de servidor completo. A remoção desse recurso converte uma instalação de servidor completo em uma instalação Server Core.
XPS Viewer	É um programa que pode ser usado para visualizar, pesquisar, aplicar permissões de documento e realizar a assinatura digital de documento XPS.

OBSERVAÇÃO A Desktop Experience agora é um sub-recurso do recurso de alto nível chamado User Interfaces and Infrastructure. A Desktop Experience oferece funcionalidades de desktop do Windows no servidor. Os recursos do Windows que são adicionados incluem o Windows Media Player, temas da área de trabalho, Vídeo para Windows (suporte para AVI), Windows Defender, Disk Cleanup (limpeza de disco), Sync Center (central de sincronização), Sound Recorder (gravador de som), Characters Map (mapa de caracteres) e Snipping Tool (ferramenta de captura). Embora esses recursos permitam que um servidor seja utilizado como um computador desktop, eles podem reduzir o desempenho geral do servidor.

Como administrador, podem solicitar que você instale ou desinstale dynamic-link libraries (DLLs, bibliotecas de vínculo dinâmico), especialmente se você trabalha com equipes de desenvolvimento de TI. Para trabalhar com DLLs, você usará o utilitário Regsvr32, que é executado em linha de comando.

Para instalar ou registrar uma DLL, abra uma janela do prompt de comando e digite **regsvr32 name.dll**. Por exemplo:

```
regsvr32 mylibs.dll
```

Se precisar, você pode desinstalar ou cancelar o registro de uma DLL. Para isso, digite **regsvr32 /u name.dll**. Por exemplo:

```
regsvr32 /u mylibs.dll
```

A Windows File Protection (Proteção de Arquivo do Windows) impede a substituição de arquivos de sistema protegidos. Só é possível substituir DLLs instaladas pelo sistema operacional Windows Server como parte de um hotfix, atualizações de pacotes de serviços, Windows update ou Windows upgrade. A Windows File Protection é uma parte importante da arquitetura de segurança do Windows Server.

Instalações de servidor completo, interface mínima e Server Core

O Windows Server 2012 suporta instalações de servidor completo, interface mínima e Server Core. As instalações de servidor completo, também conhecidas como instalações de servidor com GUI, possuem Graphical Management Tools And Infrastructure e recursos do Server Graphical Shell (que fazem parte do recurso User And Infrastructure) e o framework WoW64 Support instalado. Instalações de interface mínima, também conhecidas como instalações com interface de servidor mínima, são instalações completas onde o Server Graphical Shell foi removido. Instalações Server Core possuem uma interface de usuário limitada e não incluem os recursos de User Interfaces And Infrastructure, nem mesmo o framework WoW64 Support.

Como discutiremos em “Alteração do Tipo de Instalação” mais adiante neste capítulo, o tipo de instalação pode ser alterado a qualquer momento. Com uma instalação de servidor completo, você possui uma versão de trabalho completa do Windows Server 2012 que pode ser implantada com qualquer combinação permitida de funções, serviços de função e recursos. Com uma instalação de interface mínima também é possível implantar qualquer combinação permitida de funções, serviços de função e recursos. Por outro lado, com uma instalação Server Core você tem uma instalação mínima do Windows Server 2012 que suporta um conjunto limitado de funções e combinações de função. As funções suportadas incluem AD CS, AD DS, AD LDS, DHCP Server, DNS Server, File Services, Hyper-V, Media Services (Serviços de Mídia), Print And Document Services (Serviços de Impressão e Documentos), Routing And Remote Access Server (Servidor de Roteamento e Acesso Remoto), Streaming Media Services (Serviços de Mídia de Streaming), Web Server (IIS) e Windows Server Update Services. Na sua implementação atual, uma instalação Server Core não é uma plataforma para executar aplicativos de servidor.

Embora os três tipos de instalação utilizem os mesmos termos de licença e possam ser gerenciados remotamente com qualquer técnica de administração remota permitida que esteja disponível, as instalações completa, interface mínima e Server Core são completamente diferentes em termos de console de administração local. Com uma instalação completa, você recebe uma interface de usuário que inclui um ambiente de área de trabalho completo para o console de gerenciamento local do servidor. Com uma interface mínima, você tem apenas Microsoft Management Consoles, Server Manager e um subconjunto do Control Panel disponível para tarefas de gerenciamento. Não constam nem na instalação de interface mínima nem na instalação Server Core: File Explorer, barra de tarefas, área de notificação, Internet Explorer, centro de ajuda integrado, temas, aplicativos estilo Metro e Windows Media Player.

Navegação no Server Core

Com uma instalação Server Core, você recebe uma interface de usuário que inclui um ambiente limitado de área de trabalho para o console de gerenciamento local do servidor. Essa interface mínima inclui os seguintes itens:

- Tela de Logon do Windows para entrar e sair
- Notepad (Notepad.exe) para a edição de arquivos
- Registry Editor (Regedit.exe) para o gerenciamento do registro

- Task Manager (Taskmgr.exe) para o gerenciamento de tarefas e início de novas tarefas
- Prompt de comando (Cmd.exe) para a administração usando linhas de comando
- Prompt do PowerShell para a administração usando o Windows PowerShell
- Ferramenta File Signature Verification (Sigverif.exe) para a verificação de assinaturas digitais de arquivos do sistema
- System Information (Msinfo32.exe) para a obtenção de informações do sistema
- Windows Installer (Msiexec.exe) para o gerenciamento do Windows Installer
- Painel de controle *Date and Time* (Timedate.cpl) para a visualização ou configuração de data, hora e fuso horário
- Painel de controle *Region and Language* (Intl.cpl) para a visualização ou configuração de opções regionais ou de idioma, incluindo formatos e o layout do teclado
- Utilitário Server Configuration (Sconfig) para o fornecimento de um menu de sistema baseado em texto para o gerenciamento das configurações de um servidor

Ao iniciar um servidor com instalação Server Core você pode usar a tela de Logon do Windows para efetuar o logon, da mesma forma que faria em uma instalação completa. Em um domínio, as restrições padrão se aplicam para fazer logon nos servidores. Qualquer pessoa com direitos de usuário apropriados e permissões de logon pode fazer logon no servidor. Em servidores que não estiverem agindo como controladores de domínio e em servidores em ambientes de grupos de trabalho, pode-se utilizar o comando NET USER para adicionar usuários e o comando NET LOCALGROUP para adicionar usuários aos grupos locais a fim de que possam efetuar o logon localmente.

Após efetuar o logon em uma instalação Server Core, você terá um ambiente limitado de área de trabalho com um prompt de comando de administrador. Esse prompt de comando pode ser utilizado para a administração do servidor. Se você fechar o prompt de comando accidentalmente, pode abrir um novo prompt de comando. Siga as etapas:

1. Pressione Ctrl+Shift+Esc para exibir o Task Manager (Gerenciador de Tarefas).
2. No menu File, toque ou clique em Run New Task.
3. Na caixa de diálogo Create New Task, digite **cmd** na caixa de texto Open e depois toque ou clique em OK.

Essa técnica também pode ser usada para abrir janelas de prompt de comando adicionais. Embora você possa trabalhar com o Notepad e com o Regedit ao digitar **notepad.exe** ou **regedit.exe** em vez de **cmd**, também é possível iniciar o Notepad e o Regedit diretamente de um prompt de comando. Basta digitar **notepad.exe** ou **regedit.exe**, de acordo com o que for desejado.

O utilitário Server Configuration (Sconfig) fornece um menu do sistema baseado em texto que facilita as seguintes ações:

- Configurar associação a um grupo de trabalho ou domínio
- Alterar o nome de um servidor
- Adicionar uma conta de Administrador local
- Configurar recursos de gerenciamento remoto

- Modificar as configurações do Windows Update
- Fazer o download e instalar atualizações do Windows
- Habilitar ou desabilitar Remote Desktop
- Ajustar configurações de rede para TCP/IP
- Ajustar a data e a hora
- Fazer logoff, reiniciar ou desligar

Quando estiver logado, você pode pressionar Ctrl+Alt+Delete para exibir a tela de Logon do Windows a qualquer momento. Nas instalações Server Core e completa a tela de Logon do Windows apresenta as mesmas opções, permitindo que você bloquee o computador, altere usuários, faça logoff, altere a senha ou inicie o Task Manager. No prompt de comando você tem todos os comandos padrão e utilitários de linha de comando disponíveis para o gerenciamento do servidor. Porém, os comandos, utilitários e programas só são executados se todas as suas dependências estiverem disponíveis na instalação Server Core.

Ainda que uma instalação Server Core suporte apenas um conjunto limitado de funções e serviços de função, pode-se instalar a maioria dos recursos. O Windows Server 2012 também suporta .NET Framework, Windows PowerShell 3.0 e Windows Remote Management (WinRM) 2.0. Esse suporte permite que você realize administração local e remota através do PowerShell. Os Serviços de Remote Desktop também servem para gerenciar remotamente uma instalação Server Core. A Tabela 2-3 resume algumas das tarefas mais comuns que podem ser realizadas quando se está logado localmente.

TABELA 2-3 Uilitários e comandos úteis no gerenciamento de instalações Server Core

COMANDO	TAREFA
Cscript Scregedit.wsf	Configurar o sistema operacional. Utilize o parâmetro /cli para listar as áreas de configuração disponíveis.
Diskraid.exe	Configurar o software de RAID.
ipconfig /all	Listar informações sobre a configuração do endereço IP do computador.
Netdom RenameComputer	Configurar o nome do servidor.
Netdom Join	Ingressar o servidor em um domínio.
Netsh	Fornece diversos contextos para gerenciar configurações de componentes de rede. Digite netsh interface ipv4 para alterar configurações IPv4. Digite netsh interface ipv6 para alterar configurações IPv6.
Ocsetup.exe	Instalar ou remover funções, serviços de função e recursos.
Pnputil.exe	Adicionar ou atualizar drivers para dispositivos de hardware.
Sc query type=driver	Listar drivers de dispositivos carregados.

Continua

TABELA 2-3 Uilitários e comandos úteis no gerenciamento de instalações Server Core (*continuação*)

COMANDO	TAREFA
Serverweroptin.exe	Configurar o Windows Error Reporting (Relatório de Erros do Windows).
Slmgr –ato	Ferramenta Windows Software Licensing Management (Gerenciador de Licença de Software do Windows) utilizada para a ativação do sistema operacional. Executar <i>Cscript slmgr.vbs –ato</i> .
Slmgr –ipk	Instalar ou substituir a chave do produto (Product Key). Executar <i>Cscript slmgr.vbs –ipk</i> .
SystemInfo	Listar os detalhes de configuração do sistema.
Wecutil.exe	Criar e gerenciar assinaturas em eventos encaminhados.
Wevtutil.exe	Visualizar e pesquisar em logs de eventos.
Winrm quickconfig	Configurar o servidor para aceitar solicitações do WS-Management de outros computadores. Executar <i>Cscript winrm.vbs quickconfig</i> . Digite sem o parâmetro <i>quickconfig</i> para exibir outras opções.
Wmic datafile where name="FullPath" get version	Listar a versão de um arquivo.
Wmic nicconfig index=9 call enabledhcp	Configurar o computador para usar endereços IP dinâmicos e não estáticos.
Wmic nicconfig index=9 call enablestatic("IPAddress"), ("SubnetMask")	Configurar o endereço IP estático e a máscara de sub-rede de um computador.
Wmic nicconfig index=9 call setgateways("GatewayIPAddress")	Configurar ou alterar o gateway padrão.
Wmic product get name /value	Listar aplicativos instalados do Microsoft Installer (MSI) por nome.
Wmic product where name="Name" call uninstall	Desinstalar um aplicativo MSI.
Wmic qfe list	Listar atualizações e hotfixes instalados.
Wusa.exe PatchName.msu /quiet	Aplicar uma atualização ou hotfix ao sistema operacional.

Instalação do Windows Server 2012

O Windows Server 2012 pode ser instalado em um hardware novo ou como uma atualização. Ao instalar o Windows Server 2012 em um computador que já tenha um sistema operacional, você pode realizar uma instalação limpa ou uma atualização. Com uma instalação limpa, o programa de instalação do Windows Server 2012 substitui o sistema operacional de origem e todas as configurações de usuário ou de

aplicativos são perdidas. Com uma atualização, o programa de instalação realiza uma instalação limpa do sistema operacional e depois migra para ele as configurações de usuário, documentos e aplicativos da versão anterior do Windows.

O Windows Server 2012 suporta apenas arquiteturas de 64 bits. Portanto, o sistema operacional só pode ser instalado em computadores com processadores de 64 bits. Antes de instalar o Windows Server 2012, certifique-se de que o seu computador atende aos requisitos mínimos da edição que você pretende implantar. A Microsoft oferece requisitos mínimos e requisitos recomendados. Se o seu computador não atender aos requisitos mínimos, você não poderá instalar o Windows Server 2012. Se o seu computador não atender aos requisitos recomendados, você experimentará problemas de desempenho.

O Windows Server 2012 requer pelo menos 10 GB de espaço em disco para a instalação do sistema operacional básico. A Microsoft recomenda que um computador com o Windows Server 2012 tenha 32 GB de espaço em disco disponível ou mais. Um espaço em disco adicional é necessário para arquivos de despejo e paginação, além de recursos, funções e serviços de função que você instalar. Para um desempenho ideal, deve-se sempre manter ao menos 10% de espaço livre nos discos de um servidor.

Ao instalar o Windows Server 2012, o programa de instalação disponibiliza automaticamente as opções de recuperação no seu servidor como uma opção avançada de inicialização. Além de uma linha de comando para a solução de problemas e de opções para alterar o comportamento de inicialização, você pode utilizar a System Image Recovery (Recuperação de Imagem do Sistema) para realizar uma recuperação completa do computador através de uma imagem do sistema criada anteriormente. Se as outras técnicas de solução de problemas não restaurarem o computador e você tiver uma imagem do sistema para recuperação, você pode utilizar esse recurso para restaurar o computador a partir da imagem de backup.

Instalação limpa

Antes de iniciar a instalação, você precisa decidir se quer gerenciar as unidades e partições do computador durante esse processo. Se desejar utilizar as opções avançadas de instalação de unidade oferecidas pelo Setup para criar e formatar partições, você precisa inicializar o computador usando a mídia de distribuição. Se você não inicializar usando a mídia de distribuição, as opções não estarão disponíveis e você não conseguirá gerenciar partições de disco em um prompt de comando através do utilitário DiskPart.

Para realizar uma instalação limpa do Windows Server 2012, siga estas etapas:

1. Inicie o programa de Instalação de uma das seguintes maneiras:

- Para uma nova instalação, ligue o computador com a mídia de distribuição do Windows Server 2012 na unidade de disco do computador e, quando solicitado, pressione qualquer tecla para iniciar o Setup a partir da sua mídia. Se não for solicitado que você inicialize a partir da unidade de disco, pode ser preciso selecionar opções avançadas de inicialização e depois inicializar a partir da mídia e não do disco rígido. Senão, pode ser preciso alterar as configurações de firmware do computador para permitir a inicialização a partir da mídia.
- Para uma instalação limpa sobre uma instalação existente, pode-se inicializar a partir da mídia de distribuição ou iniciar o computador e fazer logon utilizando uma conta com privilégios de administrador. O Setup deve iniciar automaticamente quando você inserir a mídia de distribuição do Windows Server 2012 na

unidade de disco do computador. Caso isso não ocorra, utilize o File Explorer para acessar a mídia de distribuição e depois clique duas vezes ou dê um toque duplo em Setup.exe.

2. Se você iniciou o computador usando a mídia de distribuição, será solicitado que você selecione o idioma, formatos de hora e moeda e layout do teclado. Apenas um layout de teclado está disponível durante a instalação. Se o idioma do teclado e o idioma da edição do Windows Server 2012 que você está instalando forem diferentes, podem aparecer caracteres imprevistos ao digitar. Para evitar que isso aconteça, certifique-se de fazer a seleção do idioma de teclado correto. Quando estiver pronto para prosseguir a instalação, toque ou clique em Next.
3. Selecione Install Now para iniciar a instalação. Depois que o Setup copiar os arquivos temporários para o computador, selecione se deseja receber atualizações para o procedimento de instalação durante o processo. Se você iniciou o Setup depois de fazer o logon em uma instalação existente do Windows, selecione Go Online To Install Updates Now ou No, Thanks.
4. Com as edições de licenciamentos por volume e empresa do Windows Server 2012 pode não ser preciso fornecer uma chave do produto durante a instalação. Porém, com edições do tipo comercial é preciso digitar a chave do produto quando solicitado. Toque ou clique em Next para continuar. A caixa de seleção Activate Windows When I'm Online está selecionada por padrão para garantir que você seja solicitado a ativar o sistema operacional na próxima vez que se conectar à Internet.

OBSERVAÇÃO Você precisa ativar o Windows Server 2012 após a instalação. Se você não ativar o Windows Server 2012 no período determinado, verá um erro dizendo: "Your activation period has expired" ou "Non-genuine version of Windows Server 2012 installed". O Windows Server 2012 será executado com funcionalidades reduzidas. É preciso ativar e validar o Windows Server 2012 para recuperar a funcionalidade completa.

5. Na página Select The Operating System You Want To Install são oferecidas opções para instalações completas e Server Core. Selecione a opção apropriada e toque ou clique em Next.
6. Os termos de licença do Windows Server 2012 sofreram alterações em relação às versões anteriores do Windows. Após examinar os termos de licença, toque ou clique em I Accept The License Terms e depois em Next.
7. Na página Which Type Of Installation Do You Want, selecione o tipo de instalação que o Setup deve realizar. Como você está realizando uma instalação limpa para substituir uma instalação existente ou configurar um novo computador, selecione Custom Install Windows Only (Advanced) como o tipo de instalação. Se você iniciou o Setup a partir do prompt de inicialização, e não do próprio Windows, a opção Upgrade está desabilitada. Para fazer uma atualização em vez de uma instalação limpa, é preciso que você reinicie o computador e faça a inicialização do sistema operacional instalado atualmente. Após fazer logon você precisará iniciar novamente a instalação.
8. Na página do Windows Where Do You Want To Install, selecione o disco ou o disco e a partição em você quer instalar o sistema operacional. Existem duas versões da página do Windows Where Do You Want To Install, portanto lembre-se do seguinte::
 - Quando um computador tem apenas um disco rígido com uma única partição contendo todo o disco ou uma única área de espaço não alocado, a partição

de disco inteira é selecionada por padrão. Basta clicar ou tocar em Next para selecioná-la como local de instalação e continuar. Com um disco que está completamente desalocado, pode ser desejável criar a partição necessária antes de instalar o sistema operacional, como será discutido em “Criação, formatação, remoção e extensão de partições de disco durante a instalação”, mais adiante neste capítulo.

- Quando um computador tem vários discos ou um disco com várias partições, é preciso selecionar uma partição existente para ser usada na instalação do sistema operacional, ou então criar uma nova partição. Pode-se criar e gerenciar partições, como será discutido em “Criação, formatação, remoção e extensão de partições de disco durante a instalação”, mais adiante neste capítulo.
 - Se um disco não foi inicializado para uso ou se o firmware do computador não suporta a inicialização do sistema operacional a partir do disco selecionado, é preciso inicializá-lo, criando partições no disco. Não é possível selecionar ou formatar uma partição de disco rígido FAT ou FAT32, ou que tenha outras configurações incompatíveis. Para contornar esse problema, você pode converter a partição para NTFS. Ao trabalhar com esta página, pode-se acessar um prompt de comando para realizar qualquer tarefa de pré-instalação necessária. Consulte “Criação, formatação, remoção e extensão de partições de disco durante a instalação”, mais adiante neste capítulo.
9. Se a partição que você selecionou contém uma instalação anterior do Windows, o Setup apresenta um aviso informando quais configurações de aplicativos e usuários existentes serão movidos para uma pasta chamada Windows.old e que para usar essas configurações você deve copiá-las para a nova instalação. Toque ou clique em OK.
10. Toque ou clique em Next. O Setup inicia a instalação do sistema operacional. Durante esse procedimento, o Setup copia a imagem completa do disco do Windows Server 2012 para o local selecionado e a expande. Depois, instala recursos com base nas configurações do computador e no hardware detectado. Esse processo exige vários reinícios automáticos. Quando o Setup for finalizada, o sistema operacional será carregado e você poderá realizar tarefas de configuração inicial, como configurar a senha do administrador e o nome do servidor.

MUNDO REAL Os servidores executando instalações básicas do Windows Server estão configurados por padrão para usar DHCP. Desde que o servidor tenha um cartão de rede e um cabo de rede conectado, uma instalação Server Core é capaz de conectar os servidores DHCP da sua organização e obter as configurações de rede corretas. O servidor pode ser configurado usando-se o Sconfig, que oferece opções de menu para a configuração de associações de domínio/grupo de trabalho, nome do computador, gerenciamento remoto, Windows Update, Remote Desktop, configurações de rede, data e hora, logoff, reinício e encerramento.

Também é possível configurar o servidor através de comandos individuais. Se quiser utilizar um endereço IP estático, use o Netsh para aplicar as configurações desejadas. Uma vez que a rede estiver configurada corretamente, use Slmgr -ipk para estabelecer a chave do produto e Slmgr -ato para ativar o Windows. Digite timedate.cpl para configurar a data e a hora do servidor. Se quiser habilitar o gerenciamento remoto através do protocolo WS-Management, digite winrm quickconfig.

Em seguida, é provável que queira definir o nome do computador. Para visualizar o nome padrão do computador, digite echo %computername%. Para renomear o computador, utilize o Netdom RenameComputer com a seguinte sintaxe: netdom renamecomputer current-

name /newname:newname, onde *currentname* é o nome atual do computador e *newname* é o nome que você deseja atribuir. Exemplo: **netdom renamecomputer win-k4m6bnovlhe / newname:server18**. Será necessário reiniciar o computador. Isso pode ser feito digitando **shutdown /r**.

Quando o computador reiniciar, você pode ingressá-lo em um domínio usando o Netdom Join. Para a sintaxe, digite **netdom join /?**.

Instalação de atualização

Embora o Windows Server 2012 ofereça uma opção de atualização durante a instalação, uma atualização não é o que você pensa. Com uma atualização, o Setup realiza uma instalação limpa do sistema operacional e depois migra as configurações do usuário, documentos e aplicativos da versão anterior do Windows para a nova.

Durante a parte de migração da atualização, o Setup move pastas e arquivos da instalação anterior para uma pasta nomeada Windows.old. Assim, a instalação anterior não será mais executada.

OBSERVAÇÃO Não é possível realizar uma atualização do Windows Server 2012 em um computador com um sistema operacional de 32 bits, mesmo que o computador tenha processadores de 64 bits. É preciso migrar os serviços que estão sendo fornecidos pelo computador para outros servidores e então realizar uma instalação limpa. As Ferramentas Windows Server Migration podem ser úteis para migrar o seu servidor. Essas ferramentas estão disponíveis em computadores com o Windows Server 2012.

Para realizar uma instalação de atualização do Windows Server 2012, siga as etapas:

1. Inicie o computador e faça o logon utilizando uma conta com privilégios de administrador. Após inserir a mídia de distribuição do Windows Server 2012 na unidade de DVD-ROM do computador, o Setup deve iniciar automaticamente. Caso isso não ocorra, utilize o File Explorer para acessar a mídia de distribuição e depois clique duas vezes ou dê um toque duplo em Setup.exe.
2. Como você está iniciando o Setup a partir do sistema operacional atual, não será solicitado que você selecione o idioma, formatos de hora e moeda ou layout do teclado. Apenas o layout do teclado do sistema operacional atual estará disponível durante a instalação. Se o idioma do teclado e o idioma da edição do Windows Server 2012 que você está instalando forem diferentes, podem aparecer caracteres imprevistos ao digitar.
3. Selecione Install Now para iniciar a instalação. Após o Setup ter copiado os arquivos temporários para o computador, selecione se deseja buscar atualizações durante a instalação. Selecione Go Online To Install Updates Now ou No, Thanks.
4. Com as edições de licenciamentos por volume e corporativa do Windows Server 2012 pode não ser preciso fornecer uma chave do produto durante a instalação. Porém, com edições do tipo comercial, é preciso digitar a chave do produto quando solicitado. Toque ou clique em Next para continuar. A caixa de seleção Activate Windows When I'm Online está selecionada por padrão para garantir que você seja solicitado a ativar o sistema operacional na próxima vez que se conectar à Internet.
5. Na página Select The Operating System You Want To Install são oferecidas opções para instalações completas e Server Core. Selecione a opção apropriada e toque ou clique em Next.

6. Os termos de licença do Windows Server 2012 sofreram alterações em relação às versões anteriores do Windows. Após examinar os termos de licença, toque ou clique em I Accept The License Terms e depois em Next.
7. Na página Which Type Of Installation Do You Want, selecione o tipo de instalação que deseja que o Setup realize. Já que você está realizando uma instalação limpa sobre uma instalação existente, selecione Upgrade. Se você iniciou o Setup a partir do prompt de inicialização, e não do próprio Windows, a opção Upgrade está desabilitada. Para fazer uma atualização em vez de uma instalação limpa, é preciso que você reinicie o computador e faça a inicialização do sistema operacional instalado atualmente. Após fazer o logon, pode-se iniciar a instalação.
8. O Setup iniciará o processo. Como você está atualizando o sistema operacional, não é necessário escolher o local de instalação. Durante esse processo, o Setup copia a imagem completa do disco do Windows Server 2012 para o disco do sistema. Depois, instala recursos com base nas configurações do computador e no hardware detectado. Quando o Setup for finalizado, o sistema operacional será carregado e você poderá realizar tarefas de configuração inicial, como configurar a senha do administrador e o nome do servidor.

Realização de tarefas administrativas adicionais durante a instalação

Por vezes, pode ser que você esqueça de realizar alguma tarefa de pré-instalação antes de iniciar a instalação. Em vez de reiniciar o sistema operacional, pode-se acessar um prompt de comando a partir do Setup ou utilizar opções de unidade avançadas para realizar as tarefas administrativas necessárias.

Uso da linha de comando durante a instalação

Ao acessar um prompt de comando a partir do Setup, acessa-se o ambiente MINWINPC (mini Windows PC) utilizado para instalar o sistema operacional. Durante a instalação, na página Where Do You Want To Install Windows, pode-se acessar um prompt de comando pressionando Shift+F10. Como mostra a Tabela 2-4, o ambiente *Mini Windows PC* dá acesso a várias ferramentas de linha de comando que estão disponíveis na instalação padrão do Windows Server 2012.

TABELA 2-4 Utilitários de linha de comando no ambiente Mini Windows PC

COMANDO	DESCRIÇÃO
ARP	Exibir e modificar tabelas de conversão de IP para endereços físicos utilizadas pelo Address Resolution Protocol (ARP, Protocolo de Resolução de Endereços).
ASSOC	Exibir e modificar associações das extensões de arquivo.
ATTRIB	Exibir e alterar atributos de arquivos.
CALL	Chamar um script ou rótulo de script como procedimento.
CD/CHDIR	Exibir o nome ou alterar o diretório atual.

Continua

TABELA 2-4 Utilitários de linha de comando no ambiente Mini Windows PC
(continuação)

COMANDO	DESCRIÇÃO
CHKDSK	Verificar um disco e exibir erros em relatório.
CHKNTFS	Exibir o status de volumes. Configurar ou excluir volumes no momento da verificação automática do sistema quando o computador é iniciado.
CHOICE	Criar uma lista da qual os usuários podem selecionar uma entre diversas opções em um script em lote (batch).
CLS	Limpar a janela do console.
CMD	Iniciar uma nova instância do prompt de comando do Windows.
COLOR	Configurar as cores da janela do prompt de comando.
CONVERT	Converter volumes FAT em NTFS.
COPY	Copiar ou combinar arquivos.
DATE	Exibir ou configurar a data do sistema.
DEL	Excluir um ou mais arquivos.
DIR	Exibir uma lista de arquivos e subdiretórios dentro de um diretório.
DISKPART	Invocar um interpretador de comandos em modo de texto para gerenciar discos, partições e volumes, utilizando um prompt de comando separado e os comandos que são internos ao DISKPART.
DISM	Gerenciar e fazer a manutenção de imagens do Windows.
DOSKEY	Editar linhas de comando, recuperar comandos do Windows e criar macros.
ECHO	Exibir mensagens ou ativar/desativar ecos de comando.
ENDLOCAL	Encerrar localização de alterações de ambiente em um arquivo em lote.
ERASE	Excluir um ou mais arquivos.
EXIT	Sair do interpretador de comandos.
EXPAND	Descompactar arquivos.
FIND	Localizar cadeias de texto em arquivos.
FOR	Executar um determinado comando para cada arquivo em um conjunto de arquivos.
FORMAT	Formatar um disquete ou disco rígido.
FTP	Transferir arquivos.
FTYPE	Exibir ou alterar tipos de arquivos utilizados em associações de extensões de arquivo.
GOTO	Direcionar o interpretador de comandos do Windows para uma linha rotulada em um script.

COMANDO	DESCRIÇÃO
HOSTNAME	Exibir o nome do computador.
IF	Realizar processamento condicional em arquivos em lote.
IPCONFIG	Exibir configurações TCP/IP.
LABEL	Criar, alterar ou excluir o rótulo de volume de um disco.
MD/MKDIR	Criar um diretório ou subdiretório.
MORE	Exibir saídas em uma tela de cada vez.
MOUNTVOL	Gerenciar um ponto de montagem de volume.
MOVE	Mover arquivos de um diretório para outro na mesma unidade.
NBTSTAT	Exibir o status do NetBIOS.
NET ACCOUNTS	Gerenciar conta do usuário e políticas de senha.
NET COMPUTER	Adicionar ou remover computadores de um domínio.
NET CONFIG SERVER	Exibir ou alterar a configuração de um serviço do servidor.
NET CONFIG WORKSTATION	Exibir ou alterar a configuração de um serviço em estação de trabalho.
NET CONTINUE	Continuar um serviço pausado.
NET FILE	Exibir ou gerenciar arquivos abertos em um servidor.
NET GROUP	Exibir ou gerenciar grupos globais.
NET LOCALGROUP	Exibir ou gerenciar contas de grupo locais.
NET NAME	Exibir ou alterar destinatários para mensagens do serviço mensageiro.
NET PAUSE	Suspender um serviço.
NET PRINT	Exibir ou gerenciar trabalhos de impressão e filas de impressão.
NET SEND	Enviar uma mensagem usando o serviço mensageiro.
NET SESSION	Listar ou desconectar sessões.
NET SHARE	Exibir ou gerenciar impressoras e pastas compartilhadas.
NET START	Listar ou iniciar serviços de rede.
NET STATISTICS	Exibir estatísticas de estação de trabalho ou servidor.
NET STOP	Interromper serviços.
NET TIME	Exibir ou sincronizar o horário da rede.

Continua

TABELA 2-4 Utilitários de linha de comando no ambiente Mini Windows PC
(continuação)

COMANDO	DESCRIÇÃO
NET USE	Exibir ou gerenciar conexões remotas.
NET USER	Exibir ou gerenciar contas de usuários locais.
NET VIEW	Exibir computadores ou recursos de rede.
NETSH	Invocar um prompt de comando separado que permita gerenciar as configurações de vários serviços de rede em computadores locais e remotos.
NETSTAT	Exibir o status de conexões de rede.
PATH	Exibir ou configurar caminhos para arquivos executáveis na janela de comando atual.
PATHPING	Traçar rotas e fornecer informações de perda de pacotes.
PAUSE	Suspender o processamento de um script e aguardar uma entrada do teclado.
PING	Determinar se uma conexão de rede pode ser estabelecida.
POPD	Mudar para o diretório armazenado pelo PUSHD.
PRINT	Imprimir um arquivo de texto.
PROMPT	Alterar o prompt de comando do Windows.
PUSHD	Armazena a pasta atual para uso pelo POPD e depois alterar para a pasta especificada.
RD/RMDIR	Remover um diretório.
RECOVER	Recuperar informações legíveis de um disco danificado ou defeituoso.
REG ADD	Adicionar uma nova subchave ou entrada para o registro.
REG COMPARE	Comparar subchaves ou entradas de registro.
REG COPY	Copiar uma entrada de registro para um determinado caminho de chave em um sistema local ou remoto.
REG DELETE	Escrever de volta no registro chaves e entradas salvas.
REG QUERY	Listar as entradas de uma chave e os nomes das subchaves (se houver).
REG RESTORE	Gravar subchaves salvas e entradas no registro.
REG SAVE	Salvar uma cópia de determinadas subchaves, entradas e valores em um arquivo.
REGSVR32	Registrar e cancelar o registro de DLLs.
REM	Adicionar comentários aos scripts.
REN	Renomear um arquivo.
ROUTE	Gerenciar tabelas de roteamento de rede.

COMANDO	DESCRIÇÃO
SET	Exibir ou alterar variáveis de ambiente Windows. Também utilizado para avaliar expressões numéricas na linha de comando.
SETLOCAL	Iniciar a localização de alterações de ambiente em um arquivo em lotes.
SFC	Examinar e verificar arquivos de sistema protegidos.
SHIFT	Deslocar a posição de parâmetros substituíveis nos scripts.
START	Iniciar uma nova janela de shell de comando para executar um determinado programa ou comando.
SUBST	Associar um caminho a uma letra da unidade.
TIME	Exibir ou definir o horário do sistema.
TITLE	Definir o título para a janela do prompt de comando.
TRACERT	Exibir o caminho entre computadores.
TYPE	Exibir o conteúdo de um arquivo de texto.
VER	Exibir a versão do Windows.
VERIFY	Dizer ao Windows se deve verificar se os arquivos estão copiados corretamente em um disco.
VOL	Exibir o rótulo de volume de um disco e o número de série.

Como forçar a remoção de uma partição de disco durante a instalação

Durante a Instalação, pode não ser possível selecionar o disco rígido desejado. Esse problema pode surgir se a partição do disco rígido contiver um valor inválido de deslocamento de bytes. Para solucionar essa questão, é preciso remover as partições no disco rígido (o que destrói todos os dados armazenados) e depois criar a partição necessária utilizando as opções avançadas no programa de Instalação. Durante a instalação, na página Where Do You Want To Install Windows, pode-se remover partições de disco rígido não reconhecidas. Para isso, siga as etapas:

1. Pressione Shift+F10 para abrir um prompt de comando.
2. No prompt de comando, digite **diskpart**. Isso inicia o utilitário DiskPart.
3. Para visualizar uma lista dos discos do computador, digite **list disk**.
4. Para selecionar um disco, digite **select disk DiskNumber**, onde *DiskNumber* é o número do disco em que você deseja trabalhar.
5. Para remover permanentemente as partições no disco selecionado, digite **clean**.
6. Quando o processo de limpeza estiver completo, digite **exit** para sair do utilitário DiskPart.
7. Digite **exit** para fechar o prompt de comando.
8. Na caixa de diálogo Install Windows, toque ou clique na seta voltar para retornar à janela anterior.

9. Na página Which Type Of Installation Do You Want, toque ou clique em Custom (Advanced) para iniciar uma instalação personalizada.
10. Na página Where Do You Want To Install Windows, toque ou clique no disco que você limpou anteriormente, selecionando-o como a partição de instalação. Conforme for necessário, toque ou clique no link Disk Options para exibir as opções de configuração de partição Delete, Format, New e Extend.
11. Toque ou clique em New. Na caixa Size, defina o tamanho da partição em mega-bytes. Toque ou clique em Apply para aplicar.

Como carregar drivers de dispositivos de disco durante a instalação

Durante a instalação, na página Where Do You Want To Install Windows, pode-se usar a opção Load Driver para carregar os drivers de dispositivo para uma unidade de disco rígido ou controlador de disco rígido. Normalmente essa opção é usada quando uma unidade de disco que você quer utilizar para a instalação do sistema operacional não pode ser selecionada porque o driver do dispositivo está indisponível.

Para carregar os drivers de dispositivo e disponibilizar o disco rígido, siga as etapas:

1. Durante a instalação, na página Where Do You Want To Install Windows, toque ou clique em Load Driver.
2. Quando for solicitado, insira a mídia de instalação na unidade de DVD ou flash USB e toque ou clique em OK. Em seguida, a Instalação pesquisa por drivers de dispositivos nas unidades de mídia removíveis do computador.
 - Se a Instalação localizar vários drivers de dispositivos, selecione o driver que deve ser instalado e depois toque ou clique em OK.
 - Se a Instalação não localizar o driver do dispositivo, toque ou clique em Browse para usar a caixa de diálogo Browse For Folder para selecionar o driver de dispositivo a ser carregado. Toque ou clique em OK e depois em Next.

Pode-se clicar ou tocar no botão Rescan para que a Instalação examine novamente as unidades de mídia removíveis. Se não for possível instalar um driver de dispositivo, toque ou clique na seta voltar no canto superior esquerdo da caixa de diálogo Install Windows para retornar à página anterior.

Criação, formatação, remoção e extensão de partições de disco durante a instalação

Quando estiver realizando uma instalação limpa com o computador iniciado a partir da mídia de distribuição, a página Where Do You Want To Install Windows apresentará opções adicionais. Toque ou clique em Drive Options (Advanced) para exibir essas opções. As opções são utilizadas para:

- **New** Criar uma partição. Você deve então formatar a partição.
- **Format** Formatar uma nova partição para ser usada na instalação do sistema operacional.
- **Delete** Excluir uma partição que você não quer mais.
- **Extend** Estender uma partição para aumentar o seu tamanho.

A seção a seguir aborda como utilizar cada uma das opções. Mesmo se essas opções não estiverem disponíveis, é possível trabalhar com os discos do computador. Na página Where Do You Want To Install Windows, pressione Shift+F10 para abrir um prompt de comando. No prompt de comando, digite **diskpart** para iniciar o utilitário DiskPart.

CRIAÇÃO DE PARTIÇÕES DE DISCO DURANTE A INSTALAÇÃO

A criação de uma partição permite que você defina o tamanho da mesma. Visto que só é permitida a criação de novas partições em áreas de espaço não alocado de um disco, pode ser preciso excluir partições existentes para poder criar uma partição do tamanho que você deseja. Após criar a partição, pode-se formatar essa partição para que seja usada na instalação de um sistema de arquivos. Mesmo que você não formate a partição, ainda pode utilizá-la na instalação do sistema operacional. Nesse caso, a Instalação formata a partição quando você prosseguir a instalação do sistema operacional.

Para criar uma nova partição, siga as etapas:

1. Durante a instalação, na página Where Do You Want To Install Windows, toque ou clique em Drive Options (Advanced) para exibir as opções avançadas de trabalho com unidades.
2. Toque ou clique no disco em que deseja criar a partição. Depois, toque ou clique em New.
3. Na caixa Size, defina o tamanho da partição em megabytes. Toque ou clique em Apply para que a Instalação crie a partição no disco selecionado.

Após criar uma partição, é necessário que ela seja formatada para prosseguir com a instalação.

FORMATAÇÃO DE PARTIÇÕES DE DISCO DURANTE A INSTALAÇÃO

A formatação de uma partição cria um sistema de arquivos na partição. Após a formatação ser concluída, você terá uma partição formatada onde o sistema operacional pode ser instalado. Tenha em mente que a formatação de uma partição exclui todos os dados contidos nela. Só se deve formatar partições existentes (e não partições recentemente criadas) quando você quiser remover uma partição existente e todo o seu conteúdo para iniciar a instalação de uma partição recém-formatada.

Para formatar uma partição, siga as etapas:

1. Durante a instalação, na página Where Do You Want To Install Windows, toque ou clique em Drive Options (Advanced) para exibir as opções avançadas de trabalho com unidades.
2. Toque ou clique na partição que deseja formatar.
3. Toque ou clique em Format. Quando você for solicitado a confirmar que deseja formatar a partição, toque ou clique em OK. A Instalação formatará a partição.

EXCLUSÃO DE PARTIÇÕES DE DISCO DURANTE A INSTALAÇÃO

A exclusão de uma partição remove uma partição que você não quer ou não precisa mais. Depois que o Setup excluir a partição, o espaço em disco alocado anteriormente pela partição será um espaço não alocado no disco. A exclusão de uma partição exclui

todos os dados na partição. Normalmente, uma partição só será excluída quando estiver no formato errado ou se você quiser agrupar áreas de espaço livre em um disco.

Para excluir uma partição, siga as etapas:

1. Durante a instalação, na página Where Do You Want To Install Windows, toque ou clique em Drive Options (Advanced) para exibir as opções avançadas de trabalho com unidades.
2. Toque ou clique na partição que deseja excluir.
3. Toque ou clique em Delete. Quando você for solicitado a confirmar que deseja excluir a partição, toque ou clique em OK. A Instalação excluirá a partição.

EXTENSÃO DE PARTIÇÕES DE DISCO DURANTE A INSTALAÇÃO

O Windows Server 2012 requer ao menos 10 GB de espaço em disco para a instalação, sendo recomendado ao menos 32 GB de espaço em disco disponível. Se uma partição existente for muito pequena, ela não poderá ser usada para instalar o sistema operacional. Para solucionar esse problema, pode-se estender uma partição para aumentar o seu tamanho. Para isso, usa-se áreas de espaço não alocado no disco atual. Só é possível estender uma partição com um sistema de arquivos existente se ele estiver formatado em NTFS 5.2 ou versão posterior. As novas partições criadas durante o Setup também podem ser estendidas, desde que o disco em que foi criada a partição tenha espaço não alocado.

Para estender uma partição, siga as etapas:

1. Durante a instalação, na página Where Do You Want To Install Windows, toque ou clique em Drive Options (Advanced) para exibir as opções avançadas de trabalho com unidades.
2. Toque ou clique na partição que deseja estender.
3. Toque ou clique em Extend. Na caixa Size, defina o tamanho da partição em me-gabytes. Toque ou clique em Apply para estender a partição selecionada.
4. Quando você for solicitado a confirmar que deseja estender a partição, toque ou clique em OK. O Setup estenderá a partição.

Alteração da opção de instalação

Diferentemente de versões anteriores do Windows Server, é possível alterar a opção de instalação em qualquer servidor com o Windows Server 2012. Isso acontece porque uma diferença-chave entre as opções de instalação está relacionada à existência dos seguintes recursos de interface de usuário e infraestrutura:

- Graphical Management Tools And Infrastructure
- Desktop Experience
- Server Graphical Shell

Instalações de servidor completo possuem tanto o recurso Graphical Management Tools And Infrastructure quanto o Server Graphical Shell. Podem também conter a Desktop Experience. Por outro lado, instalações de interface mínima possuem ape-

nas o recurso Graphical Management Tools And Infrastructure e instalações Server Core não possuem esses recursos.

Como o Windows também instala ou desinstala automaticamente recursos dependentes, funções de servidor e ferramentas de gerenciamento para que correspondam à opção de instalação, pode-se converter uma opção de instalação à outra ao adicionar ou remover os recursos apropriados de interface de usuário e infraestrutura.

Conversão de instalações de servidor completo e de interface mínima

Para converter uma instalação de servidor completo em uma de interface mínima, remove-se o Server Graphical Shell. Para fazer isso, você pode usar o Remove Roles And Features Wizard (Assistente de Remoção de Funções e Recursos) ou usar o prompt do PowerShell, digitando o seguinte comando:

```
uninstall-windowsfeature server-gui-shell -restart
```

Esse comando dá uma instrução ao Windows Server para desinstalar o Server Graphical Shell e reiniciar o servidor para finalizar a remoção. Se o recurso Desktop Experience estiver instalado, ele será removido também.

DICA A melhor prática antes de executar esse ou qualquer outro comando que tenha vasto efeito é executar o comando com o parâmetro *-Whatif*. Esse parâmetro diz ao Windows PowerShell para confirmar o que exatamente acontecerá quando o comando for executado.

Para converter uma instalação de interface mínima para uma de servidor completo, adiciona-se o Server Graphical Shell. Para fazer isso, você pode usar o Add Roles And Features Wizard (Assistente de Adição de Funções e Recursos) ou usar o prompt do PowerShell, digitando o seguinte comando:

```
install-windowsfeature server-gui-shell -restart
```

Esse comando dá uma instrução ao Windows Server para instalar o Server Graphical Shell e reiniciar o servidor para finalizar a instalação. Se você também quer instalar a Desktop Experience, pode usar como opção esse comando:

```
install-windowsfeature server-gui-shell, desktop-experience -restart
```

Conversão de instalações Server Core

Para converter uma instalação de servidor completo ou de interface mínima para uma instalação Server Core, remove-se as interfaces do usuário para Graphical Management Tools And Infrastructure. Se você remover o framework WoW64 Support, também converterá o servidor para uma instalação Server Core. Para remover as interfaces do usuário você pode usar o Remove Roles And Features Wizard ou usar o prompt do PowerShell, digitando este comando:

```
uninstall-windowsfeature server-gui-mgmt-infra -restart
```

Esse comando dá uma instrução ao Windows Server para desinstalar as interfaces do usuário para Graphical Management Tools And Infrastructure e reiniciar o servidor para finalizar a remoção. Como várias funções, serviços de função e recursos podem ser desinstalados juntamente com as interfaces do usuário, primeiro execute o comando com o parâmetro *-Whatif* para obter detalhes do que exatamente será desinstalado.

Se você instalou o servidor com interfaces do usuário e converteu em uma instalação Server Core, é possível reverter para a instalação de servidor completo usando este comando:

```
install-windowsfeature server-gui-mgmt-infra -restart
```

Contanto que os binários para o recurso e os seus recursos dependentes não tenham sido removidos, o comando funcionará. Porém, se os binários foram removidos ou se Server Core era a opção original de instalação, será preciso especificar uma origem para os binários necessários.

Utiliza-se o parâmetro **-Source** para restaurar os binários necessários de um arquivo de imagem Windows Imaging (WIM). Por exemplo: se a sua empresa possuísse uma imagem do Windows montada para a edição do Windows Server 2012 em que você está trabalhando disponível no caminho de rede \\ImServer18\WinS12EE, você poderia especificar a origem desta maneira:

```
install-windowsfeature server-gui-mgmt-infra -source \\imserver18\wins12ee
```

Muitas grandes empresas têm imagens padrão que podem ser montadas usando caminhos de rede. Pode-se também montar a mídia de distribuição do Windows Server 2012 e usar como origem a pasta Windows\WinSXS da imagem de instalação. Para isso, siga as etapas:

1. Insira o disco de instalação na unidade de disco do servidor e crie uma pasta para montar a imagem de Instalação, digitando o seguinte comando: **mkdir c:\mountdir**.
2. Localize o número do índice da imagem que deseja utilizar, digitando este comando em um prompt de comando elevado: **dism /get-wiminfo /wimfile:e:\sources\install.wim**, onde e: é o designador de unidade da unidade de disco do servidor.
3. Monte a imagem de instalação, digitando o seguinte comando em um prompt de comando elevado: **dism /mount-wim /wimfile:e:\sources\install.wim /index:2 /mountdir:c:\mountdir /readonly**, onde e: é o designador de unidade da unidade de disco do servidor, 2 é o índice da imagem a ser usada e c:\mountdir é o diretório de montagem. A montagem da imagem pode levar alguns minutos.
4. Utilize Install-WindowsFeature em um prompt do PowerShell com a origem especificada como **c:\mountdir\windows\winsxs**, conforme mostra o exemplo:

```
install-windowsfeature server-gui-mgmt-infra  
-source c:\mountdir\windows\winsxs
```

Gerenciamento de funções, serviços de função e recursos

Ao realizar o gerenciamento de configurações do servidor, você usará principalmente o Server Manager para gerenciar funções, serviços de função e recursos. O Server Manager não é usado apenas para adicionar ou remover funções, serviços de função e recursos. Ele também serve para visualizar os detalhes e o status de configuração desses componentes de software.

Realização de tarefas de configuração inicial

O Server Manager é o seu console de gerenciamento central para a instalação e configuração inicial de funções e recursos. Além de auxiliá-lo a realizar rapidamente a instalação de um novo servidor, o Server Manager também pode ajudá-lo a estabelecer o seu ambiente de gerenciamento.

Normalmente, o Windows Server 2012 inicia o Server Manager de forma automática sempre que você realizar o logon, podendo ser acessado na área de trabalho. Se você não deseja que o console inicie todas as vezes que realizar o logon, toque ou clique em Manage e depois em Server Manager Properties. Na caixa de diálogo Server Manager Properties, selecione Do Not Start Server Manager Automatically At Logon e depois toque ou clique em OK.

OBSERVAÇÃO A Group Policy também pode ser usada para controlar o início automático do Server Manager. Habilite ou desabilite a configuração de política Do Not Display Server Manager Automatically At Logon em Computer Configuration\Administrative Templates\System\Server Manager.

Como mostra a Figura 2-1, o modo de exibição padrão do Server Manager é o dashboard. O dashboard possui links rápidos para adicionar funções e recursos a servidores locais e remotos, adicionar servidores para gerenciamento e criar grupos de servidores. Opções similares que se encontram no menu Manage:

- **Add Roles And Features** Inicia o Assistente de Adição de Funções e Recursos, usado para instalar funções, serviços de função e recursos no servidor.
- **Add Other Servers To Manage** Abre a caixa de diálogo Add Servers, usada para adicionar servidores que você queira gerenciar. Os servidores adicionados são listados quando você seleciona o nó All Servers. Pressione e mantenha pressionado ou clique com o botão direito em um servidor no painel Servers do nó All Servers para exibir uma lista de opções de gerenciamento, incluindo: Restart Server, Manage As e Remove Server.
- **Create Server Group** Abre a caixa de diálogo Create Server Group, usada para adicionar servidores a grupos de servidores, facilitando o gerenciamento. O Server Manager cria automaticamente grupos baseados em funções. Controladores de domínio, por exemplo, estão listados sob o AD DS. Assim, você pode facilmente encontrar informações sobre qualquer controlador de domínio ao selecionar o nó referente.

DICA Quando precisar se conectar a um servidor usando credenciais alternativas, pressione e mantenha pressionado ou clique com o botão direito do mouse em um servidor no nó All Servers e depois selecione Manage As. Na caixa de diálogo Windows Security, insira as credenciais alternativas e toque ou clique em OK. As credenciais fornecidas serão limpas quando você sair do Server Manager. Para salvar as credenciais e usá-las toda vez que fizer logon, selecione Remember My Credentials na caixa de diálogo Windows Security. É necessário repetir esse procedimento sempre que você mudar a senha associada às credenciais alternativas.

MUNDO REAL Ao trabalhar com instalações Server Core, pode-se usar o Sconfig para configurar associação a domínio e grupo de trabalho, nome do computador, gerenciamento remoto, Windows Update, Remote Desktop, configurações da rede e data e hora. O Sconfig também pode ser usado para fazer logoff, reiniciar e desligar o servidor. Para iniciar o Sconfig, digite sconfig no prompt de comando. Depois, você pode selecionar opções do menu e seguir as indicações para configurar o servidor.

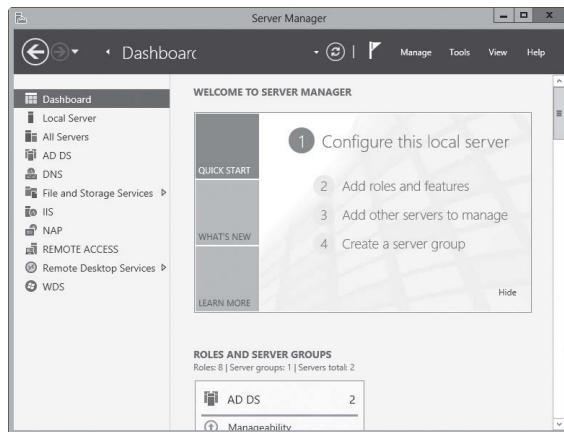


FIGURA 2-1 Use o dashboard para a administração geral.

No painel esquerdo do Server Manager (também conhecido como árvore de console ou *console tree*), encontram-se opções de acesso ao dashboard, servidor local, todos os servidores adicionados para gerenciamento e grupos de servidores. Ao selecionar Local Server na árvore de console, como mostra a Figura 2-2, pode-se gerenciar a configuração básica do servidor em você está logado localmente.

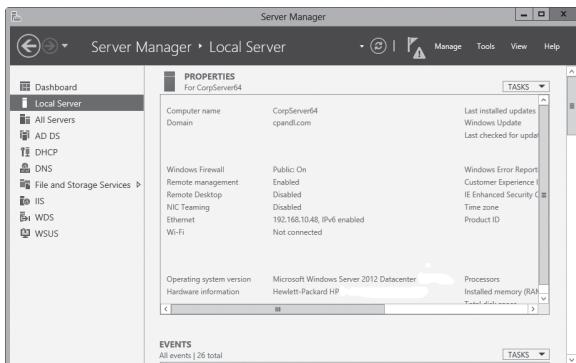


FIGURA 2-2 Gerencie as propriedades do servidor local.

As informações sobre o servidor local estão organizadas em diversos tópicos principais, cada um com um painel de gerenciamento associado:

- **Best Practices Analyzer** Permite que você execute o Best Practices Analyzer (Analizador de Práticas Recomendadas) no servidor e examine os resultados. Para iniciar um exame, toque ou clique em Tasks e depois em Start BPA Scan.

- **Events** Fornece informações resumidas sobre eventos de aviso e de erro do log de eventos do servidor. Toque ou clique em um evento para exibir mais informações sobre ele.
- **Performance** Permite que você configure e visualize o status dos alertas de desempenho de uso da CPU e da memória. Para configurar os alertas de desempenho, toque ou clique em Tasks e depois em Configure Performance Alerts.
- **Properties** Exibe o nome do computador, domínio, configuração da rede IP, fuso horário, entre outras. Pode-se clicar sobre cada uma das propriedades para exibir uma interface de gerenciamento relacionada.
- **Roles And Features** Lista as funções e recursos instalados no servidor, em uma ordem aproximada de instalação. Para remover uma função ou um recurso, pressione e mantenha pressionado ou clique com o botão direito do mouse sobre o que deseja remover e depois selecione Remove Role or Feature.
- **Services** Lista os serviços rodando no servidor por nome, status e tipo de inicialização. Pressione e mantenha pressionado ou clique com o botão direito do mouse em um serviço para gerenciar o seu status de execução.

No painel Properties, é feita a maior parte da configuração inicial do servidor. As propriedades disponíveis para gerenciamento rápido incluem:

- **Computer Name/Domain** Exibe o nome e o domínio do computador. Toque ou clique em um dos links relacionados para exibir a caixa de diálogo System Properties com a aba Computer Name selecionada. Para alterar informações de nome ou domínio do computador, toque ou clique em Change, insira as informações de nome e domínio do computador e depois toque ou clique em OK. Por padrão, os servidores recebem um nome gerado aleatoriamente e são configurados como parte de um grupo de trabalho chamado WORKGROUP. Nos modos de exibição Small Icons ou Large Icons do Control Panel é possível exibir a caixa de diálogo System Properties com a aba Computer Name já selecionada. Para isso, toque ou clique em System e depois toque ou clique em Change Settings, sob as configurações Computer Name, Domain e Workgroup.
- **Customer Experience Improvement Program** Mostra se o servidor está participando do Customer Experience Improvement Program (CEIP, Programa de Aperfeiçoamento da Experiência do Usuário). Toque ou clique no vínculo relacionado para alterar as configurações de participação. A participação no programa CEIP possibilita que a Microsoft reúna informações sobre a forma como você utiliza o servidor. A Microsoft coleta esses dados para ajudar na melhoria de versões futuras do Windows e nenhuma coleta de dados que faça parte do CEIP identifica você ou a sua empresa pessoalmente. Caso escolha participar, você também pode fornecer informações sobre o número de servidores e computadores desktop que integram a sua organização, bem como o setor em que a organização trabalha. Se você optar por não participar do CEIP, desativando esse recurso, você perderá uma oportunidade de ajudar na melhoria do Windows.
- **Ethernet** Exibe a configuração TCP/IP de Conexões Com Fio Seguras (Ethernet). Toque ou clique no vínculo relacionado para exibir o console Network Connections. Para configurar conexões de rede, toque ou clique duas vezes na conexão com a qual deseja trabalhar e depois toque ou clique em Properties para abrir a

caixa de diálogo Properties. Por padrão, os servidores estão configurados para usar endereçamento dinâmico tanto para IPv4 quanto para IPv6. O console Network Connections também pode ser exibido clicando ou tocando em Change Adapter Settings em Tasks no Network And Sharing Center.

- **IE Enhanced Security Configuration** Exibe o status da Internet Explorer Enhanced Security Configuration (IE ESC, Configuração de Segurança Reforçada do Internet Explorer). Toque ou clique no vínculo relacionado para habilitar ou desabilitar a IE ESC. Ao tocar ou clicar no vínculo dessa opção você pode ativar ou desativar o recurso para administradores, usuários ou ambos. A IE ESC é um recurso de segurança que reduz a exposição de um servidor a ataques em potencial, aumentando os níveis padrão de segurança nas zonas de segurança do Internet Explorer e alterando as configurações padrão do Internet Explorer. A IE ESC está ativada para administradores e usuários por padrão.

MUNDO REAL Na maioria dos casos, você deveria ativar a IE ESC em um servidor tanto para usuários quanto para administradores. Entretanto, a ativação da IE ESC reduz a funcionalidade do Internet Explorer. Quando a IE ESC é ativada, as zonas de segurança são configuradas da seguinte maneira: para a zona Internet o nível é definido como Médio-alto, para a zona Sites confiáveis o nível é definido como Médio, para a zona Local Intranet o nível é definido como Médio-baixo e para a zona Sites restritos o nível é definido como Alto. Quando a IE ESC é ativada, as seguintes configurações de Internet são alteradas: a caixa de diálogo Enhanced Security Configuration está ativada, extensões de navegador de terceiros estão desabilitadas, sons em página da Web estão desabilitados, animações em páginas da Web estão desabilitadas, configurações de assinatura para programas baixados estão habilitadas, revogação de certificados do servidor está habilitada, páginas criptografadas não são salvas, arquivos de Internet temporários são excluídos quando o navegador é fechado, avisos para alterações de modo seguro e inseguro estão habilitados e a proteção da memória está habilitada.

- **NIC Teaming** Exibe o status e a configuração de NIC teaming (agrupamento NIC). Toque ou clique no vínculo relacionado para adicionar ou remover interfaces agrupadas e gerenciar opções relacionadas.
- **Product ID** Exibe a identificação do produto para o Windows Server. Toque ou clique no vínculo relacionado para inserir uma chave de produto e ativar o sistema operacional pela Internet.
- **Remote Desktop** Toque ou clique no vínculo relacionado para exibir a caixa de diálogo System Properties com a aba Remote selecionada. Para configurar a Remote Desktop, selecione a opção de configuração que você deseja utilizar e toque ou clique em OK. Por padrão, nenhuma conexão remota ao servidor é permitida. Nos modos de exibição Small Icons ou Large Icons do Control Panel é possível exibir a caixa de diálogo System Properties com a aba Remote já selecionada. Para isso, toque ou clique duas vezes em System e depois toque ou clique em Remote Settings no painel esquerdo.
- **Remote Management** Mostra se o gerenciamento remoto deste servidor a partir de outros servidores está habilitado. Toque ou clique no vínculo relacionado para habilitar ou desabilitar o gerenciamento remoto.
- **Time Zone** Mostra o fuso horário atual do servidor. Toque ou clique no vínculo relacionado para exibir a caixa de diálogo Date and Time. Para configurar o fuso horário do servidor, toque ou clique em Change Time Zone e selecione o fuso

horário adequado. Depois, toque ou clique duas vezes em OK. A caixa de diálogo Date and Time também é exibida ao pressionar e manter pressionado ou clicar com o botão direito do mouse sobre o relógio na barra de tarefas, selecionando Adjust Date/Time em seguida. Embora todos os servidores estejam configurados para sincronizar o horário com um servidor de horário na Internet, o processo de sincronização do horário não altera o fuso horário de um computador.

- **Windows Error Reporting** Mostra o status do Windows Error Reporting (WER, Relatório de Erros do Windows). Toque ou clique no vínculo relacionado para alterar as configurações de participação para o WER. Na maioria dos casos, é desejável habilitar o WER pelo menos nos primeiros 60 dias após a instalação do sistema operacional. Com o WER habilitado, o seu servidor envia descrições de problemas à Microsoft e o Windows notifica sobre possíveis soluções para esses problemas. Pode-se visualizar relatórios de problemas e possíveis soluções em Action Center (Central de Ações). Para abrir a Action Center, toque ou clique no ícone Action Center na área de notificação da barra de tarefas e depois selecione Open Action Center.
- **Windows Firewall** Mostra o status do Windows Firewall. Se o Windows Firewall estiver ativado, essa propriedade exibe o nome do perfil de firewall que está aplicado e o status do firewall. Toque ou clique no vínculo relacionado para exibir o utilitário Windows Firewall. Por padrão, ele está habilitado. Nos modos de exibição Small Icons ou Large Icons do Control Panel é possível exibir o Windows Firewall ao clicar ou tocar na opção Windows Firewall.
- **Windows Update** Mostra a configuração atual do Windows Update. Toque ou clique no vínculo relacionado para exibir o utilitário Windows Update no Control Panel, que pode ser usado para habilitar atualizações automáticas (se o Windows Update estiver desabilitado) ou para buscar atualizações (se o Windows Update estiver habilitado). Para exibir o Windows Update nos modos de exibição Small Icons ou Large Icons do Control Panel, selecione a opção Windows Update.

OBSERVAÇÃO Este resumo das opções serve como introdução e referência rápida. As tecnologias e tarefas de configuração relacionadas serão abordadas com maiores detalhes ao longo deste e de outros capítulos no livro.

Princípios básicos do Server Manager e binários

O console Server Manager é projetado para dar conta de tarefas de administração do sistema. Como você passará bastante tempo trabalhando com essa ferramenta, é bom conhecer cada detalhe dela. O Server Manager é inicializado automaticamente por padrão. Caso você tenha fechado o console ou desabilitado a inicialização automática, toque ou clique na opção relacionada na barra de tarefas para abrir o console. Uma outra maneira de abri-lo é pressionar a tecla Windows, digitar **ServerManager.exe** na caixa de pesquisa Apps e depois pressionar a tecla Enter.

O equivalente da linha de comando do Server Manager é o módulo ServerManager para o Windows PowerShell. Se você estiver logado no Windows Server 2012, esse módulo é importado para o Windows PowerShell por padrão. Caso contrário, é preciso importar o módulo para poder utilizar os cmdlets que ele oferece. Para importar o módulo ServerManager, digite **Import-Module ServerManager** no prompt do Windows PowerShell. Uma vez que o módulo tenha sido importado, ele pode ser usado

na sessão sendo executada no Windows PowerShell no momento. Na próxima vez que você inicializar o Windows PowerShell, será preciso importar o módulo novamente se desejar usar os recursos que ele oferece.

Digite **get-windowsfeature** em um prompt do Windows PowerShell para obter uma lista detalhada do estado atual de um servidor no que diz respeito às funções, serviços de função e recursos. Cada uma das funções, dos serviços de função e dos recursos instalados são destacados e marcados como tais. Uma nomenclatura para componentes de gerenciamento é exibida entre colchetes após o nome de exibição de cada função, serviço de função e recurso. Use o `Install-WindowsFeature` ou o `Uninstall-WindowsFeature` seguido pelo nome de gerenciamento para instalar ou desinstalar uma função, serviço de função ou recurso. Para instalar o Network Load Balancing (Balanceamento de Carga de Rede), por exemplo, digite **install-windowsfeature nlb**. Pode-se acrescentar **-includeallsubfeature** ao instalar componentes para adicionar todos os serviços de função e recursos subordinados. As ferramentas de gerenciamento não estão inclusas por padrão. Para adicionar ferramentas de gerenciamento, acrescente **-includemanagementtools** ao instalar componentes.

Os binários necessários para a instalação de funções e recursos são chamados de *payloads*. No Windows Server 2012 eles são armazenados em subpastas da pasta `%SystemDrive%\Windows\WinSXS`. Utilizando o parâmetro `-Remove` do cmdlet `Uninstall-WindowsFeature` pode-se desinstalar uma função ou recurso e ainda desinstalar e remover os binários de uma função ou recurso. Os subcomponentes da função ou do recurso também serão excluídos. Para remover as ferramentas de gerenciamento, adicione o parâmetro **-includeallmanagementtools**.

Quando quiser instalar uma função ou recurso, você pode instalar os componentes relacionados e restaurar os binários removidos para esses componentes usando o cmdlet `Install-WindowsFeature`. Ao usar o `Install-WindowsFeature`, as cargas são restauradas via Windows Update por padrão.

No exemplo a seguir, os binários AD DS e todos os sub-recursos relacionados via Windows Update são restaurados:

```
install-windowsfeature -name ad-domain-services -includeallsubfeature
```

Utiliza-se o parâmetro `-Source` para restaurar os binários a partir de uma imagem montada de Windows Imaging (WIM). Por exemplo: se a sua empresa possuísse uma imagem do Windows montada para a edição do Windows Server 2012 em que você está trabalhando disponível no caminho de rede `\\\ImServer18\WinS12EE`, você poderia especificar a origem desta maneira:

```
install-windowsfeature -name ad-domain-services -includeallsubfeature -source \\imserver18\wins12ee
```

Tenha em mente que o caminho especificado só será utilizado se os binários necessários não forem encontrados na pasta Windows Side-By-Side do servidor de destino. Muitas grandes empresas têm imagens padrão que podem ser montadas usando caminhos de rede. Pode-se também montar a mídia de distribuição do Windows Server 2012 e usar como origem a pasta `Windows\WinSXS` da imagem de instalação. Para isso, siga as etapas:

1. Insira o disco de instalação na unidade de disco do servidor e crie uma pasta para montar a imagem de Instalação, digitando o comando: **mkdir c:\mountdir**.

2. Localize o número do índice da imagem que deseja utilizar, digitando o seguinte comando em um prompt de comando elevado: **dism /get-wiminfo /wimfile:e:\sources\install.wim**, onde e: é o designador de unidade da unidade de disco do servidor.
3. Monte a imagem de instalação, digitando o seguinte comando em um prompt de comando elevado: **dism /mount-wim /wimfile:e:\sources\install.wim /index:2 /mountdir:c:\mountdir /readonly**, onde e: é o designador de unidade da unidade de disco do servidor, 2 é o índice da imagem a ser usada e c:\mountdir é o diretório de montagem. A montagem da imagem pode levar alguns minutos.
4. Utilize Install-WindowsFeature em um prompt do PowerShell com a origem específica como **c:\mountdir\windows\winsxs**, conforme mostra o exemplo:

```
install-windowsfeature -name ad-domain-services  
-includeallsubfeature  
-source c:\mountdir\windows\winsxs
```

Use a Group Policy (política de grupo) para controlar se o Windows Update deve ser utilizado para restaurar os payloads e fornecer caminhos de origem alternativos para a restauração destes. A política para esse caso é Specify Settings For Optional Component Installation And Component Repair, que está em Computer Configuration\Administrative Templates\System. A política também é utilizada para obter os payloads necessários ao reparo de componentes.

Ao habilitar essa política (como mostra a Figura 2-3), você pode:

- Definir o caminho de arquivo de origem alternativo para payloads como um local de rede. Para compartilhamentos de rede, insira o caminho UNC para o compartilhamento, como por exemplo \\CorpServer82\WinServer2012\. Para imagens montadas do Windows, insira o caminho WIM com o prefixo **WIM:** e inclua o índice da imagem a ser usada, como por exemplo WIM:\\CorpServer82\WinServer2012\install.wim:4.
- Determinar que o Windows Update nunca seja usado para baixar payloads. Se você habilitar a política e usar essa opção, não é necessário especificar um caminho alternativo. Nesse caso, os payloads não serão obtidos automaticamente e os administradores terão que especificar claramente o caminho de origem alternativo.
- Determinar que o Windows Update deve ser usado para o reparo de componentes, e não o Windows Server Update Services.

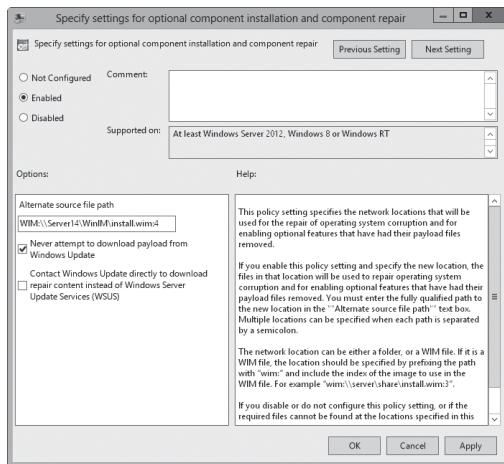


FIGURA 2-3 Instalação de componentes de controle por meio de Group Policy.

Como gerenciar servidores remotamente

Tanto o Server Manager quanto outros Microsoft Management Consoles (MMCs, Consoles de Gerenciamento Microsoft) podem ser usados para realizar algumas tarefas de gerenciamento em computadores remotos, desde que esses computadores estejam no mesmo domínio ou que você esteja trabalhando em um grupo de trabalho e tenha adicionado os computadores remotos como hosts confiáveis. É possível conectar-se a servidores executando instalações de servidor completo, de interface mínima e Server Core. O computador que será usado para gerenciar computadores remotos deve estar executando o Windows Server 2012 ou Windows 8. Além disso, é preciso instalar as Remote Server Administration Tools (Ferramentas de Administração de Servidor Remoto).

No Windows Server 2012, as Remote Server Administration Tools são instaladas como um recurso usando o Add Roles And Features Wizard. Caso os binários para as ferramentas tenham sido removidos, é preciso instalar as ferramentas especificando a origem, como foi discutido em “Princípios básicos do Server Manager e binários” anteriormente neste capítulo.

Você pode obter as Remote Server Administration Tools para o Windows 8 fazendo um download no Download Center da Microsoft (<http://download.microsoft.com>). Existem diferentes versões disponíveis para sistemas x64 e x86.

O gerenciamento remoto está habilitado por padrão para dois tipos de aplicativos e comandos em servidores executando o Windows Server 2012:

- Aplicativos e comandos que usam o Windows Remote Management (WinRM, Gerenciamento Remoto do Windows) e o acesso remoto para gerenciamento do Windows PowerShell
- Aplicativos e comandos que usam a Windows Management Instrumentation (WMI, Instrumentação de Gerenciamento do Windows) e o acesso remoto para gerenciamento do Component Object Model (DCOM)

Esses tipos de aplicativos e comandos são permitidos para gerenciamento remoto devido às exceções configuradas no Windows Firewall, habilitadas por padrão para o Windows Server 2012. No Windows Firewall, as exceções para aplicativos permitidos que dão suporte ao gerenciamento remoto incluem:

- Windows Management Instrumentation
- Windows Remote Management
- Windows Remote Management (Compatibility)

No Windows Firewall With Advanced Security (Firewall do Windows com Segurança Avançada) existem regras de entrada que correspondem ao padrão de aplicativos permitidos pelo firewall:

- Para a WMI, as regras de entrada são: Windows Management Instrumentation (WMI-In), Windows Management Instrumentation (DCOM-In) e Windows Management Instrumentation (ASync-In).
- Para o WinRM, a regra de entrada correspondente é o Windows Remote Management (HTTP-In).
- Para o modo de compatibilidade do WinRM, a regra de entrada correspondente é o Windows Remote Management (HTTP-In).

Para gerenciar essas exceções ou regras, use o Windows Firewall padrão ou o Windows Firewall With Advanced Security – e não ambos. Se quiser permitir o gerenciamento remoto usando Server Manager, MMCs e Windows PowerShell, normalmente você permitirá as exceções WMI, WinRM e modo de compatibilidade WinRM no Windows Firewall.

Ao trabalhar com o Server Manager, pode-se selecionar o Local Server na árvore de console para visualizar o status da propriedade de gerenciamento remoto. Caso não queira permitir o gerenciamento remoto do servidor local, clique no vínculo relacionado. Na caixa de diálogo Configure Remote Management desmarque Enable Remote Management Of This Server From Other Computers e depois toque ou clique em OK.

Quando a opção Enable Remote Management Of This Server From Other Computers é desmarcada e você clica ou toca em OK, o Server Manager realiza várias tarefas de segundo plano que desabilitam o WinRM e o acesso remoto para gerenciamento do Windows PowerShell no servidor local. Uma dessas tarefas é a desativação das exceções relacionadas que permitem aos aplicativos se comunicarem através do Windows Firewall usando o Windows Remote Management. As exceções para a Windows Management Instrumentation e para o Windows Remote Management (Compatibility) não são afetadas.

É preciso que você seja um membro do grupo Administrators nos computadores que deseja gerenciar usando o Server Manager. Para conexões remotas em configurações *grupo de trabalho para grupo de trabalho ou grupo de trabalho para domínio*, você deve estar logado utilizando uma conta de Administrador interno ou configurar a chave do registro *LocalAccountTokenFilterPolicy* para que seja permitido o acesso remoto do seu computador. Para configurar essa chave, digite o seguinte comando em um prompt de comando de administrador elevado:

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /vLocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

OBSERVAÇÃO Outra forma de habilitar o gerenciamento remoto é digitar **configure-SMRemoting.exe -enable** em um prompt de administrador elevado.

OBSERVAÇÃO Se você quer que seja possível gerenciar remotamente um computador com o Windows 8 através do protocolo WS-Management, digite **winrm quickconfig** em um prompt elevado. Cada vez que você for solicitado a realizar mudanças de configuração, digite **Y**. Isso iniciará o serviço WinRM, configurará o WinRM para aceitar solicitações WS-Management em qualquer endereço IP, criará uma exceção do Windows Firewall para o Windows Remote Management e configurará *LocalAccountTokenFilterPolicy* para conceder os direitos administrativos apropriados para o gerenciamento remoto.

Vários outros tipos de tarefas de gerenciamento remoto são dependentes de outras exceções do Windows Firewall. Lembre-se:

- Remote Desktop e o gerenciamento remoto são habilitados ou desabilitados separadamente. Para permitir que alguém conecte ao servidor local usando Remote Desktop, é preciso permitir conexões relacionadas ao computador e configurar o acesso, como será discutido no Capítulo 4 “Automatização de tarefas administrativas, políticas e procedimentos.”
- O Remote Service Management deve ser configurado como um aplicativo permitido no Windows Firewall para que se possa gerenciar remotamente os serviços de um computador. No firewall avançado existem várias regras relacionadas que permitem o gerenciamento via Named Pipes (NP, Pipes Nomeados) e Remote Procedure Calls (RPC, Chamadas de Procedimento Remoto).
- O Remote Event Log Management (Gerenciamento Remoto do Log de Eventos) deve ser configurado como um aplicativo permitido no Windows Firewall para que se possa gerenciar remotamente os logs de eventos de um computador. No firewall avançado existem várias regras relacionadas que permitem o gerenciamento via NP e RPC.
- O Remote Volume Management (Gerenciamento de Volumes Remoto) deve ser configurado como um aplicativo permitido no Windows Firewall para que se possa gerenciar remotamente os volumes de um computador. No firewall avançado existem várias regras relacionadas que permitem o gerenciamento do Virtual Disk Service (Serviço de Disco Virtual) e do Virtual Disk Service Loader (Carregador de Serviço de Disco Virtual).
- O Remote Scheduled Task Management (Gerenciamento de Tarefas Programadas) deve ser configurado como um aplicativo permitido no Windows Firewall para que se possa gerenciar remotamente as tarefas programadas de um computador. No firewall avançado existem várias regras relacionadas que permitem o gerenciamento de tarefas programadas via RPC.

Apenas o Remote Service Management (Gerenciamento Remoto de Serviços) está habilitado por padrão.

O gerenciamento remoto em uma instalação Server Core do Windows Server 2012 pode ser configurado com o Sconfig. Para iniciar o utilitário Server Configuration, digite **sconfig**.

Conexão e trabalho em servidores remotos

Com o Server Manager você pode se conectar a servidores remotos e gerenciá-los. Para isso, basta que você tenha adicionado o servidor para gerenciamento. Para adicionar um servidor por vez ao Server Manager, siga as etapas:

1. Abra o Server Manager. No painel esquerdo, selecione All Servers para visualizar os servidores que já foram adicionados para gerenciamento. Se o servidor em que você deseja trabalhar não está na lista, selecione Add Servers no menu Manage para exibir a caixa de diálogo Add Servers.
2. A caixa de diálogo Add Servers possui vários painéis para a adição de servidores:
 - O painel Active Directory está selecionado por padrão. Ele permite que você insira o nome do computador ou o nome de domínio totalmente qualificado do servidor remoto que está executando o Windows Server. Após inserir um nome, toque ou clique em Find Now.
 - O painel DNS permite que você adicione servidores por nome do computador ou endereço IP. Após inserir o nome ou o endereço IP, toque ou clique no botão Search.
3. Na lista Name, toque ou clique duas vezes no servidor para que ele seja adicionado à lista Selected.
4. Repita as etapas 2 e 3 para adicionar outros servidores. Toque ou clique em OK.

Para adicionar vários servidores ao Server Manager, use o processo Import, seguindo as etapas:

1. Crie um arquivo de texto que contenha um nome de host, um nome de domínio totalmente qualificado ou um endereço IP por linha.
2. No Server Manager, selecione Add Servers no menu Manage. Na caixa de diálogo Add Servers, selecione o painel Import.
3. Toque ou clique no botão Options, à direita da caixa File, e use a caixa de diálogo Open para localizar e abrir a lista de servidores.
4. Na lista Computer, toque ou clique duas vezes em cada servidor que você quer adicionar à lista Selected. Toque ou clique em OK.

Após adicionar um computador remoto, o console Server Manager exibe o nome do computador remoto no modo de exibição All Servers. O Server Manager sempre resolve endereços IP em nomes de host. Como mostra a Figura 2-4, o modo de exibição All Servers também lista o status da Capacidade de Gerenciamento do servidor. Se um servidor estiver listado como "Not accessible", pode ser necessário realizar o logon localmente para solucionar o problema.

No modo de exibição All Servers, os servidores que você adicionou estão listados no painel Servers. Assim, você pode gerenciá-los sempre que estiver trabalhando com o Server Manager. O Server Manager controla os serviços, eventos e outros para cada servidor adicionado e cada servidor é incluso nos grupos de servidores apropriados com base nas funções e recursos instalados.

Os grupos de servidores criados automaticamente facilitam o gerenciamento de várias funções e recursos instalados nos seus servidores. Se você selecionar um grupo AD DS, por exemplo, verá uma lista de controladores de domínio que você adicionou para gerenciamento, bem como qualquer evento crítico ou de aviso para esses servidores e o status dos serviços de que dependem as funções.

Caso queira agrupar servidores por departamento, localização geográfica ou outra classificação, você pode criar o seu próprio grupo de servidores. Para criar grupos, não é necessário que os servidores com os quais você deseja trabalhar tenham sido adicionados ao Server Manager. Para adicionar servidores, procure no Active Directory

ou no DNS ou importe uma lista de nomes de host, nomes de domínio totalmente qualificados ou endereços IP. Um servidor adicionado a um grupo personalizado também é adicionado automaticamente para gerenciamento.

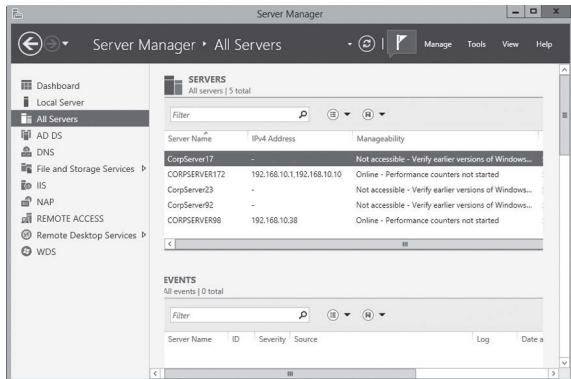


FIGURA 2-4 Observe o status de Capacidade de Gerenciamento de cada servidor e execute ações corretivas quando necessário.

Para criar um grupo de servidores, siga as etapas:

1. Abra o Server Manager. Selecione Create Server Group no menu Manage para exibir a caixa de diálogo Create Server Group.
2. Insira um nome descritivo para o grupo. Utilize os painéis e as opções existentes para adicionar servidores ao grupo. Lembre-se do seguinte:
 - O painel Server Pool (Pool de Servidores), que está selecionado por padrão, lista os servidores que já foram adicionados para gerenciamento. Se um servidor que você quer adicionar ao grupo está na lista, toque ou clique nele duas vezes para adicioná-lo ao grupo.
 - O painel Active Directory permite que você insira o nome do computador ou o nome de domínio totalmente qualificado do servidor remoto que está executando o Windows Server. Após inserir um nome, toque ou clique em Find Now. Na lista Name, toque ou clique duas vezes no servidor para que ele seja adicionado à lista Selected.
 - O painel DNS permite que você adicione servidores por nome do computador ou endereço IP. Após inserir o nome ou o endereço IP, toque ou clique no botão Search. Na lista Name, toque ou clique duas vezes no servidor para que ele seja adicionado à lista Selected.
 - O painel Import permite a importação de uma lista de servidores. Toque ou clique no botão Options, à direita da caixa File, e use a caixa de diálogo Open para localizar e abrir a lista de servidores. Na lista Computer, toque ou clique duas vezes no servidor para que ele seja adicionado à lista Selected.
3. Toque ou clique em OK para criar o grupo de servidores.

Se você pressionar e manter pressionado ou clicar com o botão direito do mouse no nome de um servidor no painel Servers de um grupo de servidores ou no modo de exibição All Servers, será exibida uma lista estendida de opções de gerenciamento. Essas opções realizam a tarefa correspondente ou abrem a ferramenta de gerenciamento correspondente, com o servidor selecionado em foco. Por exemplo: se você clica com o botão direito do mouse em CorpServer172 e depois selecionasse Computer Management, o Computer Management se conectararia com o CorpServer172 e abriria.

Pode-se trabalhar com um computador remoto usando uma sessão remota interativa do Windows PowerShell. Para isso, abra um prompt de administrador elevado do Windows PowerShell. Digite **enter-pssession ComputerName –credential UserName**, onde *ComputerName* é o nome do computador remoto e *UserName* é o nome de um usuário que é membro do grupo Administrators no computador remoto ou no domínio do qual o computador remoto é membro. Quando for solicitado que você insira a senha de usuário autorizado, digite a senha e pressione a tecla Enter. Agora você pode inserir comandos na sessão, da mesma maneira que faria ao usar o Windows PowerShell localmente. Para sair da sessão, digite **exit-pssession**.

O exemplo a seguir entra em uma sessão interativa remota com o Server85 utilizando as credenciais de Williams:

```
enter-pssession server85 –credential williams
```

Adição e remoção de funções, serviços de função e recursos

O Server Manager cria automaticamente grupos de servidores baseados nas funções dos servidores adicionados para gerenciamento. Na primeira vez que você adicionou um controlador de domínio, por exemplo, o Server Manager pode criar grupos AD DS, DNS e File and Storage Services para facilitar o controle das funções dos controladores de domínio.

Se você selecionar um grupo baseado em funções no painel esquerdo, o painel Servers exibirá os servidores que você adicionou para gerenciamento que possuem essa função. Os detalhes do grupo de servidores selecionado fornecem as seguintes informações:

- Informações resumidas sobre eventos. O Server Manager lista os eventos de aviso e erro recentes. Toque ou clique em um evento para exibir mais informações sobre ele.
- Informações resumidas sobre o status de serviços do sistema relacionados. Pressione e mantenha pressionado ou clique com o botão direito do mouse sobre um serviço para gerenciar o seu status de execução.

DICA O Server Manager atualiza os detalhes a cada dez minutos por padrão. Você pode atualizar os detalhes manualmente, clicando ou tocando no botão Refresh Servers na barra de ferramentas. Se deseja definir um intervalo de atualização padrão diferente, toque ou clique em Manage e depois em Server Manager Properties. Depois, defina o novo intervalo de atualização em minutos e toque ou clique em OK.

Para gerenciar um serviço, pressione e mantenha pressionado ou clique com o botão direito do mouse no serviço e toque ou clique na opção que for conveniente: Stop Service (Parar o Serviço), Start Service (Iniciar o Serviço), Pause Service (Pausar o Serviço), Resume Service (Continuar o Serviço) ou Restart Service (Reiniciar o Serviço). Em muitos casos em que um serviço não está rodando como deveria, pode-se usar a opção Restart para solucionar o problema, o que interrompe e depois inicia o serviço. Consulte o Capítulo 3, “Monitoramento de processos, serviços e eventos” para mais informações sobre serviços do sistema e eventos.

O menu Manage possui duas opções-chave para trabalhar com funções e recursos:

- **Add Roles And Features** Inicia o Add Roles And Features Wizard, usado para instalar funções e recursos em um servidor que foi adicionado para gerenciamento.
- **Remove Roles And Features** Inicia o Remove Roles And Features Wizard, usado para desinstalar funções e recursos em um servidor que foi adicionado para gerenciamento.

Com o Windows Server 2012 é possível instalar funções e recursos em servidores (sejam elas máquinas físicas ou virtuais) e também em discos rígidos virtuais. Os servidores devem ser adicionados para gerenciamento no Server Manager e devem estar online. Os discos rígidos virtuais com os quais você quer trabalhar não precisam estar online, mas devem ser selecionáveis quando se procura por eles. Por esse motivo, pode ser preciso mapear uma unidade de rede para acessar um compartilhamento de rede. Assim, pode-se adicionar uma função de servidor ou recurso seguindo as etapas:

1. No Server Manager, selecione Add Roles And Features no menu Manage. Isso iniciará o Add Roles And Features Wizard. Se o Assistente exibir a página Before You Begin, leia o texto introdutório e depois toque ou clique em Next. Para não visualizar essa página na próxima vez em que iniciar o Assistente, selecione a caixa de seleção Skip This Page By Default antes de clicar ou tocar em Next.
2. Na página Installation Type está selecionada por padrão Role-Based Or Feature-Based Installation. Toque ou clique em Next.
3. Na página Server Selection pode-se escolher instalar funções e recursos em servidores em execução ou em discos rígidos virtuais. Selecione um servidor do pool de servidores ou selecione um servidor do pool de servidores no qual montar um disco rígido virtual (VHD). Se estiver adicionando funções e recursos a um VHD, toque ou clique em Browse e depois use a caixa de diálogo Browse For Virtual Hard Disks para localizar o VHD. Quando estiver pronto para prosseguir, toque ou clique em Next.

OBSERVAÇÃO Apenas servidores com o Windows Server 2012 e que foram adicionados para gerenciamento no Server Manager constam na lista.

4. Na página Server Roles, selecione a função ou as funções a serem instaladas. Se houver recursos obrigatórios para instalar uma função, você verá uma caixa de diálogo adicional. Toque ou clique em Add Features para fechar a caixa de diálogo e adicionar os recursos obrigatórios para a instalação do servidor. Toque ou clique em Next para continuar.

OBSERVAÇÃO Algumas funções não podem ser adicionadas ao mesmo tempo que outras, sendo preciso instalar cada função separadamente. Já outras funções não podem ser combinadas a funções existentes e você verá avisos sobre isso. Um servidor com uma instalação Server Core pode atuar como um controlador de domínio e também ser o proprietário de qualquer uma das funções de FSMO do Active Directory.

5. Na página Features, selecione o recurso ou os recursos a serem instalados. Se houver recursos adicionais obrigatórios para instalar um recurso que você selecionou, você verá uma caixa de diálogo adicional. Toque ou clique em Add Features para fechar a caixa de diálogo e adicionar os recursos obrigatórios para a instalação do servidor. Quando estiver pronto para prosseguir, toque ou clique em Next.

6. Com algumas das funções você verá uma página de assistente extra que fornece informações adicionais sobre o uso e a configuração da função. Pode ainda haver a possibilidade de instalar como parte de uma função alguns serviços de função adicionais. Para Print And Document Services, Web Server Role (IIS) e WSUS, por exemplo, você verá uma página de informações adicionais e uma página para a seleção de serviços de função a serem instalados juntamente com a função.
7. Na página Confirmation, toque ou clique no link Export Configuration Settings para gerar um relatório de instalação que pode ser exibido no Internet Explorer.
8. Se o servidor no qual você deseja instalar funções e serviços não possui todos os arquivos binários de origem necessários, o servidor buscará os arquivos através do Windows Update (por padrão) ou em um local especificado na Group Policy. Também pode-se especificar um caminho alternativo para os arquivos de origem. Para isso, clique no link Specify An Alternate Source Path, digite o caminho alternativo na caixa que aparece e toque ou clique em OK. Por exemplo: se uma imagem do Windows foi montada e disponibilizada no servidor local, como mostramos em "Princípios básicos do Server Manager e binários" anteriormente, pode-se digitar o caminho alternativo **c:\mountdir\ windows\winsxs**. Para compartilhamentos de rede, insira o caminho UNC para o compartilhamento, como por exemplo **\CorpServer82\WinServer2012**. Para imagens montadas do Windows, insira o caminho WIM com o prefixo **WIM:** e inclua o índice da imagem a ser usada, como por exemplo **WIM:\CorpServer82\WinServer2012\install.wim:4**.
9. Após examinar as opções de instalação e salvá-las se necessário, toque ou clique em Install para iniciar o processo de instalação. A página Installation Progress rastreia o progresso da instalação. Caso tenha fechado o assistente, toque ou clique no ícone Notifications no Server Manager e depois no link que aparece para reabrir o assistente.
10. Quando o assistente terminar a instalação do servidor com as funções e os recursos que você selecionou, a página Installation Progress será atualizada para mostrar isso. Examine os detalhes da instalação para se assegurar de que todas as fases de instalação foram realizadas com sucesso.
Observe qualquer ação adicional que possa ser necessária para finalizar a instalação, como reiniciar o servidor ou realizar tarefas de instalação adicionais.
Se alguma parte da instalação falhou, examine a causa da falha. Examine as entradas do Server Manager para problemas na instalação e realize as ações corretivas apropriadas.

Pode-se remover uma função de servidor ou um recurso seguindo as etapas:

1. No Server Manager, selecione Remove Roles and Features no menu Manage. Isso iniciará o Remove Roles And Features Wizard. Se o Assistente exibir a página Before You Begin, leia o texto introdutório e depois toque ou clique em Next. Para não visualizar essa página na próxima vez em que iniciar o Assistente, selecione a caixa de seleção Skip This Page By Default antes de clicar ou tocar em Next.
2. Na página Server Selection pode-se decidir pela remoção de funções e recursos de servidores em execução ou discos rígidos virtuais. Selecione um servidor do pool de servidores ou selecione um servidor do pool de servidores no qual montar um disco rígido virtual (VHD). Se estiver removendo funções e recursos de

um VHD, toque ou clique em Browse e depois use a caixa de diálogo Browse For Virtual Hard Disks para localizar o VHD. Quando estiver pronto para prosseguir, toque ou clique em Next.

3. Na página Server Roles, desmarque a caixa de seleção da função que você deseja remover. Se você tentar remover uma função de que depende outra função ou recurso, um aviso aparecerá informando que não é possível remover a função a menos que você também remova a outra função. Se você clicar ou tocar no botão Remove Features, o assistente removerá também as funções e recursos dependentes. Caso você queira manter as ferramentas de gerenciamento relacionadas, é preciso desmarcar a caixa de seleção Remove Management Tools antes de clicar ou tocar no botão Remove Features e depois clicar em Continue. Toque ou clique em Next.
4. Na página Features, os recursos instalados no momento estão selecionados. Para remover um recurso, desmarque a caixa de seleção referente. Se você tentar remover um recurso de que depende outro recurso ou função, um aviso aparecerá informando que não é possível remover o recurso a menos que você também remova o outro recurso ou função. Se você clicar ou tocar no botão Remove Features, o assistente removerá também as funções e recursos dependentes. Caso você queira manter as ferramentas de gerenciamento relacionadas, é preciso desmarcar a caixa de seleção Remove Management Tools e então clicar em Continue antes de clicar ou tocar no botão Remove Features. Toque ou clique em Next.
5. Na página Confirmation, examine os componentes relacionados que o assistente removerá tendo como base as suas seleções anteriores e toque ou clique em Remove. A página Removal Progress mostra o progresso da remoção. Caso tenha fechado o assistente, toque ou clique no ícone Notifications no Server Manager e depois no link que aparece para reabrir o assistente.
6. Quando o assistente concluir a modificação da configuração do servidor, você verá a página Removal Progress. Examine os detalhes da modificação para se assegurar de que todas as fases do processo de remoção foram realizadas com sucesso.

Observe qualquer ação adicional que possa ser necessária para finalizar a remoção, como reiniciar o servidor ou realizar tarefas de remoção adicionais.

Se alguma parte da remoção falhou, examine a causa da falha. Examine as entradas do Server Manager para problemas na remoção e realize as ações corretivas apropriadas.

Gerenciamento de propriedades do sistema

Utiliza-se o console System (Sistema) para visualizar informações do sistema e realizar tarefas de configuração básica. Para acessar o console System, toque ou clique duas vezes em System no Control Panel. Como mostra a Figura 2-5, o console System é dividido em quatro áreas básicas que oferecem links para a realização de tarefas comuns e uma visão geral do sistema:

- **Windows edition** Mostra a edição e a versão do sistema operacional e lista qualquer pacote de serviços (service pack) que você tenha aplicado.
- **System** Lista o processador, a memória e o tipo de sistema operacional instalado no computador. O tipo de sistema operacional é registrado como 32 bits ou 64 bits.

- **Computer Name, Domain, And Workgroup Settings** Fornece detalhes de nome do computador, descrição, domínio e grupos de trabalhos. Se desejar alterar alguma dessas informações, toque ou clique em Change Settings e na caixa de diálogo System Properties, toque ou clique em Change.
- **Windows Activation** Mostra se você ativou o sistema operacional e a chave do produto. Se o Windows Server 2012 ainda não estiver ativado, toque ou clique no link apresentado para iniciar o processo de ativação. Siga os avisos.

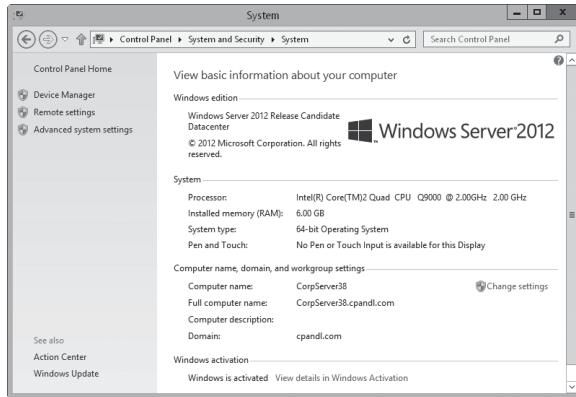


FIGURA 2-5 Utilize o Console System para visualizar e gerenciar propriedades do sistema.

Ao trabalhar com o console System, links no painel esquerdo oferecem acesso rápido às ferramentas-chave de suporte, incluindo:

- Device Manager
- Remote Settings
- Advanced System Settings

Ainda que versões de licenciamento por volume do Windows Server 2012 possam não exigir chaves de ativação ou de produto, versões comerciais do Windows Server 2012 requerem tanto chaves de ativação quanto de produto. Caso o Windows Server 2012 não tenha sido ativado, ative o sistema operacional ao selecionar Activate Windows Now em Windows Activation. Isso também pode ser feito se você digitar **slmgr -ato** em um prompt de comando.

Pode-se alterar a chave do produto que foi fornecida durante a instalação do Windows Server 2012 para que fique em conformidade com o seu plano de licenciamento. Em um prompt de comando, digite **slmgr -ipk** seguido pela chave de produto que você deseja utilizar e pressione a tecla Enter. Quando o Windows concluir a validação da chave do produto, será preciso reativar o sistema operacional.

OBSERVAÇÃO A ferramenta Windows Software Management Licensing apresenta muitas outras opções, incluindo opções para a ativação offline usando um identificador de confirmação. Para visualizar essa e outras opções, digite **slmgr** em um prompt de comando.

Dentro do console System pode-se acessar a caixa de diálogo System Properties e utilizar essa caixa para gerenciar as propriedades do sistema. Toque ou clique em Change Settings sob Computer Name, Domain e Workgroup Settings. As sessões seguintes examinam áreas-chave do sistema operacional que podem ser configuradas na caixa de diálogo System Properties.

A guia Computer Name

É possível exibir e modificar a identificação de rede do computador na guia Computer Name que fica na caixa de diálogo System Properties. A guia Computer Name exibe o nome completo do computador e do sistema e a associação do domínio. O nome completo do computador é basicamente o nome Domain Name System (DNS, Sistema de Nomes de Domínio) do computador, que também serve para identificar a posição do computador na hierarquia do Active Directory. Se um computador for um controlador de domínio ou uma autoridade de certificação só será possível alterar o nome do computador depois de remover do computador as funções relacionadas.

Para ingressar um computador em um domínio ou grupo de trabalho, siga as etapas:

1. Na aba Computer Name da caixa de diálogo System Properties, toque ou clique em Change. Isso exibirá a caixa de diálogo Computer Name/Domain Changes.
2. Para colocar o computador em um grupo de trabalho, selecione a opção Workgroup e depois digite o nome do grupo de trabalho onde deve ser adicionado.
3. Para ingressar o computador em um domínio, selecione a opção Domain, digite o nome do domínio onde deve ingressar e toque ou clique em OK.
4. Caso tenha alterado a associação ao domínio do computador, você verá um aviso do Windows Security. Insira o nome e a senha de uma conta com permissão para ingressar o computador no domínio especificado ou para remover o computador de um domínio especificado anteriormente. Toque ou clique em OK.
5. Quando o aviso de que o computador ingressou em um grupo de trabalho ou domínio especificado aparecer, toque ou clique em OK.
6. Você verá um aviso informando que é necessário reiniciar o computador. Toque ou clique em OK.
7. Toque ou clique em Close e em Restart Now para reiniciar o computador.

Para alterar o nome de um computador, siga estas etapas:

1. Na aba Computer Name da caixa de diálogo System Properties, toque ou clique em Change. Isso exibirá a caixa de diálogo Computer Name/Domain Changes.
2. Na caixa de texto Computer Name, digite um novo nome para o computador.
3. Você verá um aviso informando que é necessário reiniciar o computador. Toque ou clique em OK.
4. Toque ou clique em Close e em Restart Now para reiniciar o computador.

A guia Hardware

Na guia hardware da caixa de diálogo System Properties você pode acessar o Device Manager (Gerenciador de Dispositivos) e Advanced System Settings (Configurações

Avançadas do Sistema). Para acessar a guia hardware, abra a caixa de diálogo System Properties e toque ou clique na guia Hardware.

No caso de dispositivos instalados, você pode configurar o Windows Server para baixar software de drivers e ícones realistas para dispositivos. O Windows Server não faz isso por padrão. Se você deseja que um computador verifique se há drivers automaticamente, toque ou clique no botão Device Installation Settings e selecione Yes, Do This Automatically ou No, Let Me Choose What To Do. Se optar por escolher o que fazer, você pode especificar:

- Sempre instalar o melhor software de driver do Windows Update
- Nunca instalar o software de driver do Windows Update
- Buscar automaticamente os aplicativos e as informações do dispositivo oferecidos pelo fabricante do dispositivo

As primeiras duas opções fazem exatamente aquilo que descrevem. Já a última opção diz ao Windows Update que você deseja receber metadados e aplicativos complementares para dispositivos. Toque ou clique em Save Changes e depois em OK para aplicar as alterações.

A guia Advanced

A guia Advanced do utilitário System controla vários dos recursos-chave do sistema operacional do Windows, incluindo desempenho de aplicativos, uso da memória virtual, perfil do usuário, variáveis de ambiente e inicialização e recuperação. Para acessar a guia Advanced, abra a caixa de diálogo System Properties e toque ou clique na guia Advanced.

Como configurar o desempenho do Windows

Muitos aprimoramentos gráficos foram adicionadas à interface do Windows Server 2008 e continuam disponíveis nas versões posteriores. Essas melhorias incluem efeitos visuais para menus, barras de ferramentas, janelas e barra de tarefas. Para configurar o desempenho do Windows, siga as etapas:

1. Toque ou clique na guia Advanced na caixa de diálogo System Properties e em Settings no painel Performance para exibir a caixa de diálogo Performance Options.
2. A guia Visual Effects está selecionada por padrão. Para controlar os efeitos visuais, você tem as seguintes opções:
 - **Let Windows Choose What's Best For My Computer** Permite que o sistema operacional escolha as opções de desempenho tendo como base a configuração de hardware. Para um computador mais novo, essa opção deve surtir o mesmo efeito que a opção Adjust For Best Appearance. A principal diferença é que essa opção é escolhida pelo Windows com base no hardware disponível e na sua capacidade de desempenho.
 - **Adjust For Best Appearance** Ao otimizar o Windows para uma melhor aparência, você habilita todos os efeitos visuais e interfaces gráficas. Os menus e a barra de tarefas utilizam transições e sombras. As fontes de telas possuem cantos arredondados. As caixas de listagem são roladas suavemente. As pastas usam modos de exibição da Web e mais.

- **Adjust For Best Performance** Ao otimizar o Windows para um melhor desempenho, são desligados os efeitos visuais com uso intensivo de recursos, como transições de slide e cantos arredondados para fontes, sendo mantido um conjunto básico de efeitos visuais.
 - **Custom** Para personalizar os efeitos visuais, marque ou desmarque as opções de efeitos visuais na caixa de diálogo Performance Options. Se você desmarcar todas as opções, o Windows não utilizará efeitos visuais.
3. Toque ou clique em Apply quando terminar as alterações de efeitos visuais. Toque ou clique duas vezes em OK para fechar as caixas de diálogo abertas.

Como configurar o desempenho de aplicativos

O desempenho dos aplicativos está relacionado às opções de cache de agendamento do processador que você configurou para o sistema Windows Server 2012. O agendamento do processador determina a capacidade de resposta dos aplicativos que estão sendo executados interativamente (em oposição a aplicativos em segundo plano que possam estar sendo executados como serviços no sistema). Para controlar o desempenho de aplicativos, siga as etapas:

1. Acesse a guia Advanced na caixa de diálogo System Properties. Toque ou clique em Settings no painel Performance para exibir a caixa de diálogo Performance Options.
2. Na caixa de diálogo Performance Options, toque ou clique na guia Advanced.
3. No painel Processor Scheduling (Agendamento do Processador), as seguintes opções são apresentadas:
 - **Programs** Utilize essa opção para conferir ao aplicativo ativo o melhor tempo de resposta e a maior parte dos recursos disponíveis. Normalmente, você só usará essa opção em servidores de desenvolvimento ou quando estiver usando o Windows Server 2012 como sistema operacional de desktop.
 - **Background Services** Utilize essa opção para dar um melhor tempo de resposta aos aplicativos em segundo plano do que ao aplicativo ativo. Normalmente, essa opção é utilizada para servidores de produção.
4. Toque ou clique em OK.

Como configurar a memória virtual

Com a memória virtual, pode-se utilizar o espaço em disco para aumentar a memória disponível em um sistema, usando uma parcela do disco rígido como parte da memória do sistema. Esse recurso grava parte do conteúdo da memória RAM em discos através de um processo chamado *paging* (paginação). Com a paginação, uma área definida para ser usada como memória RAM, como, por exemplo, 8192 megabytes (MB), é gravada no disco como um arquivo de paginação. Quando necessário, o arquivo de paginação pode ser usado no disco em vez da memória física RAM.

Um arquivo de paginação inicial é criado automaticamente na unidade que contém o sistema operacional. As outras unidades não possuem arquivos de paginação por padrão e, se você quiser, é preciso criá-los. Ao criar um arquivo de paginação, você

define um tamanho inicial e um tamanho máximo. Arquivos de paginação são gravados no volume como um arquivo nomeado Pagefile.sys.

MUNDO REAL As versões atuais do Windows Server fazem o gerenciamento automático da memória virtual muito melhor que as versões mais antigas. Normalmente, o Windows Server aloca a memória virtual em uma quantidade pelo menos igual à memória física total instalada no computador. Isso ajuda a garantir que arquivos de paginação não sejam fragmentados, o que poderia resultar em um desempenho ruim do sistema. Se você deseja gerenciar a memória virtual manualmente, deve usar um tamanho de memória virtual fixo na maioria dos casos. Para isso, defina um mesmo valor para o tamanho inicial e para o tamanho máximo. Isso assegura que o arquivo de paginação seja consistente e possa ser gravado em um único arquivo contíguo (se possível, dependendo da quantidade de espaço livre no volume). Na maioria dos casos, para computadores com 8 GB de memória RAM ou menos, recomenda-se definir o tamanho total de arquivos de paginação em um valor que seja o dobro da memória física RAM no sistema. Em um computador com 8 GB de RAM, por exemplo, você definiria a configuração Total Paging File Size For All Drives em pelo menos 16,384 MB. Em sistemas com mais de 8GB de RAM, deve-se seguir as diretrizes do fabricante do hardware para fazer a configuração do arquivo de paginação. Isso normalmente significa configurar o arquivo de paginação para ter o mesmo tamanho da memória física.

Para configurar a memória virtual, siga as etapas:

1. Acesse a guia Advanced na caixa de diálogo System Properties. Toque ou clique em Settings no painel Performance para exibir a caixa de diálogo Performance Options.
2. Na caixa de diálogo Performance Options, toque ou clique na guia Advanced e depois em Change para exibir a caixa de diálogo Virtual Memory, como mostra a Figura 2-6.

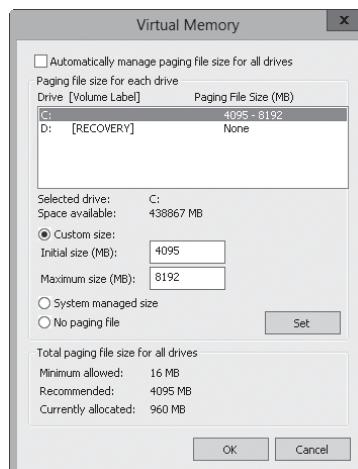


FIGURA 2-6 A memória virtual aumenta a quantidade de RAM de um sistema.

São fornecidas as seguintes informações:

- **Paging File Size For Each Drive** Fornece informações sobre a unidade selecionada no momento e permite que você defina o tamanho do arquivo de paginação. Space Available indica quanto espaço está disponível na unidade.
 - **Drive [Volume Label] and Paging File Size** Mostra a configuração atual da memória virtual no sistema. Cada volume é listado com o seu arquivo de paginação referente (se houver). O intervalo do arquivo de paginação mostra os valores definidos para o tamanho inicial e para o tamanho máximo.
 - **Total Paging File Size For All Drives** Fornece um tamanho recomendado para a memória RAM virtual no sistema e informa a quantidade alocada no momento. Se esta é a primeira vez que você está configurando uma memória RAM virtual, observe que a quantidade recomendada já foi conferida à unidade do sistema (na maioria das instâncias).
3. O Windows Server gerencia o tamanho de arquivos de paginação para todas as unidades por padrão. Se quiser configurar a memória virtual manualmente, desmarque a caixa de seleção Automatically Manage Paging File Size For All Drives.
 4. Na lista Drive, selecione o volume com o qual deseja trabalhar.
 5. Selecione Custom Size e depois insira valores nas caixas Initial Size (Tamanho Inicial) e Maximum Size (Tamanho Máximo).
 6. Toque ou clique em Set para salvar as alterações.
 7. Repita as etapas de 4 a 6 para cada volume que quiser configurar.

OBSERVAÇÃO O arquivo de paginação também é usado para fins de depuração quando ocorre um erro de parada no sistema. Se o arquivo de paginação na unidade do sistema for menor que o tamanho mínimo necessário para a gravação de informações de depuração no arquivo de paginação, esse recurso é desabilitado. Se você deseja usar a depuração, defina um tamanho mínimo igual à quantidade de RAM no sistema. Por exemplo: um sistema com 4 GB de RAM precisaria de um arquivo de paginação de 4 GB na unidade do sistema.

8. Toque ou clique em OK. Se aparecer um aviso de que você irá substituir um arquivo Pagefile.sys existente, toque ou clique em Yes.
9. Se você atualizou as configurações para um arquivo de paginação que está em uso no momento, você verá um aviso indicando que é preciso reiniciar o sistema para que as alterações tenham efeito. Toque ou clique em OK.
10. Toque ou clique duas vezes em OK para fechar as caixas de diálogo abertas. Ao fechar o utilitário System, você verá um aviso perguntando se você deseja reiniciar o sistema. Toque ou clique em Restart.

Para que o Windows Server 2012 gerencie automaticamente a memória virtual, siga as etapas:

1. Acesse a guia Advanced na caixa de diálogo System Properties. Toque ou clique em Settings no painel Performance para exibir a caixa de diálogo Performance Options.
2. Toque ou clique na guia Advanced e depois em Change para exibir a caixa de diálogo Virtual Memory.

3. Marque a caixa de seleção Automatically Manage Paging File Size For All Drives.
4. Toque ou clique em OK três vezes para fechar todas as caixas de diálogo.

OBSERVAÇÃO Se você atualizou as configurações para o arquivo de paginação em uso no momento, você verá um aviso indicando que é preciso reiniciar o servidor para que as alterações tenham efeito. Toque ou clique em OK. Quando você fechar a caixa de diálogo System Properties, verá um aviso informando que é preciso reiniciar o sistema para que as alterações tenham efeito. Em um servidor de produção, deve-se agendar essa reinicialização fora do horário comercial.

Como configurar a Data Execution Prevention

A Data Execution Prevention (DEP, Prevenção de Execução de Dados) é uma tecnologia de proteção da memória. A DEP diz ao processador do computador para marcar todos os locais usados na memória por um aplicativo como conteúdos não executáveis, a menos que o local contenga claramente um código executável. Se um código for executado a partir de uma página de memória marcada como não executável, o processador pode criar uma exceção e evitar a execução. Isso evita que códigos mal-intencionados, como vírus, se infiltrarem na maioria das áreas da memória, porque apenas áreas específicas da memória são marcadas como possuindo códigos executáveis.

OBSERVAÇÃO Versões de 32 bits do Windows suportam a DEP como é implementada pelos processadores Advanced Micro Devices (AMD) que oferecem o recurso no-execute page-protection (NX). Esses processadores suportam as instruções relacionadas e devem ser executados no modo Physical Address Extension (PAE, Extensão de Endereço Físico). As versões de 64 bits do Windows também suportam o recurso de processador da proteção NX.

COMO USAR E CONFIGURAR A DEP

Pode-se determinar se um computador suporta a DEP através do utilitário System. Se o computador suportar a DEP, siga as etapas para realizar a configuração:

1. Acesse a guia Advanced na caixa de diálogo System Properties. Toque ou clique em Settings no painel Performance para exibir a caixa de diálogo Performance Options.
2. Na caixa de diálogo Performance Options, toque ou clique na guia Data Execution Prevention. O texto no final dessa guia indica se o computador suporta a proteção de execução.
3. Se o computador suporta a proteção de execução e possui uma configuração apropriada, pode-se configurar a DEP usando uma das seguintes opções:
 - **Turn On DEP For Essential Windows Programs And Services Only** Habilite a DEP apenas para serviços, programas e componentes do sistema operacional. Essa é a opção padrão e recomendada para computadores que suportam proteção de execução e possuem a configuração apropriada.
 - **Turn On DEP For All Programs Except Those I Select** Configura a DEP e as permissões para exceções. Selecione essa opção e depois clique e toque em Add para especificar os programas que devem ser executados sem a proteção de execução. Com essa opção, a proteção de execução funcionará para todos os programas exceto os que você selecionou.
4. Toque ou clique em OK.

Se você ativou a DEP e permitiu exceções, siga as etapas para adicionar ou remover um programa definido como exceção:

1. Acesse a guia Advanced na caixa de diálogo System Properties. Toque ou clique em Settings no painel Performance para exibir a caixa de diálogo Performance Options.
2. Na caixa de diálogo Performance Options, toque ou clique na guia Data Execution Prevention.
3. Para adicionar um programa como uma exceção, toque ou clique em Add. Use a caixa de diálogo Open para localizar o arquivo executável do programa que está sendo configurado como exceção e depois toque ou clique em Open.
4. Para desabilitar temporariamente a exceção a um programa (o que pode ser necessário para alguma solução de problemas), desmarque a caixa de seleção ao lado do nome do programa.
5. Para remover a exceção de um programa, toque ou clique no nome do programa e depois em Remove.
6. Toque ou clique em OK para salvar as alterações.

Noções básicas sobre DEP Compatibility

Para serem compatíveis com a DEP, os aplicativos devem marcar explicitamente a memória com a permissão Execute. Os aplicativos que não tiverem essa capacidade não serão compatíveis com este recurso NX do processador. Caso você tenha problemas relacionados à memória ao executar aplicativos, determine quais são os aplicativos com problemas e configure-os como exceções em vez de desativar completamente a proteção de execução. Dessa forma você ainda terá os benefícios da proteção da memória, podendo desativá-la seletivamente para programas que não sejam executados da forma adequada com o recurso NX do processador.

A proteção de execução é aplicada tanto em programas modo usuário quanto modo kernel. Uma exceção da proteção de execução do modo usuário resulta em uma exceção STATUS_ACCESS_VIOLATION. Na maioria dos processos, essa exceção será uma exceção sem tratamento, resultando no término do processo. Esse é o comportamento desejável porque a maioria dos programas que violam essas regras, como vírus e worms, serão mal-intencionados nesse aspecto.

Não é possível habilitar ou desabilitar seletivamente (como se pode fazer com aplicativos) a proteção de execução para drivers de dispositivos de modo kernel. Além disso, em sistemas compatíveis com 32 bits, a proteção de execução é aplicada por padrão à pilha de memória. Em sistemas compatíveis com 64 bits, a proteção de execução é aplicada por padrão à pilha de memória, à reserva de memória paginável e ao pool de sessão. A violação de acesso de uma proteção de execução de modo kernel para um driver de dispositivo resulta em uma exceção ATTEMPTED_EXECUTE_OF_NOEXECUTE_MEMORY.

Como configurar variáveis de ambiente do usuário e do sistema

O Windows usa variáveis de ambiente para controlar cadeias importantes, como por exemplo um caminho onde estejam localizados os arquivos ou o nome de host do controlador de domínio de logon. As variáveis de ambiente definidas para o uso pelo Windows – chamadas *system environment variables* – são as mesmas, independentemente

mente de quem está logado em um determinado computador. As variáveis de ambiente definidas por usuários ou programas – chamadas *user environment variables* – são diferentes para cada usuário de um determinado computador.

As variáveis de ambiente do sistema e do usuário são configuradas na caixa de diálogo Environment Variables, como mostra a Figura 2-7. Para acessar essa caixa de diálogo, abra a caixa de diálogo System Properties, toque ou clique na guia Advanced e depois em Environment Variables.

COMO CRIAR UMA VARIÁVEL DE AMBIENTE

Para criar uma variável de ambiente, siga as etapas:

1. Toque ou clique em New, sob User Variables ou System Variables, dependendo do que você deseja. Isso abrirá a caixa de diálogo New User Variable ou New System Variable, respectivamente.
2. Na caixa de texto Variable Name, digite o nome da variável. Na caixa de texto Variable Value, digite o valor da variável.
3. Toque ou clique em OK.

COMO EDITAR UMA VARIÁVEL DE AMBIENTE

Para editar uma variável de ambiente, siga as etapas:

1. Selecione a variável na lista User Variables ou na lista System Variables.
2. Toque ou clique em Edit, sob User Variables ou System Variables, dependendo do que você deseja. Isso abrirá a caixa de diálogo Edit User Variable ou Edit System Variable, respectivamente.
3. Insira um novo valor na caixa de texto Variable Value e depois toque ou clique em OK.

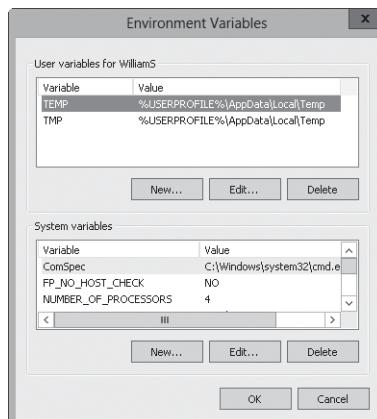


FIGURA 2-7 Configure variáveis de ambiente do usuário ou do sistema na caixa de diálogo Environment Variables.

COMO EXCLUIR UMA VARIÁVEL DE AMBIENTE

Para excluir uma variável de ambiente, selecione-a e toque ou clique em Delete.

OBSERVAÇÃO Ao criar e alterar variáveis de ambiente, a maioria das variáveis serão válidas imediatamente depois que forem criadas ou alteradas. Com variáveis do sistema, algumas alterações terão efeito após reiniciar o computador. Com variáveis do usuário, algumas alterações terão efeito na próxima vez que o usuário fizer logon no sistema.

Como configurar a inicialização e a recuperação do sistema

A configuração de propriedades de inicialização e recuperação do sistema é feita na caixa de diálogo Startup And Recovery, como mostra a Figura 2-8. Para acessar essa caixa de diálogo, abra a caixa de diálogo System Properties, toque ou clique na guia Advanced e depois em Settings, no painel Startup and Recovery.

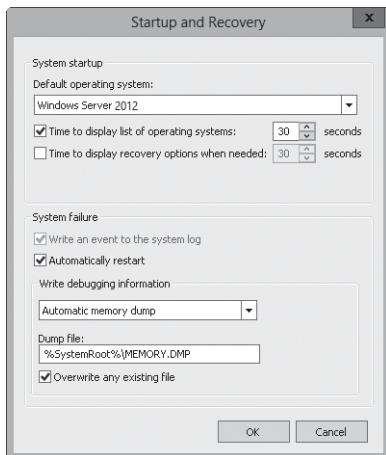


FIGURA 2-8 Configure as propriedades de inicialização e recuperação do sistema na caixa de diálogo Startup And Recovery.

PARA CONFIGURAR AS OPÇÕES DE INICIALIZAÇÃO

A área System Startup da caixa de diálogo Startup And Recovery controla a inicialização do sistema. Para definir o sistema operacional padrão para um computador com múltiplas inicializações de sistemas operacionais, selecione um dos sistemas operacionais que constam na lista Default Operating System. Essas opções alteram as configurações usadas pelo Windows Boot Manager (Gerenciador de Inicialização do Windows).

Por padrão, ao inicializar um computador com múltiplas inicializações de sistemas operacionais, o Windows Server exibe o menu de configuração de inicialização por 30 segundos. Isso pode ser alterado com uma das seguintes ações:

- Para inicializar imediatamente o sistema operacional padrão, desmarque a caixa de seleção Time To Display List Of Operating Systems.

- Para exibir as opções disponíveis por um determinado espaço de tempo, selecione a caixa de seleção Time To Display List Of Operating Systems e defina um tempo de espera em segundos.

Na maioria dos sistemas, utiliza-se um valor entre três e cinco segundos. É tempo suficiente para fazer a seleção e curto o bastante para acelerar o processo de inicialização do sistema.

Quando o sistema estiver em modo de recuperação ao inicializar, pode ser exibida uma lista de opções de recuperação. Da mesma forma que se pode fazer com opções de inicialização padrão, é possível configurar as opções de recuperação na inicialização em uma das seguintes maneiras. Você pode configurar o computador para inicializar imediatamente usando a opção de recuperação padrão. Para isso, desmarque a caixa de seleção Time To Display Recovery Options When Needed. A outra forma é configurá-lo para exibir as opções disponíveis por um determinado tempo. Para isso, selecione Time To Display Recovery Options When Needed e configure um tempo de espera em segundos.

CÓMO CONFIGURAR AS OPÇÕES DE RECUPERAÇÃO

A recuperação do sistema é controlada nas áreas System Failure e Write Debugging Information da caixa de diálogo Startup And Recovery. Os administradores utilizam as opções de recuperação para controlar com precisão o que ocorre quando o sistema encontra um erro fatal do sistema (também conhecido como erro de parada). As opções disponíveis para a área System Failure são:

- **Write An Event To The System Log** Seleccione essa opção para registrar o erro no log do sistema, possibilitando que os administradores examinem o erro mais tarde no Event Viewer.
- **Automatically Restart** Seleccione essa opção para que o sistema tente reiniciar quando ocorrer um erro fatal do sistema.

OBSERVAÇÃO Nem sempre é bom configurar reinicializações automáticas. Às vezes pode ser preferível que o sistema pare em vez de reiniciar, garantindo que o sistema receba a atenção necessária. Caso contrário, você só descobriria que o sistema foi reinicializado quando visualizasse os logs do sistema ou se por acaso estivesse na frente do monitor no momento em que o sistema reinicializasse.

A lista Write Debugging Information é usada para escolher o tipo de informação de depuração que você deseja gravar em um arquivo de despejo. Os arquivos de despejo (dump) podem ser utilizados para diagnosticar falhas no sistema. As opções são:

- **None** Use essa opção caso não deseje gravar informações de depuração.
- **Small Memory Dump** Use essa opção para despejar o segmento de memória física em que ocorreu o erro. Esse despejo possui 256 KB.
- **Kernel Memory Dump** Use essa opção para despejar a área de memória física sendo utilizada pelo kernel do Windows. O tamanho do arquivo de despejo (dump) depende do tamanho do kernel do Windows.
- **Complete Memory Dump** Use essa opção para despejar toda a memória física. O tamanho do arquivo de despejo depende da quantidade de memória física sendo usada, podendo ter até o tamanho igual ao total da memória física RAM no servidor.

- **Automatic Memory Dump** Use essa opção para deixar que o Windows determine que tipo de despejo de memória é melhor e crie o arquivo de despejo adequado.

Se você escolher fazer a gravação de um arquivo de despejo, é preciso definir um local. Os locais de despejo padrão são %SystemRoot%\Minidump para despejos de memória pequenos e %SystemRoot%\Memory.dmp para os outros despejos de memória. Normalmente, você também selecionará Overwrite Any Existing File. A seleção dessa opção garante que qualquer arquivo de despejo existente seja substituído se ocorrer um novo erro de parada.

MELHORES PRÁTICAS Só é possível criar o arquivo de despejo se o sistema estiver com a configuração adequada. A unidade do sistema deve ter um arquivo de paginação suficientemente grande (como foi definido para a memória virtual na guia Advanced) e a unidade na qual o arquivo de despejo será gravado deve possuir espaço livre suficiente. O meu servidor, por exemplo, possui 8 GB de RAM e requer um arquivo de paginação do mesmo tamanho na unidade do sistema (8 GB). Ao estabelecer uma linha de base para o uso de memória kernel, descobriu-se que o servidor usa entre 892 e 1076 MB de memória kernel. Como a mesma unidade é usada para o arquivo de despejo, a unidade deve ter ao menos 9 GB de espaço livre para criar um despejo de informações de depuração. (Isto é: 8 GB para o arquivo de paginação e em torno de 1 GB para o arquivo de despejo.)

A guia Remote

A guia Remote da caixa de diálogo System Properties controla Remote Assistance invitations e Remote Desktop connections. Essas opções serão discutidas no Capítulo 4.

CAPÍTULO 3

Monitoramento de processos, serviços e eventos

- Gerenciamento de aplicativos, processos e desempenho **85**
- Gerenciamento de serviços do sistema **98**
- Log e visualização de eventos **106**
- Monitoramento de desempenho e atividade do servidor **116**
- Ajuste do desempenho do sistema **128**

Como administrador, você precisa ficar atento aos sistemas em rede. O status e o uso dos recursos do sistema podem se alterar drasticamente ao longo do tempo; os serviços podem parar de funcionar; os sistemas de arquivos podem ficar sem espaço; os aplicativos podem permitir exceções que, por sua vez, podem causar problemas no sistema; usuários não autorizados podem tentar invadir o sistema. As técnicas abordadas neste capítulo podem ajudar a identificar e solucionar esses e outros problemas do sistema.

Gerenciamento de aplicativos, processos e desempenho

Toda vez que iniciar um aplicativo ou digitar um comando na linha de comando, o Microsoft Windows Server iniciará um ou mais processos para lidar com o programa relacionado. Geralmente, os processos iniciados dessa maneira são chamados de *processos interativos* – , ou seja, você inicia os processos interativamente com o teclado ou o mouse. Se o aplicativo ou programa estiver ativo e selecionado, o processo interativo tem controle sobre o teclado e o mouse até que o controle seja alternado encerrando o programa ou selecionando outro. Quando um processo tem o controle, é dito que está sendo executando *em primeiro plano*.

Os processos também podem ser executados *em segundo plano*. Para processos iniciados por usuários, isso significa que os programas que não estejam ativos no momento podem continuar a operar, só que, geralmente, não terão a mesma prioridade que os processos ativos. Você também pode configurar os processos em segundo plano para execução independentemente da sessão de logon do usuário; o sistema operacional normalmente inicializa esses processos. Um exemplo desse tipo de processo em segundo plano é uma tarefa agendada executada pelo sistema operacional. As configurações para a tarefa dizem ao sistema para executar um comando em um momento especificado.

Task Manager

A principal ferramenta utilizada para gerenciar processos do sistema e aplicativos é o Task Manager (Gerenciador de Tarefas). Você pode utilizar qualquer uma das técnicas a seguir para exibi-lo:

- Pressionar Ctrl+Shift+Esc.
- Pressionar Ctrl+Alt+Del e tocar ou clicar em Task Manager.
- Pressionar a tecla Windows, digitar **taskmgr** e pressionar Enter.
- Pressionar e segurar ou clicar com o botão direito do mouse na barra de tarefas e tocar ou clicar em Task Manager no menu de atalho.

OBSERVAÇÃO Ao pressionar a tecla Windows e digitar **taskmgr**, você verá duas correspondências. Uma correspondência é o nome completo, Task Manager. A outra é o nome do comando, taskmgr.

As seções a seguir abrangem técnicas usadas trabalhando com o Task Manager.

Como visualizar e trabalhar com processos

O Task Manager tem dois modos gerais de exibição:

- **Summary (resumido)** Mostra apenas os aplicativos em execução em primeiro plano, o que permite rapidamente selecionar e trabalhar com aplicativos em primeiro plano
- **Expanded (expandido)** Expande o modo de exibição, apresentando guias adicionais que podem ser utilizadas para obter informações sobre todos os processos em execução, o desempenho do sistema, os usuários conectados e os serviços configurados

Se estiver no modo de exibição resumido, pode alternar para o modo de exibição expandido tocando ou clicando em More Details. Se estiver no modo de exibição expandido, pode alternar para o modo de exibição resumido tocando ou clicando em Fewer Details. Ao fechar e reabrir o Task Manager, o modo de exibição utilizado na última vez será exibido.

Geralmente, como administrador, você trabalhará no modo de exibição expandido. Como mostrado na Figura 3-1, o modo de exibição expandido tem várias tabelas que podem ser selecionadas para trabalhar com processos em execução, desempenho do sistema, usuários conectados e serviços configurados. A guia Processes, também mostrada na Figura 3-1, exibe o status geral dos processos. Os processos estão agrupados por tipo e listados alfabeticamente dentro de cada tipo por padrão. Há três tipos gerais:

- Apps, que são programas em execução em primeiro plano
- Background processes, que são programas em execução em segundo plano
- Windows processes, que são processos executados pelo sistema operacional

OBSERVAÇÃO A opção Group By Type no menu View controla se o agrupamento é utilizado. Se desmarcar essa opção, todos os processos serão listados alfabeticamente sem agrupamento por tipo. Note também que você pode iniciar um novo programa no Task Manager tocando ou clicando em Run New Task no menu File e digitando um comando para executar o aplicativo. As opções incluem execução da tarefa com privilégios de Administrador e pesquisa para localizar o executável com o qual quer trabalhar.

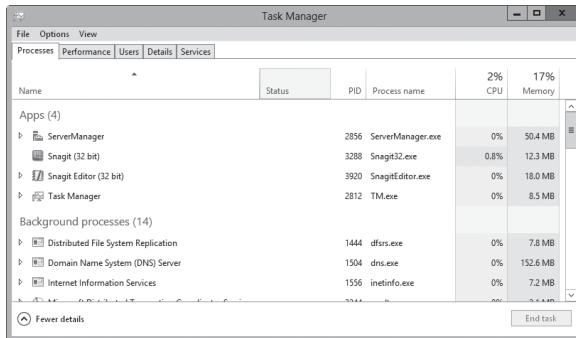


FIGURA 3-1 Visualize o status dos processos em execução no momento no servidor.

MUNDO REAL Muitos processos do Windows também são agrupados pelo host de serviço (Service Host) sob o qual estão em execução, que pode incluir Local Service, Local System e Network Service. O número de processos agrupados é mostrado entre parênteses e você pode expandir o nó relacionado para visualizar os processos reais. Selecione Expand All no menu View para expandir todos os grupos de processos para uma visualização facilitada.

A coluna Status informa se o aplicativo está em execução normalmente ou parou de responder. Um status em branco é normal e indica que o processo está em execução normalmente. Qualquer outro status indica um problema, como quando um aplicativo pode estar travado e você talvez queira encerrar a tarefa relacionada a ele. Contudo, alguns aplicativos podem não responder ao sistema operacional durante certas tarefas que exijam muitos processos. Por causa disso, você deve estar seguro de que o aplicativo realmente está travado antes de encerrar sua tarefa relacionada.

Pode-se interromper um processo selecionando-o e tocando ou clicando em End Task. Você não deve tentar interromper processos do Windows utilizando essa técnica. Se tentar interromper um processo do Windows ou um grupo deles, o Task Manager exibirá um aviso similar ao mostrado na Figura 3-2. Esse aviso informa que a interrupção desse processo fará com que o Windows se torne não utilizável ou se desligue. Para prosseguir, você deve selecionar Abandon Unsaved Data And Shut Down e toque ou clique em Shut Down. O Windows exibirá uma tela azul com um código de erro. Após reunir as informações sobre o erro, o Windows será reiniciado.

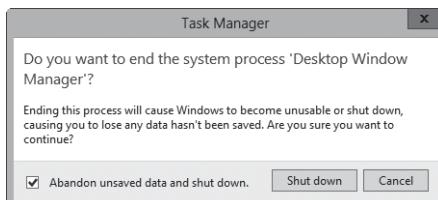


FIGURA 3-2 A interrupção de processos de serviços essenciais do Windows faz com que ele se torne inutilizável ou se desligue.

Outras colunas na guia Processes fornecem muitas informações sobre os processos em execução. Você pode utilizar essas informações para determinar quais processos estão consumindo demasiados recursos do sistema, como tempo de CPU e memória. Embora apenas as colunas CPU e Memory sejam exibidas por padrão, outras podem ser adicionadas pressionando e segurando ou clicando com o botão direito do mouse no cabeçalho de qualquer coluna e selecionando as opções para a exibição das colunas adicionais. Além de nome e status, as outras colunas disponíveis incluem:

- **CPU** O percentual de utilização da CPU para o processo (em todos os núcleos). O valor em negrito no cabeçalho da coluna representa o total de utilização da CPU para o servidor (em todos os núcleos).
- **Memory** O total de memória física reservado para o processo. O valor em negrito no cabeçalho da coluna representa o total de utilização de memória física para o servidor.
- **Command Line** O caminho completo do arquivo executável do processo, bem como qualquer argumento de linha de comando passado quando o processo foi iniciado.
- **PID** O identificador numérico do processo.
- **Process Name** O nome do processo ou do executável do processo.
- **Publisher** Lista o fornecedor do processo, como a Microsoft Corporation.
- **Type** Exibe o tipo geral de processo, como aplicativo, processo em segundo plano ou processo do Windows. Essas informações serão úteis caso a opção Group By Type no menu View seja desmarcada.

Pressionando e segurando ou clicando com o botão direito do mouse no aplicativo listado no Task Manager, um menu de atalho será exibido que pode ser usado para:

- Finalizar a tarefa do aplicativo
- Criar um arquivo de despejo para depurar o processo
- Ir para o processo relacionado na guia Details
- Abrir a localização do arquivo executável relacionado
- Abrir a caixa de diálogo Properties do executável relacionado

OBSERVAÇÃO A opção Go To Details é muito útil quando se tenta localizar o processo principal de um aplicativo específico. A seleção dessa opção destaca o processo relacionado na guia Details.

Administração de Processos

A guia Details do Task Manager é mostrada na Figura 3-3. Essa guia fornece informações detalhadas sobre os processos em execução. As colunas exibidas por padrão na guia Details são similares às apresentadas na guia Processes:

- **Name** O nome do processo ou do executável do processo
- **User Name** O nome do usuário ou do serviço do sistema executando o processo

- **CPU** O percentual de utilização da CPU pelo processo
- **Memory (Private Working Set)** A quantidade de memória física reservada pelo processo
- **Status** O status de execução do processo
- **Description** Uma descrição do processo

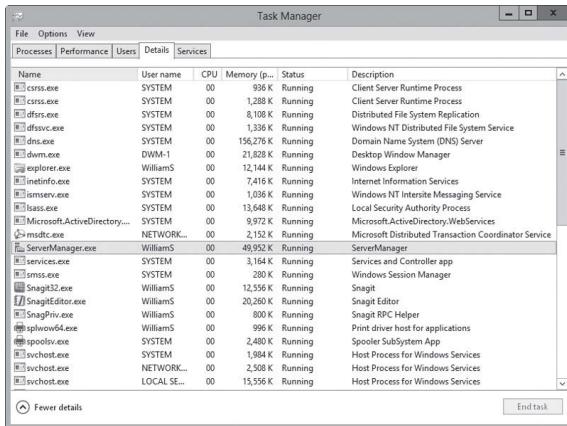


FIGURA 3-3 A guia Details fornece informações detalhadas sobre os processos em execução.

Outras colunas podem ser adicionadas pressionando ou segurando ou clicando com o botão direito do mouse no cabeçalho de qualquer coluna e tocando ou clicando em Select Columns. Quando estiver tentando solucionar problemas do sistema utilizando informações de processos, talvez queira adicionar as seguintes colunas à exibição:

- **Base Priority** A prioridade determina quanto dos recursos do sistema será alocado para um processo. Para definir a prioridade de um processo, pressione e segure ou clique com o botão direito do mouse nele, escolha Set Priority e selecione a nova prioridade a partir destas opções: Low, Below Normal, Normal, Above Normal, High e RealTime. A maioria dos processos tem uma prioridade normal por padrão. A prioridade mais alta é dada aos processos em tempo real.
- **CPU Time** A quantidade total do tempo do ciclo da CPU utilizada por um processo desde que foi iniciado. Para ver rapidamente os processos que estão utilizando mais tempo da CPU, exiba esta coluna e toque ou clique no cabeçalho dela para classificar as entradas de processos por tempo de CPU.
- **Data Execution Protection** Especifica se a DEP está habilitada ou desabilitada para o processo.
- **Elevated** Especifica se o processo está sendo executado com privilégios elevados de administrador.

- **Handles** O número total de arquivos manipulados e mantidos pelo processo. Utilize o número de handles para aferir quão dependente o processo é do sistema de arquivos. Alguns processos, como os utilizados pelo Microsoft Internet Information Services (IIS, Serviços de Informações da Internet da Microsoft), têm milhares de handles de arquivos abertos. Cada manipulador de arquivo requer memória do sistema para ser mantido.
- **I/O Reads, I/O Writes** O número total de leituras ou gravações de entrada/saída de disco (I/O) desde que o processo foi iniciado. Juntos, os números de leituras e gravações de I/O informam quanta atividade de I/O de disco ocorreu. Se o número de leituras e gravações de I/O estiver crescendo desproporcionalmente à atividade real no servidor, o processo pode não estar armazenando arquivos em cache ou esse armazenamento pode não estar configurado adequadamente. De maneira ideal, o armazenamento de arquivos em cache reduz a necessidade de leituras e gravações de I/O.
- **Page Faults** Uma falha de página ocorre quando um processo solicita uma página na memória e o sistema não consegue localizá-la no local solicitado. Se a página solicitada estiver em outro lugar da memória, a falha é chamada de *soft page fault* (falha de página menor). Se a página solicitada tiver de ser recuperada do disco, a falha é chamada de *hard page fault* (falha de página maior). A maioria dos processadores pode lidar com grandes quantidades de falhas menores. As falhas maiores, no entanto, podem causar atrasos significativos.
- **Paged Pool, NP Pool** *Paged pool* (*reserva de memória paginável*) é uma área da memória do sistema para objetos que podem ser gravados em disco quando não são utilizados. *NP pool*, ou *nonpaged pool* (*reserva de memória não paginável*), é uma área da memória do sistema para objetos que não podem ser gravados em disco. Deve-se observar os processos que exigem uma grande quantidade de memória da reserva de memória não paginável. Se não houver memória livre suficiente no servidor, esses processos podem ser a razão de um alto nível de falhas de página.
- **Peak Working Set** A mais alta quantidade de memória utilizada pelo processo. Também é importante notar a alteração, ou delta, entre o uso de memória atual e o pico do uso de memória. Os aplicativos que têm um alto delta entre o uso básico de memória e o pico do uso de memória, como o Microsoft SQL Server, podem necessitar de mais memória alocada na inicialização, a fim de que possam ter um melhor desempenho.
- **Platform** Especifica se o processo está em execução na plataforma de 64 bits ou de 32 bits. As edições de 64 bits do Windows suportam aplicativos de 64 bits e 32 bits utilizando a camada de emulação x86 chamada de Windows on Windows 64 (WoW64). O subsistema WoW64 isola os aplicativos de 32 bits dos de 64 bits. Isso evita problemas no sistema de arquivos e no registro. O sistema operacional proporciona interoperabilidade através do limite de 32 bits/64 bits para o Component Object Model (COM) e para operações básicas. Contudo, os processos de 32 bits não podem carregar dynamic-link libraries (DLLs, bibliotecas de vínculo dinâmico) de 64 bits e os processos de 64 bits não podem carregar DLLs de 32 bits.

- **Process ID (PID)** O identificador numérico do processo.
- **Session ID** O identificador da sessão sob a qual o processo está em execução.
- **Threads** O número atual de threads que o processo está utilizando. A maioria dos aplicativos para servidores são multithread (de múltiplas threads). O multi-threading permite a execução simultânea de solicitações de processos. Alguns aplicativos podem controlar dinamicamente o número de threads em execução simultânea para melhorar o desempenho do aplicativo. Threads demais, no entanto, podem na realidade reduzir o desempenho, pois o sistema operacional tem de alternar entre contextos de thread com muita frequência.
- **UAC Virtualization** Indica se a virtualização do User Account Control (UAC, Controle de Conta de Usuário) está habilitado, desabilitado ou não é permitido no processo. A virtualização do UAC é necessária para aplicativos herdados desenvolvidos para o Windows XP, o Windows Server 2003 e versões anteriores do Windows. Quando a virtualização do UAC está habilitada para esses aplicativos, as notificações de erros e o registro em log dos erros relacionados a arquivos virtualizados e valores de registro são gravados no local virtualizado, em vez de no local real em que o processo estava tentando a gravação. Se a virtualização for necessária, mas estiver desabilitada ou não for permitida, o processo irá falhar silenciosamente ao tentar gravar em pastas ou áreas protegidas do registro.

Se examinar processos em execução no Task Manager, notará um processo chamado System Idle Process. Não é possível definir a prioridade desse processo. Diferentemente dos processos que rastreiam o uso de recursos, o System Idle Process rastreia a quantidade de recursos do sistema que não é utilizada. Portanto, um 99 na coluna CPU do System Idle Process significa que 99% dos recursos da CPU não estão sendo utilizados atualmente.

O processos que estão esperando para utilizar um recurso que esteja bloqueado por outro processo estão em um estado de espera e podem prosseguir somente quando o recurso bloqueado for liberado. Como parte das operações normais, os recursos são bloqueados por um ou outro processo e, depois, liberados para serem utilizados por outro processo. Algumas vezes, no entanto, programas com arquitetura fraca podem deixar um processo preso, esperando por um recurso que nunca é liberado.

Você pode visualizar a cadeia de espera para processos pressionando e segurando ou clicando com o botão direito do mouse no processo e tocando ou clicando em Analyze Wait Chain. Se o processo estiver esperando para que um recurso seja liberado, você pode ver a cadeia de espera para esse processo (como mostrado na Figura 3-4). O nó raiz na árvore de espera é o processo utilizando, ou esperando para utilizar, o recurso necessário. Um processo esperando por outro processo para um recurso pode explicar por que um processo não parece responder como esperado.

Se suspeitar que há um problema de bloqueamento, você pode selecionar um ou mais processos na cadeia de espera e tocar ou clicar em End Process. O Task Manager irá interromper os processos, o que deverá liberar o recurso bloqueado. Contudo, lembre-se de que é rotineiro e normal que processos bloqueiem recursos, enquanto estes estão sendo utilizados, e os liberem quando tiverem terminado. Um problema ocorre quando um processo não libera um recurso, como pode acontecer com um programa com arquitetura fraca.

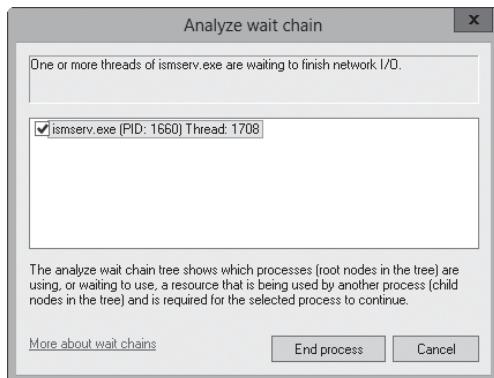


FIGURA 3-4 Análise de cadeias de espera.

Ao examinar processos, lembre-se de que um único aplicativo pode iniciar vários processos. Geralmente, esses processos são dependentes de um processo central. A partir desse processo principal, uma árvore de processos contendo os processos dependentes será formada. Você pode localizar o processo principal de um aplicativo pressionando e segurando ou clicando com o botão direito do mouse no aplicativo na guia Processes e selecionando Go To Details. Quando finalizar os processos, normalmente terá como destino o processo principal do aplicativo ou o próprio aplicativo, em vez dos processos dependentes. Isso assegura que o aplicativo seja interrompido com precisão.

Para interromper o processo principal do aplicativo e os processos dependentes, há diversas opções:

- Pressionar e segurar ou clicar com o botão direito do mouse no aplicativo na guia Processes e tocar ou clicar em End Task.
- Pressionar e segurar ou clicar com o botão direito do mouse no processo principal do aplicativo na guia Details e tocar ou clicar em End Task.
- Pressionar e segurar ou clicar com o botão direito do mouse no processo principal ou nos dependentes na guia Processes e tocar ou clicar em End Process Tree.

Visualização de serviços do sistema

A guia Services do Task Manager fornece uma visão geral dos serviços do sistema. Essa guia exibe serviços por nome, ID de processo, descrição, status e grupo. Como mostrado na Figura 3-5, vários serviços normalmente são executados sob o mesmo ID de processo. Você pode classificar os serviços rapidamente por seus IDs de processo tocando ou clicando no cabeçalho da coluna relacionada. Pode tocar ou clicar no cabeçalho da coluna Status para classificar os serviços de acordo com seu status, Running (em execução) ou Stopped (interrompido).

A coluna Group fornece opções adicionais sobre identidades ou contextos de host de serviço (Service Host) relacionados sob os quais um serviço é executado:

- Os serviços executados sob uma identidade com uma restrição têm a restrição listada na coluna Group. Por exemplo, um serviço executado sob a identidade Local Service pode ser listado como LocalServiceNoNetwork para indicar que não tem acesso à rede, ou pode ser listado como LocalSystemNetworkRestricted para indicar que tem acesso restrito à rede.
- Serviços que utilizam Svhost.exe têm seu contexto associado ao parâmetro `-k`. Por exemplo, o serviço RemoteRegistry é executado com a linha de comando svchost.exe `-k regsvc`. Você verá uma entrada na coluna Group para esse serviço.

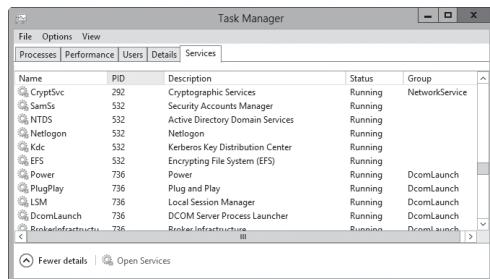


FIGURA 3-5 A guia Services fornece uma visão geral rápida do status de serviços do sistema.

Pressionando e segurando ou clicando com o botão direito do mouse no serviço na lista do Task Manager um menu de atalho será exibido que permite fazer o seguinte:

- Iniciar um serviço interrompido
- Interromper um serviço iniciado
- Ir para o processo relacionado na guia Details

Visualização e gerenciamento de desempenho do sistema

A guia Performance no Task Manager fornece uma visão geral do uso da CPU e memória. Como mostrado na Figura 3-6, a guia exibe gráficos e estatísticas. Essas informações mostram uma verificação rápida do uso de recursos do sistema. Para obter informações mais detalhadas, utilize o Performance Monitor, como explicado posteriormente neste capítulo.

Os gráficos na guia Performance fornecem as seguintes informações:

- **CPU** Um gráfico do uso de CPU plotado ao longo do tempo
- **Memory** Um gráfico do uso de memória plotado ao longo do tempo
- **Ethernet** Um gráfico da taxa de transferência de rede plotado ao longo do tempo

Toque ou clique em um gráfico resumido no painel esquerdo para visualizar informações detalhadas sobre ele no painel direito. Para exibir uma ampliação de qualquer gráfico, toque ou clique duas vezes nele. Com um novo toque ou clique duplo, volta-se ao modo de exibição normal.

A opção Update Speed no menu View permite alterar a velocidade de atualização do gráfico, bem como pausá-lo. As atualizações ocorrem uma vez a cada quatro segundos para Low, uma vez a cada dois segundos para Normal e duas vezes por segundo para High.

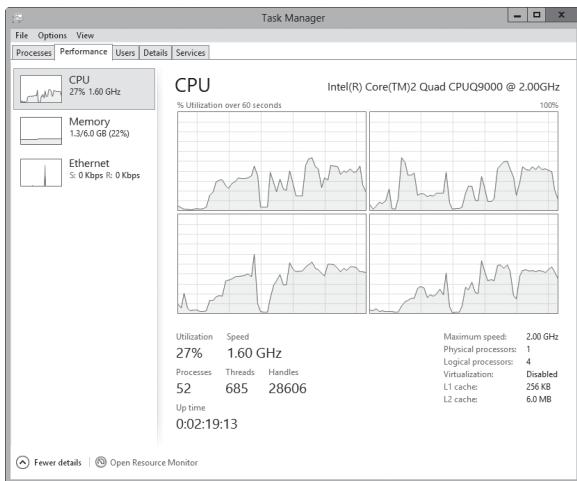


FIGURA 3-6 A guia Performance fornece uma verificação rápida do uso de recursos do sistema.

Uso da CPU: Conceitos básicos

Quando você seleciona CPU, o gráfico % Utilization mostra a utilização geral do processador nos últimos 60 segundos. Se um sistema tiver várias CPUs, você verá um gráfico para cada CPU, por padrão. Você também pode visualizar processadores lógicos ou nós NUMA pressionando e segurando ou clicando com o botão direito do mouse no gráfico de uma CPU, selecionando Change Graph To e Logical Processors ou NUMA Nodes, conforme apropriado.

Para visualizar tempos do kernel, pressione e segure ou clique com o botão direito do mouse no gráfico de uma CPU e selecione Show Kernel Times. Como o uso pelo kernel é plotado separadamente, você pode acompanhar com mais facilidade a quantidade de tempo da CPU utilizada pelo kernel do sistema operacional.

DICA O acompanhamento do uso do kernel pode ser útil para solucionar problemas. Por exemplo, se estiver utilizando o IIS com armazenamento em cache de saídas no modo kernel, você pode obter um melhor entendimento de como o armazenamento em cache do kernel pode estar afetando o uso de CPU e o desempenho geral exibindo os tempos do kernel. O rastreamento de uso do kernel não está habilitado por padrão, pois adiciona sobrecarga ao monitorar um servidor no Task Manager.

Você pode utilizar as informações de CPU fornecidas para determinar rapidamente o tempo que o servidor está iniciado, o número de processadores físicos, o número de processadores lógicos, se a virtualização de hardware está habilitada e a quantidade de cache no processador para cada registro disponível (L1, L2, L3). Lembre-se:

- Handles mostra o número de manipulações de I/O em uso; handles de I/O agem como tokens permitindo que programas acessem recursos. A taxa de transferência de I/O e o desempenho do disco afetam mais um sistema do que um número consistentemente alto de handles de I/O.
- Threads mostra o número de threads em uso; as threads são as unidades básicas de execução dentro dos processos.
- Processes mostra o número de processos em uso; os processos são instâncias em execução de aplicativos ou arquivos executáveis.
- Up Time mostra há quanto tempo o sistema está funcionando desde a última inicialização.

Se o uso de CPU for consistentemente alto, mesmo sob condições normais de uso, você talvez queira realizar um monitoramento de desempenho mais detalhado para determinar a causa do problema. A memória muitas vezes é a fonte de problemas de desempenho e você deve descartá-la antes de atualizar ou adicionar CPUs. Para mais detalhes, consulte “Ajuste do desempenho do sistema” mais adiante neste capítulo.

Uso de memória: Conceitos básicos

Quando você seleciona Memory, o gráfico Memory Usage mostra o uso geral do conjunto privado em funcionamento nos últimos 60 segundos. Os histogramas Memory Composition mostram o seguinte:

- **In-Use Memory** A quantidade de memória sendo utilizada pelos processos
- **Modified Memory** A quantidade de memória cujo conteúdo deve ser gravado em disco antes que possa ser utilizada para outra finalidade
- **Standby Memory** A quantidade de memória com dados e código armazenados em cache não sendo utilizada ativamente
- **Free Memory** A quantidade de memória que não está alocada no momento para qualquer finalidade

OBSERVAÇÃO Você pode utilizar as informações da memória fornecidas para determinar rapidamente a velocidade da memória e o número de slots de memória utilizados e disponíveis.

A quantidade total de RAM física configurada no servidor será listada no canto superior direito quando você estiver trabalhando com os gráficos de memória. Outras estatísticas de memória mostradas abaixo dos gráficos de memória fornecem as seguintes informações:

- **In Use** Mostra a quantidade de RAM física que está em uso no servidor.
- **Available** Mostra a quantidade de RAM física que está disponível para uso (inclui as memórias marcadas como *standby* e *free*). Se um servidor tiver pouquíssima memória física disponível, talvez seja preciso adicionar memória ao sistema. Em geral, você desejará que a memória disponível seja não menos que 5% da memória física total no servidor.
- **Committed** Lista a memória virtual em uso no momento seguida da quantidade de total de memória virtual disponível. Se o uso de arquivo de paginação atual estiver dentro de 10% do valor máximo (significando uso consistente de 90%

ou mais), você pode querer adicionar memória física, aumentar a quantidade de memória virtual ou optar por ambas as medidas.

- **Cached** Mostra a quantidade de memória utilizada para o armazenamento em cache do sistema.
- **Paged Pool** Fornece informações sobre memória kernel não crítica utilizada pelo kernel do sistema operacional.
- **Nonpaged Pool** Fornece informações sobre memória kernel crítica utilizada pelo kernel do sistema operacional.

Porções críticas da memória usada pelo kernel devem operar na RAM e não podem ser paginadas para a memória virtual. Por causa disso, esse tipo de memória kernel é listada como estando na reserva de memória não paginável. O restante da memória kernel pode ser paginado para a memória virtual e está listado como presente na reserva de memória paginável.

Uso de rede: Conceitos básicos

Quando você seleciona Ethernet, o Task Manager fornece uma visão geral dos adaptadores de rede utilizados pelo sistema. Você pode utilizar as informações fornecidas para determinar rapidamente o percentual de utilização, a velocidade do link e o status de uso operacional de cada adaptador de rede configurado em um sistema.

O nome do adaptador de rede ativo na pasta Network Connections é mostrado no canto superior direito. Se o sistema tiver um adaptador de rede, o gráfico resumido mostrará detalhes do tráfego de rede nesse adaptador ao longo do tempo. Se o sistema tiver vários adaptadores de rede, o gráfico exibirá um índice composto de todas as conexões de rede, que representa todo o tráfego de rede.

Você pode visualizar informações detalhadas sobre velocidade do link, estado do link, bytes enviados, bytes recebidos e mais pressionando e segurando ou clicando com o botão direito do mouse no gráfico Network Throughput e selecionando View Network Details. Ao trabalhar com detalhes de rede, lembre-se do seguinte:

- **Network Utilization** Percentagem de uso da rede baseado na velocidade de conexão inicial para a interface ou na velocidade combinada de interfaces agrupadas. Por exemplo, um adaptador com uma velocidade de link inicial de 10 gigabits por segundo (Gbps) e tráfego atual de 100 megabits por segundo (Mbps) é utilizado a 1%.
- **Link Speed** A velocidade de conexão da interface, conforme determinado pela velocidade de conexão inicial, como 1 Gbps ou 10 Gbps.
- **State** O status operacional de adaptadores de rede, como Connected ou Disconnected.
- **Bytes Sent Throughput** Percentagem de largura de banda da conexão atual utilizada pelo tráfego enviado do sistema.
- **Bytes Received Throughput** Percentagem de largura de banda da conexão atual utilizada pelo tráfego recebido pelo sistema.
- **Bytes Throughput** Percentagem de largura de banda da conexão atual utilizada para todo o tráfego no adaptador de rede.
- **Bytes Sent** O total cumulativo de bytes enviados na conexão até o momento.

- **Bytes Received** O total cumulativo de bytes recebidos na conexão até o momento.
- **Bytes** O total cumulativo de bytes na conexão até o momento.

MUNDO REAL Em qualquer momento que vir o uso se aproximando consistentemente ou excedendo 50% da capacidade total, você deve começar a monitorar o servidor com mais atenção e talvez queira considerar a adição de adaptadores de rede. Planeje cuidadosamente todas as atualizações; é preciso muito mais planejamento do que possa imaginar. Considere as implicações não apenas para esse servidor, mas também para a rede como um todo. Você também pode ter problemas de conectividade se exceder a largura de banda alocada de seu provedor de serviços – muitas vezes pode levar meses para obter largura de banda adicional para conexões externas.

Visualização e gerenciamento de sessões de usuário remoto

Os usuários remotos podem utilizar Remote Desktop (Área de Trabalho Remota) para se conectar a sistemas remotos. A Área de Trabalho Remota permite administrar sistemas remotamente, como se estivesse sentado à frente do console. O Windows Server 2012 permite até duas sessões de console ativas por vez.

Uma forma de visualizar e gerenciar as conexões de área de trabalho é utilizar o Task Manager. Para isso, inicie o Task Manager e toque ou clique na guia Users, mostrada na Figura 3-7. A guia Users mostra sessões interativas tanto de usuários locais quanto de remotos.

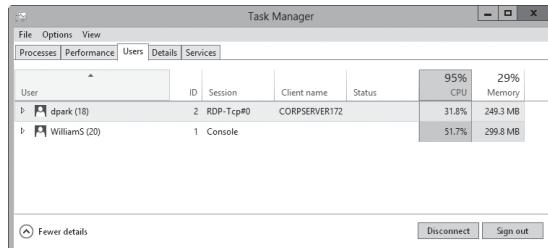


FIGURA 3-7 A guia Users permite visualizar e gerenciar sessões de usuário.

Cada conexão de usuário é listada com o nome do usuário, o status, a utilização da CPU e o uso de memória por padrão. Outras colunas podem ser adicionadas pressionando e segurando ou clicando com o botão direito do mouse no cabeçalho de qualquer coluna e tocando ou clicando nas colunas a adicionar. As colunas disponíveis incluem:

- **ID** O ID da sessão. O primeiro logon tem um ID de sessão de 1. O segundo logon tem um ID de 2.
- **Session** O tipo de sessão. Um usuário conectado ao sistema local é listado com Console no tipo de sessão. Outros usuários têm um tipo de sessão que indica o tipo de conexão e protocolo sendo utilizados, como RDP-TCP para uma conexão utilizando o Remote Desktop Protocol (RDP, Protocolo de Área de Trabalho Remota) com TCP como o protocolo de transporte.

- **Client name** Para conexões remotas, lista o nome do computador cliente de origem.

Os detalhes da utilização de CPU e memória são novos no Windows Server 2012 e são realmente úteis para solucionar problemas de desempenho relacionados a usuários conectados. O valor de utilização combinada é listado acima da coluna e os valores de utilização individual para cada usuário conectado são listados abaixo dele.

No exemplo mostrado na Figura 3-7, a CPU do servidor é 95% utilizada pelos usuários conectados. Esse alto nível de uso poderia afetar o desempenho geral do servidor e ele poderia não responder tão bem ao realizar outras tarefas.

Se pressionar e segurar ou clicar com o botão direito do mouse em uma sessão de usuário, terá as seguintes opções:

- **Connect** Permite que você conecte uma sessão de usuário remoto se estiver inativa.
- **Disconnect** Permite que você desconecte uma sessão de usuário local ou remoto, parando todos os aplicativos iniciados pelo usuário sem salvar os dados do aplicativo.
- **Sign Off** Permite desconectar um usuário utilizando o processo normal para fazer logoff. Os dados do aplicativo e as informações sobre o estado do sistema serão salvos, como em um logoff normal.
- **Send Message** Permite que você envie uma mensagem via console para um usuário conectado.

Também uma novidade no Windows Server 2012, o nome do usuário é seguido pelo número de processos que ele está executando. Se tocar ou clicar duas vezes no nome do usuário, verá uma entrada para cada processo em execução. Os processos são listados por nome, uso de CPU e uso de memória.

Gerenciamento de serviços do sistema

Os serviços proporcionam funções-chave para estações de trabalho e servidores. Para gerenciar os serviços do sistema no servidor local ou em um servidor remoto, você utiliza o painel Services no Server Manager (Gerenciador de Servidores) ou o nó Services no Computer Management. Para trabalhar com serviços em servidores remotos, o gerenciamento remoto e as exceções de entrada para o Remote Service Management devem estar habilitados. Para mais informações, consulte “Como gerenciar servidores remotamente” no Capítulo 2, “Gerenciamento de servidores com o Windows Server 2012”.

Navegação por serviços no Server Manager

Quando estiver trabalhando com o Server Manager e selecionar o nó Local Server, o nó All Servers ou um nó de grupo de servidores, o painel direito terá um painel Services, como o mostrado na Figura 3-8. Se selecionar o servidor com o qual quer trabalhar no painel Servers, seus serviços serão listados nesse painel. Você pode utilizar esse painel como se segue:

- Para um servidor em que esteja conectado localmente, você pode utilizar o painel Services no nó Local Server.
- Para um servidor local ou remoto, pode-se utilizar o painel Services no nó All Servers para trabalhar com serviços.
- Os nós de grupo de servidores criados automaticamente são organizados por funções de servidor, como Active Directory Domain Services (AD DS, Serviços de Domínio do Active Directory) ou Domain Name System (DNS, Sistema de Nomes de Domínio), e você poderá gerenciar os serviços em execução nos servidores dos quais essa função depende.
- Para grupos de servidores personalizados criados por você ou por outros administradores, será possível utilizar o painel Services relacionado para gerenciar serviços em qualquer servidor remoto que tenha sido adicionado ao grupo.

SERVICES				
All services 151 total				
Server Name	Display Name	Service Name	Status	Start Type
CORPSERVER172	Print Spooler	Spooler	Running	Automatic
CORPSERVER172	SNMP Trap	SNMPTRAP	Stopped	Manual
CORPSERVER172	SSDP Discovery	SSDPTRV	Stopped	Disabled
CORPSERVER172	Software Protection	sppsvc	Start Pending	Automatic (Delayed Start)
CORPSERVER172	Shell Hardware Detection	ShellHWDetection	Running	Automatic
CORPSERVER172	System Event Notification Service	SENS	Running	Automatic

FIGURA 3-8 Utilize os painéis Services no Server Manager para gerenciar serviços em servidores locais e remotos.

As colunas no painel Services podem ser ajustadas pressionando e segurando ou clicando com o botão direito do mouse no cabeçalho de qualquer coluna e tocando ou clicando nas colunas a adicionar ou remover. As colunas que podem ser utilizadas incluem:

- **Server Name** O nome do servidor em que o serviço está em execução.
- **FQDN** O nome de domínio totalmente qualificado do servidor em que o serviço está em execução.
- **Display Name** O nome descritivo do serviço.
- **Service Name** O nome interno do serviço.
- **Description** Uma breve descrição do serviço e de sua finalidade.
- **Status** Se o status do serviço é em execução, pausado ou parado.
- **Start Type** A configuração de inicialização para o serviço. Os serviços automáticos são iniciados na inicialização. Os usuários ou outros serviços iniciam serviços manuais. Os serviços desabilitados estão desativados e não podem ser iniciados enquanto assim permanecerem.

DICA Quando estiver trabalhando com muitos servidores, utilize as opções de agrupamento de serviços para ajudar a gerenciá-los com mais facilidade. Você pode agrupar serviços por nome do servidor, FQDN, nome para exibição, nome do serviço, status e tipo de inicialização pressionando e segurando ou clicando com o botão direito do mouse no cabeçalho de qualquer coluna, selecionando Group By e sua opção de agrupamento.

Navegação por serviços no Computer Management

Para um gerenciamento rápido e fácil de qualquer serviço em um servidor remoto, você pode utilizar o nó Services no Computer Management. Você pode abrir o Computer Management e conectar-se automaticamente a um servidor remoto a partir do Server Manager. Para isso, siga as etapas:

1. Selecione All Servers ou qualquer nó de servidores no painel esquerdo.
2. No painel Servers, pressione e segure ou clique com o botão direito do mouse no servidor ao qual quer se conectar.
3. Toque ou clique em Computer Management.

DICA Quando estiver trabalhando com servidores remotos no Computer Management, muitos recursos dependerão do gerenciamento remoto e de exceções de firewall apropriadas estarem habilitadas, conforme abordado no Capítulo 2. Se a conta de usuário que estiver utilizando atualmente não tiver as credenciais apropriadas para trabalhar com o servidor remoto, você não poderá se conectar ao servidor no Computer Management. Para utilizar credenciais alternativas, pressione e segure ou clique com o botão direito do mouse no servidor ao qual quer se conectar, selecione Manage As, digite suas credenciais alternativas e clique em OK. Opcionalmente, você pode selecionar Remember My Credentials antes de clicar em OK para salvar as credenciais para toda vez que fizer logon e quiser trabalhar com o servidor remotamente. Após definir suas credenciais, pressione e segure ou clique com o botão direito do mouse no servidor ao qual quer se conectar e selecione Computer Management. Agora o Computer Management será aberto e se conectará ao servidor utilizando as credenciais especificadas.

Ao trabalhar com o Computer Management, você visualiza e trabalha com serviços expandindo o nó Services And Applications e selecionando o nó Services, conforme mostrado na Figura 3-9. As colunas do painel Services são ligeiramente diferentes das mostradas quando você está trabalhando com o nó Services no Computer Management:

- **Name** O nome do serviço. Apenas serviços instalados no sistema são listados aqui. Toque ou clique duas vezes em uma entrada para configurar suas opções de inicialização. Se um serviço de que precise não estiver listado, você pode instalá-lo instalando a função ou o recurso relacionados, conforme abordado no Capítulo 2.
- **Description** Uma breve descrição do serviço e de sua finalidade.
- **Status** Indica se o status do serviço é em execução, pausado ou interrompido. (Parado é indicado por uma entrada em branco.)
- **Startup Type** A configuração de inicialização para o serviço. Os serviços automáticos são iniciados na inicialização. Os usuários ou outros serviços iniciam serviços manuais. Os serviços desabilitados estão desativados e não podem ser iniciados enquanto assim permanecerem.
- **Log On As** A conta com a qual o serviço faz logon. O padrão, na maioria dos casos, é a conta do sistema local.

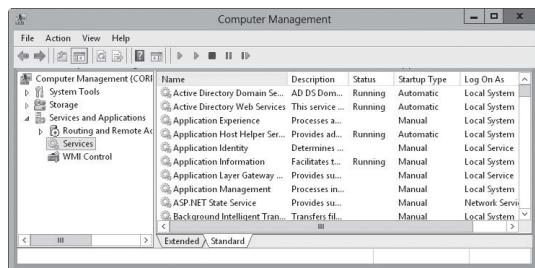


FIGURA 3-9 Utilize os painéis Services para gerenciar serviços em servidores locais e remotos.

O painel Services tem dois modos de exibição: Extended (estendido) e Standard (padrão). Para alterar o modo de exibição, utilize as guias no inferior do painel Services. No modo de exibição Extended, links rápidos são fornecidos para o gerenciamento de serviços. Toque ou clique em Start para iniciar um serviço interrompido. Toque ou clique em Restart para interromper e iniciar um serviço – essencialmente, para reiniciar esse serviço. Se selecionar um serviço quando o painel Services estiver no modo de exibição Extended, você verá uma descrição que detalha a finalidade do serviço.

OBSERVAÇÃO Tanto o sistema operacional quanto um usuário podem desabilitar serviços. Geralmente, o Windows Server 2012 desabilita um serviço se um possível conflito com outro existir.

Como iniciar, interromper e pausar serviços

Como administrador, você muitas vezes tem de iniciar, interromper ou pausar serviços. Para iniciar, interromper ou pausar um serviço, pressione e segure ou clique com o botão direito do mouse no serviço que quer gerenciar e selecione Start, Stop ou Pause, conforme apropriado. Você também pode escolher Restart para fazer com que o Windows interrompa e inicie o serviço após uma breve pausa. Além disso, se pausar um serviço, pode utilizar a opção Resume para retomar a operação normal.

OBSERVAÇÃO Quando os serviços que estão configurados para iniciar automaticamente fazem, o status será listado em branco e, geralmente, você receberá uma notificação em uma caixa de diálogo pop-up. As falhas de serviços também podem estar registradas nos logs de eventos do sistema. No Windows Server 2012, você pode configurar ações para lidar com falhas de serviços automaticamente. Por exemplo, você pode fazer com que o Windows Server 2012 tente reiniciar o serviço para você. Para detalhes, consulte “Configuração de recuperação de serviço” mais adiante neste capítulo.

Configuração de inicialização de serviço

Você pode configurar os serviços para iniciarem manual ou automaticamente. Pode-se também desativá-los permanentemente, desabilitando-os. Você configura a inicialização de serviço no Computer Management seguindo estas etapas:

1. Pressione e segure ou clique com o botão direito do mouse no serviço que quer configurar e escolha Properties.

2. Na guia General, utilize a lista Startup Type para escolher uma opção de inicialização entre as seguintes alternativas, conforme mostrado na Figura 3-10:

- **Automatic** Selecione Automatic para iniciar os serviços na inicialização.
- **Automatic (Delayed Start)** Selecione Automatic (Delayed Start) para adiar a inicialização do serviço até que todos os serviços automáticos não adiados tenham sido iniciados.
- **Manual** Selecione Manual para permitir que os serviços sejam iniciados manualmente.
- **Disabled** Selecione Disabled para desativar o serviço.

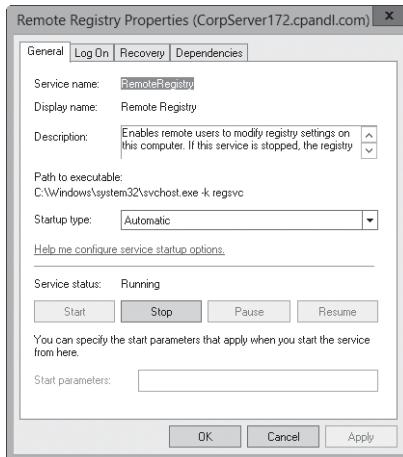


FIGURA 3-10 Configure as opções de inicialização de serviço utilizando a lista Startup Type da guia General.

3. Toque ou clique em OK.

Configuração de logon de serviço

Você pode configurar os serviços para fazerem logon como uma conta do sistema ou como um usuário específico. Para isso, siga as etapas:

1. Em Computer Management, pressione e segure ou clique com o botão direito do mouse no serviço que quer configurar e escolha Properties.
2. Selecione a guia Log On, mostrada na Figura 3-11.

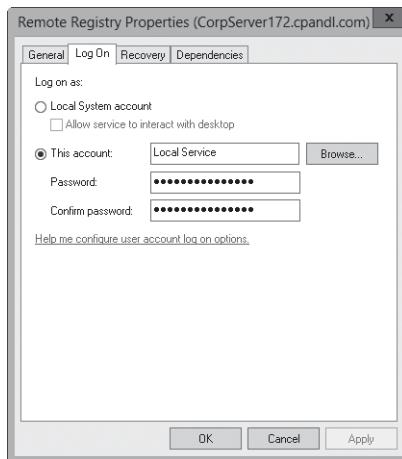


FIGURA 3-11 Utilize a guia Log On para configurar a conta de logon do serviço.

3. Selecione Local System Account se quiser que o serviço faça logon utilizando a conta do sistema (o padrão para a maioria dos serviços). Se o serviço fornecer uma interface de usuário que possa ser manipulada, selecione Allow Service To Interact With Desktop para permitir que os usuários controlem a interface do serviço.
4. Selecione This Account se quiser que o serviço faça logon utilizando uma conta de usuário específica. Certifique-se de digitar o nome de conta e a senha nas caixas de texto fornecidas. Utilize o botão Browse para procurar uma conta de usuário, se necessário.
5. Toque ou clique em OK.

ALERTA DE SEGURANÇA Você deve monitorar qualquer conta que seja utilizada com serviços. Essas contas podem ser fonte de problemas de segurança se não forem configuradas adequadamente. As contas de serviço devem ter as configurações de segurança mais rigorosas e tão poucas permissões quanto possível, ao passo que permitam que o serviço realize as funções necessárias. Normalmente, as contas utilizadas com serviços não precisam de muitas das permissões que você atribuiria a uma conta de usuário normal. Por exemplo, a maioria das contas de serviço não precisa do direito para fazer logon localmente. Todo administrador deve saber para que as contas de serviço são utilizadas (a fim de que possam melhor monitorar o uso delas) e devem tratá-las como se fossem contas de administrador. Isso significa utilizar senhas seguras, monitorar cuidadosamente o uso da conta, aplicar criteriosamente permissões e privilégios de conta, e assim por diante.

Configuração de recuperação de serviço

Você pode configurar os serviços para agirem de forma específica quando um serviço falhar. Por exemplo, você pode tentar reiniciar o serviço ou executar um aplicativo. Para configurar as opções de recuperação para um serviço, siga estas etapas:

1. Em Computer Management, pressione e segure ou clique com o botão direito do mouse no serviço que quer configurar e escolha Properties.
2. Toque ou clique na guia Recovery, mostrada na Figura 3-12.

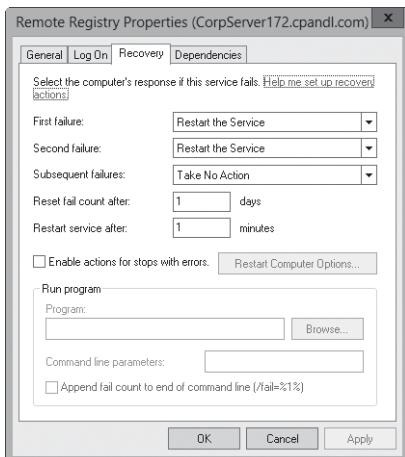


FIGURA 3-12 Utilize a guia Recovery para especificar as ações que devem ser feitas em caso de falha do serviço.

OBSERVAÇÃO O Windows Server 2012 configura automaticamente a recuperação para serviços críticos do sistema durante a instalação. Na maioria dos casos, você verá que os serviços críticos estão configurados para reiniciar automaticamente se o serviço falhar. Alguns serviços extremamente críticos, como DCOM Server Process Launcher e Group Policy Client (Cliente de Política de Grupo), estão configurados para reiniciar o computador se o serviço falhar. Você não pode alterar essas configurações, pois não estão disponíveis.

3. Você pode agora configurar as opções de recuperação para a primeira, a segunda e as tentativas subsequentes de recuperação. As opções a seguir estão disponíveis:
 - **Take No Action** O sistema operacional não tentará uma recuperação para essa falha, mas ainda pode tentar a recuperação de falhas anteriores ou subsequentes.
 - **Restart The Service** Interrompe e inicia o serviço após uma breve pausa.
 - **Run A Program** Permite executar um programa ou um script em caso de falha. O script pode ser um programa de lote ou um script do Windows. Se

selecionar esta opção, defina o caminho completo do arquivo para o programa que quer executar e qualquer parâmetro de linha de comando necessário para rodar o programa quando for iniciado.

- **Restart The Computer** Desliga e reinicia o computador. Antes de escolher esta opção, verifique de novo as opções Startup e Recovery do computador. Você precisa que o sistema selecione as opções padrão de forma rápida e automática.

PRÁTICAS RECOMENDADAS Ao configurar opções de recuperação para serviços críticos, você talvez queira tentar reiniciar o serviço na primeira e na segunda tentativa, e reinicializar o servidor na terceira tentativa.

4. Configure outras opções baseado nas opções de recuperação selecionadas anteriormente. Se escolheu executar um programa como uma opção de recuperação, é preciso definir as opções no painel Run Program. Se escolheu reiniciar o serviço, precisa especificar o atraso de reinicialização. Após interromper o serviço, o Windows Server espera pelo atraso especificado antes de tentar iniciar o serviço. Na maioria dos casos, um atraso de um a dois minutos deve ser suficiente.
5. Toque ou clique em OK.

Como desabilitar serviços desnecessários

Como administrador, você precisa garantir que os servidores e a rede sejam seguros, e serviços desnecessários são uma potencial fonte de problemas de segurança. Por exemplo, em muitas empresas que examinei problemas de segurança, encontrei servidores executando Worldwide Web Publishing Service (Serviço de Publicação na World Wide Web), Simple Mail Transfer Protocol (protocolo SMTP) e File Transfer Protocol (protocolo FTP) Publishing Service quando esses serviços não eram necessários. Infelizmente, esses serviços podem fazer usuários anônimos acessarem servidores e podem também expor o servidor a ataques, se não forem configurados adequadamente.

Se encontrar serviços desnecessários, você tem diversas opções. Com serviços instalados por meio de funções, serviços de função ou recursos, você pode remover a função, o serviço de função ou o recurso relacionados para remover o componente desnecessário e seus serviços relacionados. Ou pode simplesmente desabilitar os serviços que não estão em uso. Normalmente, você desejará começar desabilitando serviços, em vez de desinstalar componentes. Dessa forma, se desabilitar um serviço e outro administrador ou um usuário disser que não consegue realizar mais a tarefa X, poderá habilitar o serviço relacionado de novo, se necessário.

Para desabilitar um serviço, siga estas etapas:

1. Em Computer Management, pressione e segure ou clique com o botão direito do mouse no serviço que quer configurar e escolha Properties. Na guia General, selecione Disabled na lista Startup Type.
2. Desabilitar um serviço não interrompe um serviço em execução. Apenas impede que seja iniciado da próxima vez que o computador for inicializado, significando que o risco à segurança ainda existe. Para tratar disso, toque ou clique em Stop na guia General da caixa de diálogo Properties e em OK.

Log e visualização de eventos

Os logs de eventos fornecem informações históricas que podem ajudar a monitorar problemas de sistema e segurança. Para trabalhar com serviços em servidores remotos, o gerenciamento remoto e as exceções de entrada para o Remote Service Management devem estar habilitados. Para mais informações, consulte “Como gerenciar servidores remotamente” no Capítulo 2.

O serviço Windows Event Log controla se os eventos são monitorados. Quando se inicia esse serviço, você pode monitorar ações de usuário e eventos de uso de recursos por meio dos logs de eventos. Dois tipos gerais de arquivos de log são utilizados:

- **Windows logs** Logs que o sistema operacional utiliza para registrar eventos gerais do sistema relacionados a aplicativos, segurança, instalação e componentes do sistema.
- **Applications and services logs** Logs que aplicativos e serviços específicos utilizam para registrar eventos específicos para o aplicativo ou para o serviço.

Os logs do Windows que você verá incluem:

- **Application** Este log registra eventos registrados em log por aplicativos, como a falha do SQL Server em acessar um banco de dados. A localização padrão é %SystemRoot%\System32\Winevt\Logs\Application.evtx.
- **Forwarded Events** Quando o encaminhamento de eventos está configurado, este log registra eventos encaminhados de outros servidores. A localização padrão é %SystemRoot%\System32\Config\ForwardedEvents.evtx.
- **Security** Este log registra eventos definidos pela auditoria com políticas de grupo. A localização padrão é %SystemRoot%\System32\Winevt\Logs\Security.evtx.

OBSERVAÇÃO Qualquer usuário que precise de acesso ao log de segurança deve receber o direito de usuário para Manage Auditing and Security Log (Log de segurança). Por padrão, os membros do grupo Administrators têm esse direito de usuário. Para aprender como atribuir direitos de usuário, consulte “Configuração das políticas de direitos do usuário” no Capítulo 8, “Como criar contas de usuário e de grupo”.

- **Setup** Este log registra eventos registrados em log pelo sistema operacional ou seus componentes durante a configuração e instalação. A localização padrão é %SystemRoot%\System32\Winevt\Logs\Setup.evtx.
- **System** Este log registra eventos registrados em log pelo sistema operacional ou seus componentes, como a falha de um serviço ao ser iniciado na inicialização. A localização padrão é %SystemRoot%\System32\Winevt\Logs\System.evtx.

ALERTA DE SEGURANÇA Como administradores, tendemos a monitorar mais os logs de aplicativos e sistema – mas não se esqueça do log de segurança. O log de segurança é um dos logs mais importantes, e deve ser monitorado rigorosamente. Se o log de segurança em um servidor não contiver eventos, a razão mais provável é que a auditoria local não tenha sido configurada ou que a auditoria de todo o domínio esteja configurada – neste último caso, você deve monitorar os logs de segurança em controladores de domínio, e não em servidores membros.

Os logs de aplicativos e serviços que você verá incluem os seguintes:

- **DFS Replication** Este log registra as atividades de replicação do Distributed File System (DFS, Sistema de Arquivos Distribuído). A localização padrão é %SystemRoot%\System32\Winevt\Logs\DfsReplication.evtx.
- **Directory Service** Este log registra eventos registrados em log pelo Active Directory Domain Services (AD DS, Serviços de Domínio do Active Directory) e seus serviços relacionados. A localização padrão é %SystemRoot%\System32\Winevt\Logs\Directory Service.evtx.
- **DNS Server** Este log registra consultas DNS, respostas e outras atividades do DNS. A localização padrão é %SystemRoot%\System32\Winevt\Logs\DNS Server.evtx.
- **File Replication Service** Este log registra as atividades de replicação de arquivos no sistema. A localização padrão é %SystemRoot%\System32\Winevt\Logs\File Replication Service.evtx.
- **Hardware Events** Quando o relatório de eventos do subsistema de hardware está configurado, este log registra os eventos de hardware relatados para o sistema operacional. A localização padrão é %SystemRoot%\System32\Config\Hardware.evtx.
- **Microsoft\Windows** Fornece logs que monitoram eventos relacionados a serviços e recursos específicos do Windows. Os logs são organizados por tipo de componente e categoria de eventos. Os logs operacionais monitoram eventos gerados pelas operações padrão do componente relacionado. Em alguns casos, você verá logs suplementares para análise, depuração e gravação de tarefas relacionadas à administração.
- **Windows PowerShell** Este log registra atividades relacionadas ao uso do Windows PowerShell. A localização padrão é %SystemRoot%\System32\Winevt\Logs\Windows PowerShell.evtx.

Acesso a eventos no Server Manager

Quando estiver trabalhando com o Server Manager e selecionar o nó Local Server, o nó All Servers ou um nó de grupo de servidores, o painel direito terá um painel Events, como o mostrado na Figura 3-13. Quando selecionar o servidor com o qual quer trabalhar no painel Servers, seus eventos serão listados no painel Events. Você pode utilizar esse painel como se segue:

- Para um servidor ao qual esteja conectado localmente, você pode utilizar o painel Events no nó Local Server ou no nó All Servers para visualizar eventos recentes de aviso e erro nos logs de aplicativos e sistema.
- Nós de grupos de servidores criados automaticamente estão organizados por funções de servidor, como AD DS ou DNS, e você poderá visualizar eventos recentes de erro e aviso em logs relacionados à função de servidor, se aplicável. Nem todas as funções têm logs associados, mas algumas, como o AD DS, têm vários logs associados.
- Para grupos de servidores personalizados criados por você ou por outros administradores, você poderá utilizar o painel Events relacionado para visualizar eventos recentes de aviso e erro nos logs de aplicativos ou sistema.

EVENTS						
All events 17 total						
Server Name	ID	Severity	Source	Log	Date	
CORPSERVER172	5008	Error	DFSR	DFS Replication	5/17,	
CORPSERVER172	5014	Warning	DFSR	DFS Replication	5/17,	
CORPSERVER172	1308	Warning	Microsoft-Windows-ActiveDirectory_DomainService	Directory Service	5/17,	
CORPSERVER172	1308	Warning	Microsoft-Windows-ActiveDirectory_DomainService	Directory Service	5/17,	
CORPSERVER172	5002	Error	DFSR	DFS Replication	5/17,	
CORPSERVER172	1308	Warning	Microsoft-Windows-ActiveDirectory_DomainService	Directory Service	5/17,	

FIGURA 3-13 Utilize os painéis Events no Server Manager para monitorar erros e avisos.

As colunas no painel Events podem ser ajustadas pressionando e segurando ou clicando com o botão direito do mouse no cabeçalho de qualquer coluna e tocando ou clicando nas colunas a adicionar ou remover. As colunas que podem ser utilizadas incluem:

- **Server Name** O nome do servidor em que o serviço está em execução
- **FQDN** O nome de domínio totalmente qualificado do servidor em que o serviço está em execução
- **ID** Geralmente, um identificador numérico para o evento específico, que pode ser útil ao consultar bases de dados de conhecimento
- **Severity** A severidade do evento, como erro ou aviso
- **Source** O aplicativo, serviço ou componente que registrou em log o evento
- **Log** O log em que o evento foi registrado
- **Date And Time** A data e a hora em que o evento foi registrado

DICA Quando estiver trabalhando com muitos servidores, utilize as opções de agrupamento para ajudar a gerenciar eventos com mais facilidade. Você pode agrupar os eventos por nome do servidor, FDQN, ID, severidade, fonte, log e data e hora pressionando e segurando ou clicando com o botão direito do mouse no cabeçalho de qualquer coluna, selecionando Group By e sua opção de agrupamento.

Acesso a eventos no Event Viewer

Para trabalhar com logs de eventos em servidores remotos, o gerenciamento remoto e as exceções de entrada para o Remote Event Log Management devem estar habilitados. Para mais informações, consulte “Como gerenciar servidores remotamente” no Capítulo 2.

Você pode acessar os logs de eventos seguindo estas etapas:

1. No Server Manager, selecione All Servers ou qualquer nó de grupo de servidores no painel esquerdo.
2. No painel Servers, pressione e segure ou clique com o botão direito do mouse no servidor ao qual quer se conectar.
3. Toque ou clique em Computer Management para se conectar automaticamente ao servidor selecionado.

- 4.** Em Computer Management, você visualiza e trabalha com os logs de eventos expandindo o nó System Tools e selecionando o nó Event Viewer, como mostrado na Figura 3-14.

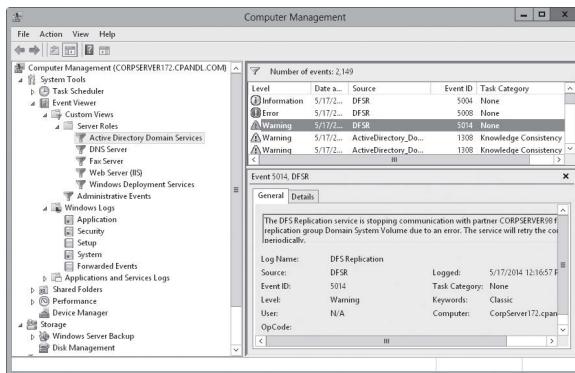


FIGURA 3-14 O Event Viewer exibe eventos usando o modo de exibição de log de ou personalizado.

- 5.** Expanda o nó Event Viewer. Você pode trabalhar com os logs de eventos do servidor das seguintes maneiras:
- Para visualizar todos os erros e avisos para todos os logs, expanda Custom Views e selecione Administrative Events. No painel principal, você verá uma lista de todos os eventos de aviso e erro para o servidor.
 - Para visualizar todos os erros e avisos para uma função de servidor específica, expanda Custom Views, Server Roles e selecione a função a exibir. No painel principal, você verá uma lista de todos os eventos para a função selecionada.
 - Para visualizar eventos em um log específico, expanda o nó Windows Logs, o nó Applications And Services Logs, ou ambos. Selecione o log que quer visualizar, como Application ou System.
- 6.** Utilize as informações na coluna Source para determinar qual serviço ou processo registrou no log um evento específico.

Como mostrado na Figura 3-14, as entradas no painel principal do Event Viewer apresentam uma visão geral rápida de quando, onde e como um evento ocorreu. Para obter informações detalhadas sobre um evento, examine os detalhes apresentados na guia General na porção inferior do painel principal. O nível ou a palavra-chave do evento precede a data e hora dele. Os níveis de eventos incluem o seguinte:

- **Information** Um evento informativo, que geralmente é relacionado a uma ação bem-sucedida.

- **Audit Success** Um evento relacionado à execução bem-sucedida de uma ação.
- **Audit Failure** Um evento relacionado à execução com falhas de uma ação.
- **Warning** Um aviso. Os detalhes de avisos muitas vezes são úteis para prevenir futuros problemas de sistema.
- **Error** Um erro não crítico, como a falha de uma solicitação de transferência de zona em um servidor DNS.
- **Critical** Um erro crítico, como o Serviço de cluster se desligando porque um quorum foi perdido.

OBSERVAÇÃO Os avisos e erros são os dois tipos-chave de eventos a examinar minuciosamente. Sempre que esses tipos de eventos ocorrerem e você não tiver certeza da causa, examine a descrição detalhada do evento.

Além da severidade, hora e data registradas em log, as entradas de eventos resumidas e detalhadas fornecem as seguintes informações:

- **Source** O aplicativo, serviço ou componente que registrou no log o evento
- **Event ID** Geralmente, um identificador numérico para o evento específico, que pode ser útil ao consultar bases de dados de conhecimento
- **Task Category** A categoria do evento, que quase sempre está definida para None, mas algumas vezes é utilizada para descrever melhor a ação relacionada, como um processo ou serviço
- **User** A conta de usuário que estava conectada quando o evento ocorreu, se aplicável
- **Computer** O nome do computador em que o evento ocorreu
- **Description** Nas entradas detalhadas, uma descrição textual do evento
- **Data** Nas entradas detalhadas, qualquer dado ou código de erro fornecido pelo evento

Filtragem de logs de eventos

O Event Viewer cria diversas exibições filtradas dos logs de eventos para você automaticamente. As exibições filtradas são listadas sob o nó Custom Views. Quando selecionar o nó Administrative Events, você verá uma lista de todos os erros e avisos para todos os logs. Quando expandir o nó Server Roles e selecionar um modo de exibição específico de uma função, verá uma lista de todos os eventos para a função selecionada.

Se quiser criar seu próprio modo de exibição personalizado, pode fazê-lo no Computer Management seguindo estas etapas:

1. No painel esquerdo, pressione e segure ou clique com o botão direito do mouse no nó Custom Views e toque ou clique em Create Custom View. A caixa de diálogo mostrada na Figura 3-15 será aberta.

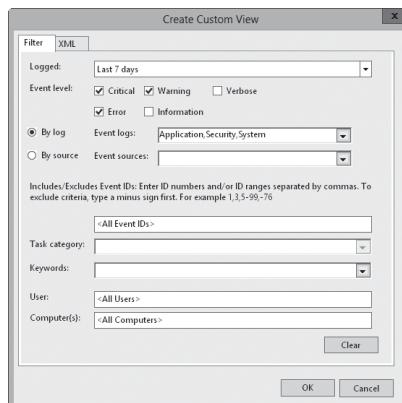


FIGURA 3-15 Você pode filtrar logs a fim de que apenas eventos específicos sejam exibidos.

2. Utilize a lista Logged para selecionar um intervalo de tempo para registrar eventos em log. Você pode escolher incluir eventos da última hora, das últimas 12 horas, últimas 24 horas, últimos sete dias ou últimos 30 dias. Como opção, você pode definir um intervalo personalizado.
3. Utilize as caixas de seleção Event Level para especificar o nível dos eventos a serem incluídos. Selecione Verbose para exibir detalhes adicionais de eventos.
4. Você pode criar um modo de exibição personalizado para um conjunto específico de logs ou para um conjunto específico de fontes de eventos:
 - Utilize a lista Event Logs para selecionar os logs de eventos a incluir. Você pode selecionar vários logs de eventos marcando suas caixas de seleção. Se selecionar logs de eventos específicos, todos os outros logs de eventos serão excluídos.
 - Utilize a lista Event Sources para selecionar as fontes de eventos a incluir. Você pode selecionar várias fontes de eventos marcando suas caixas de seleção. Se selecionar fontes de eventos específicas, todas as outras fontes de eventos serão excluídas.
5. Opcionalmente, utilize as caixas User e Computer(s) para especificar os usuários e computadores que devem ser incluídos. Se não especificar os usuários e computadores a incluir, os eventos gerados por todos os usuários e computadores serão incluídos.
6. Ao tocar ou clicar em OK, o Windows exibirá a caixa de diálogo Save Filter To Custom View, mostrada na Figura 3-16.

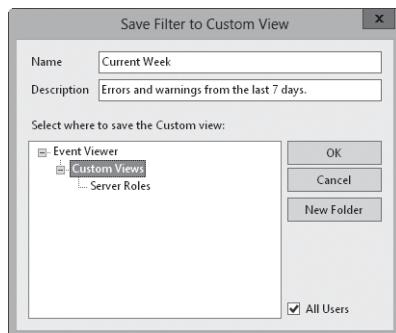


FIGURA 3-16 Salve a exibição filtrada.

7. Digite um nome e uma descrição para o modo de exibição personalizado.
8. Selecione onde salvar o modo de exibição personalizado. Por padrão, os modos de exibição personalizados são salvos sob o nó Custom Views. Você pode criar um novo nó tocando ou clicando em New Folder, digitando um nome para a pasta e tocando ou clicando em OK.
9. Toque ou clique em OK para fechar a caixa de diálogo Save Filter To Custom View. Você verá uma lista filtrada de eventos. Examine esses eventos cuidadosamente e tome medidas para corrigir qualquer problema que exista.

Se quiser ver um tipo específico de evento, você pode filtrar o log no Computer Management seguindo estas etapas:

1. Expanda Windows Logs ou Applications And Services Logs, conforme apropriado para o tipo de log que quer configurar. Você verá uma lista de logs de eventos.
2. Pressione e segure ou clique com o botão direito do mouse no log com o qual quer trabalhar e toque ou clique em Filter Current Log. Uma caixa de diálogo similar à mostrada anteriormente na Figura 3-15 será aberta.
3. Utilize a lista Logged para selecionar um intervalo de tempo para registrar eventos em log. Você pode escolher incluir eventos da última hora, das últimas 12 horas, últimas 24 horas, últimos sete dias ou últimos 30 dias.
4. Utilize as caixas de seleção Event Level para especificar o nível dos eventos a serem incluídos. Selecione Verbose para obter detalhes adicionais.
5. Utilize a lista Event Source para selecionar as fontes de eventos a incluir. Se selecionar fontes de eventos específicas, todas as outras fontes de eventos serão excluídas.
6. Opcionalmente, utilize as caixas User e Computer(s) para especificar os usuários e computadores que devem ser incluídos. Se não especificar os usuários e computadores a incluir, os eventos gerados por todos os usuários e computadores serão incluídos.

7. Toque ou clique em OK. Você verá uma lista filtrada de eventos. Examine esses eventos cuidadosamente e execute medidas para corrigir qualquer problema que exista. Para limpar o filtro e ver todos os eventos do log, toque ou clique em Clear Filter no painel Actions ou no menu Action.

Configuração das opções de log de eventos

As opções de log permitem que você controle o tamanho dos logs de eventos, bem como a maneira como o registro em log é manipulado. Por padrão, os logs de eventos estão definidos com um tamanho máximo de arquivo. Quando um log alcança esse limite, os eventos são substituídos para impedir que o log exceda o tamanho máximo de arquivo.

Para definir as opções de log no Computer Management, siga estas etapas:

1. Expanda Windows Logs ou Applications And Services Logs, conforme apropriado para o tipo de log que quer configurar. Você verá uma lista de logs de eventos.
2. Pressione e segure ou clique com o botão direito do mouse no log de eventos cujas propriedades quer definir e toque ou clique em Properties no menu de atalho. A caixa de diálogo mostrada na Figura 3-17 será aberta.

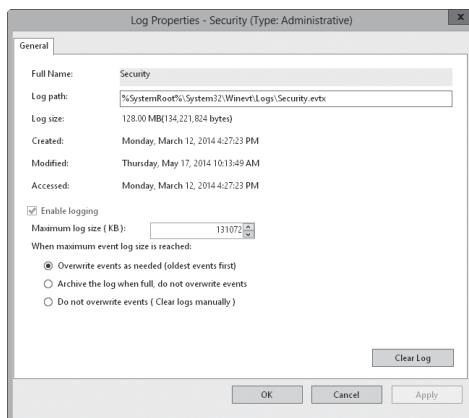


FIGURA 3-17 Faça as configurações de log de acordo com o nível de auditoria do sistema.

3. Digite ou defina um tamanho máximo em quilobytes (KB) na caixa de texto Maximum Log Size. Certifique-se de que a unidade contendo o sistema operacional tem espaço livre suficiente para o tamanho máximo de log especificado. Os arquivos de log são armazenados no diretório %SystemRoot%\System32\Winevt\Logs por padrão.
4. Selecione um modo de retenção do log de eventos. As opções a seguir estão disponíveis:

- **Overwrite Events As Needed (Oldest Events First)** Os eventos mais antigos no log são substituídos quando o tamanho máximo de arquivo é alcançado. Geralmente, esta é a melhor opção em um sistema com baixa prioridade.
- **Archive The Log When Full, Do Not Overwrite Events** Quando o tamanho máximo de arquivo é alcançado, o Windows arquiva os eventos salvando uma cópia do log atual no diretório padrão. A seguir, o Windows cria um novo log para armazenar os eventos atuais.
- **Do Not Overwrite Events (Clear Logs Manually)** Quando o tamanho máximo de arquivo é alcançado, o sistema gera mensagens de erro informando que o log de eventos está cheio.

5. Toque ou clique em OK ao terminar.

OBSERVAÇÃO Em sistemas críticos em que a segurança e o registro em log de eventos for muito importante, você deve utilizar Archive The Log When Full, Do Not Overwrite Events. Ao usar esse método, garante-se que o histórico dos eventos seja preservado automaticamente em arquivos.

Limpeza de logs de eventos

Quando um log de eventos está cheio, é preciso limpá-lo. Para isso, no Computer Management, siga as etapas:

1. Expanda Windows Logs ou Applications And Services Logs, conforme apropriado para o tipo de log que quer configurar. Você verá uma lista de logs de eventos.
2. Pressione e segure ou clique com o botão direito do mouse no log de eventos cujas propriedades quer definir e toque ou clique em Clear Log no menu de atalho.
3. Escolha Save And Clear para salvar uma cópia do log antes de limpá-lo. Escolha Clear para prosseguir sem salvar o arquivo de log.

Arquivamento de logs de eventos

Em sistemas-chave, como controladores de domínio e servidores de aplicativos, você desejará manter vários meses de registros de logs. No entanto, normalmente não é prático definir um tamanho maior de log para consegui-lo. Em vez disso, você deve permitir que o Windows arquive periodicamente os logs de eventos, ou deve fazê-lo manualmente.

Formatos de arquivos de log

Os logs podem ser arquivados em quatro formatos:

- Event files (arquivos de evento, .evtx) formato para acesso no Event Viewer
- Tab-delimited text (texto delimitado por tabulação, .txt) formato para acesso em editores ou processadores de texto ou para importação em planilhas e bancos de dados
- Comma-delimited text (texto delimitado por vírgula, .csv) formato para importação em planilhas ou bancos de dados
- XML (.xml) formato para salvar como um arquivo XML

Quando você exporta arquivos de log para um arquivo delimitado por vírgula, uma vírgula separa cada coluna na entrada do evento. As entradas de eventos têm esta aparência:

```
Information,07/21/14 3:43:24 PM,DNS Server,2,None,The DNS server has started.  
Error,07/21/14 3:40:04 PM,DNS Server,4015,None,The DNS server has encountered a critical error from the Directory Service (DS). The data is the error code.
```

O formato para as entradas é o seguinte:

Level, Date and time, Source, Event ID, Task Category, Description

Criação de arquivos de log

O Windows cria automaticamente arquivos de log quando você seleciona o modo de retenção de log Archive The Log When Full, Do Not Overwrite Events. Você pode criar um arquivo de log manualmente no Computer Management seguindo estas etapas:

1. Expanda Windows Logs ou Applications And Services Logs, conforme apropriado para o tipo de log que quer configurar. Você verá uma lista de logs de eventos.
2. Pressione e segure ou clique com o botão direito do mouse no log de eventos que quer arquivar e toque ou clique em Save All Events As no menu de atalho.
3. Na caixa de diálogo Save As, selecione um diretório e digite um nome de arquivo de log.
4. Na lista Save As Type, Event Files (*.evtx) é o tipo de arquivo padrão. Selecione o formato de log que quer utilizar e escolha Save. Note que talvez não seja possível utilizar o formato .evtx para salvar eventos de um computador remoto em uma pasta local. Nesse caso, é preciso salvar os eventos no computador local em um formato de arquivo diferente, como o .xml. Senão, salve os eventos no formato .evtx no computador remoto.
5. Se planeja visualizar o log em outros computadores, talvez precise incluir informações de exibição. Para salvar informações de exibição, selecione Display Information For These Languages, escolha o idioma na lista fornecida e toque ou clique em OK. Senão, apenas toque ou clique em OK para salvar o log sem essas informações.

OBSERVAÇÃO Se planeja arquivar logs regularmente, talvez queira criar um diretório de arquivo morto no qual possa localizar os arquivos de log com facilidade. Você também deve nomear o arquivo de log de modo que possa determinar com facilidade o tipo de arquivo de log e o período do arquivamento. Por exemplo, se estiver arquivando o arquivo de log do sistema de janeiro de 2014, talvez queira utilizar o nome de arquivo Log do sistema Janeiro 2014.

DICA O melhor formato a utilizar para arquivamento é o formato .evtx. Utilize esse formato se planeja examinar os logs抗igos no Event Viewer. No entanto, se planeja examinar os logs em outros aplicativos, talvez precise salvá-los em um formato delimitado por tabulação ou por vírgula. Com o formato delimitado por tabulação ou por vírgula, algumas vezes é necessário editar o arquivo de log em um editor de texto para que o log seja interpretado adequadamente. Se tiver salvo o log no formato .evtx, poderá salvar outra cópia no formato delimitado por tabulação ou por vírgula posteriormente, fazendo outra operação Save As após abrir o arquivo no Event Viewer.

Visualização de arquivos de log

Você pode visualizar arquivos de log em formato de texto em qualquer editor ou processador de texto. Deve-se visualizar os arquivos de log no formato de log de eventos no Event Viewer. É possível visualizar arquivos de log no Event Viewer seguindo estas etapas:

1. Em Computer Management, selecione e pressione e segure ou clique com o botão direito do mouse no nó Event Viewer. No menu de atalho, selecione Open Saved Log.
2. Na caixa de diálogo Open Saved Log, selecione um diretório e um nome de arquivo de log. Por padrão, o formato Event Logs Files está selecionado. Isso assegura que os logs salvos como .evtx, .evt e .etl sejam listados. Você também pode filtrar a lista selecionando um tipo de arquivo específico.
3. Toque ou clique em Open. Se for perguntado sobre converter o log para o novo formato de log de eventos, toque ou clique em Yes.
4. O Windows exibirá a caixa de diálogo Open Saved Log. Digite um nome e uma descrição para o log salvo.
5. Especifique onde salvar o log. Por padrão, os logs salvos são listados sob Saved Logs. Você pode criar um novo nó tocando ou clicando em New Folder, digitando um nome para a pasta e tocando ou clicando em OK.
6. Toque ou clique em OK para fechar a caixa de diálogo Open Saved Log. Você verá o conteúdo do log salvo.

DICA Para remover o log salvo do Event Viewer, toque ou clique em Delete no painel Actions ou no menu Action. Quando solicitado que confirme, toque ou clique em Yes. O arquivo de log salvo ainda existirá em sua localização original.

Monitoramento de desempenho e atividade do servidor

O monitoramento de um servidor não é algo que deva ser feito casualmente. É preciso ter um plano claro – um conjunto de objetivos que se espera alcançar. Vejamos as razões por que você pode querer monitorar um servidor e as ferramentas que pode utilizar para isso.

Por que monitorar seu servidor?

A solução de problemas do desempenho do servidor é uma razão-chave para o monitoramento. Por exemplo, os usuários podem estar com problemas para se conectar ao servidor, e você pode querer monitorá-lo para solucioná-los. Seu objetivo é encontrar o problema, utilizando os recursos disponíveis de monitoramento, e resolvê-lo.

Outra razão comum para querer monitorar um servidor é para melhorar o desempenho dele. Você faz isso melhorando I/O de disco, reduzindo o uso da CPU e a carga de tráfego de rede no servidor. Infelizmente, muitas vezes é preciso fazer alterações quanto ao uso dos recursos. Por exemplo, conforme o número de usuários acessando o servidor aumente, talvez não seja possível reduzir a carga de tráfego de rede, mas você pode melhorar o desempenho do servidor por meio de平衡amento de carga ou distribuição de arquivos de dados-chave em unidades separadas.

Preparação para o monitoramento

Antes de começar a monitorar um servidor, talvez queira estabelecer a medição de desempenho de linha de base para seu servidor. Para isso, meça o desempenho do servidor em vários momentos e sob diferentes condições de carga. Você pode então comparar o desempenho de linha de base com o desempenho subsequente para determinar como está o desempenho do servidor. As medições de desempenho que estiverem muito acima das de linha de base podem indicar áreas em que o servidor precisa ser otimizado ou reconfigurado.

Após estabelecer a medição de linha de base, você deve formular um plano de monitoramento. Um plano de monitoramento inclui estas etapas:

1. Determinar quais eventos do servidor devem ser monitorados para ajudá-lo a conseguir seu objetivo.
2. Definir filtros para reduzir a quantidade de informações coletadas.
3. Configurar contadores de desempenho para inspecionar o uso de recursos.
4. Registrar em log os dados de eventos a fim de que possam ser analisados.
5. Analisar os dados de eventos para ajudar a encontrar soluções para os problemas.

Esses procedimentos serão examinados mais adiante neste capítulo. Embora normalmente se deva desenvolver um plano de monitoramento, algumas vezes você pode não querer passar por todas essas etapas para monitorar seu servidor. Por exemplo, você pode querer monitorar e analisar as atividades conforme aconteçam, em vez de registrar em log e analisar os dados posteriormente.

As principais ferramentas utilizadas para monitorar os servidores incluem o seguinte:

- **Performance Monitor** Utilizado para configurar contadores para inspecionar o uso de recursos ao longo do tempo. Você pode utilizar essas informações para aferir o desempenho do servidor e determinar as áreas que podem ser otimizadas.
- **Reliability Monitor** Monitora alterações no sistema e as compara com as alterações na estabilidade do sistema. Apresenta uma representação gráfica da relação entre as alterações na configuração do sistema e as alterações na confiabilidade do sistema.
- **Resource Monitor** Fornece informações detalhadas sobre o uso de recursos no servidor. As informações fornecidas são similares às fornecidas pelo Task Manager (embora mais minuciosas).
- **Event logs** Utilize as informações nos logs de eventos para solucionar problemas no sistema, inclusive aqueles do sistema operacional e de aplicativos configurados. Os principais logs com que se trabalha são os logs de sistema, de segurança e de aplicativo, bem como os logs para funções de servidor configuradas.

Uso dos consoles de monitoramento

Resource Monitor, Reliability Monitor e Performance Monitor são as opções de ferramentas para o ajuste do desempenho. Você pode acessar o Resource Monitor pressionando Ctrl+Shift+Esc e tocando ou clicando no botão Open Resource Monitor na guia Performance do Task Manager. Como mostrado na Figura 3-18, as estatísticas de uso de recursos estão divididas em quatro categorias:

- **CPU usage** Os detalhes resumidos mostram a utilização atual da CPU e a frequência máxima da CPU (relacionadas à inatividade do processador). Se expandir a entrada CPU (tocando ou clicando no botão de opções), você verá uma lista de executáveis rodando no momento por nome, ID de processo, descrição, status e número de threads utilizadas, a utilização atual da CPU e a utilização média da CPU.
- **Disk usage** Os detalhes resumidos mostram o número de quilobytes por segundo sendo lidos do disco e gravados nele e a mais alta percentagem de uso. Se expandir a entrada Disk abaixo do gráfico (tocando ou clicando no botão de opções), você verá uma lista de executáveis rodando no momento que estão realizando ou realizaram operações de I/O por nome, ID de processo, arquivo sendo lido ou gravado, número médio de bytes sendo lidos por segundo, número médio de bytes sendo gravados por segundo, número total de bytes sendo lidos e gravados por segundo, prioridade de I/O e o tempo de resposta de disco associado.
- **Network usage** Os detalhes resumidos mostram a utilização de largura de banda da rede atual em quilobytes e a percentagem de utilização de largura de banda total. Se expandir a entrada Network abaixo do gráfico (tocando ou clicando no botão de opções), você verá uma lista de executáveis rodando no momento que estejam transferindo ou tenham transferido dados na rede por nome, ID de processo, servidor ou endereço IP sendo contatado, número médio de bytes sendo enviados por segundo, número médio de bytes recebidos por segundo e total de bytes enviados ou recebidos por segundo.
- **Memory usage** Os detalhes resumidos mostram a utilização de memória atual e o número de falhas graves ocorrendo por segundo. Se expandir a entrada Memory abaixo do gráfico (tocando ou clicando no botão de opções), você verá uma lista de executáveis rodando no momento por nome, ID de processo, falhas graves por segundo, memória confirmada em KB, memória do conjunto de trabalho em KB, memória compartilhável em KB e memória privada (não compartilhável) em KB.

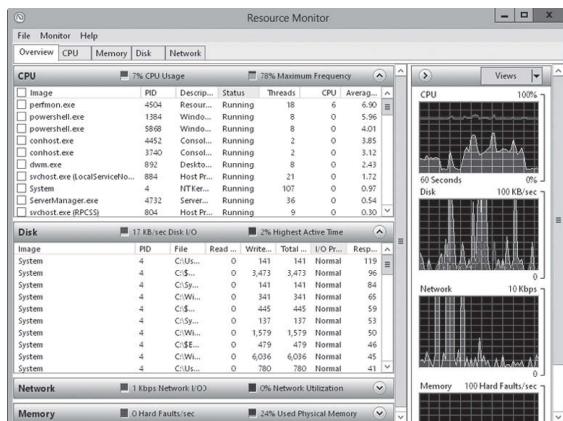


FIGURA 3-18 Examine o uso de recursos no servidor.

O Performance Monitor exibe graficamente estatísticas para o conjunto de parâmetros de desempenho selecionado para exibição. Esses parâmetros de desempenho são referidos como *contadores*. Quando você instala certos aplicativos em um sistema, o Performance Monitor pode ser atualizado com um conjunto de contadores para monitorar o desempenho desse aplicativo. Você atualiza esses contadores ao instalar serviços adicionais e add-ons para aplicativos também.

No Server Manager, pode-se acessar o Performance Monitor em um console autônomo tocando ou clicando em Tools e em Performance Monitor.

No Computer Management, você pode acessar a ferramenta como um snap-in sob o nó System Tools. Expanda System Tools, Performance, Monitoring Tools e selecione Performance Monitor.

Como a Figura 3-19 mostra, o Performance Monitor cria um gráfico representando os contadores sendo monitorados. O intervalo de atualização desse gráfico está definido para um segundo, por padrão, mas pode ser configurado com um valor diferente. Como verá ao trabalhar com o Performance Monitor, as informações de monitoramento são muito valiosas quando se registra informações de desempenho em um arquivo de log a fim de que possam ser reproduzidas de novo. Além disso, o Performance Monitor é útil ao configurar alertas para enviar mensagens quando certos eventos ocorrerem.

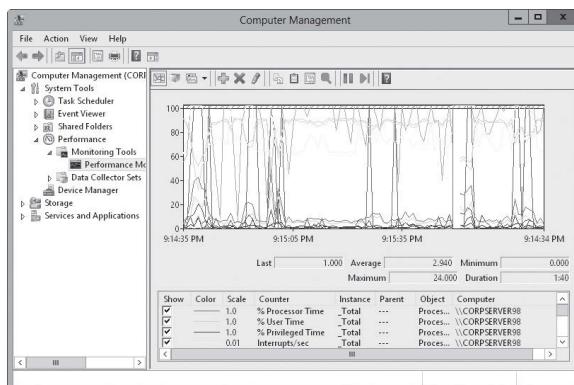


FIGURA 3-19 Examine as medidas de desempenho para o servidor.

O Windows Server 2012 também inclui o Reliability Monitor. Para acessar o Reliability Monitor, siga estas etapas:

1. No Control Panel (Painel de Controle), toque ou clique em Review Your Computer's Status sob o título System And Security.
2. Em Action Center, expanda o painel Maintenance e toque ou clique em View Reliability History.

Com opção, você pode executar o Reliability Monitor digitando **perfmon /rel** em um prompt de comando ou na caixa de pesquisa.

O Reliability Monitor monitora alterações no servidor e as compara com as alterações na estabilidade do sistema. Dessa forma, você pode ver uma representação gráfica da relação entre as alterações na configuração do sistema e as alterações na confiabilidade do sistema. Registrando instalação de software, remoção de software, falhas de aplicativos, falhas de hardware, falhas do Windows e eventos-chave que dizem respeito à configuração do servidor, você pode ver uma linha do tempo de alterações no servidor e em sua confiabilidade e utilizar essas informações para identificar alterações que estejam causando problemas na estabilidade. Por exemplo, se vir uma baixa repentina na confiabilidade, pode tocar ou clicar em um ponto de dados e expandir o conjunto de dados relacionados para localizar o evento específico que causou essa baixa.

Embora o monitoramento de confiabilidade esteja habilitado por padrão para os clientes Windows, pode estar desabilitado para servidores Windows. Quando abrir o Reliability Monitor em um servidor em que o monitoramento de confiabilidade estiver desabilitado, verá um painel de informações dizendo para clicar aqui para ver como ativar ou reconfigurar a RACTask. A RACTask é uma tarefa agendada que é executada em segundo plano para coletar dados de confiabilidade.

Escolha de contadores para monitoramento

O Performance Monitor exibe informações apenas para contadores sendo monitorados. Milhares de contadores estão disponíveis, e você encontrará contadores relacionados a praticamente qualquer função de servidor que tiver instalado. A maneira mais fácil de aprender sobre esses contadores é ler as explicações disponíveis na caixa de diálogo Add Counters. Inicie o Performance Monitor, toque ou clique em Add na barra de ferramentas e expanda um objeto na lista Available Counters. Marque a caixa de seleção Show Description e percorra a lista de contadores desse objeto.

Quando o Performance Monitor está monitorando um objeto específico, pode rastrear todas as instâncias de todos os contadores desse objeto. As *instâncias* são várias ocorrências de um contador específico. Por exemplo, quando você monitora contadores do objeto Processor em um sistema multiprocessador, tem a escolha de monitorar todas as instâncias de processadores ou instâncias específicas de processadores. Se achar que um processador específico está falhando ou experimentando outros problemas, pode monitorar apenas essa instância do processador.

Para selecionar quais contadores deseja monitorar, siga estas etapas:

1. O Performance Monitor tem vários modos de exibição e tipos de exibição. Certifique-se de que a atividade atual é exibida tocando ou clicando em View Current Activity na barra de ferramentas ou pressionando Ctrl+T. Você pode alternar entre os tipos de exibição (Line, Histogram Bar e Report) tocando ou clicando em Change Graph Type ou pressionando Ctrl+G.
2. Para adicionar contadores, toque ou clique em Add na barra de ferramentas ou pressione Ctrl+N. A caixa de diálogo Add Counters, mostrada na Figura 3-20, será exibida.

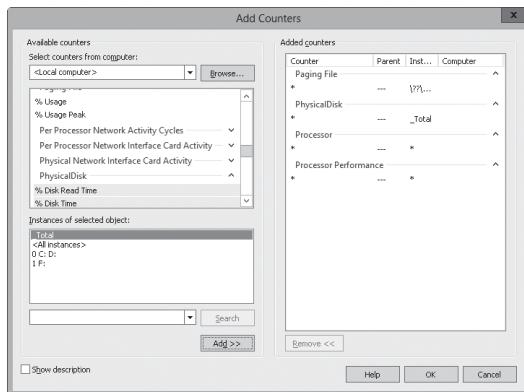


FIGURA 3-20 Selecione os objetos e contadores que deseja monitorar.

3. Na lista Select Counters From Computer, digite o nome Universal Naming Convention (UNC) do servidor com o qual quer trabalhar, como \\CorpServer84, ou escolha <Local Computer> para trabalhar com o computador local.

OBSERVAÇÃO Você precisa ao menos ser membro do grupo Performance Monitor Users no domínio ou no computador local para realizar o monitoramento remoto. Ao usar o registro em log de desempenho, é preciso ao menos ser membro do grupo Performance Log Users no domínio ou no computador local para trabalhar com logs de desempenho em computadores remotos.

4. No painel Available Counters, os objetos de desempenho estão listados em ordem alfabética. Se selecionar a entrada de um objeto tocando ou clicando nela, todos os contadores relacionados serão selecionados. Se expandir a entrada de um objeto, poderá ver todos os contadores relacionados e selecionar contadores individuais tocando ou clicando neles. Por exemplo, você poderia expandir a entrada do objeto Active Server Pages e selecionar os contadores Requests Failed Total, Requests Not Found, Requests Queued e Requests Total.
5. Ao selecionar um objeto ou qualquer de seus contadores, você verá as instâncias relacionadas. Escolha All Instances para selecionar todas as instâncias de contadores para monitoramento, ou selecione uma ou mais instâncias de processadores a monitorar. Por exemplo, você poderia selecionar instância de Anonymous Users/Sec para sites individuais ou para todos os sites.
6. Quando tiver selecionado um objeto ou um grupo de contadores para um objeto, bem como as instâncias do objeto, toque ou clique em Add para adicionar os contadores ao gráfico.
7. Repita as etapas de 4 a 6 para adicionar outros contadores de desempenho.
8. Toque ou clique em OK ao terminar.

DICA Não tente usar um gráfico com muitos contadores ou instâncias de contadores de uma vez só. Isso tornará a exibição muito difícil de ler e utilizará recursos do sistema – isto é, memória e tempo de CPU – que podem afetar a resposta do servidor.

Registro em log de desempenho

O Windows Server 2008 R2 introduziu conjuntos de coletores de dados e relatórios. Os conjuntos de coletores de dados permitem especificar conjuntos de objetos e contadores de desempenho que você queira monitorar. Uma vez que tenha criado um conjunto de coletores de dados, poderá iniciar ou interromper o monitoramento de objetos e contadores de desempenho incluídos no conjunto com facilidade. De certa forma, isso torna os conjuntos de coletores de dados similares aos logs de desempenho utilizados em versões anteriores do Windows. Contudo, os conjuntos de coletores de dados são muito mais sofisticados. Você pode utilizar um único conjunto de dados para gerar vários contadores de desempenho e logs de rastreamento. Também é possível fazer o seguinte:

- Atribuir controles de acesso para gerenciar quem pode acessar os dados coletados
- Criar vários cronogramas de execução e condições de interrupção para monitoramento
- Utilizar gerenciadores de dados para controlar o tamanho de dados coletados e relatórios
- Gerar relatórios baseados nos dados coletados

Na ferramenta Performance, pode-se examinar conjuntos de coletores de dados e relatórios configurados atualmente sob os nós Data Collector Sets e Reports, respectivamente. Como mostrado na Figura 3-21, você encontrará conjuntos de dados e relatórios que são definidos pelo usuário e definidos pelo sistema. Os conjuntos de dados definidos pelo usuário são criados por usuários para monitoramento geral e ajuste de desempenho. Os conjuntos de dados definidos pelo sistema são criados pelo sistema operacional para auxiliar nos diagnósticos automáticos.

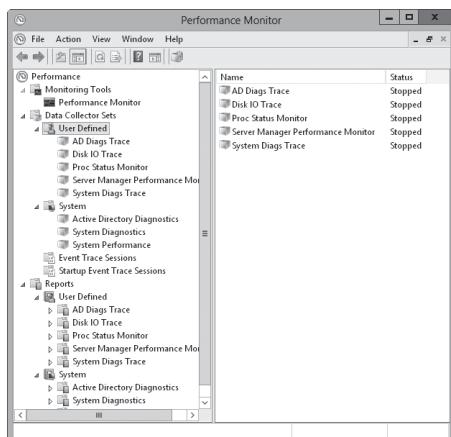


FIGURA 3-21 Acesse os conjuntos de coletores de dados e relatórios.

Como criar e gerenciar conjuntos de coletores de dados

Para visualizar os conjuntos de coletores de dados configurados no momento, selecione a opção Performance Monitor no grupo de programas Administrative Tools e expanda o nó Data Collector Sets. Pode-se trabalhar com coletores de dados de diversas maneiras:

- Você pode visualizar os conjuntos de coletores de dados definidos pelo usuário ou pelo sistema selecionando User Defined ou System, conforme apropriado. Quando selecionar um conjunto de coletores de dados no painel esquerdo, verá os coletores de dados relacionados no painel principal listados por nome e tipo. O tipo Trace é para coletores de dados que registrem dados de desempenho sempre que eventos relacionados ocorrerem. O tipo Performance Counter é para coletores de dados que registram dados em contadores selecionados quando um intervalo predeterminado tiver decorrido. O tipo Configuration é para coletores de dados que registram alterações em caminhos de registro específicos.
- Você pode visualizar rastreamentos de eventos em execução selecionando Event Trace Sessions. Pode-se então interromper um coletor de dados que esteja executando um rastreamento pressionando e segurando ou clicando com o botão direito do mouse nele e selecionando Stop.
- Você pode visualizar o status habilitado ou desabilitado de rastreamentos de eventos configurados para executar automaticamente quando o computador é iniciado selecionando Startup Event Trace Sessions. Pode-se iniciar um rastreamento pressionando e segurando ou clicando com o botão direito do mouse em um coletor de dados e selecionando Start As Event Trace Session. Você pode excluir um coletor de dados pressionando e segurando ou clicando com o botão direito do mouse e tocando ou clicando em Delete.
- Você pode salvar um coletor de dados como um modelo que pode ser utilizado como base para outros coletores de dados pressionando e segurando ou clicando com o botão direito do mouse no coletor de dados e selecionando Save Template. Na caixa de diálogo Save As, selecione um diretório, digite um nome para o modelo e toque ou clique em Save. O modelo de coletor de dados será salvo como um arquivo XML que pode ser copiado para outros sistemas.
- Você pode excluir um coletor de dados definido pelo usuário pressionando e segurando ou clicando com o botão direito do mouse nele e selecionando Delete. Se um coletor de dados estiver em execução, primeiro é preciso parar de coletar dados e então excluir o coletor. A exclusão do coletor exclui também os relatórios relacionados.

Como coletar dados de contadores de desempenho

Os coletores de dados podem ser utilizados para registrar os dados de desempenho nos contadores selecionados em um intervalo de amostragem específico. Por exemplo, você poderia coletar dados de desempenho da CPU a cada 15 minutos.

Para coletar dados de contadores de desempenho, siga estas etapas:

1. No Performance Monitor, sob o nó Data Collector Sets, pressione e segure ou clique com o botão direito do mouse no nó User Defined no painel esquerdo, aponte para New e escolha Data Collector Set.

2. No Create New Data Collector Set Wizard, digite um nome para o coletor de dados, como **System Performance Monitor** ou **Processor Status Monitor**. Note que, se digitar um nome inválido, como um caractere não alfanumérico, não será possível prosseguir.
3. Selecione a opção Create Manually e toque ou clique em Next.
4. Na página What Type Of Data Do You Want To Include, a opção Create Data Logs está selecionada por padrão. Marque a caixa de seleção Performance Counter e toque ou clique em Next.
5. Na página Which Performance Counters Would You Like To Log, toque ou clique em Add. A caixa de diálogo Add Counters, que pode ser utilizada como abordado anteriormente para selecionar os contadores de desempenho a monitorar, será exibida. Quando tiver terminado de selecionar os contadores, toque ou clique em OK.
6. Na página Which Performance Counters Would You Like To Log, digite um intervalo de amostragem e selecione uma unidade de tempo em segundos, minutos, horas, dias ou semanas. O intervalo de amostragem especifica quando os novos dados serão coletados. Por exemplo, se coletar uma amostra a cada 15 minutos, o log de dados será atualizado a cada 15 minutos. Toque ou clique em Next quando estiver pronto para continuar.
7. Na página Where Would You Like The Data To Be Saved, digite o caminho a ser utilizado para armazenar os log dos dados coletados. Como opção, toque ou clique em Browse e utilize a caixa de diálogo Browse For Folder para selecionar o diretório onde será armazenado o registro em log. Toque ou clique em Next quando estiver pronto para continuar.

PRÁTICAS RECOMENDADAS A localização padrão para o arquivo do registro em log é %SystemDrive%\PerfLogs\Admin. Os arquivos de log podem aumentar de tamanho rapidamente. Se planeja registrar dados em log por um período longo, certifique-se de colocar o arquivo de log em uma unidade com muito espaço livre. Lembre-se, quanto maior a frequência de atualização do arquivo de log, maior o espaço na unidade e uso de recursos da CPU no sistema.

8. Na página Create Data Collector Set, a caixa Run As mostra <Default> para indicar que o log será executado sob os privilégios e permissões da conta padrão do sistema. Para executar o log com os privilégios e permissões de outro usuário, toque ou clique em Change. Digite o nome de usuário e a senha da conta e toque ou clique em OK. Os nomes de usuário podem ser digitados no formato domínio\ nome de usuário, como cpandl\williams para a conta Williams no domínio Cpndl.
9. Selecione a opção Open Properties For This Data Collector Set e toque ou clique em Finish. O conjunto de coletores de dados será salvo, o assistente fechado, e a caixa de diálogo Properties relacionada será aberta.
10. Por padrão, o registro em log está configurado para iniciar manualmente. Para configurar um cronograma de registro em log, toque ou clique na guia Schedule e em Add. Agora você pode definir Active Range, Start Time e dias de execução para a coleta de dados.
11. Por padrão, o registro em log para somente se for definido um prazo de validade como parte do cronograma de registro em log. Utilizando as opções na guia Stop Condition, você pode configurar o arquivo de log para parar automaticamente

após um período de tempo especificado, como sete dias, ou quando o arquivo de log estiver cheio (se um limite de tamanho máximo for definido).

12. Toque ou clique em OK quando terminar de definir o cronograma de registro em log e as condições de interrupção. Você pode gerenciar o coletor de dados conforme explicado anteriormente.

OBSERVAÇÃO Você pode configurar o Windows para executar uma tarefa agendada quando a coleta de dados parar. Configure a execução de tarefas na guia Tasks da caixa de diálogo Properties.

Como coletar dados de rastreamento de desempenho

Você pode utilizar os coletores de dados para registrar dados de rastreamento de desempenho sempre que eventos relacionados a seus provedores de origem ocorrerem. Um provedor de origem é um aplicativo ou serviço do sistema operacional que tenha eventos rastreáveis.

Para coletar dados de rastreamento de desempenho, siga estas etapas:

1. No Performance Monitor, sob o nó Data Collector Sets, pressione e segure ou clique com o botão direito do mouse no nó User Defined no painel esquerdo, aponte para New e escolha Data Collector Set.
2. No Create New Data Collector Set Wizard, digite um nome para o coletor de dados, como **Logon Trace** ou **Disk IO Trace**. Note que, se digitar um nome inválido, como um caractere não alfanumérico, não será possível prosseguir.
3. Selecione a opção Create Manually e toque ou clique em Next.
4. Na página What Type Of Data Do You Want To Include, a opção Create Data Logs está selecionada por padrão. Marque a caixa de seleção Event Trace Data e toque ou clique em Next.
5. Na página Which Event Trace Providers Would You Like To Enable, toque ou clique em Add. Selecione um provedor de rastreamento de evento a rastrear e toque ou clique em Next. Selecionando propriedades individuais na lista Properties e tocando ou clicando em Edit, você pode rastrear valores de propriedades específicas, em vez de todos os valores do provedor. Repita esse processo para selecionar outros provedores de rastreamento de evento a rastrear. Toque ou clique em Next quando estiver pronto para continuar.
6. Complete as etapas de 7 a 12 do procedimento na seção anterior, "Como coletar dados de contadores de desempenho".

Como coletar dados de configuração

Você pode utilizar coletores de dados para registrar alterações na configuração do registro. Para coletar dados de configuração, siga estas etapas:

1. No Performance Monitor, sob o nó Data Collector Sets, pressione e segure ou clique com o botão direito do mouse no nó User Defined no painel esquerdo, aponte para New e escolha Data Collector Set.
2. No Create New Data Collector Set Wizard, digite um nome para o coletor de dados, como **AD Registry** ou **Registry Adapter Info**.
3. Selecione a opção Create Manually e toque ou clique em Next.

4. Na página What Type Of Data Do You Want To Include, a opção Create Data Logs está selecionada por padrão. Marque a caixa de seleção System Configuration Information e toque ou clique em Next.
5. Na página Which Registry Keys Would You Like To Record, toque ou clique em Add. Digite o caminho de registro a monitorar. Repita esse processo para adicionar outros caminhos de registro a monitorar. Toque ou clique em Next quando estiver pronto para continuar.
6. Complete as etapas de 7 a 12 do procedimento na seção “Como coletar dados de contadores de desempenho”.

Visualização de relatórios de coletores de dados

Ao solucionar problemas, muitas vezes você irá querer registrar em log dados de desempenho por um período longo de tempo e examinar os dados para analisar os resultados. Para cada coletor de dados que tiver estado ou estiver inativo no momento, você encontrará relatórios do coletor de dados relacionado. Como com os próprios conjuntos de coletores de dados, os relatórios de coletores de dados estão organizados em duas categorias gerais: definidos pelo usuário e pelo sistema.

Você pode visualizar os relatórios dos coletores de dados no Performance Monitor. Expanda o nó Reports e o nó do relatório individual para o coletor de dados que quiser analisar. Sob o nó de relatório do coletor de dados, você encontrará relatórios individuais para cada sessão de registro em log. Uma sessão de registro em log começa quando o registro em log inicia e termina quando ele é encerrado.

O log mais recente é aquele com o maior número de log. Se um coletor de dados estiver registrando ativamente em log, não será possível visualizar o log mais recente. Pode-se interromper a coleta de dados pressionando e segurando ou clicando com o botão direito do mouse em um conjunto de coletores de dados e selecionando Stop. Para contadores de desempenho, os dados coletados são mostrados por padrão em uma exibição gráfica desde o início da coleta de dados até o fim dela, como mostrado na Figura 3-22.

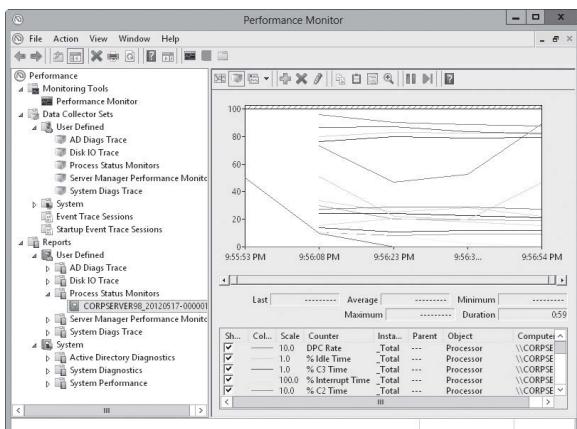


FIGURA 3-22 Visualize os relatórios de coletores de dados.

Você pode modificar os detalhes do relatório utilizando estas técnicas:

1. No painel de monitoramento, pressione Ctrl+Q ou toque ou clique no botão Properties na barra de ferramentas. A caixa de diálogo Performance Monitor Properties será exibida.
2. Toque ou clique na guia Source.
3. Especifique as fontes de dados a analisar. Sob Data Source, toque ou clique em Log Files e em Add para abrir a caixa de diálogo Select Log File. Agora você pode selecionar os arquivos de log adicionais a analisar.
4. Especifique a janela de tempo que quer analisar. Toque ou clique em Time Range e arraste a barra Total Range para especificar os momentos de início e fim apropriados. Arraste a borda esquerda para a direita para adiar o momento inicial. Arraste a borda direita para a esquerda para adiar o momento final.
5. Toque ou clique na guia Data. Pode-se agora selecionar os contadores para visualização. Selecione um contador e toque ou clique em Remove para removê-lo da exibição gráfica. Toque ou clique em Add para exibir a caixa de diálogo Add Counter, que pode ser utilizada para selecionar os contadores que se quer analisar.

OBSERVAÇÃO Somente os contadores selecionados para o registro em log estão disponíveis. Se não vir um contador com o qual quer trabalhar, é preciso modificar as propriedades do coletor de dados, reiniciar o processo de registro em log e verificar os logs em uma data posterior.

6. Toque ou clique em OK. No painel de monitoramento, toque ou clique no botão Change Graph Type para selecionar o tipo de gráfico.

Configuração de alertas de contadores de desempenho

Você pode configurar alertas para notificá-lo quando certos eventos ocorrerem ou quando certos limites de desempenho forem alcançados. Pode-se enviar esses alertas como mensagens de rede e como eventos registrados em log no log de eventos de aplicativo. Você também pode configurar alertas para iniciar aplicativos e logs de desempenho.

Para configurar um alerta, siga estas etapas:

1. No Performance Monitor, sob o nó Data Collector Sets, pressione e segure ou clique com o botão direito do mouse no nó User Defined no painel esquerdo, aponte para New e escolha Data Collector Set.
2. No Create New Data Collector Set Wizard, digite um nome para o coletor de dados, como **Processor Alert** ou **Disk IO Alert**.
3. Selecione a opção Create Manually e toque ou clique em Next.
4. Na página What Type Of Data Do You Want To Include, selecione a opção Performance Counter Alert e toque ou clique em Next.
5. Na página Which Performance Counters Would You Like To Monitor, toque ou clique em Add para exibir a caixa de diálogo Add Counters. Essa caixa de diálogo é idêntica à caixa de diálogo Add Counters comentada anteriormente. Utilize a caixa de diálogo para adicionar contadores que disparem o alerta. Toque ou clique em OK ao terminar.

6. No painel Performance Counters, selecione o primeiro contador e utilize a caixa de texto Alert When Value Is para definir a ocasião em que um alerta desse contador será disparado. Os alertas podem ser disparados quando o contador estiver acima ou abaixo de um valor específico. Selecione Above ou Below e defina o valor para disparo. A unidade de medida é qualquer uma que faça sentido para os contadores selecionados no momento. Por exemplo, para gerar um alerta se o tempo do processador for acima de 95%, selecione Over e digite **95**. Repita esse processo para configurar outros contadores selecionados.
7. Complete as etapas de 7 a 12 do procedimento na seção “Como coletar dados de contadores de desempenho”.

Ajuste do desempenho do sistema

Agora que você sabe como monitorar seu sistema, vejamos como pode ajustar o sistema operacional e o desempenho de hardware. Examinaremos as seguintes áreas:

- Uso de memória e cache
- Utilização do processador
- I/O de disco
- Largura de banda e conectividade de rede

Monitoramento e ajuste do uso de memória

A memória é muitas vezes a fonte de problemas de desempenho e você deve sempre descartar problemas nela antes de examinar outras áreas do sistema. Os sistemas utilizam tanto a memória física quanto a virtual. Para descartar problemas de memória em um sistema, deve-se configurar o desempenho dos aplicativos, o uso de memória e as configurações de taxa de transferência de dados e, então, monitorar o uso de memória do servidor para verificar problemas.

As configurações de desempenho do aplicativo e uso de memória determinam como os recursos do sistema serão alocados. Na maioria dos casos, você irá querer dar ao sistema operacional e aplicativos em segundo plano a maior parte dos recursos. Isso é especialmente verdadeiro para servidores do Active Directory, de arquivos, de impressão e de rede e comunicações. Por outro lado, para servidores de aplicativos, de banco de dados e de streaming de mídia, você deve dar aos programas em execução no servidor a maioria dos recursos, como abordado em “Como configurar o desempenho de aplicativos” no Capítulo 2.

Utilizando as técnicas de monitoramento discutidas anteriormente neste capítulo, você pode determinar como o sistema está usando a memória e verificar problemas. A Tabela 3-1 fornece uma visão geral dos contadores que você desejará monitorar para descobrir gargalos de memória, cache e memória virtual (paginação). A tabela está organizada por categoria de problema.

TABELA 3-1 Descoberta de gargalos relacionados à memória

PROBLEMA	CONTADORES A MONITORAR	DETALHES
Uso de memória física e virtual	Memory\Available Kbytes Memory\Committed Bytes	Memory\Available Kbytes é a quantidade de memória física disponível para processos em execução no servidor. Memory\Committed Bytes é a quantidade de memória virtual confirmada. Se um servidor tiver pouquíssima memória disponível, talvez seja preciso adicionar memória ao sistema. Em geral, você desejará que a memória disponível seja não menos do que 5% da memória física total no servidor. Se o servidor tiver uma alta proporção de bytes confirmados para a memória física total no sistema, talvez também seja preciso adicionar memória. Em geral, você desejará que o valor dos bytes confirmados não seja mais do que 75% da memória física total.
Falha de página de memória	Memory\Page Faults/sec Memory\Pages Input/sec Memory\Page Reads/sec	Uma falha de página ocorre quando um processo solicita uma página na memória e o sistema não consegue localizá-la no local solicitado. Se a página solicitada estiver em outro lugar da memória, a falha é chamada de soft page fault (<i>falha de página menor</i>). Se a página solicitada tiver de ser recuperada do disco, a falha é chamada de hard page fault (<i>falha de página grave</i>). A maioria dos processadores pode lidar com grandes quantidades de falhas menores. As falhas graves, no entanto, podem causar atrasos significativos. Page Faults/sec é a taxa geral na qual o processador lida com todos os tipos de falhas de página. Pages Input/sec é o número total de páginas lidas do disco para resolver falhas de página graves. Page Reads/sec é o total de leituras de disco necessárias para resolver falhas de página graves. Pages Input/sec será maior ou igual a Page Reads/sec e pode dar uma boa ideia da taxa de falhas de página graves. Um número alto de falhas de página graves poderia indicar que é preciso aumentar a quantidade de memória ou reduzir o tamanho de cache no servidor.

Continua

TABELA 3-1 Descoberta de gargalos relacionados à memória (*continuação*)

PROBLEMA	CONTADORES A MONITORAR	DETALHES
Paginação de memória	Memory\Pool Paged Bytes Memory\Pool Nonpaged Bytes	Esses contadores monitoram o número de bytes para reserva de memória paginável e não paginável. A reserva de memória paginável é uma área da memória do sistema para objetos que podem ser gravados em disco quando não são utilizados. A reserva de memória não paginável é uma área da memória do sistema para objetos que não podem ser gravados em disco. Se o tamanho da reserva de memória paginável for grande em relação à quantidade total de memória física no sistema, pode ser necessário adicionar memória ao sistema. Se o tamanho da reserva de memória não paginável for grande em relação à quantidade total de memória virtual alocada para o servidor, você pode querer aumentar o tamanho da memória virtual.

Monitoramento e ajuste do uso de processador

A CPU faz o processamento real das informações no servidor. Ao examinar o desempenho de um servidor, você deve focar na CPU após eliminar os gargalos de memória. Se os processadores do servidor forem o gargalo de desempenho, adicionar memória, unidades de disco ou conexões de rede não irá resolver o problema. Em vez disso, talvez seja necessário atualizar os processadores para velocidades de clock mais rápidas ou adicionar processadores para aumentar a capacidade do servidor. Você também poderia mover aplicativos que exigem muito do processador, como o SQL Server, para outro servidor.

Antes de tomar uma decisão de atualizar ou adicionar CPUs, você deve descartar problemas com a memória e o cache. Se os sinais ainda apontarem para um problema de processador, você deve monitorar os contadores de desempenho listados na Tabela 3-2. Certifique-se de monitorar esses contadores para cada CPU instalada no servidor.

TABELA 3-2 Descoberta de gargalos relacionados ao processador

PROBLEMA	CONTADORES A MONITORAR	DETALHES
Enfileiramento de threads	System\Processor Queue Length	Este contador exibe o número de threads esperando para serem executadas. Essas threads são enfileiradas em uma área compartilhada por todos os processadores no sistema. Se esse contador tiver um valor mantido em mais que 10 threads por processador, é preciso atualizar ou adicionar processadores.

PROBLEMA	CONTADORES A MONITORAR	DETALHES
Uso da CPU	Processor\% Processor Time	Este contador exibe a percentagem de tempo que a CPU selecionada está executando uma thread não ociosa. Você deve monitorar esse contador separadamente para todas as instâncias de processador no servidor. Se os valores de % Processor Time forem altos enquanto as taxas de interface de rede e de transferência de I/O de disco forem relativamente baixas, é preciso atualizar ou adicionar processadores.

Monitoramento e ajuste de I/O de disco

Com os discos de alta velocidade atuais, a taxa de transferência de disco raramente será a causa de um gargalo. Dito isso, o acesso à memória é muito mais rápido do que o acesso aos discos. Portanto, se o servidor tiver de fazer muitas leituras e gravações em disco, o desempenho geral do servidor pode ser diminuído. Para reduzir a quantidade de I/O de disco, você desejará que o servidor gerencie a memória de maneira eficaz e page para o disco somente quando necessário. O uso de memória é monitorado e ajustado conforme abordado em "Monitoramento e ajuste do uso de memória".

Além do ajuste de memória, pode-se monitorar alguns contadores para aferir a atividade de I/O do disco. Especificamente, deve-se monitorar os contadores listados na Tabela 3-3.

TABELA 3-3 Descoberta de gargalos relacionados à unidade

PROBLEMA	CONTADORES A MONITORAR	DETALHES
Desempenho geral da unidade	PhysicalDisk%\ Disk Time in conjunction with Processor\% Processor Time and Network Interface Connection\Bytes Total/sec	Se o valor de % Disk Time for alto e os valores do processador e da conexão de rede não o forem, as unidades de disco rígido do sistema podem estar criando um gargalo. Certifique-se de monitorar % Disk Time para todas as unidades de disco rígido no servidor.
Disk I/O	PhysicalDisk\Disk Writes/sec, PhysicalDisk\Disk Reads/sec, PhysicalDisk\Avg. Disk Write Queue Length, PhysicalDisk\Avg. Disk Read Queue Length, PhysicalDisk\CurrentDisk Queue Length	O número de gravações e leituras por segundo informa quanta atividade de I/O de disco existe. O tamanho de fila de espera de gravação e leitura dizem quantas solicitações de gravação ou leitura estão esperando para ser processadas. Em geral, você desejará ter pouquíssimas solicitações em espera. Lembre-se de que os atrasos de solicitação são proporcionais ao tamanho das filas menos o número de unidades em um conjunto de redundant array of independent disks (RAID).

Monitoramento e ajuste de largura de banda e conectividade de rede

Nenhum outro fator importa mais para a maneira como o usuário percebe o desempenho do servidor do que a rede que conecta o servidor ao computador do usuário. O atraso, ou a latência, entre o momento em que uma solicitação é feita e aquele em que é recebida pode fazer toda a diferença. Com um alto grau de latência, não importa se você tem o servidor mais rápido do planeta: o usuário se depara com um atraso e considera que os servidores são lentos.

Falando em termos gerais, a latência com a qual o usuário se depara está fora de seu controle. É uma função do tipo de conexão que o usuário tem e da rota que a solicitação faz para o servidor. A capacidade total do servidor para lidar com solicitações e a quantidade de largura de banda disponível para os servidores, no entanto, estão sob seu controle. A disponibilidade de largura de banda da rede é uma função da infraestrutura de rede de sua empresa. A capacidade de rede é uma função das placas e interfaces de rede configurada nos servidores.

A capacidade da sua placa de rede pode ser um fator limitante em algumas instâncias. Embora a rede de 10 Gbps seja cada vez mais utilizada, a maioria dos servidores utiliza placas de rede de 100 Mbps ou 1 Gbps, que podem ser configuradas de várias maneiras. Alguém poderia ter configurado uma placa de 1 Gbps para 100 Mbps, ou a placa pode estar configurada para half duplex, em vez de full duplex. Se suspeitar de um problema de capacidade com uma placa de rede, você sempre deve verificar a configuração.

Para determinar a taxa de transferência e a atividade atual nas placas de rede de um servidor, pode-se verificar os seguintes contadores:

- Network\Bytes Received/sec
- Network\Bytes Sent/sec
- Network\Bytes Total/sec
- Network Current Bandwidth

Se o valor total de bytes por segundo for mais do que 50% da capacidade total sob condições típicas de carga, o servidor pode ter problemas sob condições de pico de carga. Você pode querer garantir que as operações que usem muita largura de banda da rede, como backups de rede, sejam realizadas em uma interface separada. Lembre-se de que você deve comparar esse valores em conjunto com PhysicalDisk%\ Disk Time e Processor%\ Processor Time. Se os valores de tempo do disco e tempo do processador forem baixos, mas os valores de rede forem muito altos, pode haver um problema de capacidade. Solucione o problema otimizando as configurações da placa de rede ou adicionando uma placa de rede. Lembre, planejamento é tudo – nem sempre é tão simples quanto inserir uma placa e ligá-la na rede.

CAPÍTULO 4

Automatização de tarefas administrativas, políticas e procedimentos

- Group Policies **135**
- Navegação pelas alterações em Group Policy **139**
- Gerenciamento de Group Policies locais **141**
- Gerenciamento de políticas de site, domínio e unidade organizacional **144**
- Manutenção e solução de problemas de Group Policy **156**
- Gerenciamento de usuários e computadores por meio de Group Policy **171**

Executar todos os dias tarefas de rotina, lidar com sistemas de políticas e apresentar aos usuários princípios básicos não são usos eficientes de seu tempo. O seu trabalho seria muito mais eficaz se você pudesse automatizar essas tarefas e manter o foco em questões mais significativas. Os serviços de suporte têm como objetivo aumentar a produtividade e permitir que você se dedique menos a questões irrelevantes e mais ao que é importante.

O Microsoft Windows Server 2012 inclui diversas funções, serviços de função e recursos que ajudam a dar suporte a instalações de servidor. Alguns desses componentes podem ser instalados e usados com facilidade. Se você precisa de uma ferramenta administrativa para gerenciar uma função ou recurso em um computador remoto, pode selecionar a ferramenta para ser instalada como parte do recurso Remote Server Administration Tools (RSAT, Ferramentas de Administração de Servidor Remoto). Se um servidor tiver um adaptador sem fio, você pode instalar o recurso Wireless LAN Service para habilitar conexões sem fio. Além desses e outros componentes básicos de suporte, você pode usar muitos outros recursos de suporte, entre eles:

- **Automatic Updates** Garante que o sistema operacional permaneça atualizado e com as atualizações de segurança mais recentes. Se a atualização de um servidor for realizada por meio do Microsoft Update e não do Windows Updates padrão, você pode obter atualizações também para outros produtos. Por padrão, o recurso Automatic Updates está instalado, mas não habilitado em servidores com Windows Server 2012. Você pode configurá-lo com o utilitário Windows Update no Control Panel. Em Control Panel, System And Security, toque ou clique em Turn Automatic Updating On or Off. Para aprender a configurar o Automatic Updates por meio de Group Policy (política de grupo), consulte “Configuração do Automatic Updates” mais adiante neste capítulo.

- **BitLocker Drive Encryption** Fornece uma camada adicional de segurança para os discos rígidos de um servidor. Isso protege os discos de ataques por parte de quem tem acesso físico ao servidor. A criptografia do BitLocker pode ser usada em servidores com ou sem um Trusted Platform Module (TPM). Quando você adiciona esse recurso a um servidor por meio do Add Roles And Features Wizard, é possível gerenciá-lo usando o utilitário BitLocker Drive Encryption no Control Panel. Em Control Panel, System And Security, toque ou clique em BitLocker Drive Encryption. O Windows Server 2008 R2 e versões superiores (como Windows 7 e superior) incluem o BitLocker To Go, que permite a criptografia de unidades flash USB. Se seu servidor não tiver o BitLocker, execute o BitLocker To Go Reader, que está armazenado em uma área não criptografada da unidade flash USB criptografada.
- **Remote Assistance** Fornece um recurso de assistência que permite a um administrador enviar uma solicitação de assistência remota para um administrador mais sênior. O administrador sênior pode, então, aceitar a solicitação para visualizar a área de trabalho do usuário e controlar temporariamente o computador para solucionar o problema. Quando você adiciona esse recurso a um servidor por meio do Add Roles And Features Wizard, é possível gerenciá-lo usando as opções da guia Remote da caixa de diálogo System Properties. Em Control Panel, System And Security, toque ou clique em Allow Remote Access sob o título System para ver as opções relacionadas.
- **Remote Desktop** Fornece um recurso de conectividade remota que permite a você se conectar a um servidor e fazer seu gerenciamento a partir de outro computador. Por padrão, o recurso Remote Desktop está instalado, mas não habilitado em servidores Windows Server 2012. A configuração do Remote Desktop pode ser realizada com as opções da guia Remote da caixa de diálogo System Properties. Em Control Panel, System And Security, toque ou clique em Allow Remote Access sob o título System para ver as opções relacionadas. Você pode estabelecer conexões remotas usando o utilitário Remote Desktop Connection.
- **Task Scheduler** Permite que você agende a execução de tarefas únicas e também recorrentes, como tarefas de manutenção de rotina. O Windows Server 2012 usa amplamente as funcionalidades das tarefas agendadas. Você pode visualizar e trabalhar com as tarefas agendadas em Computer Management. Expanda os nós System Tools, Task Scheduler e Task Scheduler Library para exibir as tarefas agendadas configuradas.
- **Desktop Experience** Este sub-recurso do User Interfaces And Infrastructure instala a funcionalidade de área de trabalho do Windows no servidor. Você pode usar esse recurso quando o Windows Server 2012 for usado como seu sistema operacional de área de trabalho. Quando você adicionar esse recurso usando o Add Roles And Features Wizard, a funcionalidade de área de trabalho do servidor é aprimorada e os programas a seguir também são instalados: Windows Media Player, Desktop Themes, Video for Windows (compatível com AVI), Disk Cleanup, Sound Recorder, Character Map e Snipping Tool.
- **Windows Firewall** Ajuda a proteger o computador de ataques por parte de usuários não autorizados. O Windows Server inclui um firewall básico chamado Windows Firewall e um firewall avançado chamado Windows Firewall With Advanced Security. Por padrão, os firewalls estão habilitados nas instalações de servidor. Para acessar o firewall básico, toque ou clique em Windows Firewall no

Control Panel. Para acessar o firewall avançado, selecione Windows Firewall With Advanced Security no menu Tools do Server Manager.

- **Windows Time** Sincroniza o sistema com a hora mundial para garantir que a hora do sistema esteja certa. Você também pode configurar os computadores para sincronizarem com um servidor de horário específico. O modo de funcionamento do Windows Time depende do fato do computador ser membro de um domínio ou grupo de trabalho. Em um domínio, controladores de domínio são usados para sincronização de horário, e você pode gerenciar esse recurso por meio de Group Policy. Em um grupo de trabalho, servidores de horário da Internet são usados para sincronização de horário, e você pode gerenciar esse recurso por meio do utilitário Date And Time.

A configuração e o gerenciamento desses componentes de suporte podem ser feitos da mesma forma no Windows 8 e no Windows Server 2012. Você encontrará uma grande abrangência desses componentes de suporte no livro *Windows 8 Administration Pocket Consultant* (Microsoft Press, 2012).

Muitos outros componentes fornecem serviços de suporte. No entanto, você precisará desses serviços adicionais de suporte apenas em situações específicas. Você pode usar servidores IP Address Management (IPAM) quando desejar gerenciar seu espaço de endereços IP e rastrear tendências de uso de endereços IP. O Remote Desktop Services pode ser usado quando você desejar permitir que usuários executem aplicativos em um servidor remoto. Você pode usar o Windows Deployment Services (WDS, Serviços de Implantação do Windows) quando desejar habilitar a implantação automatizada de sistemas operacionais baseados em Windows. O único serviço de suporte constantemente ativado que deve ser dominado para se obter êxito com o Windows Server 2012 é a Group Policy.

MUNDO REAL A barra de charms da tela inicial tem o item Search, que pode ter como foco Apps, Settings ou Files. Quando você pressiona a tecla Windows e digita, o texto é inserido na caixa Search. Como o foco padrão é de uma busca por aplicativos, isso permite que você procure por um programa instalado em um servidor com rapidez.

Ao longo deste texto, quando me referir a inserir algo na caixa Apps Search, estou me referindo a inserir texto de busca com Apps como o foco. À medida que você insere texto, resultados correspondentes são exibidos. Quando você pressiona a tecla Enter, o Windows inicia o resultado selecionado no momento. Você também pode usar a caixa Apps Search para transmitir comandos com parâmetros e opções. Basta digitar o comando juntamente com seus parâmetros e opções da mesma maneira como você faria em um prompt de comando.

Deseja executar comandos do Windows PowerShell a partir da caixa Apps Search? Digite **powershell** e insira seu comando.

Group Policies

Group Policies (Políticas de Grupo) simplificam a administração oferecendo aos administradores um controle centralizado sobre os privilégios, as permissões e as capacidades tanto de usuários quanto de computadores. Por meio de Group Policies, você pode:

- Controlar o acesso aos componentes, recursos do sistema, recursos de rede, utilitários do Control Panel, área de trabalho e tela inicial do Windows. Consulte “Uso de modelos administrativos para configurar políticas” mais adiante neste capítulo para obter mais detalhes.

- Criar diretórios centralizados para gerenciar pastas especiais, como a pasta Documents de um usuário. Consulte “Gerenciamento centralizado de pastas especiais” mais adiante neste capítulo para obter mais detalhes.
- Definir scripts para usuário e computador para serem executados em momentos específicos. Esse assunto é abordado em “Gerenciamento de script de usuário e computador” mais adiante neste capítulo.
- Configurar políticas para senhas e bloqueio de conta, auditoria, atribuição de direitos do usuário e segurança. Muitos desses pontos são discutidos em “Configuração e organização da conta de usuário” no Capítulo 8, “Como criar contas de usuário e de grupo”.

As seções a seguir explicam como você pode trabalhar com Group Policies e aplicá-las.

Noções básicas sobre Group Policies

Você pode pensar em uma política como um conjunto de regras que ajudam a gerenciar usuários e computadores. As Group Policies podem ser aplicadas a vários domínios, domínios individuais, subgrupos dentro de um domínio ou sistemas individuais. As políticas que se aplicam a sistemas individuais são chamadas de *Local Group Policies* e são armazenadas apenas no sistema local. Outras Group Policies são vinculadas como objetos no armazenamento de dados do Active Directory.

Para entender as Group Policies, você precisa saber um pouco sobre a estrutura do Active Directory. No Active Directory, os sites representam a estrutura física de sua rede. Um site é um conjunto de sub-redes TCP/IP, com cada sub-rede representando um segmento físico da rede. Um domínio é um agrupamento lógico de objetos para gerenciamento centralizado, enquanto as subdivisões de um domínio são chamados de *organizational units* (OUs, unidades organizacionais). Sua rede pode ter sites chamados NewYorkPrincipal, CaliforniaPrincipal e WashingtonPrincipal. Dentro do site WashingtonPrincipal, você poderia ter domínios chamados SeattleLeste, SeattleOeste, SeattleNorte e SeattleSul. Dentro do domínio SeattleLeste, você poderia ter OUs chamadas Information Services (IS, Serviços de Informações), Engenharia e Vendas.

As Group Policies se aplicam apenas a sistemas com Windows 2000 e versões superiores do Windows. As configurações de Group Policy são armazenadas em uma Group Policy Object (GPO, objeto de diretiva de grupo). Você pode imaginar a GPO como um contêiner para as políticas que você aplicar e suas configurações. É possível aplicar várias GPOs em um único site, domínio ou OU. Como a Group Policy é descrita usando objetos, muitos conceitos orientados a objetos são aplicáveis. Se você sabe um pouco sobre programação orientada a objeto, pode imaginar que os conceitos de relação pai-filho e herança se aplicam a GPOs – e essa percepção está correta.

Um *contêiner* é um objeto de nível superior que contém outros objetos. Por meio da herança, a política aplicada a um contêiner-pai é herdada por um contêiner-filho. Basicamente, isso significa que uma configuração de política aplicada a um objeto pai é passada a um objeto filho. Por exemplo, se você aplicar uma configuração de política em um domínio, a configuração é herdada pelas OUs de dentro do domínio. Nesse caso, a GPO para o domínio é o objeto-pai e as GPOs para as OUs são objetos-filho.

A ordem de herança é site, domínio e OU. Isso significa que as configurações de Group Policy para um site são passadas adiante para os domínios de dentro do site, enquanto as configurações de um domínio são passadas adiante para as OUs desse domínio.

Como você pode imaginar, é possível modificar a herança. Para isso, você atribui uma configuração de política para um contêiner-filho que seja diferente da configuração de política do contêiner-pai. Desde que a modificação da política seja permitida (ou seja, que a modificação não esteja restringida), a configuração de política do contêiner-filho será aplicada corretamente. Para saber mais sobre a modificação e o bloqueio de GPOs, consulte “Bloqueio, modificação e desabilitação de políticas” mais adiante neste capítulo.

Em que ordem são aplicadas as políticas quando há várias políticas?

Quando várias políticas são configuradas, elas são aplicadas nesta ordem:

1. Group Policies locais
2. Group Policies do site
3. Group Policies do domínio
4. Group Policies da OU
5. Group Policies da sub OU

Se configurações de políticas entrarem em conflito, as configurações de política aplicadas posteriormente têm precedência e substituem as configurações de política anteriores. Por exemplo, políticas de OU têm precedência sobre Group Policies de domínio. Como já deve ser esperado, há exceções à regra de precedência. Essas exceções são discutidas em “Bloqueio, modoficação e desabilitação de políticas” mais adiante neste capítulo.

Quando as Group Policies são aplicadas?

Como você descobrirá ao começar a trabalhar com Group Policies, as configurações de política são separadas em duas amplas categorias:

- Aquelas aplicadas a computadores
- Aquelas aplicadas a usuários

Normalmente, as políticas de computador são aplicadas durante a inicialização do sistema, enquanto as políticas de usuário são aplicadas durante o logon. A sequência exata dos eventos é frequentemente importante para a solução de problemas de comportamento do sistema. Os eventos que ocorrem na inicialização e no logon são:

1. A rede é iniciada e o Windows Server aplica as políticas de computador. Por padrão, as políticas de computador são aplicadas uma de cada vez na ordem anteriormente especificada. Enquanto as políticas de computador estão sendo processadas, não há exibição da interface de usuário.
2. O Windows Server executa scripts de inicialização. Por padrão, os scripts de inicialização são executados um de cada vez, sendo que cada script é concluído ou atinge o tempo limite antes que o próximo seja iniciado. A execução do script não é exibida ao usuário a menos que isso seja especificado.
3. Um usuário efetua logon. Após o usuário ser validado, o Windows Server carrega o perfil do usuário.

4. O Windows Server aplica as políticas de usuário. Por padrão, as políticas de usuário são aplicadas uma de cada vez na ordem anteriormente especificada. Enquanto as políticas de usuário estão sendo processadas, a interface de usuário é exibida.
5. O Windows Server executa scripts de logon. Scripts de logon via Group Policy são executados simultaneamente por padrão. A execução do script não é exibida ao usuário a menos que isso seja especificado. Os scripts do compartilhamento Netlogon são os últimos a serem executados em uma janela do prompt de comando comum.
6. O Windows Server exibe a interface inicial do shell configurada na Group Policy.
7. Por padrão, a Group Policy é atualizada quando um usuário efetuar logoff ou um computador for reiniciado e, também, automaticamente dentro de um período de 90 a 120 minutos. Você pode alterar esse comportamento configurando um intervalo de atualização de Group Policy, conforme discutido em “Atualização de Group Policy” mais adiante neste capítulo. Para atualizar manualmente, abra um prompt e digite **gpupdate**.

MUNDO REAL Algumas configurações de usuários, como Folder Redirection, não podem ser atualizadas enquanto um usuário estiver conectado. O usuário deve efetuar logoff e depois logon para que essas configurações sejam aplicadas. Você pode digitar **gpupdate /logoff** em um prompt ou na caixa Apps Search para efetuar logoff do usuário automaticamente após a atualização. Da mesma forma, algumas configurações de computador podem ser atualizadas apenas durante a inicialização. O computador deve ser reiniciado para que essas configurações sejam aplicadas. Você pode digitar **gpupdate /boot** em um prompt ou na caixa Apps Search para reiniciar o computador após a atualização.

Requisitos de Group Policy e compatibilidade de versões

As Group Policies se aplicam apenas a sistemas com versões profissionais e de servidor do Windows. Como já deve ser esperado, cada nova versão do sistema operacional Windows trouxe mudanças à Group Policy. Algumas vezes, essas mudanças tornaram políticas mais antigas obsoletas em versões mais novas do Windows. Nesse caso, a política opera apenas em versões específicas do Windows, como apenas no Windows XP Professional e no Windows Server 2003.

De modo geral, a maioria das políticas é compatível de sua versão em diante. Isso significa que, na maioria dos casos, as políticas introduzidas no Windows Server 2003 podem ser usadas no Windows 7 e superior, assim como no Windows Server 2008 e superior. Por outro lado, isso também significa que políticas para Windows 8 e Windows Server 2012 normalmente não são aplicáveis a versões anteriores do Windows. Se uma política não for aplicável a uma determinada versão do sistema operacional Windows, você não poderá impor a política em computadores com essa versão do Windows.

Como você poderá saber se uma política é suportada por uma determinada versão do Windows? Fácil. A caixa de diálogo Properties de cada configuração de política apresenta uma caixa de texto Supported On. Esse campo somente de texto lista a compatibilidade da política com as várias versões do Windows. Se você selecionar uma política em um editor de Group Policy e selecionar a guia Extended em vez da guia Standard, não precisará abrir a caixa de diálogo mencionada. Você encontrará uma entrada chamada Requirements que lista a compatibilidade.

Além disso, você pode instalar novas políticas ao adicionar um service pack, instalar aplicativos do Windows ou adicionar componentes do Windows. Isso significa que você verá uma ampla variedade de entradas de compatibilidade.

Navegação pelas alterações em Group Policy

Com o intuito de simplificar o gerenciamento de Group Policy, a Microsoft removeu recursos de gerenciamento de ferramentas relacionadas ao Active Directory e moveu-os para um console primário chamado Group Policy Management Console (GPMC, Console de Gerenciamento de Group Policy) desde o Windows Vista e Windows Server 2008. O GPMC é um recurso que você pode incluir em qualquer instalação do Windows Server 2008 ou superior usando o Add Roles And Features Wizard. O GPMC está disponível no Windows Vista e superior quando você instala o RSAT. Após adicionar o GPMC a um computador, ele ficará disponível no menu Tools do Server Manager.

Quando você desejar editar uma GPO no GPMC, o console abre o Group Policy Management Editor, usado para gerenciar as configurações de política. Se a Microsoft tivesse ficado apenas com essas duas ferramentas, teríamos um ambiente de gerenciamento de políticas maravilhoso e fácil de usar. Infelizmente, diversos outros editores quase idênticos também existem:

- **Group Policy Starter GPO Editor** Um editor que pode ser usado para criar e gerenciar objetos de diretiva de início. Como o nome sugere, as Starter GPOs têm por objetivo fornecer um ponto de partida para os objetos de diretivas que você usará em toda sua organização. Quando você cria um objeto de diretiva, pode especificar uma Starter GPO como fonte ou base do objeto.
- **Local Group Policy Object Editor** Um editor que pode ser usado para criar e gerenciar objetos de diretivas para o computador local. Como o nome sugere, as GPOs locais têm por objetivo fornecer configurações de política para um computador específico e não para um site, domínio ou OU.

Se você já trabalhou com versões anteriores do Windows, também pode conhecer o Group Policy Object Editor (GPOE). Com o Windows Server 2003 e versões anteriores do Windows, o GPOE é a principal ferramenta de edição para objetos de diretivas. O GPOE, o Group Policy Management Editor, o Group Policy Starter GPO Editor e o Local Group Policy Object Editor são essencialmente idênticos exceto pelo conjunto de objetos de diretivas ao qual você obtém acesso. Por isso e porque você usa essas ferramentas para gerenciar objetos de diretivas individuais da mesma maneira, não farei distinção entre elas a menos que seja necessário. Por uma questão de preferência, refiro-me a essas ferramentas coletivamente como *editores de políticas*. Às vezes, posso usar o acrônimo GPOE para me referir a editores de políticas em geral, pois ele é mais facilmente diferenciado do console de gerenciamento, o GPMC.

O gerenciamento das configurações de política para Windows Vista e superior pode ser realizado apenas a partir de computadores com Windows Vista ou superior. Isso acontece porque o GPOE e o GPMC para o Windows Vista e versões superiores foram atualizados para operarem com o formato de modelos administrativos baseados em XML chamado ADMX.

OBSERVAÇÃO Não é possível usar versões anteriores de editores de políticas com ADMX. Você pode editar GPOs usando arquivos ADMX apenas em computadores com Windows Vista ou superior.

A Microsoft teve muitas razões para optar pelo formato ADMX. Os principais motivos foram permitir uma maior flexibilidade e extensibilidade. Como os arquivos ADMX são criados usando XML, os arquivos são rigorosamente estruturados e po-

dem ser analisados com mais facilidade e rapidez na inicialização. Isso pode ajudar a melhorar o desempenho enquanto o sistema operacional processa a Group Policy durante as fases de inicialização, logon, logoff e desligamento, bem como durante as atualizações de políticas. Além disso, a estrutura rigorosa dos arquivos ADMX viabiliza que a Microsoft continue seus esforços de internacionalização.

Os arquivos ADMX são divididos em arquivos com independência de idioma com a extensão de arquivo .admx e arquivos específicos a um idioma com a extensão .adml. Os arquivos com independência de idioma garantem que uma GPO tenha as políticas principais idênticas. Os arquivos específicos a um idioma, por sua vez, permitem que as políticas sejam exibidas e editadas em vários idiomas. Como os arquivos com independência de idioma armazenam as configurações centrais da política, as políticas podem ser editadas em qualquer idioma no qual o computador estiver configurado, permitindo assim que um usuário exiba e edite as políticas em inglês e outro em espanhol, por exemplo. O mecanismo que determina o idioma usado é o pacote de idiomas instalado no computador.

Os arquivos ADMX com independência de idioma são instalados no computador com Windows Vista ou posterior na pasta %SystemRoot%\PolicyDefinitions. Por sua vez, os arquivos ADMX específicos a um idioma são instalados em computadores com Windows 7 e Windows 8, bem como Windows Server 2008 R2 e Windows Server 2012 na pasta %SystemRoot%\PolicyDefinitions\LanguageCulture. Cada subpasta é nomeada usando o nome correspondente no padrão idioma/cultura da International Organization for Standardization (ISO, Organização Internacional para Padronização), como EN-US para inglês dos EUA.

Quando você inicia um editor de políticas, ele automaticamente lê os arquivos ADMX das pastas de definições de políticas. Por isso, você pode copiar os arquivos ADMX que quiser usar para pasta apropriada de definições de políticas para torná-los disponíveis na edição de GPOs. Se o editor de políticas estiver em execução quando você copiar o arquivo, ou os arquivos, é necessário reiniciar o editor de políticas para que ele leia os itens copiados.

Em domínios, os arquivos ADMX podem ser armazenados em um local central – o diretório que contém toda a informação abaixo do diretório SYSVOL (%SystemRoot%\Sysvol\Domain\Policies). Quando você usa um armazenamento central, os modelos administrativos deixam de ser armazenados com cada GPO. Em vez disso, apenas o estado atual da configuração é armazenado na GPO e os arquivos ADMX são armazenados centralmente. Isso reduz o volume de espaço de armazenamento usado à medida que o número de GPOs aumenta, além de reduzir a quantidade de dados que é replicada por toda a empresa. Desde que você edite as GPOs usando o Windows Vista ou superior, as novas GPOs não incluirão arquivos ADM e ADMX em seu interior. Para obter mais informações, consulte o Capítulo 2, "Deploying Group Policy", do livro *Windows Group Policy Administrator's Pocket Consultant* (Microsoft Press, 2009).

Quando executado em nível funcional de domínio Windows Server 2008 ou superior, os servidores com Windows Server 2008 ou superior usam o serviço de replicação do Distributed File System (DFS, Sistema de Arquivos Distribuído) para replicar Group Policies. Com a replicação do DFS, apenas as alterações das GPOs são replicadas, assim eliminando a necessidade de replicar uma GPO inteira após uma alteração.

Diferentemente do Windows XP e do Windows Server 2003, o Windows Vista e as versões superiores usam o serviço de cliente de Group Policy para isolar a notificação

e o processamento de Group Policy da fase de logon do Windows. Separar a Group Policy do processo de logon do Windows reduz o número de recursos usados para o processamento em segundo plano da política. Ao mesmo tempo, isso aumenta o desempenho geral e permite o fornecimento e a aplicação de novos arquivos de Group Policy como parte do processo de atualização sem que haja a necessidade de uma reinicialização.

Os computadores com Windows Vista ou superior não usam a funcionalidade de registro de rastreamento no Userenv.dll e, em vez disso, gravam mensagens de eventos de Group Policy no log do sistema. Além disso, o log operacional de Group Policy substitui o registro em log Userenv anterior. Quando você está solucionando problemas de Group Policy, você usa as mensagens detalhadas de eventos no log operacional em vez do log Userenv. No Event Viewer, você pode acessar o log operacional sob Applications And Services Logs\Microsoft\Windows\GroupPolicy.

Os computadores com Windows Vista ou superior usam o Network Location Awareness no lugar do Internet Control Message Protocol (ICMP) ou ping. Com o Network Location Awareness, um computador reconhece o tipo de rede com o qual está conectado e pode responder a alterações no status do sistema ou na configuração da rede. Por meio do Network Location Awareness, o cliente de Group Policy pode determinar o estado do computador, o estado da rede e a largura de banda disponível para a detecção de link lento.

Gerenciamento de Group Policies locais

Os computadores com Windows Vista ou superior permitem o uso de várias GPOs locais em um computador único (desde que o computador não seja um controlador de domínio). Anteriormente, os computadores tinham apenas uma GPO local. O Windows permite que você atribua uma GPO local diferente para cada usuário local ou tipo de usuário geral. Isso permite que a aplicação de políticas seja mais flexível e compatível com uma maior variedade de cenários de implementação.

Objetos de Group Policy locais

Quando os computadores estiverem sendo usados em uma configuração autônoma e não em uma configuração de domínio, você pode perceber que várias GPOs locais são úteis, pois você não precisará mais explicitamente desabilitar ou remover configurações que interfiram na sua capacidade de gerenciar um computador antes de realizar tarefas de administrador. Em vez disso, é possível implementar uma GPO local para administradores e outra GPO local para não administradores. No entanto, em uma configuração de domínio não é recomendável que você use várias GPOs locais. Em domínios, a maioria dos computadores e usuários já apresenta várias GPOs aplicadas a eles – adicionar várias GPOs locais a essa combinação que já é variada pode tornar o gerenciamento de Group Policy confuso.

Os computadores com Windows Vista ou superior possuem três camadas de GPOs locais:

- **Local Group Policy** É a única GPO local que permite que tanto as definições de configuração de computador quanto de usuário sejam aplicadas a todos os usuários do computador.

- **Local Group Policy para administradores e não administradores** Contém apenas as definições de configuração de usuário. Essa política é aplicada dependendo se a conta de usuário que está sendo usada é membro, ou não, do grupo local de administradores.
- **Local Group Policy específica para usuários** Contém apenas as definições de configuração de usuário. Essa política é aplicada a usuários individuais.

Tais camadas de GPOs locais são processadas na seguinte ordem: Local Group Policy, Local Group Policy para administradores e não administradores e Local Group Policy específica para usuários.

Como as definições de configuração de usuário disponíveis são as mesmas para todas as GPOs locais, uma definição de uma GPO pode entrar em conflito com uma definição de outra GPO. O Windows resolve os conflitos de configurações substituindo qualquer definição anterior com as configurações mais recentes e lidas por último. A configuração final é a que o Windows usa. Quando o Windows resolve conflitos, apenas o estado habilitado ou desabilitado das configurações são levados em consideração. Uma configuração determinada como Not Configured não tem efeito no estado da definição de uma aplicação anterior de política. Para simplificar a administração de um domínio, você pode desabilitar o processamento de GPOs locais em computadores com Windows Vista ou versões superiores habilitando a configuração de política Turn Off Local Group Policy Objects Processing em uma GPO de domínio. Em uma Group Policy, essa configuração está localizada sob Administrative Templates de Computer Configuration, abaixo de System\Group Policy.

Acesso às configurações de política local de nível superior

Todos os computadores com versões recentes do Windows têm uma GPO local editável. Embora um controlador de domínio tenha uma GPO local, as suas configurações não devem ser editadas.

A maneira mais rápida de acessar a GPO local é digitar o comando a seguir em um prompt de comando ou na caixa Apps Search:

```
gpedit.msc /gpcomputer: "%ComputerName%"
```

OBSERVAÇÃO Devido aos argumentos adicionais passados com o comando, o comando não é executado corretamente no prompt de comando a partir de um prompt do PowerShell. Coloque os argumentos entre aspas simples para que eles sejam interpretados corretamente, como mostrado no exemplo a seguir: **gpedit.msc '/gpcomputer: "%ComputerName%"'**.

Esse comando inicia o GPOE em um Microsoft Management Console (MMC, Console de Gerenciamento Microsoft) com seu foco apontando para o computador local. Aqui, %ComputerName% é uma variável de ambiente que determina o nome do computador local; ela deve ser colocada entre aspas duplas conforme mostrado acima. Para acessar a GPO local de nível superior em um computador remoto, digite o comando a seguir em um prompt ou na caixa Apps Search:

```
gpedit.msc /gpcomputer: "RemoteComputer"
```

Aqui, RemoteComputer é o nome do host ou o fully qualified domain name (FQDN, nome de domínio totalmente qualificado) do computador remoto. Novamente, as aspas duplas são necessárias, conforme mostrado no exemplo a seguir:

```
gpedit.msc /gpcomputer: "corpsvr82"
```

Você também pode gerenciar a GPO local de nível superior em um computador seguindo estas etapas:

1. Em um prompt ou na caixa Apps Search, digite **mmc** e pressione a tecla Enter.
2. No MMC, toque ou clique em File e em Add/Remove Snap-In.
3. Na caixa de diálogo Add Or Remove Snap-Ins, toque ou clique em Group Policy Object Editor e em Add.
4. Na caixa de diálogo Select Group Policy Object, toque ou clique em Finish, pois o computador local é o foco padrão. Toque ou clique em OK.

Como mostrado na Figura 4-1, agora você pode gerenciar as configurações de política local usando as opções fornecidas.

DICA Você pode usar o mesmo snap-in do MMC para gerenciar mais de uma GPO local. Na caixa de diálogo Add Or Remove Snap-Ins, basta adicionar uma instância do Group Policy Object Editor para cada objeto com o qual você deseja trabalhar.

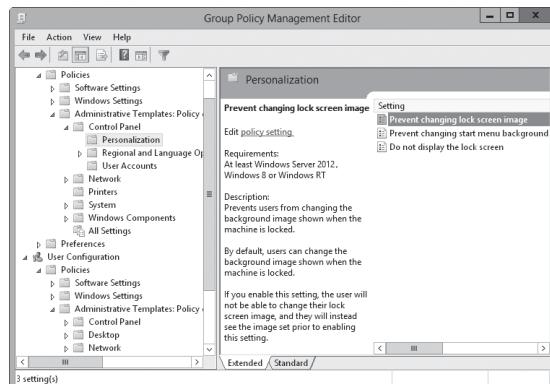


FIGURA 4-1 Use o editor de políticas para gerenciar as configurações de política local.

Configurações de objetos de Group Policy locais

As Group Policies locais são armazenadas na pasta %SystemRoot%\System32\GroupPolicy de cada computador com Windows Server. Nessa pasta, você encontrará as seguintes subpastas:

- **Machine** Armazena os scripts de computador na pasta Script e informações de políticas baseadas em registro para HKEY_LOCAL_MACHINE (HKLM) no arquivo Registry.pol
- **User** Armazena os scripts de usuário na pasta Script e informações de políticas baseada em registro para HKEY_CURRENT_USER (HKCU) no arquivo Registry.pol

ATENÇÃO Você não deve editar essas pastas e arquivos diretamente. Em vez disso, use os recursos adequados de uma das ferramentas de gerenciamento de Group Policy. Por padrão, esses arquivos e pastas são ocultos. Se você desejar exibir os arquivos e pastas ocultos no File Explorer, toque ou clique na guia View e selecione Hidden Items. Talvez também seja recomendável que você selecione File Name Extensions.

Como acessar Group Policies locais específicas para usuários, para administradores e para não administradores

Por padrão, o único objeto de diretiva local que existe em um computador é a GPO local. Você pode criar e gerenciar outras políticas locais conforme necessário (exceto em controladores de domínio). É possível criar ou acessar uma GPO local para administradores, para não administradores e específica para usuários por meio das seguintes etapas:

1. Em um prompt ou na caixa Apps Search, digite **mmc** e pressione a tecla Enter. No MMC, toque ou clique em File e em Add/Remove Snap-In.
2. Na caixa de diálogo Add Or Remove Snap-Ins, toque ou clique em Group Policy Object Editor e em Add.
3. Na caixa de diálogo Select Group Policy Object, toque ou clique em Browse. Na caixa de diálogo Browse For A Group Policy Object, toque ou clique na guia Users.
4. Na guia Users, as entradas na coluna Group Policy Object Exists especificam se um determinado objeto de diretiva local foi criado. Siga uma destas etapas:
 - Selecione Administrators para criar ou acessar a GPO local para administradores.
 - Selecione Non-Administrators para criar ou acessar a GPO local para não administradores.
 - Selecione o usuário local para o qual você deseja criar ou acessar a GPO local específica para esse usuário.
5. Toque ou clique em OK. Se o objeto selecionado não existir, ele será criado. Caso contrário, o objeto existente abre para revisão e edição.

As configurações de política para administradores, não administradores e usuários são armazenadas na pasta %SystemRoot%\System32\GroupPolicyUsers em cada computador com Windows Server. Como essas GPOs locais aplicam-se apenas para definições de configuração de usuário, as configurações de política específicas para um usuário sob %SystemRoot%\System32\GroupPolicyUsers apresentam apenas uma subpasta User e essa subpasta armazena scripts de usuários na pasta Script e informações de políticas baseadas em registro para HKCU no arquivo Registry.pol.

Gerenciamento de políticas de site, domínio e unidade organizacional

Quando você implanta os Active Directory Domain Services (AD DS, Serviços de Domínio do Active Directory), é possível usar Group Policy a partir do Active Directory. Cada

site, domínio e OU pode ter uma ou mais Group Policies. As Group Policies apresentadas mais acima na lista de Group Policies têm precedência mais alta que as políticas listadas mais abaixo. Isso garante que as políticas sejam aplicadas apropriadamente por todos os sites, domínios e OUs relacionadas.

Introdução às políticas padrão de domínio

Quando trabalhar com uma Group Policy baseada em Active Directory, você perceberá que cada domínio de sua organização apresenta duas GPOs padrão:

- **Default Domain Controllers Policy GPO** Uma GPO padrão criada para e vinculada à OU de controladores de domínio. Essa GPO é aplicável a todos os controladores de domínio de um domínio (desde que eles não sejam movidos dessa OU). Use-a para gerenciar configurações de segurança para controladores de domínio de um domínio.
- **Default Domain Policy GPO** Uma GPO padrão criada para e vinculada ao próprio domínio do Active Directory. Use essa GPO para estabelecer as linhas de base de uma grande variedade de configurações de política que se aplicam a todos os usuários e computadores de um domínio.

Normalmente, a Default Domain Policy GPO é a GPO de precedência mais alta vinculada ao nível de domínio e a Default Domain Controllers Policy GPO é a GPO de precedência mais alta vinculada ao contêiner Domain Controllers. É possível vincular GPOs adicionais ao nível de domínio e ao contêiner Domain Controllers. Ao fazer isso, as configurações da GPO de precedência mais alta substituem as configurações da GPO de precedência mais baixa. Essas GPOs não foram elaboradas para o gerenciamento geral de Group Policy.

A Default Domain Policy GPO é usada apenas para gerenciar as configurações padrão das políticas de conta e, em especial, de três áreas dessas políticas: política de senha, política de bloqueio de conta e política de Kerberos. Várias outras opções de segurança também podem ser gerenciadas por meio dessa GPO. Entre elas, Accounts: Rename Administrator Account, Accounts: Administrator Account Status, Accounts: Guest Account Status, Accounts: Rename Guest Account, Network Security: Force Logoff When Logon Hours Expire, Network Security: Do Not Store LAN Manager Hash Value On Next Password Change e Network Access: Allow Anonymous SID/Name Translation. Um modo de modificar essas configurações é criar uma GPO com as novas configurações e vinculá-la com uma precedência mais alta ao contêiner de domínio.

A Default Domain Controllers Policy GPO inclui configurações específicas de atribuição de direitos do usuário e de opções de segurança que limitam a forma com que os controladores de domínio podem ser usados. Um modo de modificar essas configurações é criar uma GPO com as novas configurações e vinculá-la com uma precedência mais alta ao contêiner Domain Controllers.

Para gerenciar outras áreas da política, você deve criar uma GPO e vinculá-la ao domínio ou a uma OU apropriada dentro do domínio.

As Group Policies de site, domínio e OU são armazenadas na pasta %SystemRoot%\Sysvol\Domain\Policies nos controladores de domínio. Nessa pasta, você encontrará uma subpasta para cada política que for definida no controlador de domínio. O nome da pasta da política é o globally unique identifier (GUID, identificador global exclusivo) da política. Você pode encontrar o GUID da política na página Properties na

guia General do quadro Summary. Dentro dessas pastas de políticas individuais, você encontrará as pastas:

- **Machine** Armazena os scripts de computador na pasta Script e informações de políticas baseadas em registro para HKEY_LOCAL_MACHINE (HKLM) no arquivo Registry.pol
- **User** Armazena os scripts de computador na pasta Script e informações de políticas baseada em registro para HKEY_CURRENT_USER (HKCU) no arquivo Registry.pol

ATENÇÃO Não edite essas pastas e arquivos diretamente. Em vez disso, use os recursos adequados de uma das ferramentas de gerenciamento de Group Policy.

Como usar o Group Policy Management Console

O GPMC pode ser executado a partir do menu Tools no Server Manager. Em um prompt ou na caixa Apps Search, digite **gpmc.msc** e pressione a tecla Enter.

Como mostrado na Figura 4-2, o nó da raiz do console é chamado de Group Policy Management e, abaixo dele, está o nó Forest. O nó Forest representa a floresta com a qual você está atualmente conectado e é chamado pelo nome do domínio-raiz dessa floresta. Se você apresentar as credenciais adequadas, pode adicionar conexões a outras florestas. Para isso, pressione e mantenha pressionado ou clique com o botão direito do mouse no nó Group Policy Management e toque ou clique em Add Forest. Na caixa de diálogo Add Forest, digite o nome do domínio-raiz da floresta na caixa de texto Domain e toque ou clique em OK.

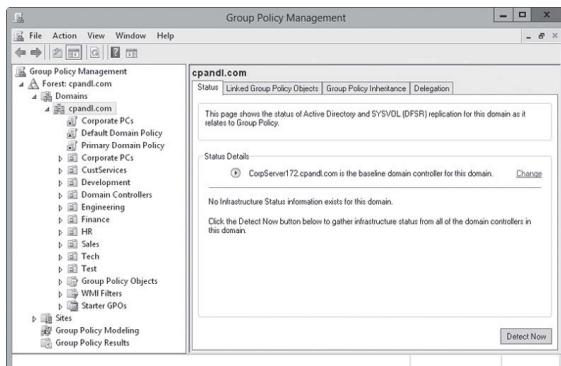


FIGURA 4-2 Use o GPMC para trabalhar com GPOs em sites, florestas e domínios.

Ao expandir o nó Forest, você verá os nós:

- **Domains** Fornece acesso às configurações de política para domínios na floresta relacionada. Por padrão, você é conectado a seu domínio de logon. Se você apresentar as credenciais adequadas, pode adicionar conexões a outros domínios na floresta relacionada. Para isso, pressione e mantenha pressionado ou clique com o botão direito do mouse no nó Domains e toque ou clique em Show Domains. Na

caixa de diálogo Show Domains, marque as caixas de seleção para os domínios que você deseja adicionar e toque ou clique em OK.

- **Sites** Fornece acesso às configurações de política para sites na floresta relacionada. Os sites são ocultos por padrão. Se você apresentar as credenciais adequadas, pode adicionar conexões para sites. Para isso, pressione e mantenha pressionado ou clique com o botão direito do mouse no nó Sites e toque ou clique em Show Sites. Na caixa de diálogo Show Sites, marque as caixas de seleção para os sites que você deseja adicionar e toque ou clique em OK.
- **Group Policy Modeling** Fornece acesso ao Group Policy Modeling Wizard, que ajuda você a planejar a implantação da política e simula as configurações para fins de teste. Qualquer modelo salvo de política também está disponível.
- **Group Policy Results** Fornece acesso ao Group Policy Results Wizard. Para cada domínio com o qual você estiver conectado, todas as GPOs relacionadas e as OUs estarão disponíveis para operarem em um local.

As GPOs listadas sob contêineres de domínio, site e OU no GPMC são links das GPOs e não as próprias GPOs. Você pode acessar as GPOs reais por meio do contêiner de GPOs do domínio selecionado. Observe que os ícones para os links de GPOs apresentam pequenas setas na parte inferior esquerda, similar a ícones de atalho, enquanto as GPOs reais não.

Ao iniciar o GPMC, o console se conecta com o Active Directory que está sendo executado no controlador de domínio que age como o emulador de PDC para seu domínio de logon e obtém uma lista de todas as GPOs e OUs do domínio. Esse processo é realizado por meio do Lightweight Directory Access Protocol (LDAP) para acessar o repositório de diretórios e o protocolo Server Message Block (SMB) para acessar o diretório SYSVOL. Se o emulador de PDC não estiver disponível por algum motivo, como quando o servidor está offline, o GPMC exibe um prompt para que você possa escolher trabalhar com as configurações de política no controlador de domínio com o qual você estiver conectado no momento ou em qualquer controlador de domínio disponível. Para alterar o controlador de domínio com o qual você está conectado, pressione e mantenha pressionado ou clique com o botão direito do mouse no nó do domínio para o qual você deseja configurar o foco para o controlador de domínio e toque ou clique em Change Domain Controller. Na caixa de diálogo Change Domain Controller, o controlador de domínio com o qual você estiver conectado no momento estará listado sob Current Domain Controller. Nas opções Change To, especifique o controlador de domínio a ser usado e toque ou clique em OK.

Apresentação do editor de políticas

Com o GPMC, você pode editar uma GPO pressionando-a e mantendo-a pressionada ou clicando com o botão direito do mouse nela e selecionando Edit no menu de atalho. Como a Figura 4-3 mostra, o editor de políticas tem dois nós principais:

- **Computer Configuration** Permite que você configure políticas que devem ser aplicadas aos computadores, independente de quem efetuar logon
- **User Configuration** Permite que você configure políticas que devem ser aplicadas aos usuários, independente de qual computador for usado para efetuar logon

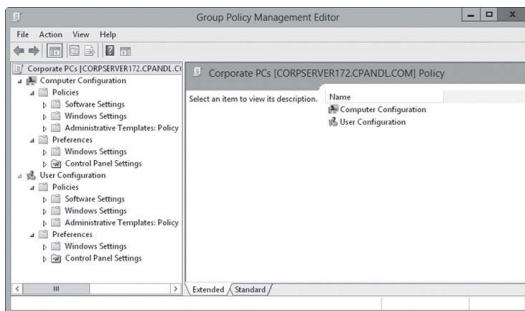


FIGURA 4-3 A configuração do editor de políticas depende do tipo de política que estiver sendo criada e dos add-ons instalados.

Sob os nós Computer Configuration e User Configuration, você encontrará os nós Policies e Preferences. As configurações para políticas gerais estão listadas sob o nó Policies. As configurações para preferências gerais estão listadas sob o nó Preferences.

OBSERVAÇÃO Quando eu fizer referência às configurações sob o nó Policies, às vezes usarei um atalho como User Configuration\Administrative Templates\Windows Components em vez de User Configuration\Policies\Administrative Templates: Policy Definitions\Windows Components. Esse atalho mostra que a configuração de política em questão está sob User Configuration e não em Computer Configuration e que ela pode ser encontrada sob Administrative Templates\Windows Components.

A configuração exata de Computer Configuration e User Configuration depende dos add-ons instalados e do tipo de política que está sendo criada. Ainda assim, você verá que normalmente Computer Configuration e User Configuration apresentam subnós para:

- **Software Settings** Estabelece políticas para configurações de software e instalação de software. Ao instalar um software, subnós adicionais podem ser criados em Software Settings.
- **Windows Settings** Estabelece políticas para redirecionamento de pasta, scripts e segurança.
- **Administrative Templates** Estabelece políticas para o sistema operacional, componentes do Windows e programas. Os modelos administrativos são configurados por meio de arquivos de modelo. Você pode adicionar ou remover arquivos de modelo sempre que precisar.

OBSERVAÇÃO Uma discussão completa de todas as opções disponíveis está além do escopo deste livro. As seções a seguir focam o redirecionamento de pasta e os modelos administrativos. Os scripts são abordados em “Gerenciamento de script de usuário e computador” mais adiante neste capítulo. A segurança é assunto de capítulos posteriores deste livro.

Uso de modelos administrativos para configurar políticas

Os modelos administrativos fornecem acesso fácil às configurações de políticas baseadas em registro que talvez você queira configurar. Um conjunto padrão de modelos administrativos está configurado para usuários e computadores no editor de políticas.

Você também pode adicionar ou remover modelos administrativos. Todas as alterações que forem feitas a políticas disponíveis por meio de modelos administrativos são salvas no registro. As configurações de computador são salvas em HKLM e as configurações de usuário em HKCU.

Os modelos configurados no momento podem ser visualizados no nó Administrative Templates do editor de políticas. Esse nó contém políticas que você pode configurar para computadores locais, OUs, domínios e sites. Diferentes conjuntos de modelos podem ser encontrados sob Computer Configuration e User Configuration. É possível adicionar modelos contendo novas políticas no editor de políticas e também quando você instalar novos componentes do Windows.

Você pode usar modelos administrativos para gerenciar o seguinte:

- **Control Panel (Painel de Controle)** Determine a configuração e as opções disponíveis do Control Panel e de seus utilitários
- **Área de trabalho** Configure a área de trabalho do Windows e as opções disponíveis para ela
- **Rede** Configure os sistemas de rede e as opções de cliente de rede para arquivos offline, clientes DNS e conexões de rede
- **Impressoras** Configure as configurações, a localização, o processo de spool e as opções de diretório para impressora
- **Pastas compartilhadas** Permita a publicação de pastas compartilhadas e raízes do DFS
- **Tela inicial e barra de tarefas** Controle a configuração e as opções disponíveis da tela inicial e da barra de tarefas
- **Sistema** Defina as configurações do sistema para cotas de disco, perfis de usuário, logon de usuário, restauração do sistema, relatórios de erros e assim por diante
- **Componentes do Windows** Determine a configuração e as opções disponíveis de vários componentes do Windows, inclusive do Event Viewer, Internet Explorer, Task Scheduler, Windows Installer e Windows Updates

A melhor maneira de saber quais políticas de modelos administrativos estão disponíveis é procurar nos nós Administrative Templates. Ao navegar pelos modelos, você verá que as políticas estão em um destes três estados:

- **Not Configured** A política não está configurada e nenhuma configuração para ela será salva no registro.
- **Enabled** A política está sendo ativamente imposta e suas configurações serão salvas no registro.
- **Disabled** A política está desativada e não é imposta a menos que esteja sendo modificada. Essa configuração será salva no registro.

Você pode habilitar, desabilitar e configurar políticas seguindo estas etapas:

1. No editor de políticas, abra a pasta Administrative Templates no nó Computer Configuration ou User Configuration – o que for mais adequado para o tipo de política que você deseja configurar.
2. No painel esquerdo, selecione a pasta que contém as políticas com as quais você deseja trabalhar. As políticas relacionadas são exibidas no painel direito.

3. Dê um toque duplo ou clique duas vezes em uma política para exibir sua caixa de diálogo Properties relacionada.

Você pode ler uma descrição da política no painel Help. A descrição estará disponível apenas se houver alguma definida no arquivo de modelo associado.

4. Para configurar o estado da política, selecione uma das seguintes opções:

- **Not Configured** A política não está configurada.
- **Enabled** A política está habilitada.
- **Disabled** A política está desabilitada.

5. Se você habilitar a política, configure se necessário parâmetros adicionais e toque ou clique em OK.

OBSERVAÇÃO Normalmente, as políticas de computador têm precedência no Windows Server. Se houver um conflito entre uma configuração de política de computador e uma configuração de política de usuário, a política de computador é imposta.

Criação e vinculação de GPOs

Quando você trabalha com um objeto de diretiva, criar um objeto e vinculá-lo a um contêiner específico do Active Directory são duas ações diferentes. Você pode criar uma GPO sem vinculá-la a domínio, OU ou site algum. Assim, quando apropriado, você pode fazer essa vinculação a um domínio, OU ou site específico. Você também pode criar uma GPO e vinculá-la automaticamente a um domínio, OU ou site. A técnica escolhida primeiramente depende de sua preferência e de como você planeja trabalhar com a GPO. Lembre-se de que quando você cria e vincula uma GPO a um site, domínio ou OU, a GPO é aplicada aos objetos de usuário e computador desse site, domínio ou OU de acordo com as opções do Active Directory que estão definindo a herança, a ordem de precedência das GPOs e outras configurações.

Você pode criar e vincular uma GPO a um site, domínio ou OU seguindo estas etapas:

1. No GPMC, expanda a entrada para a floresta com a qual você quer trabalhar e o nó Domains relacionado dando um toque duplo ou clicando duas vezes em cada nó.
2. Pressione e mantenha pressionado ou clique com o botão direito do mouse em Group Policy Objects e toque ou clique em New. Na caixa de diálogo New GPO, digite um nome descritivo para a GPO, como **GPO para estação de trabalho segura**. Se você desejar usar uma GPO de início como fonte para as configurações iniciais, selecione a GPO de início para usar na lista Source Starter GPO. Quando você tocar ou clicar em OK, a nova GPO será adicionada ao contêiner Group Policy Objects.
3. Pressione e mantenha pressionada ou clique com o botão direito do mouse na nova GPO e toque ou clique em Edit. No editor de políticas, determine as configurações necessárias de política e feche o editor de políticas.
4. No GPMC, selecione o site, domínio ou OU. Expanda o nó Sites com o qual você deseja trabalhar. No painel direito, a guia Linked Group Policy Objects mostra as GPOs que estão vinculadas no momento ao contêiner selecionado (se houver).
5. Pressione e mantenha pressionado ou clique com o botão direito do mouse no site, domínio ou OU ao qual você deseja vincular a GPO e toque ou clique em

Link An Existing GPO. Na caixa de diálogo Select GPO, selecione a GPO que você deseja vincular e toque ou clique em OK. Quando a Group Policy for atualizada para computadores e usuários no site, domínio ou OU aplicável, as configurações de política da GPO serão aplicadas.

Você pode criar e vincular uma GPO como uma operação única seguindo estas etapas:

1. No GPMC, pressione e mantenha pressionado ou clique com o botão direito do mouse no site, domínio ou OU para o qual você deseja criar e vincular a GPO e toque ou clique em Create A GPO In This Domain, And Link It Here.
2. Na caixa de diálogo New GPO, digite um nome descritivo para a GPO, como **GPO de estação de trabalho segura**. Se você desejar usar uma GPO de início como fonte para as configurações iniciais, selecione a GPO de início para usar na lista Source Starter GPO. Quando você tocar ou clicar em OK, a nova GPO será adicionada ao contêiner Group Policy Objects e vinculada ao site, domínio ou OU anteriormente selecionado.
3. Pressione e mantenha pressionada ou clique com o botão direito do mouse na nova GPO e toque ou clique em Edit. No editor de políticas, determine as configurações necessárias de política e feche o editor de políticas. Quando a Group Policy for atualizada para computadores e usuários no site, domínio ou OU aplicável, as configurações de política da GPO serão aplicadas.

Criação e uso de GPOs de início

Ao criar uma GPO no GPMC, você pode baseá-lo em uma GPO de início. Assim, as configurações da GPO de início são importadas para a nova GPO, permitindo que você use uma GPO de início para definir as configuração de base para uma nova GPO. Em uma organização de grande porte, você deve criar categorias diferentes de GPOs de início de acordo com os usuários e computadores com os quais elas serão usadas ou com a configuração de segurança exigida.

Você pode criar uma GPO de início seguindo estas etapas:

1. No GPMC, expanda a entrada para a floresta com a qual você quer trabalhar e dê um toque duplo ou clique duas vezes no nó Domains relacionado para expandi-lo.
2. Pressione e mantenha pressionado ou clique com o botão direito do mouse em Starter GPOs e toque ou clique em New. Na caixa de diálogo New Starter GPO, digite um nome descritivo para a GPO, como **GPO de usuário para gerenciamento geral**. Você também pode incluir comentários descrevendo a finalidade da GPO. Toque ou clique em OK.
3. Pressione e mantenha pressionada ou clique com o botão direito do mouse na nova GPO e toque ou clique em Edit. No editor de políticas, determine as configurações necessárias de política e feche o editor de políticas.

Delegação de privilégios para o gerenciamento de Group Policy

No Active Directory, todos os administradores têm algum nível de privilégios para realizar tarefas de gerenciamento de Group Policy. Por meio da delegação, permissões

podem ser concedidas a outras pessoas para que elas realizem todas (ou algumas) as tarefas a seguir ou alguma delas:

- Criar GPOs e gerenciar as GPOs criadas
- Exibir as configurações, modificar as configurações, deletar uma GPO e modificar a segurança
- Gerenciar links a GPOs existentes ou gerar o Resultant Set of Policy (RSOP)

No Active Directory, os administradores podem criar GPOs e qualquer pessoa que criar uma GPO tem o direito de gerenciá-la. No GPMC, você pode determinar quem pode criar GPOs em um domínio selecionando o nó Group Policy Objects desse domínio e tocando ou clicando na guia Delegation. Na guia Delegation, você verá uma lista de grupos e usuários que podem criar GPOs no domínio. Para conceder a permissão de criar GPOs a um usuário ou grupo, toque ou clique em Add. Na caixa de diálogo Select User, Computer, Or Group, selecione o usuário ou grupo e toque ou clique em OK.

No GPMC, você tem várias maneiras de determinar quem tem permissões de acesso para o gerenciamento de Group Policy. Para permissões de domínio, site e OU, selecione o domínio, site ou OU com o qual você deseja trabalhar e toque ou clique na guia Delegation no painel direito, como mostrado na Figura 4-4. Na lista Permission, selecione a permissão a ser delegada. As opções são:

- **Link GPOs** Lista os usuários e grupos que podem criar e gerenciar vínculos a GPOs no site, OU ou domínio selecionado
- **Perform Group Policy Modeling Analyses** Lista os usuários e grupos que podem determinar o RSOP para fins de planejamento
- **Read Group Policy Results Data** Lista os usuários e grupos que podem determinar o RSOP que está sendo aplicado no momento para fins de verificação ou registro em log

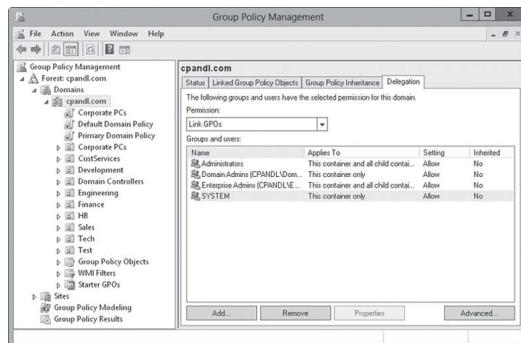


FIGURA 4-4 Examine permissões para o gerenciamento de Group Policy.

Para conceder permissões de domínio, site ou OU, execute as etapas a seguir:

1. No GPMC, selecione o domínio, site ou OU com o qual você deseja trabalhar e toque ou clique na guia Delegation no painel direito.

2. Na lista Permission, selecione a permissão a ser concedida. As opções são Link GPOs, Perform Group Policy Modeling Analyses e Read Group Policy Results Data.
3. Toque ou clique em Add. Na caixa de diálogo Select User, Computer Or Group, selecione o usuário ou grupo e toque ou clique em OK.
4. Na caixa de diálogo Add Group Or User, especifique como a permissão deve ser aplicada. Para aplicar a permissão ao contêiner atual e a todos os contêineres filhos, selecione This Container And All Child Containers. Para aplicar a permissão apenas ao contêiner atual, selecione This Container Only. Toque ou clique em OK.

Para permissões de GPO individuais, selecione a GPO com a qual você deseja trabalhar no GPMC e toque ou clique na guia Delegation no painel direito. Assim, você verá uma ou mais das permissões a seguir para usuários e grupos individuais:

- **Read** Indica que o usuário ou grupo pode exibir a GPO e suas configurações.
- **Edit Settings** Indica que o usuário ou grupo pode exibir a GPO e alterar suas configurações. O usuário ou grupo não pode excluir a GPO ou modificar a segurança.
- **Edit Settings, Delete, Modify Security** Indica que o usuário ou grupo pode exibir a GPO e alterar suas configurações. O usuário ou grupo também pode excluir a GPO ou modificar a segurança.

Para conceder permissões para trabalhar com a GPO, execute as etapas a seguir:

1. No GPMC, selecione a GPO com a qual você deseja trabalhar e toque ou clique na guia Delegation no painel direito. Toque ou clique em Add.
2. Para conceder permissão na GPO a um usuário ou grupo, toque ou clique em Add. Na caixa de diálogo Select User, Computer, Or Group, selecione o usuário ou grupo e toque ou clique em OK.
3. Na caixa de diálogo Add Group Or User, selecione o nível de permissão e toque ou clique em OK.

Bloqueio, modificação e desabilitação de políticas

A herança garante que todos os objetos de computador e usuário de um domínio, site ou OU sejam afetados pela Group Policy. A maioria das políticas apresentam três opções de configuração: Not Configured, Enabled ou Disabled. Not Configured é o estado padrão para a maioria das configurações de política. Se uma política estiver configurada como Enabled, ela é imposta e aplicada diretamente ou por meio da herança a todos os usuários e computadores que estão sujeitos à política. No entanto, se uma política estiver configurada como Disabled, a política não é imposta nem aplicada.

Você pode alterar o modo de atuação da herança por meio destas quatro maneiras principais:

- Alterar a ordem e a precedência das vinculações
- Modificar a herança (desde que não haja imposição)
- Bloquear a herança (impedir completamente a herança)
- Impor a herança (sobrepor e impedir a modificação e o bloqueio)

Para Group Policy, a ordem da herança segue do nível de site, ao nível de domínio e, após, a cada nível aninhado de OU. Lembre-se do seguinte:

- Quando vários objetos de diretiva estão vinculados a um determinado nível, a ordem das vinculações determina a ordem em que as configurações de política são aplicadas. Os objetos de diretiva vinculados sempre são aplicados na ordem de classificação das vinculações. Os objetos de diretiva com classificação mais baixa são processados primeiro, enquanto os objetos de diretiva com classificação mais alta são processados posteriormente. O objeto de diretiva processado por último tem prioridade. Assim, qualquer configuração definida nesse objeto de diretiva é definitiva e substitui as configurações de outros objetos de diretiva (exceto se houver bloqueio ou imposição de herança).
- Quando vários objetos de diretiva são herdados de um nível superior, a ordem de precedência mostra exatamente como os objetos de diretiva estão sendo processados. Assim como na ordem das vinculações, os objetos de diretiva com classificação mais baixa são processados antes dos objetos de diretiva com classificação mais alta. O objeto de diretiva processado por último tem precedência. Assim, qualquer configuração definida nesse objeto de diretiva é definitiva e substitui as configurações de outros objetos de diretiva (exceto se houver bloqueio ou imposição de herança).

Quando vários objetos de diretiva estão vinculados a um determinado nível, você pode alterar a ordem das vinculações (e, portanto, a ordem de precedência) de objetos de diretiva seguindo estas etapas:

1. No GPMC, selecione o contêiner do site, domínio ou OU com o qual você deseja trabalhar.
2. No painel direito, selecione a guia Linked Group Policy Objects (como mostrado na Figura 4-5). Toque ou clique no objeto de diretiva com o qual você deseja trabalhar.

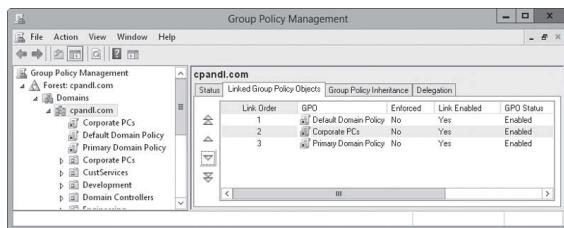


FIGURA 4-5 Altere a ordem das vinculações para modificar a ordem de processamento e a precedência.

3. Toque ou clique nos botões Move Link Up ou Move Link Down conforme for apropriado para alterar a ordem das vinculações do objeto de diretiva selecionado.
4. Ao concluir a alteração da ordem das vinculações, verifique se os objetos de diretiva estão sendo processados na ordem esperada conferindo a ordem de preferência na guia Group Policy Inheritance.

A modificação da herança é uma técnica básica para alterar o modo de atuação da herança. Quando uma política está habilitada em um objeto de diretiva de nível superior, é possível modificar a herança desabilitando a política em um objeto de diretiva de nível inferior. Quando uma política está desabilitada em um objeto de diretiva

de nível superior, é possível modificar a herança habilitando a política em um objeto de diretiva de nível inferior. Desde que uma política não esteja bloqueada ou imposta, essa técnica atinge os resultados esperados.

Haverá situações em que você desejará bloquear a herança para que nenhuma configuração de política de contêineres de nível superior seja aplicada a usuários e computadores em um contêiner específico. Quando a herança é bloqueada, apenas as configurações de política de objetos de diretiva vinculados a esse nível são aplicadas e as configurações de contêineres de nível superior são bloqueadas (exceto se houver imposição de herança).

Os administradores de domínio podem usar o bloqueio de herança para bloquear as configurações de política herdadas do nível de site. Os administradores de OU podem usar o bloqueio de herança para bloquear as configurações de política herdadas tanto do nível de domínio quanto do nível de site. Com o uso do bloqueio para assegurar a autonomia de um domínio ou OU, você pode garantir que os administradores de domínio ou OU tenham total controle sobre as políticas que se aplicam a usuários e computadores sob a administração deles.

Por meio do GPMC, você pode bloquear a herança pressionando e mantendo pressionado ou clicando com o botão direito do mouse no domínio ou OU que não deve herdar as configurações de contêineres de nível superior e selecionando Block Inheritance. Se a opção Block Inheritance já estiver selecionada, selecione-a novamente para remove a configuração. Quando você bloqueia a herança no GPMC, um círculo azul com um ponto de exclamação é adicionado ao nó do contêiner na árvore de console. Esse ícone de notificação fornece uma maneira rápida de informar se algum domínio ou OU apresenta a configuração Block Inheritance habilitada.

Para evitar que administradores com autoridade sobre um contêiner modifique ou bloquie configurações de Group Policy herdadas, você pode impor uma política. Quando uma política é imposta, todas as configurações de política definidas nesse objeto de diretiva de nível superior são herdadas e aplicadas independentemente das configurações de política definidas em objetos de diretiva de nível inferior. Assim, a imposição de política é usada para sobrepor uma modificação e o bloqueio das configurações de política.

Os administradores de floresta podem usar a imposição de política para garantir que as configurações de política definidas no nível de site sejam aplicadas e para impedir a modificação e o bloqueio de configurações de política realizados por administradores de domínio e OU. Os administradores de domínio podem usar a imposição de política para garantir que as configurações de política definidas no nível de domínio sejam aplicadas e para impedir a modificação e o bloqueio de configurações de política realizados por administradores de OU.

Com o uso do GPMC, é possível impor a herança de política expandindo o contêiner de nível mais alto do qual a imposição terá início, pressionando e mantendo pressionada ou clicando com o botão direito do mouse no vínculo (link) para a GPO e tocando ou clicando em Enforced. Por exemplo, se você desejar garantir que uma GPO de nível de domínio seja herdada por todas as OUs do domínio, expanda o contêiner de domínio, pressione e mantenha pressionada ou clique com o botão direito do mouse na GPO de nível de domínio e toque ou clique em Enforced. Se a opção Enforced já estiver selecionada, selecione-a novamente para anular a imposição. No GPMC, é possível determinar com facilidade quais políticas são herdadas e quais políticas são impostas. Basta selecionar um objeto de diretiva em qualquer lugar do GPMC e visualizar a guia Scope relacionada no painel direito. Se a política for imposta, a coluna Enforced abaixo de Links exibirá Yes, como mostrado na Figura 4-6.

Após selecionar um objeto de diretiva, você pode pressionar e manter pressionada ou clicar com o botão direito do mouse em uma entrada na lista location na guia Scope para exibir um menu de atalho que permite o gerenciamento do vínculo e da imposição de política. Habilite ou desabilite vínculos marcando ou desmarcando a opção Link Enabled. Habilite ou desabilite a imposição marcando ou desmarcando a opção Enforced.

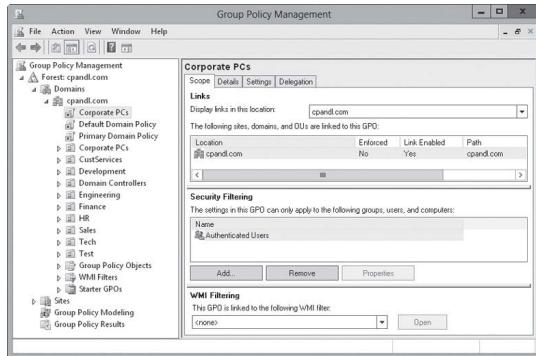


FIGURA 4-6 Faça a imposição da herança de política para garantir que as configurações sejam aplicadas.

Manutenção e solução de problemas de Group Policy

A Group Policy é uma ampla área de administração que requer um gerenciamento cuidadoso. Como qualquer outra área de administração, a Group Policy deve ser mantida com atenção para garantir seu funcionamento correto, e você deve diagnosticar e solucionar eventuais problemas. Para realizar a solução de problemas de Group Policy, você precisa ter uma compreensão sólida de como uma política é atualizada e processada. Além disso, também é necessário conhecer profundamente as tarefas gerais de manutenção e solução de problemas.

Atualização de Group Policy

Quando você altera uma política, tais alterações são imediatas. No entanto, elas não são propagadas automaticamente. Os computadores clientes solicitam as políticas nos seguintes momentos:

- Quando o computador é inicializado
- Quando um usuário efetua logon
- Quando um aplicativo ou usuário solicita uma atualização
- Quando um intervalo de atualização estiver configurado para Group Policy e tiver decorrido

As definições de configuração de computador são aplicadas durante a inicialização do sistema operacional. As definições de configuração de usuário, por sua vez,

são aplicadas quando um usuário efetuar logon em um computador. Normalmente, se houver conflito entre as configurações de computador e usuário, as configurações de computador têm prioridade e precedência.

Assim que as configurações de política forem aplicadas, as configurações são atualizadas automaticamente para garantir que sejam as mais recentes. O intervalo de atualização padrão para controladores de domínio é de cinco minutos. Para todos os outros computadores, o intervalo de atualização padrão é de 90 minutos, com uma variação de até 30 minutos para evitar a sobrecarga do controlador de domínio com muitas solicitações simultâneas de clientes. Isso significa que a janela de atualização efetiva para computadores não controladores de domínio tem duração de 90 a 120 minutos.

Durante a atualização de Group Policy, o computador cliente entra em contato com um controlador de domínio disponível em seu site local. Se um ou mais objetos de diretiva definidos no domínio tiverem sido alterados, o controlador de domínio fornece uma lista dos objetos de diretiva que se aplicam ao computador e ao usuário que está conectado no momento, conforme apropriado. O controlador de domínio realiza esse processo independentemente se os números de versão de todos os objetos de diretiva listados tiverem sido alterados ou não. Por padrão, o computador processa os objetos de diretiva apenas se o número de versão de pelo menos um dos objetos de diretiva tiver sido alterado. Se alguma das políticas relacionadas tiver sofrido alterações, todas as políticas precisam ser processadas novamente em razão da herança e da interdependência entre as políticas.

As configurações de segurança são uma exceção relevante à regra de processamento. Por padrão, essas configurações são atualizadas a cada 16 horas (960 minutos) independentemente se os objetos de diretiva apresentam alterações ou não. Uma diferença aleatória de até 30 minutos é adicionada para reduzir o impacto nos controladores de domínio e na rede durante as atualizações (fazendo a janela de atualização efetiva ter entre 960 e 990 minutos). Além disso, se o computador cliente detectar que está se conectando por meio de uma conexão de rede lenta, ele passa a informação ao controlador de domínio e apenas as configurações de segurança e os modelos administrativos são transferidos via rede. Isso significa que, por padrão, apenas as configurações de segurança e os modelos administrativos são aplicados quando um computador estiver conectado por meio de um link lento. É possível configurar o modo de detectar links lentos na Group Policy.

Você deve equilibrar com cuidado a frequência de atualização e a quantidade real de alterações de políticas. Se a política não for alterada com frequência, é recomendável que você aumente a janela de atualização para reduzir o uso de recursos. Por exemplo, talvez seja mais adequado usar um intervalo de atualização de 20 minutos em controladores de domínio e 180 minutos em outros computadores.

Configuração do intervalo de atualização

Você pode alterar o intervalo de atualização da Group Policy por objeto de diretiva. Para configurar o intervalo de atualização de controladores de domínio, siga estas etapas:

1. No GPMC, pressione e mantenha pressionada ou clique com o botão direito do mouse na GPO a ser modificada e toque ou clique em Edit. Essa GPO deve estar vinculada a um contêiner que inclua objetos de computador de controladores de domínio.
2. Em Administrative Templates de Computer Configuration sob System\Group Policy, dê um toque duplo ou clique duas vezes na política Set Group Policy Refresh

Interval For Domain Controllers. Isso exibe a caixa de diálogo Properties da política, mostrada na Figura 4-7.

3. Defina a política selecionando Enabled. Configure o intervalo de atualização na primeira caixa Minutes. Normalmente é recomendável que esse valor seja de cinco a 59 minutos.
4. Na outra caixa Minutes, determine a variação de tempo mínima ou máxima para o intervalo de atualização. A variação cria efetivamente uma janela de atualização com o objetivo de evitar a sobrecarga resultante do grande número de clientes que solicita simultaneamente uma atualização de Group Policy. Toque ou clique em OK.

OBSERVAÇÃO Um intervalo menor de atualização aumenta a probabilidade de um computador ter a configuração de política mais recente. Um intervalo maior de atualização reduz a frequência com que uma política é atualizada, fato que pode reduzir a sobrecarga devido ao uso de recursos, mas que também aumenta a probabilidade de um computador não ter a configuração de política mais recente.

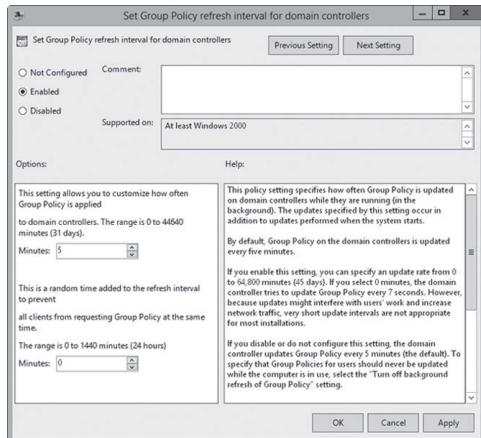


FIGURA 4-7 Configure o intervalo de atualização de Group Policy.

Para configurar o intervalo de atualização de servidores membros e estações de trabalho, siga estas etapas:

1. No GPMC, pressione e mantenha pressionada ou clique com o botão direito do mouse na GPO a ser modificada e toque ou clique em Edit. Essa GPO deve estar vinculada a um contêiner que inclua os objetos de computador.
2. Em Administrative Templates de Computer Configuration sob System\Group Policy, dê um toque duplo ou clique duas vezes na política Set Group Policy Refresh Interval For Computers. Isso exibe uma caixa de diálogo similar à mostrada anteriormente na Figura 4-7.
3. Defina a política selecionando Enabled. Na primeira caixa Minutes, configure o intervalo de atualização. Normalmente, é recomendável que esse valor seja de 60 a 240 minutos.

4. Na caixa Minutes, determine a variação de tempo mínima ou máxima para o intervalo de atualização. A variação cria efetivamente uma janela de atualização com o objetivo de evitar a sobrecarga resultante do grande número de clientes que solicita simultaneamente uma atualização de Group Policy. Toque ou clique em OK.

MUNDO REAL Você quer se certificar de que as atualizações não ocorram muito frequentemente, mas que ainda assim tenham um intervalo suficiente para atender às expectativas e exigências. Quanto maior a frequência de atualização de uma política, mais tráfego é gerado na rede. Em uma grande instalação, normalmente é recomendável configurar uma taxa de atualização que seja maior que a taxa padrão para reduzir o tráfego da rede, especialmente se a política afetar centenas de usuários ou computadores. Em qualquer instalação em que os usuários reclamem sobre seus computadores ficarem lentos periodicamente, talvez também seja apropriado que você aumente o intervalo de atualização da política. Pense se uma atualização por dia ou semana já não é o bastante para manter as políticas atualizadas o suficiente para atender às necessidades de sua organização.

Como administrador, é possível que muitas vezes você precise ou queira atualizar a Group Policy manualmente. Por exemplo, talvez você não queira esperar para que a Group Policy seja atualizada no intervalo automático ou você pode estar tentando resolver um problema com as atualizações e deseja forçar uma atualização de Group Policy. É possível atualizar a Group Policy manualmente por meio do utilitário de linha de comando Gpupdate.

Você pode iniciar uma atualização de diversas formas. Digitar **gpupdate** em um prompt ou na caixa Apps Search atualiza as configurações tanto no nó Computer Configuration quanto no User Configuration do computador local. Apenas as configurações de política que tiverem sido alteradas são processadas e aplicadas quando Gpupdate é executado. Você pode alterar esse comportamento por meio do parâmetro **/Force** para forçar uma atualização de todas as configurações de política.

Além disso, é possível atualizar as definições das configurações de usuário e computador separadamente. Para atualizar apenas as configurações de computador, digite **gpupdate /target:computer** no prompt de comando. Para atualizar apenas as configurações de usuário, digite **gpupdate /target:user** no prompt de comando.

Você também pode usar o Gpupdate para efetuar logoff de um usuário ou reiniciar um computador após a Group Policy ser atualizada. Isso é útil porque algumas Group Policies são aplicadas apenas quando um usuário efetuar logon ou quando um computador é iniciado. Para efetuar logoff do usuário após uma atualização, adicione o parâmetro **/Logoff**. Para reiniciar o computador após uma atualização, adicione o parâmetro **/Boot**.

Modelagem de Group Policy para fins de planejamento

A modelagem de Group Policy para fins de planejamento é útil para quando você deseja testar vários cenários de implementação e configuração. Por exemplo, talvez você queira modelar o efeito do processamento de loopback ou da detecção de links lentos. Você também pode modelar o efeito de mover usuários ou computadores a outro contêiner no Active Directory ou o efeito de alterar a associação de grupo de segurança para usuários ou computadores.

Todos os administradores corporativos e de domínio apresentam a permissão de modelar a Group Policy para planejamento, assim como as pessoas para as quais a permissão Perform Group Policy Modeling Analyses foi delegada. Para modelar a Group Policy e testar vários cenários de implementação e atualização, siga estas etapas:

1. No GPMC, pressione e mantenha pressionado ou clique com o botão direito do mouse no nó Group Policy Modeling, selecione Group Policy Modeling Wizard e toque ou clique em Next.
2. Na página Domain Controller Selection, selecione o domínio a ser modelado na lista Show Domain Controllers In This Domain. Por padrão, você fará a simulação de uma política em qualquer controlador de domínio disponível no domínio selecionado. Se você desejar usar um controlador de domínio específico, selecione This Domain Controller e toque ou clique no controlador de domínio a ser usado. Toque ou clique em Next.
3. Na página User And Computer Selection, mostrada na Figura 4-8, há a opção de simular a política com base em contêineres ou contas individuais. Use uma das técnicas a seguir para escolher contas e toque ou clique em Next:
 - Usar contêineres para simular alterações para OUs e outros contêineres inteiros. Sob User Information, selecione Container e toque ou clique em Browse para exibir a caixa de diálogo Choose User Container. Use a caixa de diálogo para escolher um dos contêineres de usuário disponíveis no domínio selecionado. Sob Computer Information, selecione Container, toque ou clique em Browse para exibir a caixa de diálogo Choose Computer Container e escolha um dos contêineres de computador disponíveis no domínio selecionado.
 - Selecionar as contas específicas para simular alterações para um usuário e computador específicos. Sob User Information, selecione User, toque ou clique em Browse para exibir a caixa de diálogo Select User e especifique uma conta de usuário. Sob Computer Information, selecione Computer, toque ou clique em Browse para exibir a caixa de diálogo Select Computer e especifique uma conta de computador.

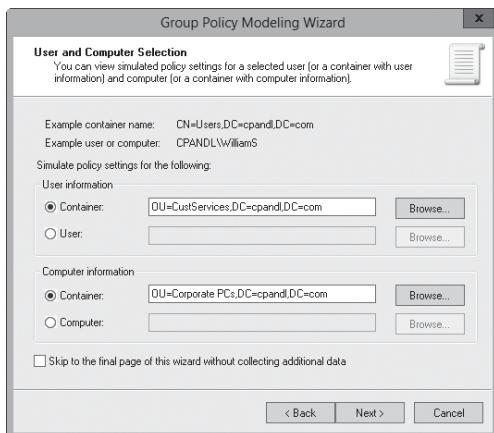


FIGURA 4-8 Selecione contêineres ou contas individuais para usar na simulação.

4. Na página Advanced Simulation Options, selecione conforme necessário as opções avançadas para Slow Network Connections, Loopback Processing e Site e toque ou clique em Next.
5. Na página User Security Groups, é possível simular alterações à associação de grupo de segurança do usuário aplicável ou ainda dos usuários aplicáveis. Qualquer alteração que você fizer na associação de grupo afeta o usuário ou contêiner de usuário selecionado anteriormente. Por exemplo, se você desejar ver o que acontece se um usuário no contêiner de usuário designado for membro do grupo GerentesCorp, adicione esse grupo à lista Security Groups. Toque ou clique em Next.
6. Na página Computer Security Groups, você pode simular alterações à associação de grupo de segurança para um computador ou para computadores. Qualquer alteração que você fizer na associação de grupo afeta o computador ou contêiner de computador selecionado anteriormente. Por exemplo, se você desejar ver o que acontece se um computador no contêiner de computador designado for membro do grupo ComputadoresRemotos, adicione esse grupo à lista Security Groups. Toque ou clique em Next.
7. Você pode vincular filtros do Windows Management Instrumentation (WMI) a GPOs. Por padrão, presume-se que os usuários e computadores selecionados atendam a todos os requisitos do filtro WMI, o que é recomendável na maioria dos casos para fins de planejamento. Toque ou clique em Next para aceitar as opções padrão.
8. Examine as seleções feitas e toque ou clique em Next. Após o assistente reunir informações de política, toque ou clique em Finish. Quando o assistente concluir a geração do relatório, o relatório é mostrado no painel esquerdo e os resultados são exibidos no painel direito.
9. Quando você seleciona a guia Details no painel direito, como mostrado na Figura 4-9, é possível determinar as configurações que seriam aplicadas analisando o relatório. As informações de política do computador estão listadas sob Computer Details. As informações de política do usuário estão listadas sob User Details.

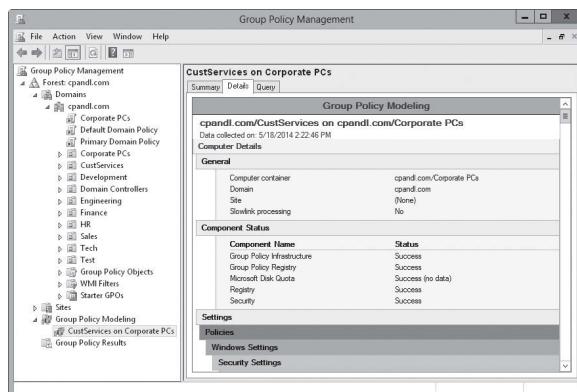


FIGURA 4-9 Examine o relatório para determinar os resultados da modelagem.

Como copiar, colar e importar objetos de diretiva

O GPMC apresenta as operações integradas de copiar, colar e importar. Usar os recursos de copiar e colar é bastante simples. As opções Copy e Paste tornam-se disponíveis quando você pressiona e mantém pressionada ou clica com o botão direito do mouse em uma GPO no GPMC. Você pode copiar um objeto de diretiva e todas as suas configurações em um domínio e navegar até o domínio no qual quer colar a cópia do objeto de diretiva. Os domínios de origem e destino podem ser qualquer domínio com o qual você consegue se conectar no GPMC e para o qual tem permissão de gerenciar os objetos de diretiva relacionados. No domínio de origem, é necessária a permissão Read para criar uma cópia do objeto de diretiva. No domínio de destino, é necessária a permissão Write para gravar (colar) o objeto de diretiva copiado. Os administradores têm esse privilégio, assim como as pessoas que receberam a permissão de criar objetos de diretiva.

Copiar objetos de diretiva entre domínios é uma boa opção quando há conectividade entre domínios e as permissões apropriadas. No entanto, se você for um administrador em um escritório remoto ou recebeu permissões manualmente talvez não tenha acesso ao domínio de origem para criar uma cópia de um objeto de diretiva. Nesse caso, outro administrador pode fazer uma cópia de backup do objeto de diretiva e enviar os dados relacionados a você. Após receber os dados, você pode importar ao domínio a cópia de backup do objeto de diretiva para criar um objeto de diretiva com as mesmas configurações.

Qualquer pessoa com o privilégio de gerenciamento de Group Policy Edit Settings pode realizar uma operação de importação. Essa operação substitui todas as configurações do objeto de diretiva selecionado. Para importar uma cópia de backup de um objeto de diretiva a um domínio, siga estas etapas:

1. No GPMC, pressione e mantenha pressionado ou clique com o botão direito do mouse em Group Policy Objects e selecione New. Na caixa de diálogo New GPO, digite um nome descritivo para a nova GPO e toque ou clique em OK.
2. Agora, a nova GPO está listada no contêiner Group Policy Objects. Pressione e mantenha pressionado ou clique com o botão direito do mouse no novo objeto de diretiva e toque ou clique em Import Settings. O Import Settings Wizard será iniciado.
3. Toque ou clique em Next duas vezes para passar a página de backup da GPO. Dessa vez, não é preciso criar um backup da GPO, pois ela é nova.
4. Na página Backup Location, toque ou clique em Browse. Na caixa de diálogo Browse For Folder, selecione a pasta que contém a cópia de backup do objeto de diretiva a ser importado e toque ou clique em OK. Toque ou clique em Next para continuar.
5. Se vários backups estiverem armazenados na pasta de backup selecionada, será exibida uma lista deles na página Source GPO. Toque ou clique no item que você quer usar e em Next.
6. O Import Settings Wizard examina o objeto de diretiva procurando por referências de entidades de segurança (Security Principals) e caminhos UNC que talvez precisem ser migrados. Se algo for encontrado, é fornecida a opção de criar tabelas de migração ou usar tabelas de migração existentes.
7. Avance no assistente tocando ou clicando em Next e toque ou clique em Finish para começar o processo de importação. Quando a importação for concluída, toque ou clique em OK.

Backup e restauração de objetos de diretiva

Como parte de suas tarefas periódicas de administração, você deve fazer backup das GPOs para protegê-las. O GPMC pode ser usado para fazer backup de objetos de diretiva individuais em um domínio ou de todos os objetos de diretiva de um domínio seguindo estas etapas:

1. No GPMC, expanda e selecione o nó Group Policy Objects. Se desejar fazer backup de todos os objetos de diretiva do domínio, pressione e mantenha pressionado ou clique com o botão direito do mouse no nó Group Policy Objects e toque ou clique em Back Up All. Se desejar fazer backup de um objeto de diretiva específico do domínio, pressione e mantenha pressionado ou clique com o botão direito do mouse no objeto de diretiva e selecione Back Up.
2. Na caixa de diálogo Back Up Group Policy Object, toque ou clique em Browse. Na caixa de diálogo Browse For Folder, selecione o local em que o backup da GPO deve estar armazenado.
3. Na caixa de texto Description, digite uma descrição do conteúdo do backup. Toque ou clique em Back Up para iniciar o processo de backup.
4. A caixa de diálogo Backup mostra o progresso e o status do backup. Toque ou clique em OK depois da conclusão do backup. Se um backup falhar, verifique as permissões da política e da pasta na qual o backup está sendo gravado. São necessárias a permissão Read na política e a permissão Write na pasta de backup para criar um backup. Por padrão, os membros dos grupos Domain Admins e Enterprise Admins têm tais permissões.

Por meio do GPMC, também é possível restaurar um objeto de diretiva para o estado em que ele estava quando foi feito seu backup. O GPMC rastreia o backup de cada objeto de diretiva separadamente, mesmo se você fizer o backup de todos os objetos de diretiva de uma só vez. Como as informações de versão também são rastreadas de acordo com o carimbo de data/hora e a descrição do backup, é possível restaurar a última versão de cada objeto de diretiva ou uma determinada versão de qualquer objeto de diretiva.

Você pode restaurar um objeto de diretiva seguindo estas etapas:

1. No GPMC, pressione e mantenha pressionado ou clique com o botão direito do mouse no nó Group Policy Objects e toque ou clique em Manage Backups. A caixa de diálogo Manage Backups será exibida.
2. Na caixa de texto Backup Location, toque ou clique em Browse. Na caixa de diálogo Browse For Folder, localize a pasta do backup e toque ou clique em OK.
3. Todos os backups de objetos de diretiva da pasta selecionada são listados sob Backed Up GPOs. Para visualizar apenas a última versão dos objetos de diretiva de acordo com o carimbo de data/hora, selecione Show Only The Latest Version Of Each GPO.
4. Selecione a GPO a ser restaurada. Se desejar confirmar suas configurações, toque ou clique em View Settings e use o Internet Explorer para verificar se as configurações encontram-se conforme esperado. Quando estiver pronto para continuar, toque ou clique em Restore. Confirme que você quer restaurar o objeto de diretiva selecionado tocando ou clicando em OK.

5. A caixa de diálogo Restore mostra o progresso e o status da operação de restauração. Se uma operação de restauração falhar, verifique as permissões do objeto de diretiva e da pasta a partir da qual o backup está sendo lido. Para restaurar uma GPO, você precisa da permissão Edit Settings, Delete, Modify Security no objeto de diretiva e a permissão Read na pasta que contém o backup. Por padrão, os membros dos grupos Domain Admins e Enterprise Admins têm tais permissões.

Como determinar as configurações e o status de atualização da Group Policy

Você pode usar o Group Policy Result para registrar em log o RSOP. Quando o Group Policy Result é usado dessa maneira, você pode examinar todos os objetos de diretiva que se aplicam a um computador e a última vez que os objetos de diretiva aplicáveis foram processados (atualizados). Todos os administradores corporativos e de domínio possuem a permissão de verificar a Group Policy para registro em log, assim como as pessoas para as quais a permissão Read Group Policy Results Data foi delegada. No GPMC, é possível verificar a Group Policy para fins de registrar em log o RSOP pressionando e mantendo pressionado ou clicando com o botão direito do mouse no nó Group Policy Results e selecionando Group Policy Results Wizard. Quando o Group Policy Results Wizard iniciar, siga os prompts.

Como desabilitar uma parte não usada da Group Policy

Outra maneira de desabilitar uma política é desabilitar uma parte não usada da GPO. Ao fazer isso, você bloqueia definições das configurações de computador ou de usuário (ou de ambas) e não permite que elas sejam aplicadas. Quando parte de uma política que não é usada é desabilitada, a aplicação de GPOs será mais rápida.

Você pode habilitar e desabilitar políticas parcialmente ou completamente seguindo estas etapas:

1. No GPMC, selecione o contêiner do site, domínio ou OU com o qual você deseja trabalhar.
2. Selecione o objeto de diretiva com o qual você deseja trabalhar e toque ou clique na guia Details no painel direito.
3. Escolha uma das configurações de status a seguir da lista GPO Status e toque ou clique em OK quando solicitado a confirmação de que você deseja alterar o status dessa GPO:
 - **All Settings Disabled** Não permite o processamento do objeto de diretiva e suas configurações.
 - **Computer Configuration Settings Disabled** Desabilita o processamento das definições da configuração de computador. Isso significa que apenas as definições da configuração de usuário são processadas.
 - **Enabled** Permite o processamento do objeto de diretiva e suas configurações.
 - **User Configuration Settings Disabled** Desabilita o processamento das definições da configuração de usuário. Isso significa que apenas as definições da configuração de computador são processadas.

Alteração das preferências de processamento da política

Na Group Policy, as definições da configuração de computador são processadas quando o computador é iniciado e acessa a rede. As definições de configuração de usuário, por sua vez, são processadas quando um usuário efetua logon na rede. No caso de conflito entre as configurações sob Computer Configuration e User Configuration, as definições da configuração de computador têm preferência. Também é importante lembrar que as configurações de computador são aplicadas a partir das GPOs do computador e as configurações de usuário são aplicadas a partir das GPOs do usuário.

Em algumas situações especiais, tal comportamento talvez não seja o ideal. Em um computador compartilhado, talvez seja mais adequado que as configurações de usuário sejam aplicadas a partir das GPOs do computador, mas você também pode querer permitir que as configurações de usuário das GPOs do usuário sejam aplicadas. Em um ambiente seguro de laboratório ou quiosque, talvez você deseje que as configurações de usuário sejam aplicadas a partir das GPOs do computador para garantir a conformidade com regras ou diretrizes rigorosas de segurança para o laboratório. Por meio do processamento de loopback, é possível permitir esses tipos de exceção e obter configurações de usuário a partir de GPOs do computador.

Para alterar o modo de operação do processamento de loopback, siga estas etapas:

1. No GPMC, pressione e mantenha pressionada ou clique com o botão direito do mouse na GPO a ser modificada e toque ou clique em Edit.
2. Em Administrative Templates de Computer Configuration sob System\Group Policy, dê um toque duplo ou clique duas vezes na diretiva Configure User Group Policy Loopback Processing Mode. Uma caixa de diálogo Properties é exibida para a política.
3. Defina a política selecionando Enabled, selecionando um dos modos a seguir de processamento da lista Mode e tocando ou clicando em OK:
 - **Replace** Selecione a opção Replace para garantir que as configurações de usuário de GPOs do computador sejam processadas e que as configurações de usuário de GPOs de usuário não sejam processadas. Isso significa que as configurações de usuário de GPOs do computador substituem as configurações de usuário normalmente aplicadas ao usuário.
 - **Merge** Selecione a opção Merge para garantir que as configurações de usuário de GPOs do computador sejam processadas primeiro, seguidas pelas configurações de usuário de GPOs do usuário e depois pelas configurações de usuário de GPOs do computador novamente. Essa técnica de processamento é usada para combinar as configurações de usuário tanto em GPOs do computador quanto em GPOs do usuário. No caso de conflito, as configurações de usuário de GPOs do computador têm precedência e substituem as configurações de usuário de GPOs do usuário.

Configuração da detecção de links lento

A detecção de links lento é usada por clientes de Group Policy para detectar latência elevada e capacidade de resposta reduzida na rede e para realizar uma ação corretiva com o objetivo de reduzir a probabilidade do processamento de Group Policy saturar a rede no futuro. Após a detecção de um link lento, os clientes de Group Policy reduzem suas comunicações e solicitações de rede, reduzindo, assim, a carga geral do tráfego de rede limitando a quantidade de processamentos de política.

Por padrão, se a velocidade de conexão está determinada para ser menor que 500 quilobits por segundo (que também poderia ser interpretada como alta latência/capacidade de resposta reduzida em uma rede rápida), o computador cliente interpreta que a conexão de rede é lenta e notifica o controlador de domínio. Como resultado, apenas as configurações de segurança e os modelos administrativos dos objetos de diretiva aplicáveis são enviados pelo controlador de domínio durante a atualização da política.

Você pode configurar a detecção de links lentos por meio da diretiva Configure Group Policy Slow Link Detection, que está armazenada em Administrative Templates de Computer Configuration sob System\Group Policy. Se essa política for desabilitada ou não for configurada, os clientes usarão o valor padrão de 500 quilobits por segundo para determinar se eles estão em um link lento. Se essa política for habilitada, é possível determinar um valor específico para links lento, como 384 quilobits por segundo. Além disso, pode-se especificar que as conexões 3G sejam sempre tratadas como links lentos. Por outro lado, se você desejar desabilitar completamente a detecção de links lentos, configure a opção Connection Speed como 0. Essa configuração informa efetivamente os clientes que eles não devem detectar links lentos e que todos os links devem ser considerados rápidos.

MUNDO REAL A Microsoft se refere a conexões de celular e banda larga como *redes pagas*. Várias políticas são designadas para ajudar a especificar como as conexões de rede devem ser usadas no caso de dispositivos móveis em redes pagas. Você pode

- Controlar a sincronização offline de arquivos em redes pagas por meio da política Enable File Synchronization On Costed Networks encontrada sob Computer Configuration\Administrative Templates\Network\Offline Files.
- Controlar transferências em segundo plano em redes pagas por meio da política Set Default Download Behavior For BITS Jobs On Costed Networks encontrada sob Computer Configuration\Administrative Templates\Network\Background Intelligent Transfer Services (BITS).
- Especificar que redes pagas de banda larga apresentam tarifas de uso fixas, variáveis ou irrestritas por meio da política Set Cost encontrada sob Computer Configuration\Administrative Templates\Network\WLAN Service\WLAN Media Cost.
- Especificar que redes pagas de celular apresentam tarifas de uso fixas, variáveis ou irrestritas por meio das políticas Set 3G Cost e Set 4G Cost encontradas sob Computer Configuration\Administrative Templates\Network\WWAN Service\WWAN Media Cost.

Você pode otimizar a detecção de links lentos para várias áreas de processamento da Group Policy conforme necessário. Por padrão, as áreas de política que não são processadas quando um link lento é detectado incluem

- Processamento de política de cota de disco
- Processamento de política de recuperação do EFS
- Processamento de política de redirecionamento de pasta
- Processamento de política de scripts
- Processamento de política de instalação de software

O processamento de política de segurança está sempre habilitado automaticamente para links lentos. Por padrão, a política de segurança é atualizada a cada 16 horas mesmo se a política de segurança não tiver sido alterada. A única maneira de interromper a atualização forçada é configurando o processamento de política de segurança de modo que ele não seja executado durante as atualizações periódicas

em segundo plano. Para isso, selecione a configuração de política Do Not Apply During Periodic Background Processing. No entanto, como a política de segurança é tão importante, a configuração Do Not Apply significa apenas que o processamento da política de segurança é interrompido quando o usuário estiver conectado e usando o computador. Uma das poucas razões para que talvez você queira interromper as atualizações de política de segurança é se falhas estiverem ocorrendo em aplicativos durante as operações de atualização.

A configuração da detecção de links lentos e do processamento de política relacionadas pode ser feita por meio destas etapas:

1. No GPMC, pressione e mantenha pressionado ou clique com o botão direito do mouse na GPO a ser modificada e toque ou clique em Edit.
2. Em Administrative Templates de Computer Configuration sob System\ Group Policy, dê um toque duplo ou clique duas vezes na política Configure Group Policy Slow Link Detection.
3. Selecione Enabled para definir a política, como mostrado na Figura 4-10. Na caixa Connection Speed, especifique a velocidade que deve ser usada para determinar se um computador está em um link lento. Além disso, pode-se especificar que as conexões 3G sejam sempre tratadas como links lentos. Toque ou clique em OK.

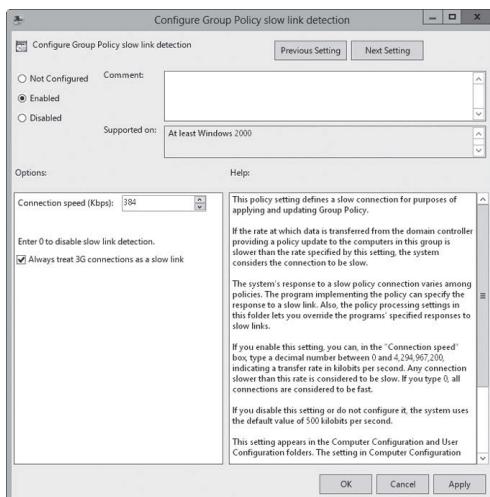


FIGURA 4-10 Configure a detecção de links lentos.

Para configurar o processamento de políticas em link lento ou em segundo plano de áreas importantes da Group Policy, siga estas etapas:

1. No GPMC, pressione e mantenha pressionado ou clique com o botão direito do mouse na GPO a ser modificada e toque ou clique em Edit.
2. Expanda Computer Configuration\Administrative Templates\System\Group Policy.

3. Dê um toque duplo ou clique duas vezes na política de processamento a ser configurada. Selecione Enabled para definir a política, como mostrado na Figura 4-11, e marque as configurações desejadas. As opções apresentam diferenças sutis dependendo da política selecionada e podem incluir:
- **Allow Processing Across A Slow Network Connection** Assegura que as configurações da política relacionada sejam processadas mesmo em uma rede lenta.
 - **Do Not Apply During Periodic Background Processing** Modifica as configurações atualizadas quando as políticas relacionadas são alteradas após a inicialização ou o logon.
 - **Process Even If The Group Policy Objects Have Not Changed** Força o computador cliente a processar as configurações da política relacionada durante a atualização mesmo se elas não tiverem sofrido alterações.

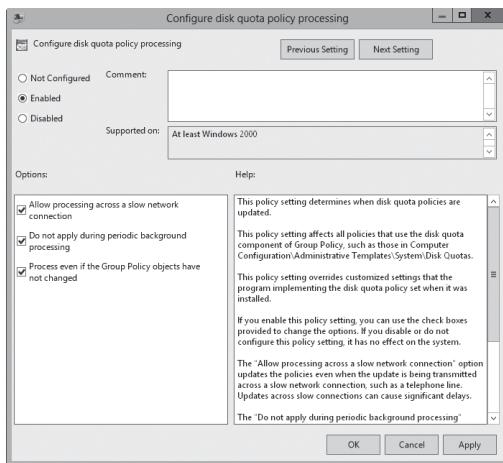


FIGURA 4-11 Configure o processamento de políticas para links lentos.

4. Toque ou clique em OK para salvar suas configurações.

Remoção de vínculos e exclusão de GPOs

No GPMC, é possível parar de executar uma GPO vinculada de duas maneiras:

- Remover um vínculo de uma GPO, mas não a GPO em si.
- Excluir permanentemente a GPO e todos os seus vínculos.

A remoção de um vínculo de GPO interrompe o processamento das configurações da política relacionada por parte do site, domínio ou OU, mas não exclui a GPO. Por isso, a GPO permanece vinculada a outros sites, domínios ou OUs conforme apropriado. No GPMC, você pode remover um vínculo de GPO pressionando e mantendo pressionado ou clicando com o botão direito do mouse no vínculo da GPO no contêiner ao qual ela

está vinculada e selecionando Delete. Quando for solicitada a confirmação de que você deseja remover o vínculo, toque ou clique em OK. Se você remover todos os vínculos de uma GPO dos sites, domínios e OUs, a GPO continua existindo no contêiner Group Policy Objects, mas suas configurações de política não afetam sua organização.

A exclusão permanente de uma GPO remove a GPO e seus vínculos. A GPO não permanecerá no contêiner Group Policy Objects e não estará vinculada a site, domínio ou OU algum. A única maneira de recuperar uma GPO excluída é fazendo a restauração de um backup (se houver). No GPMC, você pode remover uma GPO e todos os vínculos ao objeto a partir do nó Group Policy Objects. Pressione e mantenha pressionada ou clique com o botão direito do mouse na GPO e selecione Delete. Quando for solicitada a confirmação de que você deseja remover a GPO e todos os seus vínculos, toque ou clique em Yes.

Solução de problemas de Group Policy

Quando você está tentando determinar o motivo de uma política não estar sendo aplicada como esperado, uma das primeiras coisas a serem feitas é examinar o RSoP do usuário e do computador que estão apresentando problemas com as configurações de política. É possível determinar a GPO da qual uma configuração é aplicada seguindo estas etapas:

1. No GPMC, pressione e mantenha pressionado ou clique com o botão direito do mouse no nó Group Policy Results e toque ou clique em Group Policy Results Wizard. Quando o assistente for inicializado, toque ou clique em Next.
2. Na página Computer Selection, selecione This Computer para visualizar informações sobre o computador local. Para visualizar informações sobre um computador remoto, selecione Another Computer e toque ou clique em Browse. Na caixa de diálogo Select Computer, digite o nome do computador e toque ou clique em Check Names. Após selecionar a conta de computador correta, toque ou clique em OK e em Next.
3. Na página User Selection, selecione o usuário cujas informações de política você deseja visualizar. Você pode visualizar as informações de política de qualquer usuário que tiver efetuado logon no computador anteriormente selecionado. Toque ou clique em Next.
4. Examine as seleções feitas e toque ou clique em Next. Após o assistente reunir informações de política, toque ou clique em Finish. Quando o assistente concluir a geração do relatório, o relatório é mostrado no painel esquerdo e os resultados são exibidos no painel direito.
5. Para determinar as configurações que estão sendo aplicadas, examine o relatório. As informações de computador e usuário são listadas separadamente. As informações de política do computador estão listadas sob Computer Configuration Summary. As informações de política do usuário estão listadas sob User Configuration Summary.

Por meio do utilitário de linha de comando Gpresult, você também pode visualizar o RSoP. O Gpresult fornece detalhes sobre:

- Configurações especiais aplicadas para redirecionamento de pasta, instalação de software, cota de disco, IPsec e scripts

- A última vez que a Group Policy foi aplicada
- O controlador de domínio a partir do qual a política foi aplicada e as associações de grupo de segurança para o computador e usuário
- A lista completa das GPOs que foram aplicadas, bem como a lista completa de GPOs que não foram aplicadas devido a filtros

O Gpresult apresenta a sintaxe básica a seguir:

```
gpresult /s ComputerName /user Domain\UserName
```

Aqui, *ComputerName* é o nome do computador para o qual você deseja ver o log dos resultados de política e *Domain\UserName* indica o usuário para o qual você deseja ver o log dos resultados de política. Por exemplo, para visualizar o RSOP para Corppc85 e o usuário Tedg no domínio Cpandl, é necessário digitar o comando:

```
gpresult /s corppc85 /user cpandl\tedg
```

Um resultado mais detalhado pode ser visto por meio de duas opções. O parâmetro */v* ativa o modo de saída detalhado e os resultados são exibidos apenas para as configurações de política em vigor. O parâmetro */z* ativa o modo de saída detalhado com as configurações de política em vigor e todas as outras GPOs que tenham itens configurados. Como a saída do Gpresult pode ser bastante longa, é recomendável que você crie um relatório em HTML com o parâmetro */h* ou um relatório em XML com o parâmetro */x*. Os exemplos a seguir usam esses parâmetros:

```
gpresult /s corppc85 /user cpandl\tedg /h greport.html  
gpresult /s corppc85 /user cpandl\tedg /x greport.xml
```

Correção de Group Policy Objects padrão

As GPOs (objeto de diretiva de grupo) padrão Default Domain Policy e Default Domain Controller são essenciais para a integridade do AD DS. Se, por algum motivo, essas políticas forem corrompidas, a Group Policy não funcionará corretamente. Para solucionar esse problema, é necessário usar o GPMC para restaurar um backup dessas GPOs. Se você estiver em um cenário de recuperação de desastre e não tiver backups da Default Domain Policy ou da Default Domain Controller Policy, você pode usar o Dcpofix para restaurar as configurações de segurança nessas políticas. O estado para o qual o Dcpofix restaura esses objetos depende de como a segurança foi modificada e do estado de segurança do controlador de domínio antes do Dcpofix ser executado. Você deve ser membro do Domain Admins ou do Enterprise Admins para executar o Dcpofix.

Com a execução do Dcpofix, tanto a GPO Default Domain Policy quanto a Default Domain Controller Policy são restauradas por padrão e todas as alterações feitas a essas GPOs são perdidas. Algumas configurações de política são mantidas separadamente e não são perdidas, entre elas: WDS, configurações de segurança e Encrypting File System (EFS, Sistema de Arquivos com Criptografia). No entanto, as configurações de segurança não padrão não são mantidas, ou seja, outras alterações de política também podem ser perdidas. Todas as outras configurações de política são restauradas a seus valores anteriores e qualquer alteração que tiver sido feita é perdida.

Para executar o Dcpofix, efetue logon em um controlador de domínio do domínio no qual você deseja corrigir a Group Policy padrão e digite **dcpofix** em um prompt com privilégios elevados. O Dcpofix verifica o número de versão do esquema

do Active Directory para assegurar a compatibilidade entre a versão do Dcpofix a ser usado e a configuração do esquema do Active Directory. Se as versões não forem compatíveis, o Dcpofix fecha sem corrigir as GPOs padrão. Com a especificação do parâmetro `/Ignoreschema`, você pode permitir que o Dcpofix opere com diferentes versões do Active Directory. No entanto, os objetos de diretiva padrão podem não ser restaurados ao estado original. Por isso, você deve sempre se certificar de usar a versão do Dcpofix que está instalada com o sistema operacional atual.

Também há a opção de corrigir apenas a GPO Default Domain Policy ou apenas a GPO Default Domain Controller Policy. Se desejar corrigir apenas a Default Domain Policy, digite **dcpofix /target:domain**. Se desejar corrigir apenas a Default Domain Controller Policy, digite **dcpofix /target:dc**.

Gerenciamento de usuários e computadores com Group Policy

A Group Policy pode ser usada para gerenciar usuários e computadores de diversas maneiras. Nas seções a seguir, serão descritas algumas áreas de gerenciamento específicas, inclusive:

- Redirecionamento de pasta
- Scripts de computador e usuário
- Implantação de software
- Registro de certificado de computador e usuário
- Configurações de atualização automática

Gerenciamento centralizado de pastas especiais

Você pode gerenciar de maneira centralizada pastas especiais usadas pelo Windows Server por meio do redirecionamento de pasta. Isso é feito com o redirecionamento de pastas especiais para um local central na rede em vez de usar várias localizações padrão em cada computador. Para o Windows XP Professional e versões anteriores do Windows, as pastas especiais que podem ser gerenciadas de maneira centralizada são: Application Data, Start Menu, Desktop, My Documents e My Pictures. Para o Windows Vista e versões superiores do Windows, as pastas especiais que podem ser gerenciadas são AppData(Roaming), Desktop, Start Menu, Documents, Pictures, Music, Videos, Favorites, Contacts, Downloads, Links, Searches e Saved Games.

Embora o Windows Vista e versões superiores armazenem as pastas pessoais de maneira sutilmente diferente, as pastas são gerenciadas da mesma forma na Group Policy.

Há duas opções gerais para o redirecionamento. Você pode redirecionar uma pasta especial para o mesmo local de rede para todos os usuários ou designar locais com base na associação do usuário em grupos de segurança. Em ambos os casos você deve se certificar de que o local de rede que planeja usar está disponível como um compartilhamento de rede. Consulte o Capítulo 12, “Compartilhamento de dados, segurança e auditoria”, para obter detalhes sobre o compartilhamento de dados em uma rede.

Por padrão, os usuários podem redirecionar pastas independentemente de qual computador estiver usando dentro do domínio. O Windows 8 e o Windows Server

2012 permitem a modificação desse comportamento por meio da especificação de quais computadores um usuário pode usar para acessar os perfis móveis e as pastas redirecionadas. Você realiza essa ação designando que certos computadores sejam computadores primários e configurando a política de domínio para restringir aos computadores primários o download de perfis, de pastas redirecionadas ou de ambos. Para obter mais informações, consulte “Perfis locais, móveis e obrigatórios” no Capítulo 9, “Gerenciamento de contas de usuário e de grupo.”

Redirecionamento de uma pasta especial a um local único

Você pode redirecionar uma pasta especial a um local único seguindo estas etapas:

1. No GPMC, pressione e mantenha pressionada ou clique com o botão direito do mouse na GPO para o site, domínio ou OU com a qual você deseja trabalhar e toque ou clique em Edit. O editor de políticas será aberto para a GPO.
2. No editor de políticas, expanda os nós: User Configuration, Windows Settings e Folder Redirection.
3. Sob Folder Redirection, pressione e mantenha pressionada ou clique com o botão direito do mouse na pasta especial com a qual você deseja trabalhar, como AppData (Roaming), e toque ou clique em Properties. Uma caixa de diálogo Properties similar à mostrada na Figura 4-12 é aberta.

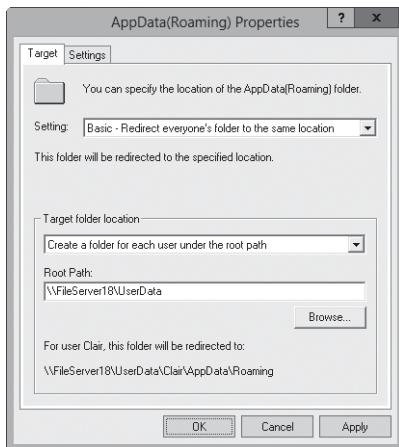


FIGURA 4-12 Configure as opções para o redirecionamento por meio da caixa de diálogo Properties de uma pasta especial.

4. Na lista Setting na guia Target, escolha Basic – Redirect Everyone’s Folder To The Same Location.
5. Sob Target Folder Location, há diversas opções. As opções disponíveis dependem da pasta com a qual você está trabalhando e incluem:

- **Redirect To The User's Home Directory** Se esta opção for selecionada, a pasta é redirecionada para um subdiretório dentro da pasta base do usuário. O local da pasta base do usuário é configurado com as variáveis de ambiente %HomeDrive% e %HomePath%.
 - **Create A Folder For Each User Under The Root Path** Se esta opção for selecionada, uma pasta é criada para cada usuário no local inserido na caixa de texto Root Path. O nome da pasta é o nome da conta de usuário como especificado por %UserName%. Assim, se o valor de caminho raiz \\Zeta\User-Documents for inserido, a pasta de Williams estará localizada em \\Zeta\User-Documents\Williams.
 - **Redirect To The Following Location** Se esta opção for selecionada, a pasta é redirecionada ao local inserido na caixa de texto Root Path. Nesse caso, normalmente é recomendável que se use uma variável de ambiente para personalizar o local da pasta para cada usuário. Por exemplo, o valor de caminho raiz \\Zeta\UserData%\%UserName%\docs poderia ser usado.
 - **Redirect To The Local UserProfile Location** Se esta opção for selecionada, a pasta é redirecionada para um subdiretório dentro do diretório do perfil de usuário. O local do perfil de usuário é configurado com a variável %UserProfile%.
6. Toque ou clique na guia Settings, configure as opções adicionais a seguir e toque ou clique em OK para concluir o processo:
- **Grant The User Exclusive Rights To** Concede aos usuários controle total para acessar os seus dados nas pastas especiais
 - **Move The Contents Of *FolderName* To The New Location** Move os dados das pastas especiais dos sistemas individuais da rede para a pasta central, ou ainda, pastas centrais
 - **Also Apply Redirection Policy To** Aplica a política de redirecionamento também em versões anteriores do Windows

Redirecionamento de uma pasta especial com base em associação de grupo

Você pode redirecionar uma pasta especial com base em associação de grupo seguindo estas etapas:

1. No GPMC, pressione e mantenha pressionada ou clique com o botão direito do mouse na GPO para o site, domínio ou OU com a qual você deseja trabalhar e toque ou clique em Edit. O editor de políticas será aberto para a GPO.
2. No editor de políticas, expanda os nós: User Configuration, Windows Settings e Folder Redirection.
3. Sob Folder Redirection, pressione e mantenha pressionada ou clique com o botão direito do mouse na pasta especial com a qual você deseja trabalhar, como AppData (Roaming), e toque ou clique em Properties.
4. Na guia Target, escolha Advanced – Specify Locations For Various User Groups na lista Setting. Como mostrado na Figura 4-13, um painel Security Group Membership é adicionado na caixa de diálogo Properties.

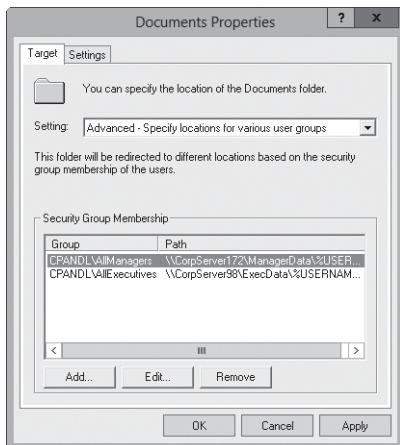


FIGURA 4-13 Configure o redirecionamento avançado por meio do painel Security Group Membership.

5. Toque ou clique em Add para abrir a caixa de diálogo Specify Group And Location. Outra opção é selecionar uma entrada já existente de grupo e tocar ou clicar em Edit para modificar suas configurações.
6. Na caixa de texto Security Group Membership, digite o nome do grupo de segurança cujo redirecionamento você deseja configurar ou toque ou clique em Browse para localizar um grupo de segurança para adicionar.
7. Assim como no caso do redirecionamento básico, as opções disponíveis dependem da pasta com a qual você está trabalhando e incluem:
 - **Redirect To The User's Home Directory** Se esta opção for selecionada, a pasta é redirecionada para um subdiretório dentro da pasta base do usuário. O local da pasta base do usuário é configurado com as variáveis de ambiente %HomeDrive% e %HomePath%.
 - **Create A Folder For Each User Under The Root Path** Se esta opção for selecionada, uma pasta é criada para cada usuário no local inserido na caixa de texto Root Path. O nome da pasta é o nome da conta de usuário como especificado por %UserName%. Assim, se o valor de caminho raiz \\Zeta\UserDocuments for inserido, a pasta de Williams estará localizada em \\Zeta\UserDocuments\Williams.
 - **Redirect To The Following Location** Se esta opção for selecionada, a pasta é redirecionada ao local inserido na caixa de texto Root Path. Nesse caso, normalmente é recomendável que se use uma variável de ambiente para personalizar o local da pasta para cada usuário. Por exemplo, o valor de caminho raiz \\Zeta\UserData%\%UserName%\docs poderia ser usado.
 - **Redirect To The Local Userprofile Location** Se esta opção for selecionada, a pasta é redirecionada para um subdiretório dentro do diretório do perfil de usuário. O local do perfil de usuário é configurado com a variável %UserProfile%.

8. Toque ou clique em OK. Repita as etapas de 5 a 7 para os outros grupos que deseja configurar.
9. Após concluir a criação das entradas de grupo, toque ou clique na guia Settings, configure as opções adicionais a seguir e toque ou clique em OK para concluir o processo:
 - **Grant The User Exclusive Rights To** Concede aos usuários controle total para acessar os seus dados nas pastas especiais
 - **Move The Contents Of FolderName To The New Location** Move os dados das pastas especiais dos sistemas individuais da rede para a pasta central, ou ainda, pastas centrais
 - **Also Apply Redirection Policy To** Aplica a política de redirecionamento também em versões anteriores do Windows

Remoção do redirecionamento

Haverá situações em que talvez você queira remover o redirecionamento de uma determinada pasta especial. A remoção do redirecionamento é feita seguindo estas etapas:

1. No GPMC, pressione e mantenha pressionada ou clique com o botão direito do mouse na GPO para o site, domínio ou OU com a qual você deseja trabalhar. Toque ou clique em Edit para abrir o editor de políticas para a GPO.
2. No editor de políticas, expanda os nós: User Configuration, Windows Settings e Folder Redirection.
3. Sob Folder Redirection, pressione e mantenha pressionada ou clique com o botão direito do mouse na pasta especial com a qual você deseja trabalhar e toque ou clique em Properties.
4. Toque ou clique na guia Settings e certifique-se de que uma opção apropriada de Policy Removal esteja selecionada. Duas opções estão disponíveis:
 - **Leave The Folder In The New Location When Policy Is Removed** Se esta opção for selecionada, a pasta e seu conteúdo permanecem no local redirecionado e os usuários atuais ainda possuem permissão para acessar a pasta e seu conteúdo nesse local.
 - **Redirect The Folder Back To The Local Userprofile Location When Policy Is Removed** Se esta opção for selecionada, a pasta e seu conteúdo são copiados de volta ao local original. No entanto, o conteúdo não é excluído do local anterior.
5. Se a opção de Policy Removal tiver sido alterada, toque ou clique em Apply e na guia Target. Caso contrário, apenas toque ou clique na guia Target.
6. Para remover todas as definições de redirecionamento da pasta especial, escolha Not Configured na lista Setting.
7. Para remover o redirecionamento de determinado grupo de segurança, selecione o grupo de segurança no painel Security Group Membership e toque ou clique em Remove. Toque ou clique em OK.

Gerenciamento de scripts de usuário e computador

Com o Windows Server, você pode configurar quatro tipos de scripts:

- **Inicialização do computador** Executado durante a inicialização
- **Desligamento do computador** Executado antes do desligamento
- **Logon do usuário** Executado quando um usuário efetua logon
- **Logoff do usuário** Executado quando um usuário efetua logoff

O Windows 2000 e versões superiores comportam scripts escritos como arquivos de lotes de prompt de comando com extensão .bat ou .cmd ou scripts que usam o Windows Script Host (WSH). O WSH é um recurso do Windows Server que permite a você usar scripts escritos em uma linguagem de scripts, como VBScript, sem a necessidade de inserir o script em uma página da Web. Para fornecer um ambiente de script multifuncional, o WSH conta com mecanismos de script. Um mecanismo de script é o componente que define a sintaxe e a estrutura principais de determinada linguagem de scripts. O Windows Server é fornecido com mecanismos de script para VBScript e JScript. Outros mecanismos de script também estão disponíveis.

O Windows 7 e o Windows 8, bem como o Windows Server 2008 R2 e o Windows Server 2012, também comportam scripts do Windows PowerShell. Se você instalou o Windows PowerShell em computadores que processam uma determinada GPO, pode usar scripts do Windows PowerShell praticamente da mesma forma com que você usa outros scripts. Você tem a opção de executar scripts do Windows PowerShell antes ou depois de outros tipos de script.

Atribuição de scripts de inicialização e desligamento do computador

Os scripts de inicialização e desligamento do computador são atribuídos como parte de uma GPO. Assim, todos os computadores que são membros do site, domínio ou OU – ou dos três – executam scripts automaticamente quando inicializados ou desligados.

Para atribuir um script de inicialização ou desligamento do computador, siga estas etapas:

1. Abra a pasta que contém o script ou scripts que você deseja usar no File Explorer.
2. No GPMC, pressione e mantenha pressionada ou clique com o botão direito do mouse na GPO para o site, domínio ou OU com a qual você deseja trabalhar e toque ou clique em Edit. O editor de políticas será aberto para a GPO.
3. No nó Computer Configuration, dê um toque duplo ou clique duas vezes na pasta Windows Settings e toque ou clique em Scripts.
4. Para trabalhar com scripts de inicialização, pressione e mantenha pressionado ou clique com o botão direito do mouse em Startup e toque ou clique em Properties. Para trabalhar com scripts de desligamento, pressione e mantenha pressionado ou clique com o botão direito do mouse em Shutdown e selecione Properties. Uma caixa de diálogo similar à mostrada na Figura 4-14 será aberta.

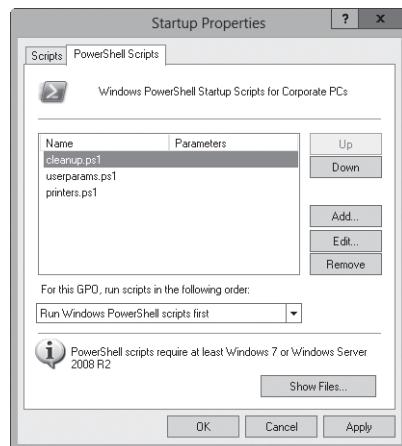


FIGURA 4-14 Adicione, edite e remova scripts de inicialização do computador por meio da caixa de diálogo Startup Properties.

5. Na guia Scripts, você pode gerenciar scripts em lotes do prompt de comando com extensão .bat ou .cmd e scripts que usam o WSH. Na guia PowerShell Scripts, você pode gerenciar scripts do Windows PowerShell. Ao trabalhar em alguma das duas guias, toque ou clique em Show Files.
6. Copie os arquivos da janela do File Explorer aberta e cole-os na janela que abriu quando você clicou em Show Files.
7. Toque ou clique em Add para atribuir um script. A caixa de diálogo Add A Script será aberta. Na caixa de texto Script Name, digite o nome do script copiado para a pasta Machine\Scripts\Startup ou Machine\Scripts\Shutdown para a política relacionada. Na caixa de texto Script Parameters, insira qualquer parâmetro a ser passado para o script. Repita esta etapa para adicionar outros scripts.
8. Durante a inicialização ou o desligamento, os scripts são executados na ordem em que estão listados na caixa de diálogo Properties. Na guia Scripts, use os botões Up e Down para reordenar os scripts conforme necessário. Faça o mesmo na guia PowerShell Scripts. Na guia PowerShell Scripts, você também pode usar a lista de seleção para especificar se os scripts do Windows PowerShell devem ser executados antes ou depois dos outros tipos de scripts.
9. Se você desejar editar o nome ou os parâmetros do script depois, selecione o script na lista Script For e toque ou clique em Edit. Para excluir um script, selecione o script na lista Script For e toque ou clique em Remove.
10. Para salvar as alterações feitas, toque ou clique em OK.

Atribuição de scripts de logon e logoff do usuário

A atribuição de scripts de usuário pode ser feita por meio de uma destas três maneiras:

- Você pode atribuir scripts de logon e logoff como parte de uma GPO. Assim, todos os usuários que são membros do site, domínio ou OU – ou dos três – executam scripts automaticamente quando efetuarem logon ou logoff.
- Você também pode atribuir scripts de logon individualmente por meio do console Active Directory Users And Computers (Usuários e Computadores do Active Directory). Assim, você pode atribuir a cada usuário um script de logon separado. Para obter mais detalhes, consulte “Configurações do ambiente do usuário” no Capítulo 9.
- A terceira maneira é atribuindo scripts de logon individuais como tarefas agendadas. As tarefas são agendadas por meio do Scheduled Task Wizard.

Para atribuir um script de logon ou logoff em uma GPO, siga estas etapas:

1. Abra a pasta que contém o script ou scripts que você deseja usar no File Explorer.
2. No GPMC, pressione e mantenha pressionada ou clique com o botão direito do mouse na GPO para o site, domínio ou OU com a qual você deseja trabalhar e toque ou clique em Edit. O editor de políticas será aberto para a GPO.
3. Dê um toque duplo ou clique duas vezes na pasta Windows Settings no nó User Configuration e toque ou clique em Scripts.
4. Para trabalhar com scripts de logon, pressione e mantenha pressionado ou clique com o botão direito do mouse em Logon e toque ou clique em Properties. Para trabalhar com scripts de logoff, pressione e mantenha pressionado ou clique com o botão direito do mouse em Logoff e toque ou clique em Properties. Uma caixa de diálogo similar à mostrada na Figura 4-15 será aberta.

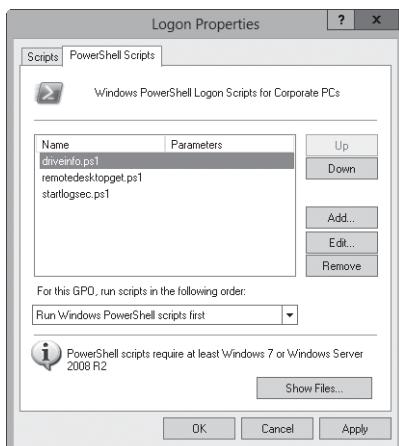


FIGURA 4-15 Adicione, edite e remova scripts de logon do usuário por meio da caixa de diálogo Logon Properties.

5. Na guia Scripts, você pode gerenciar scripts em lotes do prompt de comando com extensão .bat ou .cmd e scripts que usam o WSH. Na guia PowerShell Scripts, você pode gerenciar scripts do Windows PowerShell. Ao trabalhar em alguma das duas guias, toque ou clique em Show Files.
6. Copie os arquivos da janela do File Explorer aberta e cole-os na janela que abriu quando você clicou em Show Files.
7. Toque ou clique em Add para atribuir um script. A caixa de diálogo Add A Script será aberta. Na caixa de texto Script Name, digite o nome do script copiado para a pasta User\Scripts\Logon ou User\Scripts\Logoff para a política relacionada. Na caixa de texto Script Parameters, insira qualquer parâmetro a ser passado para o script. Repita esta etapa para adicionar outros scripts.
8. Durante o logon ou o logoff, os scripts são executados na ordem em que estão listados na caixa de diálogo Properties. Na guia Scripts, use os botões Up e Down para reordenar os scripts conforme necessário. Faça o mesmo na guia PowerShell Scripts. Na guia PowerShell Scripts, você também pode usar a lista de seleção para especificar se os scripts do Windows PowerShell devem ser executados antes ou depois dos outros tipos de scripts.
9. Se você desejar editar o nome ou os parâmetros do script depois, selecione o script na lista Script For e toque ou clique em Edit. Para excluir um script, selecione o script na lista Script For e toque ou clique em Remove.
10. Para salvar as alterações feitas, toque ou clique em OK.

Implantação de software com Group Policy

A Group Policy inclui uma funcionalidade básica, chamada Software Installation, para a implantação de software. Embora a política de Software Installation não seja designada para substituir soluções corporativas como o System Center Configuration Manager (SCCM), você pode usá-la para automatizar a implantação e a manutenção de software em organizações de todos os portes, desde que seus computadores estejam em execução por meio de edições corporativas do Windows 2000 ou superior.

Apresentação da política de Software Installation

Na Group Policy, você pode implantar software por computador ou usuário. Os aplicativos por computador permanecem disponíveis a todos os usuários de um computador e são configurados sob Computer Configuration\Software Settings\Software Installation. Os aplicativos por usuário permanecem disponíveis a usuários individuais e são configurados sob User Configuration\Software Settings\Software Installation.

Há três maneiras de implantar um software:

- **Computer assignment** Atribui o software a computadores clientes de modo que ele seja instalado quando o computador for inicializado. Essa técnica não requer a intervenção do usuário, mas requer uma reinicialização para instalar o software. O software instalado fica disponível a todos os usuários do computador.
- **User assignment** Atribui o software a usuários de modo que ele seja instalado quando o usuário efetuar logon. Essa técnica não requer a intervenção do usuário, mas requer que o usuário efetue logon para instalar o software. O software é associado apenas ao usuário e não ao computador.

- **User publishing** Publica o software de modo que os usuários possam instalá-lo manualmente por meio de Programs And Features. Essa técnica requer que o usuário instale o software explicitamente ou ative a instalação. O software é associado apenas ao usuário.

Ao usar User assignment ou User publishing, você pode anunciar o software de modo que um computador possa instalá-lo na primeira vez que for usado. Com anúncios, o software pode ser instalado automaticamente nas seguintes situações:

- Quando um usuário acessa um documento que requer o software
- Quando um usuário abre um atalho ao aplicativo
- Quando outro aplicativo requer um componente do software

Quando você configura a política de Software Installation, você normalmente não deve usar GPOs existentes. Em vez disso, você deve criar GPOs que configurem a instalação de software e vincular essas GPOs aos contêineres apropriados na Group Policy. Por meio dessa abordagem, é muito mais fácil reimplantar um software e aplicar atualizações.

Ao criar uma GPO para a implantação de software, você deve configurar um ponto de distribuição. Um ponto de distribuição é uma pasta compartilhada que está disponível aos computadores e usuários nos quais o software está sendo implantado. No caso de aplicativos básicos, o ponto de distribuição é preparado copiando o arquivo do pacote de instalação e todos os arquivos de aplicativo necessários para o compartilhamento e configurando as permissões de modo que esses arquivos possam ser acessados. Com outros aplicativos, como o Microsoft Office, o ponto de distribuição é preparado com uma instalação administrativa no compartilhamento. Com o Microsoft Office, isso pode ser feito executando o programa de instalação do aplicativo com o parâmetro /a e designando o compartilhamento como o local da instalação. A vantagem de uma instalação administrativa é que o software pode ser atualizado e reimplantado por meio da política de Software Installation.

Você pode atualizar aplicativos implantados por meio da política de Software Installation com uma atualização ou service pack ou implantando uma nova versão do aplicativo. Cada tarefa é executada de uma maneira sutilmente diferente.

Implantação de software em toda a organização

A política de Software Installation usa arquivos de pacotes do Windows Installer (.msi) ou de pacotes de aplicativos de nível inferior ZAW (.zap). Ao usar Computer assignment, User assignment ou User publishing, você pode implantar software por meio de pacotes do Windows Installer. Ao usar User publishing, você pode implantar software por meio de pacotes do Windows Installer ou pacotes de aplicativos de nível inferior ZAW. Com qualquer uma das técnicas, você deve configurar permissões de arquivo no pacote de instalação para que as contas de computador e usuário apropriadas tenham acesso de leitura.

Como a política de Software Installation é aplicada apenas durante o processamento em primeiro plano das configurações de política, as implantações de aplicativo por computador são processadas na inicialização e as implantações de aplicativo por usuário são processadas no logon. A instalação pode ser personalizada por meio de arquivos de transformação (.mst). Os arquivos de transformação modificam o processo de instalação de acordo com as configurações que você definiu para computadores e usuários específicos.

A implantação de software é feita seguindo estas etapas:

1. No GPMC, pressione e mantenha pressionada ou clique com o botão direito do mouse na GPO a ser usada para a implantação e toque ou clique em Edit.
2. No editor de políticas, abra Computer Configuration\Software Settings\Software Installation ou User Configuration\Software Settings\Software Installation conforme apropriado para o tipo de implantação de software.
3. Pressione e mantenha pressionado ou clique com o botão direito do mouse em Software Installation. No menu de atalho, toque ou clique em New e em Package.
4. Na caixa de diálogo Open, navegue até o compartilhamento de rede em que o pacote está localizado, toque ou clique no pacote para selecioná-lo e toque ou clique em Open.

OBSERVAÇÃO Os pacotes do Windows Installer (.msi) estão selecionados por padrão na lista Files Of Type. Se estiver realizando uma implantação do tipo User Publishing, você também pode escolher pacotes de aplicativos de nível inferior ZAW (.zap) como o tipo de arquivo.

5. Na caixa de diálogo Deploy Software, mostrada na Figura 4-16, selecione um dos métodos de implantação a seguir e toque ou clique em OK:
 - **Published** Publicar o aplicativo sem modificações
 - **Assigned** Atribuir o aplicativo sem modificações
 - **Advanced** Implantar o aplicativo por meio de opções avançadas de configuração

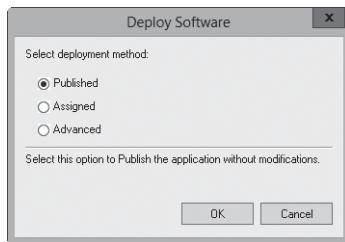


FIGURA 4-16 Selecione o método de implantação.

Configuração das opções de implantação de software

Você pode visualizar e configurar as opções gerais para um pacote de software seguindo estas etapas:

1. No GPMC, pressione e mantenha pressionada ou clique com o botão direito do mouse na GPO a ser usada para a implantação e toque ou clique em Edit.
2. No editor de políticas, acesse Computer Configuration\Software Settings\Software Installation ou User Configuration\Software Settings\Software Installation conforme apropriado para o tipo de implantação de software.

3. Dê um toque duplo ou clique duas vezes no pacote de Software Installation. Na caixa de diálogo Properties, examine ou modifique as opções de implantação de software.
4. Na guia Deployment, mostrada na Figura 4-17, você pode alterar o tipo de implantação e configurar as opções de implantação e instalação a seguir:
 - **Auto-Install This Application By File Extension Activation** Anuncia qualquer extensão de arquivo associada com esse pacote para uma implantação com instalação no primeiro uso. Esta opção é selecionada por padrão.
 - **Uninstall This Application When It Falls Out Of The Scope Of Management** Remove o aplicativo se ele deixar de ser aplicado ao usuário.
 - **Do Not Display This Package In The Add/Remove Programs Control Panel** Impede que o aplicativo apareça em Add/Remove Programs, ação que evita que um usuário desinstale um aplicativo.
 - **Install This Application At Logon** Configura a instalação completa – em vez do anúncio – de um aplicativo no momento em que o usuário efetuar logon. Esta opção não pode ser configurada quando você publica um pacote para usuários.
 - **Installation User Interface Options** Controla como a instalação é executada. Com a configuração padrão, Maximum, todas as telas e mensagens de instalação são exibidas ao usuário durante o processo de instalação. Com a opção Basic, apenas as mensagens de erro e conclusão são exibidas ao usuário durante a instalação.

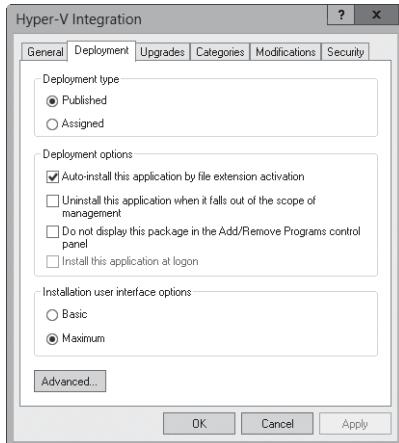


FIGURA 4-17 Examine e modifique as opções de implantação conforme necessário.

5. Toque ou clique em OK.

Atualização de software implantado

Quando um aplicativo usa um pacote do Windows Installer, você pode aplicar uma atualização ou service pack a um aplicativo implantado seguindo estas etapas:

1. Após obter um arquivo .msi ou.msp (patch) com a atualização ou o service pack a ser aplicado, copie o arquivo .msi ou .msp e qualquer outro arquivo novo de instalação para a pasta com o arquivo .msi original. Substitua os arquivos duplicados conforme necessário.
2. No GPMC, pressione e mantenha pressionada ou clique com o botão direito do mouse na GPO a ser usada para a implantação e toque ou clique em Edit.
3. No editor de políticas, acesse Computer Configuration\Software Settings\Software Installation ou User Configuration\Software Settings\Software Installation conforme apropriado para o tipo de implantação de software.
4. Pressione e mantenha pressionado ou clique com o botão direito do mouse no pacote com o qual você deseja trabalhar. No menu de atalho, toque ou clique em All Tasks e em Redeploy Application.
5. Quando solicitada a confirmação da ação, toque ou clique em Yes. O aplicativo é reimplantado a todos os usuários e computadores conforme apropriado para a GPO com a qual você está trabalhando.

No caso de aplicativos que usam pacote que não são do Windows Installer, você pode atualizar um aplicativo implantado ou aplicar um service pack seguindo estas etapas:

1. No GPMC, pressione e mantenha pressionada ou clique com o botão direito do mouse na GPO a ser usada para a implantação e toque ou clique em Edit.
2. No editor de políticas, acesse Computer Configuration\Software Settings\Software Installation ou User Configuration\Software Settings\Software Installation conforme apropriado para o tipo de implantação de software.
3. Pressione e mantenha pressionado ou clique com o botão direito do mouse no pacote. No menu de atalho, toque ou clique em All Tasks e em Remove. Toque ou clique em OK para aceitar a opção padrão de remoção imediata.
4. Copie o novo arquivo .zap e todos os arquivos relacionados para um compartilhamento de rede e reimplante o aplicativo.

Atualização de versão de software implantado

Você pode atualizar um aplicativo anteriormente implantado para uma nova versão seguindo estas etapas:

1. Obtenha um arquivo do Windows Installer para a nova versão do software e copie-o juntamente com todos os arquivos necessários para um compartilhamento de rede. Como alternativa, você pode executar uma instalação administrativa no compartilhamento de rede.
2. No GPMC, pressione e mantenha pressionada ou clique com o botão direito do mouse na GPO a ser usada para a implantação e toque ou clique em Edit.

3. No editor de políticas, acesse Computer Configuration\Software Settings\Software Installation ou User Configuration\Software Settings\Software Installation conforme apropriado para o tipo de implantação de software.
4. Pressione e mantenha pressionado ou clique com o botão direito do mouse em Software Installation. No menu de atalho, toque ou clique em New e em Package. Crie um aplicativo atribuído ou publicado para o arquivo do Windows Installer para a nova versão do software.
5. Pressione e mantenha pressionado ou clique com o botão direito do mouse no pacote de atualização e toque ou clique em Properties. Na guia Upgrades, toque ou clique em Add. Na caixa de diálogo Add Upgrade Package, realize uma das seguintes ações:
 - Se o aplicativo original e a atualização estiverem na GPO atual, selecione Current Group Policy Object e o aplicativo anteriormente implantado na lista Package To Upgrade.
 - Se o aplicativo original e a atualização estiverem em GPOs diferentes, selecione A Specific GPO, toque ou clique em Browse e selecione a GPO a partir da caixa de diálogo Browse For A Group Policy Object. Selecione o aplicativo anteriormente implantado na lista Package To Upgrade.
6. Escolha uma opção de atualização. Se você quiser substituir o aplicativo pela sua nova versão, selecione Uninstall The Existing Package, Then Install The Upgrade Package. Se você deseja executar uma atualização *in loco* sobre a instalação existente, selecione Package Can Upgrade Over The Existing Package.
7. Toque ou clique em OK para fechar a caixa de diálogo Add Upgrade Package. Se você quiser tornar essa atualização obrigatória, marque a caixa de seleção Required Upgrade For Existing Packages e toque ou clique em OK para fechar a caixa de diálogo Properties do pacote de atualização.

Registro automático de certificados de computador e usuário

Um servidor designado como uma certificate authority (CA, autoridade de certificação) é responsável por emitir certificados digitais e gerenciar a certificate revocation list (CRL, lista de certificados revogados). Os servidores com Windows Server podem ser configurados como CAs por meio da instalação do Active Directory Certificate Services (Serviços de Certificados do Active Directory). Os computadores e usuários podem usar os certificados para fins de autenticação e criptografia.

Em uma configuração corporativa, CAs corporativas são usadas para registro automático. Isso significa que usuários e computadores autorizados podem processar automaticamente a solicitação de certificado de modo que os usuários e os computadores possam instalar o certificado imediatamente.

A Group Policy controla o modo de funcionamento do registro automático. Quando há a instalação de CAs corporativas, as políticas de registro automático para usuários e computadores são habilitadas automaticamente. A política para o registro de certificado para computador é a Certificate Services Client – AutoEnrollment Settings sob Computer Configuration\Windows Settings\Security Settings\Public Key Policies. A política para o registro de certificado para usuário é a Certificate Services Client – AutoEnrollment sob User Configuration\Windows Settings\Security Settings\Public Key Policies.

O registro automático pode ser configurado seguindo estas etapas:

1. No GPMC, pressione e mantenha pressionada ou clique com o botão direito do mouse na GPO com a qual você deseja trabalhar e toque ou clique em Edit.
2. No editor de políticas, acesse User Configuration\Windows Settings\Security Settings\Public Key Policies ou Computer Configuration\Windows Settings\Security Settings\Public Key Policies de acordo com o tipo de política que você quer configurar.
3. Dê um toque duplo ou clique duas vezes em Certificate Services Client-Auto-Enrollment. Para desabilitar o registro automático, selecione Disabled na lista Configuration Model, toque ou clique em OK e não prossiga com as etapas deste procedimento. Para habilitar o registro automático, selecione Enabled a partir da lista Configuration Model.
4. Para renovar automaticamente os certificados expirados, atualizar certificados pendentes e remover certificados revogados, marque a caixa de seleção relacionada.
5. Para garantir que a última versão dos modelos de certificado seja solicitada e usada, marque a caixa de seleção Update Certificates That Use Certificate Templates.
6. Para notificar os usuários quando um certificado estiver prestes a expirar, especifique quando as notificações devem ser enviadas na caixa fornecida. Por padrão, as notificações são enviadas quando ainda há 10% do tempo de vida do certificado.
7. Toque ou clique em OK para salvar suas configurações.

Configuração do Automatic Updates na Group Policy

O Automatic Updates ajuda você a manter o sistema operacional atualizado. Embora seja possível configurar o Automatic Updates por computador, normalmente é recomendável que esse recurso seja configurado para todos os usuários e computadores por meio de uma GPO – o que é uma técnica de gerenciamento muito mais eficiente.

Observe que, por padrão, o Windows 8 e o Windows Server 2012 usam o Windows Update para baixar atualizações de componentes do Windows bem como binários para funções, serviços de função e recursos. Se a estrutura de diagnóstico do Windows detectar que um componente do Windows precisa ser corrigido, o Windows usa o Windows Update para baixar o componente. Se um administrador estiver tentando instalar uma função, um serviço de função ou um recurso e algum binário estiver faltando, o Windows usa o Windows Update para baixar os binários relacionados. Para obter mais informações, consulte “Princípios básicos do Server Manager e binários” no Capítulo 2.

Configuração do Automatic Updates

Quando o Automatic Updates é gerenciado por meio da Group Policy, você pode definir a configuração de atualização como qualquer uma das opções a seguir:

- **Auto Download And Schedule The Install** Atualizações são baixadas automaticamente e instaladas de acordo com o cronograma especificado. Quando as atualizações tiverem sido baixadas, o sistema operacional notifica o usuário para que ele examine as atualizações agendadas para serem instaladas. O usuário pode instalar as atualizações no próprio momento ou esperar pelo período de instalação agendado.

- **Auto Download And Notify For Install** O sistema operacional recupera todas as atualizações assim que elas são disponibilizadas e notifica o usuário quando elas estiverem prontas para serem instaladas. Nesse momento, o usuário pode aceitar ou rejeitar as atualizações. As instalações aceitas são instaladas. As instalações rejeitadas não são instaladas, mas permanecem no sistema, de modo que podem ser instaladas mais tarde.
- **Notify For Download And Notify For Install** O sistema operacional notifica o usuário antes de recuperar qualquer atualização. Se um usuário escolher baixar as atualizações, ele ainda tem a oportunidade de aceitá-las ou rejeitá-las. As instalações aceitas são instaladas. As instalações rejeitadas não são instaladas, mas permanecem no sistema, de modo que podem ser instaladas mais tarde.
- **Allow Local Admin To Choose Setting** Permite que o administrador local configure o Automatic Updates por computador. É importante ressaltar que se você usar qualquer outra configuração, os usuários e administradores locais não poderão alterar as configurações do Automatic Updates.

A configuração do Automatic Updates na Group Policy pode ser feita seguindo estas etapas:

1. No GPMC, pressione e mantenha pressionada ou clique com o botão direito do mouse na GPO com a qual você deseja trabalhar e toque ou clique em Edit.
2. No editor de políticas, acesse Computer Configuration\Administrative Templates\Windows Components\Windows Update.
3. Dê um toque duplo ou clique duas vezes em Configure Automatic Updates. Na caixa de diálogo Properties, você pode agora habilitar ou desabilitar o gerenciamento via Group Policy do Automatic Updates. Para habilitar o gerenciamento do Automatic Updates, selecione Enabled. Para desabilitar o gerenciamento do Automatic Updates, selecione Disabled, toque ou clique em OK e não prossiga com as etapas restantes.
4. Escolha uma configuração de atualização das opções apresentadas na lista Configure Automatic Updating.
5. Se você selecionar Auto Download And Schedule The Install, poderá agendar a data e o horário da instalação por meio das listas fornecidas. Toque ou clique em OK para salvar suas configurações.

Otimização do Automatic Updates

Normalmente, a maioria das atualizações automáticas é instalada apenas quando um computador é desligado e reiniciado. Algumas atualizações automáticas podem ser instaladas automaticamente sem a interrupção de serviços do sistema ou sem a necessidade de reiniciar o sistema. Para garantir que algumas atualizações sejam instaladas automaticamente, siga estas etapas:

1. No GPMC, pressione e mantenha pressionada ou clique com o botão direito do mouse na GPO com a qual você deseja trabalhar e toque ou clique em Edit.
2. No editor de políticas, acesse Computer Configuration\Administrative Templates\Windows Components\Windows Update.

3. Dê um toque duplo ou clique duas vezes em Allow Automatic Updates Immediate Installation. Na caixa de diálogo Properties, selecione Enabled e toque ou clique em OK.

Por padrão, somente usuários com privilégios de administrador local recebem notificações sobre as atualizações. Você pode permitir que qualquer usuário conectado a um computador receba notificações de atualizações seguindo estas etapas:

1. No GPMC, pressione e mantenha pressionada ou clique com o botão direito do mouse na GPO com a qual você deseja trabalhar e toque ou clique em Edit.
2. No editor de políticas, acesse Computer Configuration\Administrative Templates\Windows Components\Windows Update.
3. Dê um toque duplo ou clique duas vezes em Allow Non-Administrators To Receive Update Notifications. Na caixa de diálogo Properties, selecione Enabled e toque ou clique em OK.

Outra política útil é a Remove Access To Use All Windows Update Features. Essa política proíbe o acesso a todos os recursos do Windows Update. Se habilitada, todos os recursos do Automatic Updates são removidos e não podem ser configurados. Isso inclui a guia Automatic Updates no utilitário System e as atualizações de driver do site Windows Update em Device Manager. Essa política está localizada em User Configuration\Administrative Templates\Windows Components\Windows Update.

Locais do serviço de atualização da intranet

Em redes com centenas ou milhares de computadores, o processo do Automatic Updates pode usar um volume de largura de banda de rede considerável. Além disso, fazer com que todos os computadores verifiquem se há atualizações e instalem atualizações via Internet não faz sentido. Em vez disso, considere a opção de usar a política Specify Intranet Microsoft Update Service Location, que informa a computadores individuais que eles devem verificar se há atualizações em um determinado servidor interno.

Esse servidor de atualização deve executar o Windows Server Update Services (WSUS), estar configurado como um servidor Web com Microsoft Internet Information Services (IIS, Serviços de Informações da Internet da Microsoft) e ser capaz de lidar com a carga de trabalho adicional, o que pode ser significativo em uma rede de grande porte durante tempos de pico de uso. Além disso, o servidor de atualização deve ter acesso à rede externa por meio da porta 80. O uso de um servidor firewall ou proxy nessa porta não deve representar problemas.

O processo de atualização também apresenta informações e estatísticas sobre a configuração para cada computador. Essas informações são necessárias para o processo de atualização operar corretamente e podem ser armazenadas em um servidor de estatísticas separado (um servidor interno com IIS) ou no próprio servidor de atualização.

Para especificar um servidor de atualização interno, siga estas etapas:

1. Após a instalação e configuração de um servidor de atualização, abra a GPO com a qual deseja trabalhar para edição. No editor de políticas, acesse Computer Configuration\Administrative Templates\Windows Components\Windows Update.
2. Dê um toque duplo ou clique duas vezes em Specify Intranet Microsoft Update Service Location. Na caixa de diálogo Properties, selecione Enabled.

3. Na caixa de texto Set The Intranet Update Service For Detecting Updates, digite a URL do servidor de atualização. Na maioria dos casos, ela tem o formato `http://servername`, como `http://CorpUpdateServer01`.
4. Digite a URL do servidor de estatísticas na caixa de texto Set The Intranet Statistics Server. Esse não precisa ser um servidor separado; você pode especificar o próprio servidor de atualização nessa caixa de texto.

OBSERVAÇÃO Se você deseja que um servidor único manipule tanto atualizações quanto estatísticas, insira a mesma URL nas duas caixas. Caso contrário, se você prefere um servidor diferente para lidar com as atualizações e outro com as estatísticas, insira a URL de cada servidor na caixa apropriada.

5. Toque ou clique em OK. Após a atualização da GPO aplicável, os sistemas com versões apropriadas do Windows se reportarão ao servidor de atualização para obter atualizações. É recomendável que você monitore com atenção os servidores de atualização e estatísticas por vários dias ou semanas para garantir que tudo está funcionando corretamente. Diretórios e arquivos serão criados nos servidores de atualização e estatísticas.

CAPÍTULO 5

Como melhorar a segurança dos computadores

- Utilização de modelos de segurança **189**
- Utilização do Security Configuration Wizard **204**

Boas práticas e configurações de segurança são essenciais para uma bem-sucedida administração de sistemas. Duas maneiras importantes de fazer configurações de segurança são utilizar modelos e políticas de segurança. Ambos os recursos gerenciam configurações de sistema que normalmente são gerenciadas por meio da Group Policy (Política de Grupo).

Utilização de modelos de segurança

Os modelos de segurança proporcionam uma forma centralizada de gerenciar configurações relacionadas à segurança para estações de trabalho e servidores. Utiliza-se modelos de segurança para aplicar conjuntos personalizados de definições de Group Policy a computadores específicos.

Essas definições de políticas geralmente afetam as seguintes políticas:

- **Account policies** Controlam a segurança de senhas, o bloqueio de conta e a segurança do Kerberos
- **Local policies** Controlam a segurança de auditoria, atribuição de direitos do usuário e outras opções de segurança
- **Event log policies** Controlam a segurança de logs de eventos
- **Restricted groups policies** Controlam a segurança da administração de associações de grupo
- **System services policies** Controlam a segurança e o modo de inicialização de serviços
- **File system policies** Controlam a segurança de arquivos e pastas no sistema de arquivos local
- **Registry policies** Controlam as permissões nas chaves de registro relacionadas à segurança

OBSERVAÇÃO Os modelos de segurança estão disponíveis em todas as instalações do Microsoft Windows Server e podem ser importadas para qualquer Group Policy Object (objeto de diretiva de grupo). Os modelos de segurança se aplicam somente à área Computer Configuration da Group Policy. Não se aplicam à área User Configuration. Em Group Policy, você encontrará configurações aplicáveis sob Computer Configuration\Windows Settings\Security Settings. Algumas configurações de segurança não estão incluídas, como as que se aplicam a redes sem fio, chaves públicas, restrições de software e segurança de IP.

O trabalho com modelos de segurança é um processo em vários passos que envolve as seguintes etapas:

1. Utilizar o snap-in Security Templates para criar um novo modelo ou selecionar um modelo existente que queira modificar.
2. Utilizar o snap-in Security Templates para fazer as alterações necessárias nas configurações dos modelos e salvá-las.
3. Utilizar o snap-in Security Configuration And Analysis para analisar as diferenças entre o modelo com o qual se está trabalhando e as configurações de segurança atuais do computador.
4. Revisar o modelo conforme necessário após examinar as diferenças entre as configurações dos modelos e as configurações atuais do computador.
5. Utilizar o snap-in Security Configuration And Analysis para aplicar e substituir as configurações de segurança existentes.

Ao começar a trabalhar com modelos de segurança, deve-se determinar se é possível utilizar um modelo existente como ponto de partida. Outros administradores podem ter criado modelos, ou sua empresa pode ter modelos de linha de base que devam ser utilizados. Você também pode criar um novo modelo para utilizar como seu ponto de partida, como mostrado na Figura 5-1.

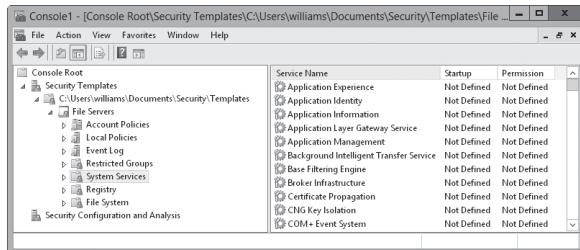


FIGURA 5-1 Visualize e crie modelos de segurança com o snap-in Security Templates.

DICA Caso selecione um modelo que queira utilizar como ponto de partida, você deve passar por cada configuração que o modelo aplique e avaliar como elas afetarão seu ambiente. Se uma configuração não fizer sentido, modifique-a apropriadamente ou a exclua.

O snap-in Security Templates não deve ser utilizado para aplicar modelos. Utilize o snap-in Security Configuration And Analysis para aplicá-los. Também pode-se utilizar o snap-in Security Configuration And Analysis para comparar as configurações em um modelo com as configurações atuais de um computador. Os resultados da análise destacam áreas em que as configurações atuais não correspondem às do modelo. Isso poderá ser útil para determinar se as configurações de segurança mudaram no decorrer do tempo.

Utilização dos snap-ins Security Templates e Security Configuration And Analysis

Pode-se abrir os snap-ins de segurança seguindo estas etapas:

1. Inicie o Microsoft Management Console (MMC). Uma maneira de fazê-lo é pressionando a tecla Windows, digitando **mmc.exe** e pressionando Enter.
2. No Microsoft Management Console, toque ou clique em File e em Add/Remove Snap-In.
3. Na caixa de diálogo Add Or Remove Snap-Ins, toque ou clique em Security Templates e em Add.
4. Toque ou clique em Security Configuration And Analysis e em Add. Toque ou clique em OK.

Por padrão, o snap-in Security Templates procura modelos de segurança na pasta %SystemDrive%\Users\%UserName%\Documents\Security\Templates. Pode-se adicionar outros caminhos de pesquisa para modelos seguindo estas etapas:

1. Com o snap-in Security Templates selecionado no MMC, escolha New Template Search Path no menu Action.
 2. Na caixa de diálogo Browse For Folder, selecione a localização do modelo a adicionar, como %SystemRoot%\Security\Templates\Policies. Toque ou clique em OK.
- Agora que localizou o caminho de pesquisa do modelo com o qual quer trabalhar, pode selecionar um modelo e expandir as opções relacionadas para examinar as suas configurações.

Você pode criar um modelo seguindo estas etapas:

1. No snap-in Security Templates, pressione e segure ou clique com o botão direito do mouse no caminho de pesquisa em que o modelo deve ser criado e toque ou clique em New Template.
2. Digite um nome e uma descrição para o modelo nas caixas de texto fornecidas.
3. Toque ou clique em OK para criá-lo. O modelo não terá configurações prévias, portanto, é preciso modificá-las cuidadosamente antes dele estar pronto para o uso.
4. Após modificar o modelo, salve as alterações pressionando e segurando ou clicando com o botão direito do mouse no modelo no snap-in Security Templates e selecionando Save. Como opção, pode-se selecionar Save As para atribuir um nome diferente ao modelo modificado.

Como examinar e alterar configurações do modelo

As seções a seguir abordam como trabalhar com configurações de modelos. Como você aprenderá, se gerencia cada tipo de configuração de modelo de uma forma ligeiramente diferente.

Como alterar configurações de políticas locais, de conta e de log de eventos

As configurações de políticas de conta controlam a segurança de senhas, o bloqueio de conta e a segurança do Kerberos. As configurações de políticas locais controlam a

segurança de auditoria, atribuição de direitos do usuário e outras opções de segurança. As configurações de diretivas de log de eventos controlam o log de eventos. Para informações detalhadas sobre configurações de políticas de conta e políticas locais, consulte o Capítulo 8, "Como criar contas de usuário e de grupo". Para informações detalhadas sobre a configuração de log de eventos, consulte o Capítulo 3, "Monitoramento de processos, serviços e eventos".

Com políticas de conta, locais e de log de eventos, pode-se alterar configurações de modelos seguindo estas etapas:

1. No snap-in Security Templates, expanda o nó Account Policies ou Local Policies, conforme necessário, e selecione um subnó relacionado, como Password Policy ou Account Lockout Policy.
2. No painel direito, as configurações de políticas são listadas em ordem alfabética. O valor na coluna Computer Setting mostra a configuração atual. Se o modelo alterar a configuração a fim de que não esteja mais definida, o valor será listado como Not Defined.
3. Toque ou clique duas vezes em uma configuração para exibir sua caixa de diálogo Properties, mostrada na Figura 5-2. Para determinar a finalidade de uma configuração, toque ou clique na guia Explain. Para definir e aplicar a configuração da política, marque a caixa de seleção Define This Policy Setting In The Template. Para limpar essa política e não aplicá-la, desmarque essa caixa de seleção.

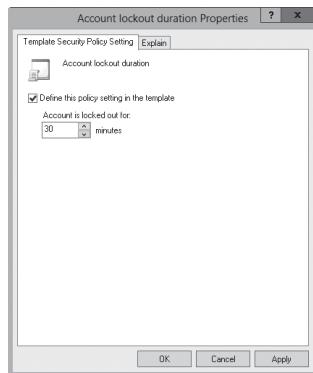


FIGURA 5-2 Altere as configurações de modelo para políticas de conta e locais.

4. Se habilitar a configuração da política, especifique como ela deverá ser utilizada configurando qualquer opção adicional.
5. Toque ou clique em OK para salvar suas alterações. Talvez você veja a caixa de diálogo Suggested Value Changes, mostrada na Figura 5-3. Essa caixa de diálogo informa sobre outros valores que podem ser modificados usando valores sugeridos baseados em sua alteração na configuração. Por exemplo, quando se altera a configuração Account Lockout Threshold, o Windows pode também alterar as configurações Account Lockout Duration e Reset Account Lockout Counter After, como mostrado na figura.

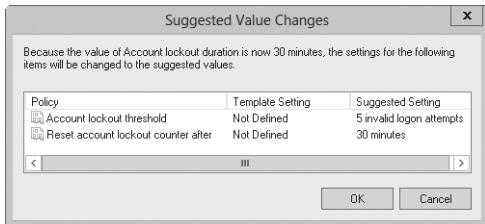


FIGURA 5-3 Examine as alterações sugeridas dos valores.

Configuração de grupos restritos

As configurações de políticas de grupos restritos controlam a lista de membros de grupos, bem como os grupos aos quais o grupo configurado pertence. Você pode restringir um grupo seguindo estas etapas:

1. No snap-in Security Templates, selecione o nó Restricted Groups. No painel direito, qualquer grupo atualmente restrito é listado por nome. Os membros do grupo também são listados, assim como os grupos dos quais o grupo restrito é membro.
2. Você pode adicionar um grupo restrito pressionando e segurando ou clicando com o botão direito do mouse no nó Restricted Groups no painel esquerdo e tocando ou clicando em Add Group. Na caixa de diálogo Add Group, toque ou clique em Browse.
3. Na caixa de diálogo Select Groups, digite o nome de um grupo que queira restringir e toque ou clique em Check Names. Se várias correspondências forem encontradas, selecione a conta que queira utilizar e toque ou clique em OK. Se não for encontrada qualquer correspondência, atualize o nome digitado e faça uma nova pesquisa. Repita esta etapa conforme necessário e toque ou clique em OK.
4. Na caixa de diálogo Properties, mostrada na Figura 5-4, pode-se utilizar a opção Add Members para adicionar membros ao grupo. Toque ou clique em Add Members e especifique os membros do grupo. Se o grupo não deve ter qualquer membro, remova todos eles tocando ou clicando em Remove. Qualquer membro que não esteja especificado na configuração de política para o grupo restrito será removido quando o modelo de segurança for aplicado.
5. Na caixa de diálogo Properties, toque ou clique em Add Groups para especificar os grupos aos quais esse grupo pertence. Se você especificar a associação nos grupos, os grupos aos quais esse grupo pertence serão listados exatamente conforme os tenha aplicado (desde que os grupos sejam válidos no grupo de trabalho ou domínio aplicável). Se não especificar a associação nos grupos, os grupos aos quais esse grupo pertence não serão modificados quando o modelo for aplicado.
6. Toque ou clique em OK para salvar suas configurações.

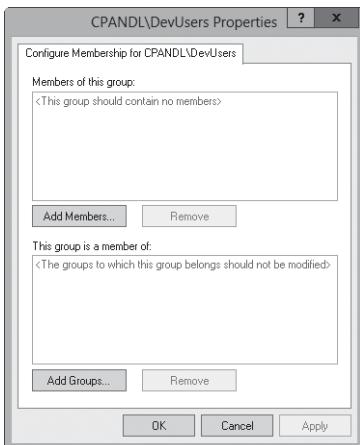


FIGURA 5-4 Adicione os membros do grupo restrito.

Você pode remover uma restrição a um grupo seguindo estas etapas:

1. No snap-in Security Templates, selecione o nó Restricted Groups. No painel direito, qualquer grupo atualmente restrito é listado por nome. Os membros do grupo são listados juntamente com os grupos dos quais o grupo restrito é membro.
2. Pressione e segure ou clique com o botão direito do mouse no grupo que não deve ser restrinido e toque ou clique em Delete. Quando for solicitada a confirmação da ação, toque ou clique em Yes.

Como habilitar, desabilitar e configurar serviços do sistema

As configurações de política para serviços do sistema controlam a segurança geral e o modo de inicialização para serviços locais. Você pode habilitar, desabilitar e configurar serviços do sistema seguindo estas etapas:

1. No snap-in Security Templates, selecione o nó System Services. No painel direito, todos os serviços instalados atualmente no computador em que está trabalhando são listados por nome, configuração de inicialização e configuração de permissões. Lembre-se do seguinte ao trabalhar com serviços do sistema:
 - Se o modelo não alterar a configuração de inicialização do serviço, o valor para a coluna Startup será listado como Not Defined. Caso contrário, a configuração de inicialização será listada com um dos seguintes valores: Automatic, Manual ou Disabled.
 - Se o modelo não alterar a configuração de segurança do serviço, o valor para a coluna Permission será listado como Not Defined. Caso contrário, a configuração de segurança será listada como Configured.

2. Toque ou clique duas vezes na entrada de um serviço do sistema para exibir sua caixa de diálogo Properties, mostrada na Figura 5-5. Para definir e aplicar a configuração da política, marque a caixa de seleção Define This Policy Setting In The Template. Para limpar essa política e não aplicá-la, desmarque essa caixa de seleção.

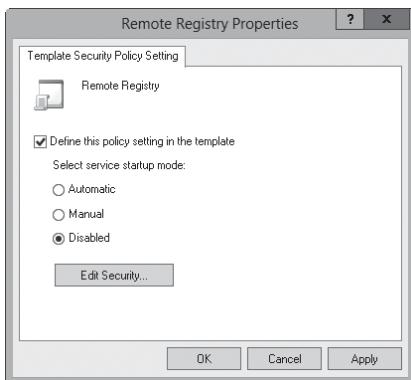


FIGURA 5-5 Altere as configurações do modelo para serviços do sistema.

3. Se habilitar a configuração da política, especifique o modo de inicialização selecionando Automatic, Manual ou Disabled. Lembre-se do seguinte:
- Automatic garante que o serviço inicie automaticamente quando o sistema operacional for inicializado. Escolha esta configuração para serviços essenciais que sejam sabidamente seguros e tenha certeza de que serão executados se estiverem instalados no computador ao qual o modelo está sendo aplicado.
 - Manual impede que o serviço inicie automaticamente e permite que só seja iniciado manualmente, seja por um usuário, aplicativo ou outro serviço. Escolha esta configuração quando quiser restringir serviços desnecessários ou não utilizados, ou quando quiser restringir serviços que saiba que não são totalmente seguros.
 - Disabled impede que o serviço inicie automática ou manualmente. Escolha esta configuração somente para serviços desnecessários ou não utilizados cuja execução queira impedir.
4. Se souber a configuração de segurança que o serviço deve utilizar, toque ou clique em Edit Security e defina as permissões do serviço na caixa de diálogo Security For. Pode-se definir permissões para que usuários e grupos específicos iniciem, interrompam e pausem o serviço no computador.
5. Toque ou clique em OK.

Como fazer configurações de segurança para os caminhos de registro e sistema de arquivos

As configurações de política para o sistema de arquivos controlam a segurança de arquivos e pastas no sistema de arquivos local. As configurações de política para o registro controlam os valores de chaves de registro relacionadas à segurança. Você pode visualizar ou alterar as configurações de segurança para os caminhos de registro e sistema de arquivos definidos atualmente seguindo estas etapas:

1. No snap-in Security Templates, selecione o nó Registry ou File System, dependendo do tipo de arquivo com o qual queira trabalhar. No painel direito, todos os caminhos protegidos atualmente são listados.
2. Toque ou clique duas vezes em um caminho de registro ou arquivo para visualizar suas configurações atuais, como mostrado na Figura 5-6.

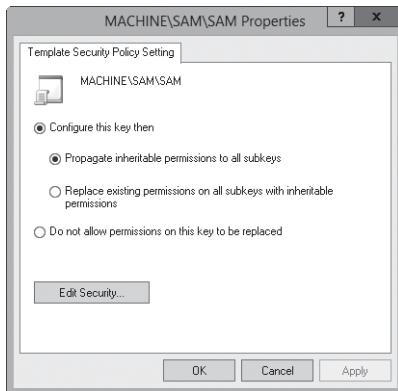


FIGURA 5-6 Altere as configurações de modelo para arquivos, pastas e chaves.

3. Para garantir que as permissões no caminho ou na chave não sejam substituídas, selecione Do Not Allow Permissions On This Key To Be Replaced e toque ou clique em OK. Ignore as etapas restantes desse procedimento.
4. Para configurar o caminho ou a chave e substituir permissões, selecione Configure This Key Then e escolha uma das seguintes opções:
 - **Propagate Inheritable Permissions To All Subkeys** Escolha esta opção para aplicar todas as permissões herdáveis a esse caminho de registro ou arquivo e a todos os caminhos de registro e arquivo abaixo dele. As permissões existentes serão substituídas somente se entrarem em conflito com uma permissão de segurança definida para esse caminho.
 - **Replace Existing Permissions On All Subkeys With Inheritable Permissions** Escolha esta opção para substituir todas as permissões existentes nesse caminho de registro ou arquivo e em todos os caminhos de registro e arquivo abaixo dele. Qualquer permissão existente será removida e apenas as permissões atuais permanecerão.

5. Toque ou clique em Edit Security. Na caixa de diálogo Security For, configure as permissões de segurança para usuários e grupos. Você tem as mesmas opções para permissões, auditoria e posse que para arquivos e pastas utilizados com NTFS. Consulte o Capítulo 12, “Compartilhamento de dados, segurança e auditoria”, para detalhes sobre permissões, auditoria e posse.
6. Toque ou clique em OK duas vezes para salvar as configurações.

Pode-se definir as configurações de segurança para caminhos de registro seguindo estas etapas:

1. No snap-in Security Templates, selecione e pressione e segure ou clique com o botão direito do mouse no nó Registro e toque ou clique em Add Key. A caixa de diálogo Select Registry Key, mostrada na Figura 5-7, será aberta.

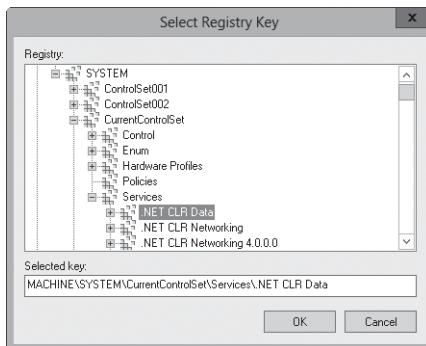


FIGURA 5-7 Selecione o caminho ou valor de registro a proteger.

2. Na caixa de diálogo Select Registry, selecione o caminho ou valor de registro com o qual quer trabalhar e toque ou clique em OK. As entradas sob CLASSES_ROOT são para HKEY_CLASSES_ROOT. As entradas sob MACHINE são para HKEY_LOCAL_MACHINE. As entradas sob USERS são para HKEY_USERS.
3. Na caixa de diálogo Database Security For, configure as permissões de segurança para usuários e grupos. Você tem as mesmas opções para permissões, auditoria e posse que para arquivos e pastas utilizados com NTFS. Consulte o Capítulo 12 para detalhes sobre permissões, auditoria e posse.
4. Toque ou clique em OK. A caixa de diálogo Add Object será exibida. Para garantir que as permissões no caminho ou na chave não sejam substituídas, selecione Do Not Allow Permissions On This Key To Be Replaced e toque ou clique em OK. Ignore as etapas restantes desse procedimento.
5. Para configurar o caminho ou a chave e substituir permissões, selecione Configure This Key Then e faça uma das seguintes opções:
 - Escolha Propagate Inheritable Permissions To All Subkeys para aplicar todas as permissões herdáveis a esse caminho de registro e todos os caminhos de registro abaixo dele. As permissões existentes serão substituídas somente se

entrarem em conflito com uma permissão de segurança definida para esse caminho.

- Escolha Replace Existing Permissions On All Subkeys With Inheritable Permissions para substituir todas as permissões existentes nesse caminho de registro e em todos os caminhos de registro abaixo dele. Qualquer permissão existente será removida e apenas as permissões atuais permanecerão.

6. Toque ou clique em OK.

Você pode definir as configurações de segurança para caminhos de arquivos seguindo estas etapas:

1. No snap-in Security Templates, selecione e pressione e segure ou clique com o botão direito do mouse no nó File System e toque ou clique em Add File. A caixa de diálogo Add A File Or Folder, mostrada na Figura 5-8, será exibida.

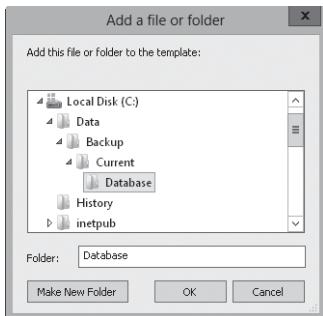


FIGURA 5-8 Selecione o caminho de arquivo ou de pasta a proteger.

2. Na caixa de diálogo Add A File Or Folder, selecione o caminho do arquivo ou pasta com o qual quer trabalhar e toque ou clique em OK.
3. Na caixa de diálogo Database Security For, configure as permissões de segurança para usuários e grupos. Você tem as mesmas opções para permissões, auditoria e posse que para arquivos e pastas utilizados com NTFS. Consulte o Capítulo 12 para detalhes sobre permissões, auditoria e posse.
4. Toque ou clique em OK. A caixa de diálogo Add Object será exibida. Para garantir que as permissões no caminho não sejam substituídas, selecione Do Not Allow Permissions On This File Or Folder To Be Replaced e toque ou clique em OK. Ignore as etapas restantes desse procedimento.
5. Para configurar o caminho e substituir permissões, selecione Configure This Path Then e faça uma das seguintes opções:
 - Escolha Propagate Inheritable Permissions To All Subfolders para aplicar todas as permissões herdáveis a esse caminho de arquivo e todos os caminhos de arquivo abaixo dele. As permissões existentes serão substituídas somente se entrarem em conflito com uma permissão de segurança definida para esse caminho.

- Escolha Replace Existing Permissions On All Subfolders With Inheritable Permissions para substituir todas as permissões existentes nesse caminho de arquivo e em todos os caminhos de arquivo abaixo dele. Qualquer permissão existente será removida e apenas as permissões atuais permanecerão.

6. Toque ou clique em OK.

Análise, exame e aplicação de modelos de segurança

Como afirmado anteriormente, utiliza-se o snap-in Security Configuration And Analysis para aplicar modelos e comparar as configurações de um modelo com as configurações atuais de um computador. A aplicação de um modelo assegura que o computador esteja de acordo com uma configuração específica de segurança. A comparação de configurações pode ajudar a identificar qualquer discrepância entre o que está atualmente implementado e o que está definido em um modelo de segurança. Isso também pode ser útil para determinar se as configurações de segurança mudaram no decorrer do tempo.

MUNDO REAL A principal desvantagem de utilizar o snap-in Security Configuration And Analysis é não se poder configurar vários computadores de uma vez só. Você pode configurar a segurança somente no computador em que esteja executando o snap-in. Se quiser utilizar essa ferramenta para implantar configurações de segurança, é preciso fazer logon e executá-la em cada computador. Embora essa técnica funcione para computadores autônomos, não é a melhor abordagem em um domínio. Na configuração de um domínio, você desejará importar as configurações do modelo de segurança para um objeto de diretiva de grupo (GPO) e implantar a configuração de segurança em vários computadores. Para mais informações, consulte “Implantação de modelos de segurança em vários computadores” posteriormente neste capítulo.

O snap-in Security Configuration And Analysis utiliza um banco de dados de trabalho para armazenar configurações de segurança do modelo e as aplica a partir dele. Para análises e comparações, as configurações do modelo são listadas como as configurações efetivas do banco de dados e as configurações atuais do computador são listadas como as configurações efetivas do computador. Lembre-se de que, se estiver editando ativamente um modelo no snap-in Security Templates, é preciso salvá-lo a fim de que as alterações possam ser analisadas e utilizadas.

Após criar um modelo ou determinar que quer utilizar um modelo existente, pode-se analisar e configurar o modelo seguindo estas etapas:

1. Abra o snap-in Security Configuration And Analysis.
2. Pressione e segure ou clique com o botão direito do mouse no nó Security Configuration And Analysis e toque ou clique em Open Database. A caixa de diálogo Open Database será exibida.
3. Por padrão, o caminho de pesquisa da caixa de diálogo Open Database está definido para %SystemDrive%\Users\%UserName%\Documents\Security\Database. Conforme necessário, selecione as opções na caixa de diálogo Open Database para navegar até uma nova localização de salvamento. Na caixa de texto File Name, digite um nome descritivo para o banco de dados, como **Current Config Comparison** e toque ou clique em Open. O banco de dados de segurança será criado no formato Security Database Files com a extensão de arquivo .sdb.

4. A caixa de diálogo Import Template será exibida com o caminho de pesquisa padrão definido para %SystemDrive%\Users%\UserName%\Documents\Security\Templates. Conforme necessário, selecione as opções na caixa de diálogo Import Template para navegar até uma nova localização do modelo. Selecione o modelo de segurança que queira utilizar e toque ou clique em Open. Os arquivos de modelos de segurança terminam com a extensão de arquivo .inf.
5. Pressione e segure ou clique com o botão direito do mouse no nó Security Configuration And Analysis e toque ou clique em Analyze Computer Now. Quando for solicitado que defina o caminho do log de erros, digite um novo caminho ou toque ou clique em OK para utilizar o caminho padrão.
6. Aguarde que o snap-in conclua a análise do modelo. Se um erro ocorrer durante a análise, você pode visualizar o log de erros pressionando e segurando ou clicando com o botão direito do mouse no nó Security Configuration And Analysis e escolhendo View Log File.

Ao trabalhar com o snap-in Security Configuration And Analysis, pode-se examinar as diferenças entre as configurações do modelo e as configurações atuais do computador. Como mostra a Figura 5-9, as configurações do modelo armazenadas no banco de dados de análise são listadas na coluna Database Setting e as configurações atuais do computador são listadas na coluna Computer Setting. Se uma configuração não tiver sido analisada, será listada como Not Defined.

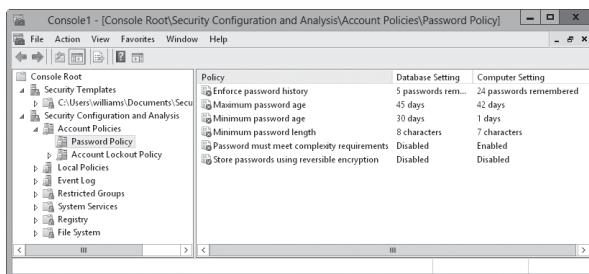


FIGURA 5-9 Examine as diferenças entre as configurações do modelo e as configurações atuais do computador.

É possível fazer alterações em uma configuração armazenada no banco de dados seguindo estas etapas:

1. No snap-in Security Configuration And Analysis, toque ou clique duas vezes na configuração com a qual queira trabalhar.
2. Na caixa de diálogo Properties, mostrada na Figura 5-10, observe a configuração atual do computador. Se as informações sobre a finalidade dessa configuração estiverem disponíveis, é possível visualizá-las tocando ou clicando na guia Explain.

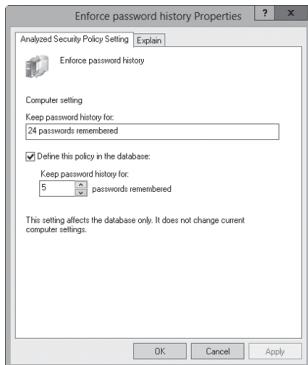


FIGURA 5-10 Altere uma configuração de política no banco de dados antes de aplicar o modelo.

3. Para definir e aplicar a configuração da política, marque a caixa de seleção Define This Policy In The Database. Para limpar essa política e não aplicá-la, desmarque essa caixa de seleção.
4. Se habilitar a configuração da política, especifique como ela deverá ser utilizada configurando qualquer opção adicional.
5. Repita esse processo conforme necessário. Para salvar suas alterações do banco de dados no modelo, pressione e segure ou clique com o botão direito do mouse no nó Security Configuration And Analysis e toque ou clique em Save.

Você também pode utilizar o utilitário de linha de comando Secedit para analisar, examinar e aplicar modelos de segurança. A técnica básica é a seguinte:

1. Abra um prompt de comando com privilégio elevado de administrador.
2. Utilize Secedit /Import para importar um modelo de segurança para um banco de dados de trabalho.
3. Utilize Secedit /Analyze para comparar as configurações do modelo com as configurações atuais do computador.
4. Utilize Secedit /Configure para aplicar as configurações do modelo.

Trabalhando com o assistente gráfico ou com o utilitário de linha de comando, talvez queira criar um modelo para reversão antes de aplicar qualquer configuração. Um modelo para reversão é um modelo inverso que permite remover a maioria das configurações aplicadas com um modelo. As únicas configurações que não podem ser removidas são aquelas para listas de controle de acesso em caminhos do sistema de arquivos e do registro.

Em um prompt de comandos com privilégios elevados de administrador, você pode criar um modelo para reversão usando o utilitário de linha de comando Secedit. Digite o seguinte:

```
secedit /generaterollback /db DatabaseName /cfg TemplateName
/rbk RollBackName /log LogName
```

em que *DatabaseName* é o nome de um novo banco de dados que será utilizado para realizar a reversão, *TemplateName* é o nome de um modelo de segurança existente

para o qual se está criando um modelo para reversão, *RollBackName* define o nome de um novo modelo de segurança em que as configurações para reversão devem ser armazenadas e *LogName* define o nome de um arquivo opcional para monitorar o status do processo de reversão.

No exemplo a seguir, você criaria um modelo para reversão para o modelo "File Servers":

```
secedit /generaterollback /db rollback.db /cfg "file servers.inf"
/rbk fs-orig.inf /log rollback.log
```

Quando estiver pronto para aplicar o modelo, pressione e segure ou clique com o botão direito do mouse no nó Security Configuration And Analysis e toque ou clique em Configure Computer Now. Quando for solicitado para definir o caminho do log de erros, toque ou clique em OK, pois o caminho padrão deve bastar. Para visualizar o log de erros da configuração, pressione e segure ou clique com o botão direito do mouse no nó Security Configuration And Analysis e toque ou clique em View Log File. Observe qualquer problema e aja conforme necessário.

Se tiver criado um modelo para reversão antes de aplicar um modelo de segurança, poderá restaurar as configurações de segurança do computador para seu estado anterior. Para aplicar um modelo de reversão, siga estas etapas:

1. No snap-in Security Configuration And Analysis, pressione e segure ou clique com o botão direito do mouse no nó Security Configuration And Analysis e toque ou clique em Import Template.
2. Na caixa de diálogo Import Template, selecione o modelo para reversão.
3. Marque a caixa de seleção Clear This Database Before Importing e toque ou clique em Open.
4. Pressione e segure ou clique com o botão direito do mouse no nó Security Configuration And Analysis e toque ou clique em Configure Computer Now. Toque ou clique em OK.

As únicas configurações que não podem ser restauradas são para listas de controle de acesso em caminhos do sistema de arquivos e do registro. Uma vez que as permissões nos caminhos de sistema de arquivos e registro tenham sido aplicadas, você não pode reverter o processo automaticamente e, ao invés disso, deve reverter manualmente as alterações, uma de cada vez.

Implantação de modelos de segurança em vários computadores

Em vez de aplicar modelos de segurança em um computador de cada vez, você pode implantar suas configurações de segurança em vários computadores por meio da Group Policy. Para fazê-lo, é preciso importar o modelo de segurança para uma GPO processada pelos computadores aos quais as configurações do modelo devam ser aplicadas. Então, quando a política for atualizada, todos os computadores dentro do escopo da GPO receberão a configuração de segurança.

Os modelos de segurança se aplicam somente à área Computer Configuration da Group Policy. Antes de implantar configurações de segurança dessa forma, você deve observar atentamente a estrutura de domínio e de organizational unit (OU, unidade organizacional) de sua empresa e fazer alterações conforme necessário para garan-

tir que a configuração de segurança seja aplicada somente a padrões específicos de computadores. Essencialmente, isso significa que é preciso criar OUs para os diferentes tipos de computadores em sua empresa e, a seguir, mover as contas de computadores deles para as OUs apropriadas. Depois, é preciso criar e vincular uma GPO para cada uma das OUs dos computadores. Por exemplo, você poderia criar as seguintes OUs de computadores:

- **Domain Controllers** Uma OU para os controladores de domínio de sua empresa. Essa OU é criada automaticamente em um domínio.
- **High-Security Member Servers** Uma OU para servidores que exijam configurações de segurança mais altas que o normal.
- **Member Servers** Uma OU para servidores que exijam configurações de segurança de servidor padrão.
- **High-Security User Workstations** Uma OU para estações de trabalho que exijam configurações de segurança mais altas que o normal.
- **User Workstations** Uma OU para estações de trabalho que exijam configurações de segurança de estação de trabalho padrão.
- **Remote Access Computers** Uma OU para computadores que accessem a rede da empresa remotamente.
- **Restricted Computers** Uma OU para computadores que exijam configurações de segurança restritivas, como computadores utilizados em laboratórios ou quiosques.

MUNDO REAL É preciso ser muito cuidadoso ao implantar modelos de segurança por meio de GPOs. Se não o tiver feito antes, pratique em um ambiente de teste primeiro e certifique-se de também praticar a recuperação de computadores para suas configurações de segurança originais. Se criar uma GPO e vinculá-la ao nível apropriado na estrutura do Active Directory, poderá recuperar os computadores para seu estado original removendo o vínculo com a GPO. Por isso é extremamente importante criar e vincular uma nova GPO, em vez de utilizar uma existente.

Para implantar um modelo de segurança em uma GPO do computador, siga estas etapas:

1. Após configurar um modelo de segurança e testá-lo para garantir que seja apropriado, abra a GPO anteriormente criada e vinculada ao nível apropriado da estrutura do Active Directory. No Group Policy Management Editor, abra Computer Configuration\Windows Settings\Security Settings.
2. Pressione e segure ou clique com o botão direito do mouse em Security Settings e toque ou clique em Import Policy.
3. Na caixa de diálogo Import Policy From, selecione o modelo de segurança a importar e toque ou clique em Open. Os modelos de segurança terminam com a extensão de arquivo .inf.
4. Verifique o estado das configurações de segurança para determinar se foram importadas conforme esperado e feche o editor de políticas. Repita esse processo para cada modelo de segurança e GPO de computador que tenha configurado. Na configuração padrão de Group Policy, levará de 90 a 120 minutos para que as configurações sejam aplicadas nos computadores na empresa.

Utilização do Security Configuration Wizard

O Security Configuration Wizard pode ajudá-lo a criar e aplicar uma política de segurança abrangente. Uma política de segurança é um arquivo XML que pode ser usado para configurar serviços, segurança de rede, valores de registro e políticas de auditoria. Como as políticas de segurança são baseadas em funções e recursos, geralmente é preciso criar uma política separada para cada configuração de servidor padrão. Por exemplo, se a empresa utilizar controladores de domínio, servidores de arquivos e servidores de impressão, talvez se queira criar uma política separada para cada um dos tipos de servidor. Se a empresa tiver servidores de email e servidores combinados de arquivos/impressão, bem como controladores de domínio, deverão ser criadas políticas separadas adequadas para esses tipos de servidores.

Você pode utilizar o Security Configuration Wizard para fazer o seguinte:

- Criar uma política de segurança.
- Editar uma política de segurança.
- Aplicar uma política de segurança.
- Reverter a última política de segurança aplicada.

As políticas de segurança podem incorporar um ou mais modelos de segurança. Muito do que se pode fazer com modelos de segurança pode ser aplicado a uma política de segurança para o computador conectado no momento utilizando o Security Configuration Wizard. Por meio da Group Policy, você também pode aplicar uma política de segurança a vários computadores. Por padrão, as políticas de segurança criadas com o Security Configuration Wizard são salvas na pasta %SystemRoot%\security\msscw\Policies.

O equivalente de linha de comando para o assistente gráfico é o utilitário Scwcmd (Scwcmd.exe). Em um prompt de comando com privilégio elevado de administrador, pode-se utilizar Scwcmd Analyze para determinar onde um computador está em conformidade com uma política de segurança e Scwcmd Configure para aplicar uma política de segurança.

Criação de políticas de segurança

O Security Configuration Wizard permite configurar políticas apenas para funções e recursos que estejam instalados no computador em que o assistente for executado. O processo exato passo a passo para criar políticas de segurança depende das funções e recursos do servidor disponíveis no computador conectado no momento. Isso dito, as seções de configuração gerais apresentadas no assistente são as mesmas, não importando a configuração do computador.

O Security Configuration Wizard tem as seguintes seções de configuração:

- **Role-Based Service Configuration** Configura o modo de inicialização dos serviços do sistema com base em funções, recursos e opções instalados em um servidor e os serviços que ele exige.
- **Network Security** Configura as regras de segurança de entrada e de saída para o Windows Firewall With Advanced Security (Firewall do Windows com Segurança Avançada) com base nas funções e opções instaladas.
- **Registry Settings** Configura os protocolos utilizados para comunicação com outros computadores com base nas funções e opções instaladas.

- **Audit Policy** Configura a auditoria no servidor selecionado com base em suas preferências.
- **Save Security Policy** Permite salvar e visualizar a política de segurança. Você também pode incluir um ou mais modelos de segurança.

Lembrando-se disso, você pode criar uma política de segurança seguindo estas etapas:

1. Inicie o Security Configuration Wizard. No Server Manager, faça-o tocando ou clicando em Tools, Security Configuration Wizard. Na página Welcome do assistente, toque ou clique em Next.
2. Na página Configuration Action, examine as ações que podem ser realizadas. (Consulte a Figura 5-11.) A opção Create A New Security Policy está selecionada por padrão. Toque ou clique em Next.



FIGURA 5-11 Examine as ações que podem ser realizadas.

3. Na página Select Server, selecione o servidor que quer utilizar como uma linha de base para essa política de segurança. O servidor de linha de base é aquele em que as funções, os recursos e as opções com os quais se quer trabalhar estão instalados. O computador conectado no momento está selecionado por padrão. Para escolher um computador diferente, toque ou clique em Browse. Na caixa de diálogo Select Computer, digite o nome do computador e toque ou clique em Check Names. Selecione a conta de computador que queira utilizar e toque ou clique em OK.
4. Ao tocar ou clicar em Next, o assistente irá coletar a configuração da segurança e armazená-la em um banco de dados de configurações de segurança. Na página Processing Security Configuration Database, toque ou clique em View Configuration Database para visualizar as configurações no banco de dados. Depois de examinar as configurações no SCW Viewer, volte ao assistente e toque ou clique em Next para prosseguir.

5. Cada seção de configuração tem uma página introdutória. A primeira página introdutória é a de Role-Based Service Configuration. Toque ou clique em Next.
6. A página Select Server Roles, mostrada na Figura 5-12, lista as funções de servidor instaladas. Selecione cada função que deva ser habilitada. Desmarque a caixa de seleção de cada função que deva ser desabilitada. A seleção de uma função habilita serviços, portas de entrada e configurações exigidas por essa função. Desmarcar uma função desabilita os serviços, as portas de entrada e as configurações exigidas para ela, desde que não sejam necessárias para uma função habilitada. Toque ou clique em Next.



FIGURA 5-12 Selecione as funções de servidor a habilitar.

7. Na página Select Client Features, você verá os recursos de cliente instalados utilizados para habilitar serviços. Selecione cada recurso que deva ser habilitado. Desmarque cada recurso que deva ser desabilitado. A seleção de um recurso habilita serviços necessários para ele. Desmarcar um recurso desabilita os serviços exigidos para ele, desde que não sejam necessários para um recurso habilitado. Toque ou clique em Next.
8. Na página Select Administration And Other Options, você verá as opções instaladas utilizadas para habilitar serviços e portas abertas. Selecione cada opção que deva ser habilitada. Desmarque cada opção que deva ser desabilitada. A seleção de uma opção habilita serviços necessários para ela. Desmarcar uma opção desabilita os serviços exigidos para ela, desde que não sejam necessários para uma opção habilitada. Toque ou clique em Next.
9. Na página Select Additional Services, você verá uma lista de serviços adicionais encontrados no servidor selecionado durante o processamento do banco de dados de configurações de segurança. Selecione cada serviço que deva ser habilitado. Desmarque cada serviço que deva ser desabilitado. A seleção de um serviço habilita serviços necessários para ele. Desmarcar um serviço desabilita os serviços

exigidos para ele, desde que não sejam necessários para um serviço habilitado. Toque ou clique em Next.

10. Na página Handling Unspecified Services, indique como se deve lidar com serviços não especificados. Os serviços não especificados são aqueles que não estão instalados no servidor selecionado e não estão listados no banco de dados de configurações de segurança. Por padrão, o modo de inicialização de serviços não especificados não será alterado. Para desabilitar serviços não especificados, selecione Disable The Service. Toque ou clique em Next.
11. Na página Confirm Service Changes, examine os serviços que serão alterados no servidor selecionado se a política de segurança for aplicada. Observe o modo de inicialização atual e o modo de inicialização que será aplicado pela política. Toque ou clique em Next.
12. Na página introdutória de Network Security, toque ou clique em Next. Na página Network Security Rules, você verá uma lista de regras de firewall necessárias para as funções, os recursos e as opções selecionados anteriormente. Você pode adicionar, editar ou remover regras de entrada e de saída utilizando as opções fornecidas. Toque ou clique em Next quando estiver pronto para continuar.
13. Na página introdutória de Registry Settings, toque ou clique em Next. Na página Require SMB Security Signatures, examine as opções de assinatura de segurança de server message block (protocolo SMB). Por padrão, os requisitos de sistema operacional e assinatura digital mínimos são utilizados e não se deseja alterar essas configurações. Toque ou clique em Next.
14. Para controladores de domínio e servidores com LDAP, na página Require LDAP Signing, pode-se definir requisitos mínimos do sistema operacional para todos os computadores com serviço de diretório habilitado que acessem o Active Directory.
15. Na página Outbound Authentication Methods, escolha os métodos que o servidor selecionado utiliza para autenticação com computadores remotos. Suas escolhas definem o nível de autenticação do LAN Manager de saída que será utilizado. Se o computador se comunicar somente com computadores de domínio, selecione Domain Accounts, mas não selecione as outras opções. Isso irá garantir que o computador utilize o nível mais alto de autenticação do LAN Manager de saída. Se o computador se comunicar com computadores de domínio e de grupo de trabalho, selecione Domain Accounts e Local Accounts On The Remote Computers. Na maioria dos casos, não se desejará selecionar a opção de compartilhamento de arquivos, pois ela resultará em um nível de autenticação substancialmente diminuído. Toque ou clique em Next.
16. Os métodos de autenticação de saída escolhidos determinam quais páginas adicionais relacionadas a Registry Settings serão exibidas. Lembre-se:
 - Se não selecionar qualquer método de autenticação de saída, o nível de autenticação do LAN Manager de saída será definido como Send NTLMv2 Response Only e uma página adicional será exibida para permitir que se defina o nível de autenticação de entrada. Na página Inbound Authentication Using Domain Accounts, escolha os tipos de computadores de que o servidor selecionado aceitará conexões. Suas escolhas definem o nível de autenticação do LAN Manager de entrada que será utilizado. Se o computador se comunicar somente com computadores Windows XP Professional ou posteriores, desmarque am-

bas as opções. Isso irá garantir que o computador utilize o nível mais alto de autenticação do LAN Manager de entrada. Se o computador se comunicar com PCs mais antigos, aceite as seleções padrão. Toque ou clique em Next.

- Se selecionar contas de domínio, contas locais ou ambas, terá páginas adicionais relacionadas que permitem definir o nível de autenticação do LAN Manager utilizado ao fazer conexões de saída. Também será possível especificar se você quer sincronizar os relógios com o relógio desse servidor. A autenticação de entrada está definida como Accept All.
 - Se permitir senhas de compartilhamento de arquivos para versões anteriores do Windows, o nível de autenticação do LAN Manager de saída será definido como Send LM & NTLM Only e o nível de autenticação de entrada será definido como Accept All. Após isso, ao tocar ou clicar em Next, a página Registry Settings Summary será exibida.
17. Na página Registry Settings Summary, examine os valores que serão alterados no servidor selecionado se a política de segurança for aplicada. Observe o valor atual e o valor que será aplicado pela política. Toque ou clique em Next.
18. Na página introdutória de Audit Policy, toque ou clique em Next. Na página System Audit Policy, configure o nível de auditoria desejado. Para desabilitar a auditoria, selecione Do Not Audit. Para habilitar a auditoria para eventos bem-sucedidos, selecione Audit Successful Activities. Para habilitar a auditoria para todos os eventos, selecione Audit Successful And Unsuccessful Activities. Toque ou clique em Next.
19. Na página Audit Policy Summary, examine as configurações que serão alteradas no servidor selecionado se a política de segurança for aplicada. Observe a configuração atual e a configuração que será aplicada pela política. Toque ou clique em Next.
20. Na página introdutória de Save Security Policy, toque ou clique em Next. Na página Security Policy File Name, pode-se configurar opções para salvar a política de segurança e adicionar um ou mais modelos de segurança à política. Para visualizar a política de segurança no SCW Viewer, toque ou clique em View Security Policy. Quando tiver terminado de visualizá-la, retorne ao assistente.
21. Para adicionar modelos de segurança à política, toque ou clique em Include Security Templates. Na caixa de diálogo Include Security Templates, toque ou clique em Add. Na caixa de diálogo Open, selecione um modelo de segurança para incluir na política de segurança. Se adicionar mais de um modelo de segurança, poderá priorizá-los, em caso de algum conflito de configuração de segurança ocorrer entre eles. As configurações de modelos mais no topo da lista têm prioridade. Selecione um modelo e toque ou clique nos botões Up e Down para priorizá-los. Toque ou clique em OK.
22. Por padrão, a política de segurança é salva na pasta %SystemRoot%\Security\Mscscw\Policies. Toque ou clique em Browse. Na caixa de diálogo Save As, selecione uma localização diferente para salvar a política, se necessário. Depois de digitar um nome para a política de segurança, toque ou clique em Save. O caminho de pasta selecionado ou padrão e o nome de arquivo serão listados na caixa de texto Security Policy File Name.
23. Toque ou clique em Next. Na página Apply Security Policy, você pode escolher aplicar a política agora ou depois. Toque ou clique em Next e em Finish.

Edição de políticas de segurança

Você pode utilizar o Security Configuration Wizard para editar uma política de segurança seguindo estas etapas:

1. Inicie o Security Configuration Wizard. No Server Manager, faça-o tocando ou clicando em Tools, Security Configuration Wizard. Quando o assistente for iniciado, toque ou clique em Next.
2. Na página Configuration Action, selecione Edit An Existing Security Policy e toque ou clique em Browse. Na caixa de diálogo Open, selecione a política de segurança com a qual quer trabalhar e toque ou clique em Open. As políticas de segurança terminam com a extensão .xml. Toque ou clique em Next.
3. Siga as etapas de 3 a 23 do procedimento na seção "Criação de políticas de segurança" para editar a configuração da política de segurança.

Aplicação de políticas de segurança

Você pode utilizar o Security Configuration Wizard para aplicar uma política de segurança seguindo estas etapas:

1. Inicie o Security Configuration Wizard. No Server Manager, faça-o tocando ou clicando em Tools, Security Configuration Wizard. Quando o assistente for iniciado, toque ou clique em Next.
2. Na página Configuration Action, selecione Apply An Existing Security Policy e toque ou clique em Browse. Na caixa de diálogo Open, selecione a política de segurança com a qual quer trabalhar e toque ou clique em Open. As políticas de segurança terminam com a extensão .xml. Toque ou clique em Next.
3. Na página Select Server, selecione o servidor ao qual queira aplicar a política de segurança. O computador conectado no momento está selecionado por padrão. Para escolher um computador diferente, toque ou clique em Browse. Na caixa de diálogo Select Computer, digite o nome do computador e toque ou clique em Check Names. Selecione a conta de computador que queira utilizar e toque ou clique em OK.
4. Toque ou clique em Next. Na página Apply Security Policy, toque ou clique em View Security Policy para visualizar a política de segurança no SCW Viewer. Quando tiver terminado de visualizá-la, retorne ao assistente.
5. Toque ou clique em Next para aplicar a política ao servidor selecionado. Quando o assistente terminar de aplicar a política, toque ou clique em Next e em Finish.

Reversão da última política de segurança aplicada

Você pode utilizar o Security Configuration Wizard para reverter a aplicação da última política de segurança seguindo estas etapas:

1. Inicie o Security Configuration Wizard. No Server Manager, faça-o tocando ou clicando em Tools, Security Configuration Wizard. Quando o assistente for iniciado, toque ou clique em Next.
2. Na página Configuration Action, selecione Rollback The Last Applied Security Policy e toque ou clique em Next.

3. Na página Select Server, selecione o servidor em que deseja reverter a última política de segurança aplicada. O computador conectado no momento está selecionado por padrão. Para escolher um computador diferente, toque ou clique em Browse. Na caixa de diálogo Select Computer, digite o nome do computador e toque ou clique em Check Names. Selecione a conta de computador que queira utilizar e toque ou clique em OK.
4. Toque ou clique em Next. Na página Rollback Security Configuration, toque ou clique em View Rollback File para visualizar os detalhes da última política de segurança aplicada no SCW Viewer. Quando tiver terminado de visualizá-la, retorne ao assistente.
5. Toque ou clique em Next para reverter a política no servidor selecionado. Quando o assistente terminar o processo de reversão, toque ou clique em Next e em Finish.

Implantação de uma política de segurança em vários computadores

Em uma empresa com muitos computadores, provavelmente não se desejará aplicar uma política de segurança separadamente a cada computador. Como abordado em “Implantação de modelos de segurança em vários computadores” anteriormente neste capítulo, pode-se querer aplicar uma política de segurança por meio da Group Policy e talvez se queira criar OUs dos computadores com essa finalidade.

Uma vez que se tenha criado as OUs necessárias, você poderá utilizar o comando de transformação do utilitário Scwcmd para criar uma GPO que inclua as configurações na política de segurança (e qualquer modelo de segurança anexado à política). Então, implante as configurações nos computadores vinculando a nova GPO às OUs apropriadas. Por padrão, as políticas de segurança criadas com o Security Configuration Wizard são salvadas na pasta %SystemRoot%\security\msscw\Policies.

Utilize a seguinte sintaxe para transformar uma política de segurança:

```
scwcmd transform /p:FullPathToSecurityPolicy /g:GPOName
```

em que *FullPathToSecurityPolicy* é o caminho completo de arquivo para o arquivo .xml da política de segurança e *GPOName* é o nome de exibição da nova GPO. Veja o seguinte exemplo:

```
scwcmd transform /p:"c:\users\wrs\documents\fspolicy.xml"  
/g:"FileServer GPO"
```

Ao criar a GPO, poderá vinculá-la seguindo estas etapas:

1. No Group Policy Management Console (GPMC), selecione a OU com a qual queira trabalhar. No painel direito, a guia Linked Group Policy Objects mostra as GPOs que estão vinculadas à OU selecionada atualmente (se houver alguma).
2. Pressione e segure ou clique com o botão direito do mouse na OU à qual queira vincular a GPO criada anteriormente e selecione Link An Existing GPO. Na caixa de diálogo Select GPO, selecione a GPO à qual queira fazer o vínculo e toque ou clique em OK.

Quando a Group Policy for atualizada para os computadores na OU aplicável, as configurações de política da GPO serão aplicadas.

Por ter criado uma nova GPO e a vinculado ao nível apropriado na estrutura do Active Directory, poderá recuperar os computadores para seu estado original removendo o vínculo da GPO. Para remover um vínculo de uma GPO, siga estas etapas:

1. No GPMC, selecione e depois expanda a OU com a qual queira trabalhar. No painel direito, a guia Linked Group Policy Objects mostra as GPOs que estão atualmente vinculadas à OU selecionada.
2. Pressione e segure ou clique com o botão direito do mouse na GPO. No menu de atalho, a opção Link Enabled deve ter uma marca de seleção para mostrar que está habilitada. Desmarque essa opção para desabilitar o vínculo.

PARTE II

Administração dos serviços de diretório do Windows Server 2012

CAPÍTULO 6	Como utilizar o Active Directory	215
CAPÍTULO 7	Administração básica do Active Directory	247
CAPÍTULO 8	Como criar contas de usuário e de grupo	293
CAPÍTULO 9	Gerenciamento de contas de usuário e de grupo	345

CAPÍTULO 6

Como utilizar o Active Directory

- Noções básicas sobre o Active Directory **215**
- Como trabalhar com estruturas de domínio **221**
- Como trabalhar com domínios do Active Directory **228**
- A estrutura de diretório **235**
- Como utilizar a Lixeira do Active Directory **242**

○ Active Directory Domain Services (AD DS) é um serviço de diretório estensível e escalável utilizado para gerenciar recursos de rede com eficiência. Como administrador, você precisa conhecer bem a forma como a tecnologia do Active Directory funciona, e é justamente esse o tópico deste capítulo. Caso você tenha trabalhado com a tecnologia do Active Directory antes, perceberá imediatamente que a tecnologia é bastante avançada e possui muitos recursos.

Noções básicas sobre o Active Directory

Desde o Windows 2000, o Active Directory tem sido o coração das redes do Microsoft Windows baseadas em domínio. Praticamente todas as tarefas administrativas que você realiza afetam o Active Directory de alguma forma. A tecnologia do Active Directory tem como base protocolos padrão da Internet e é projetada para ajudar a definir claramente a estrutura de uma rede.

Active Directory e DNS

O Active Directory utiliza o Domain Name System (DNS, Sistema de Nomes de Domínio). O DNS é um serviço de Internet padrão que organiza grupos de computadores em domínios. Os domínios DNS são organizados em uma estrutura hierárquica. A hierarquia de um domínio DNS é definida ao nível de Internet, e os diferentes níveis da hierarquia englobam os computadores, os domínios organizacionais e os domínios primários. O DNS também é utilizado para mapear nomes de host para endereços TCP/IP numéricos. Através do DNS, a hierarquia de um domínio do Active Directory pode ser definida na Internet, ou pode ser privada, separada da Internet.

Quando alguém refere-se a um recurso do tipo computador em um domínio DNS, utiliza um fully qualified domain name (FQDN, nome de domínio totalmente qualificado), como *zeta.microsoft.com*. Aqui, *zeta* representa o nome de um computador individual, *microsoft* representa o domínio organizacional e *com* é o domínio primário. Os domínios primários (TLDs, top-level domains) são a base da hierarquia DNS. Os TLDs são organizados geograficamente utilizando códigos de país contendo

duas letras, como CA para Canadá; por tipo de organizações, como em *com* para organizações comerciais; e por função, como em *mil* para instalações militares dos EUA.

Domínios normais, como o *microsoft.com*, também são chamados de *domínios-pai*, porque estão acima de outros domínios em uma estrutura organizacional. É possível dividir domínios-pai em subdomínios, para então utilizá-los em escritórios, divisões ou localizações geográficas diferentes. Por exemplo, o FQDN para um computador em um escritório da Microsoft em Seattle poderia ser chamado de *jacob.seattle.microsoft.com*. Aqui, *jacob* é o nome do computador, *seattle* é o subdomínio e *microsoft.com* é o domínio-pai. Outro termo para um subdomínio é *domínio-filho*.

O DNS é parte integrante da tecnologia do Active Directory, tanto que é necessário configurar o DNS da rede antes de instalar o Active Directory. Informações sobre como trabalhar com o DNS são apresentadas no Capítulo 16, “Otimização do DNS”.

Com o Windows Server 2012, o Active Directory é instalado em um processo de duas partes. Primeiramente, o processo é iniciado no Server Manager tocando ou clicando em Manage e em Add Roles And Features. O assistente Add Roles And Features é executado; ele é utilizado para especificar que você deseja adicionar a função AD DS ao servidor. Com isso, os binários necessários para a função são instalados, e o progresso desse processo é exibido na página Installation Progress.

MUNDO REAL Os binários necessários para a instalação de funções e recursos são chamados de payloads. Com o Windows Server 2012, além de poder desinstalar uma função ou recurso, você também pode desinstalar e remover o payload para o recurso ou função utilizando o parâmetro *-Remove* do cmdlet Uninstall-WindowsFeature.

É possível restaurar um payload removido utilizando o cmdlet Install-WindowsFeature. Por padrão, payloads são restaurados via Windows Update. Utilize o parâmetro *-Source* para restaurar um payload a partir de um ponto de montagem de um WIM. O exemplo a seguir mostra como restaurar os binários do AD DS e todos os sub-recursos relacionados por meio do Windows Update:

```
install-windowsfeature -name ad-domain-services  
-includeallsubfeature
```

Quando a instalação estiver concluída, o Assistente de Configuração do Active Directory Domain Services deve ser iniciado tocando ou clicando no link Promote This Server To A Domain Controller na página Installation Progress; utilize o assistente para configurar a função. Esse assistente substitui o Dcpromo.exe, que era utilizado anteriormente para promover controladores de domínio. O assistente também executará o Adprep.exe para preparar o esquema de forma apropriada. Se você não executar o Adprep.exe separadamente antes de instalar o primeiro controlador de domínio com Windows Server 2012 em um domínio ou esquema de floresta existente, o assistente irá solicitar suas credenciais para executar os comandos do Adprep. Para preparar o esquema da floresta, você precisa fornecer credenciais de um membro do grupo Enterprise Admins, do grupo Schema Admins e do grupo Domain Admins no domínio que hospeda o mestre de esquema. Para preparar um domínio, você precisa fornecer credenciais de um membro do grupo Domain Admins. Se estiver instalando o primeiro RODC (controlador de domínio somente leitura) em uma estrutura de floresta, precisa fornecer credenciais de um membro do grupo Enterprise Admins.

Se o DNS ainda não estiver instalado, sua instalação será solicitada. Se não houver domínio, o assistente ajudará a criar o domínio e a configurar o Active Directory para o novo domínio. O assistente também pode ajudar a adicionar domínios-filho a estruturas de domínio existentes. Para verificar se um controlador de domínio está instalado corretamente, faça o seguinte:

- Verifique se há erros no log de eventos do Directory Service.
- Certifique-se de que a pasta SYSVOL está acessível para clientes.
- Verifique se a resolução de nomes está funcionando por meio do DNS.
- Verifique a replicação de alterações no Active Directory.

OBSERVAÇÃO No restante deste capítulo, utilizarei os termos *diretório* e *domínios* para referir-me ao Active Directory e aos domínios do Active Directory, respectivamente, exceto quando precisar distinguir as estruturas do Active Directory das estruturas do DNS ou de outros tipos de diretórios.

Lembre-se de que quando utiliza o Server Manager para Windows Server 2012 e o nível funcional em estrutura de floresta é Windows Server 2003 ou mais recente, qualquer preparativo é realizado automaticamente quando você implanta um controlador de domínio. Isso significa que o Assistente de Configuração atualiza automaticamente o esquema do Active Directory da floresta e do domínio de forma a torná-lo compatível com o Windows Server 2012.

Implantação de RODC

Quando o domínio e a floresta estão operando no nível funcional Windows Server 2003 ou versão mais recente e seu emulador de PDC (Controlador de domínio primário) para o domínio utiliza o Windows Server 2008 ou versão mais recente, você pode implantar controladores de domínio somente leitura (RODCs). Qualquer controlador de domínio com Windows Server 2008 R2 ou versão mais recente pode ser configurado como um RODC. Ao instalar o serviço DNS Server em um RODC, o RODC pode agir como um servidor DNS somente leitura (RODNS). Nessa configuração, as seguintes condições são verdadeiras:

- O RODC replica as partições de diretório de aplicativo utilizadas pelo DNS, incluindo as partições *ForestDNSZones* e *DomainDNSZones*. Clientes podem consultar um servidor RODNS sobre resolução de nomes. Contudo, o servidor RODNS não dá suporte diretamente a atualizações de cliente porque o servidor RODNS não grava registros de recurso para nenhuma zona integrada do Active Directory que ele hospeda.
- Quando um cliente tenta atualizar seus registros DNS, o servidor retorna com um "referal". Assim, o cliente tenta atualizar no servidor DNS indicado. Através de uma replicação em segundo plano, o servidor RODNS tenta recuperar o registro atualizado do servidor DNS que recebeu a atualização. Essa solicitação de replicação é apenas para o registro DNS alterado. A lista completa de dados alterados na zona ou domínio não é replicada durante essa solicitação especial.

O primeiro controlador de domínio com Windows Server 2008 R2 ou versão mais recente que for instalado em uma floresta ou domínio não pode ser um RODC. Entretanto, você pode configurar controladores de domínio subsequentes como somente leitura.

MAIS INFORMAÇÕES O domínio e a floresta devem ter a versão correta do esquema para dar suporte aos RODCs e também devem estar preparados para trabalhar com RODCs. Anteriormente, em alguns casos, era necessário preparar os esquemas de floresta e domínio para o Windows Server 2008 R2 e então atualizar o esquema de floresta novamente para RODCs. Quando você utiliza o Server Manager, o Windows Server 2012 e o nível funcional da floresta é Windows

Server 2003 ou mais alto, qualquer preparativo necessário é realizado automaticamente como parte da implantação de DC e RODC.

Recursos do Active Directory para o Windows Server 2008 R2

Se estiver atualizando para o Windows Server 2012 mas ainda não tiver implantado o Windows Server 2008 R2, será necessário conhecer os novos recursos relacionados ao Active Directory. Quando estiver utilizando o Windows Server 2008 R2 e o Windows Server 2012 e tiver implantado esses sistemas operacionais em todos os controladores de domínio nos domínios da sua floresta do Active Directory, seus domínios podem operar no nível funcional de domínio Windows Server 2008 R2, e a floresta pode operar no nível funcional de floresta Windows Server 2008 R2. Esses níveis operacionais possibilitam aproveitar as diversas melhorias no Active Directory que aprimoram o desempenho e a capacidade de gerenciamento e de suporte, incluindo as seguintes melhorias:

- **Lixeira do Active Directory** Permite que os administradores desfaçam a exclusão acidental de um objeto do Active Directory de forma parecida à qual podem recuperar arquivos excluídos da lixeira do Windows. Para mais informações, consulte "Como utilizar a Lixeira do Active Directory", adiante neste capítulo.
- **Contas de serviço gerenciado** Introduz um tipo especial de conta de usuário de domínio para serviços gerenciados que reduz interrupções de serviços e outros problemas; para isso, encarrega o Windows de gerenciar automaticamente a senha da conta e os Service Principal Names (SPNs, nomes da entidade de serviço). Para mais informações, consulte "Implementação de contas gerenciadas" no Capítulo 8, "Como criar contas de usuário e de grupo".
- **Contas virtuais gerenciadas** Introduz um tipo especial de conta de computador para serviços gerenciados que fornece a possibilidade de acessar a rede com uma identidade de computador em um ambiente de domínio. Para mais informações, consulte "Uso de contas virtuais" no Capítulo 8.

MUNDO REAL Tecnicamente, é possível utilizar contas de serviço gerenciado e contas virtuais gerenciadas em um modo misto de ambiente de domínio. Entretanto, é preciso gerenciar os SPNs manualmente para contas de serviço gerenciadas, e o esquema do Active Directory deve ser compatível com o Windows Server 2008 R2 ou mais alto.

- **Garantia de mecanismo de autenticação** Aprimora o processo de autenticação; para isso, permite que os administradores controlem o acesso a recursos verificando se um usuário realizou o logon utilizando um método de logon que utiliza certificados. Assim, um administrador pode determinar que um usuário tenha um conjunto de permissões de acesso quando realizar o logon com um cartão inteligente e um conjunto diferente de permissões de acesso quando realizar o logon sem utilizar um cartão inteligente.

Outras melhorias não requerem que os níveis funcionais de domínio ou de floresta sejam elevados, mas requerem o uso do Windows Server 2012. Essas melhorias incluem as seguintes:

- **Ingresso offline no domínio** Possibilita que os administradores gerem um arquivo que pré-configura contas de computadores no domínio, preparando o am-

biente para novas implantações. Isso possibilita que os computadores ingressem em um domínio sem ter que contatar um controlador de domínio.

- **Módulo Active Directory para Windows PowerShell** Fornece cmdlets para gerenciamento do Active Directory quando você estiver trabalhando com o Windows PowerShell. Importe o módulo do Active Directory digitando **import-module activedirectory** no prompt do PowerShell.
- **Active Directory Administrative Center** Fornece uma interface com tarefas de gerenciamento do Active Directory. Em Server Manager, toque ou clique em Tools e depois em Active Directory Administrative Center.
- **Serviços Web do Active Directory** Introduz uma interface de serviços web para domínios do Active Directory.

Esses recursos são discutidos mais detalhadamente no Capítulo 7, “Administração básica do Active Directory”.

Recursos do Active Directory para o Windows Server 2012

O Active Directory Domain Service (AD DS, Serviços de Domínio do Active Directory) possui muitos recursos adicionais que dão aos administradores opções extras para a implementação e gerenciamento do Active Directory. A Tabela 6-1 lista esses recursos. No mínimo, esses recursos requerem a atualização do esquema do Active Directory em sua floresta e domínios para o Windows Server 2012. Talvez também seja necessário atualizar o domínio, a floresta ou os dois níveis funcionais para o novo nível funcional Windows Server 2012.

TABELA 6-1 Principais recursos do Active Directory para o Windows Server 2012

RECURSO	BENEFÍCIOS	REQUISITOS
Ativação com base no Active Directory	Permite utilizar o AD para ativar automaticamente os clientes com Windows 8 e Windows Server 2012. Qualquer cliente conectado ao serviço será ativado.	Licenciamento de volume; o esquema do Active Directory deve estar atualizado para o Windows Server 2012; uma chave é definida utilizando a linha de comando ou a função de servidor Volume Activation.
Controles de políticas com base em declarações (claims)	Permite que políticas de acesso e auditoria sejam definidas com flexibilidade.	As políticas usando claims devem estar habilitadas na Default Domain Controllers Policy; os servidores de arquivos devem ser executados com o Windows Server 2012; o domínio deve ter pelo menos um controlador de domínio com Windows Server 2012.
Adiamento da criação de índice	Permite adiar a criação de índice dentro do diretório até que o <i>UpdateSchemaNow</i> seja recebido ou até que o controlador de domínio seja reinicializado.	O controlador de domínio deve executar o Windows Server 2012.

Continua

TABELA 6-1 Principais recursos do Active Directory para o Windows Server 2012
(continuação)

RECURSO	BENEFÍCIOS	REQUISITOS
Diretiva refinada de senha aprimorada	Permite que os administradores utilizem o Active Directory Administrative Center do Windows Server 2012 para criar e gerenciar objetos de configuração de senha (PSOs).	Nível funcional Windows Server 2008 ou superior.
Lixeira aprimorada	Permite que os administradores recuperem objetos excluídos utilizando o Active Directory Administrative Center do Windows Server 2012.	O domínio deve ter a Lixeira habilitada e nível funcional de floresta Windows Server 2008 R2 ou superior.
Grupo de contas de serviço gerenciado	Permite que múltiplos serviços compartilhem uma única conta de serviço gerenciado.	O esquema do Active Directory deve estar atualizado para Windows Server 2012; deve haver pelo menos um controlador de domínio com Windows Server 2012; os serviços devem ser executados no Windows Server 2012.
Delegação restrita de Kerberos entre domínios	Permite que contas de serviço gerenciadas ajam em nome dos usuários nos domínios e florestas.	Cada domínio afetado deve ter pelo menos um controlador de domínio com Windows Server 2012; o servidor front-end deve executar o Windows Server 2012; o servidor back-end deve executar o Windows Server 2003 ou versão mais recente, além de outros requisitos.
Kerberos com proteção	Melhora a segurança do domínio; permite que um cliente inserido no domínio e um controlador de domínio comuniquem-se através de um canal protegido.	Controladores de domínio com Windows Server 2012; nível funcional de domínio Windows Server 2012; em clientes, habilitar a política "Require FAST"; em controladores de domínio, habilitar a política "Support CBAC and Kerberos Armoring".
Ingresso remoto no domínio	Permite que um computador ingresse em um domínio através da Internet.	O domínio deve ter o Direct Access habilitado e os controladores de domínio devem executar o Windows Server 2012.

Continua

RECURSO	BENEFÍCIOS	REQUISITOS
Limite de ID relativo (RID, Relative ID) e avisos	Fornece avisos conforme o espaço de RID é utilizado. Fornece um limite de 900 milhões de RIDs utilizado para evitar que os RIDs sejam emitidos até que o administrador sobrescreva.	Um controlador de domínio com a função RID deve executar o Windows Server 2012, e controladores de domínio devem executar o Windows Server 2012.
Integração do Server Manager	Permite que você desempenhe todos os passos necessários para implantar controladores de domínio locais e remotos.	Windows Server 2012; nível funcional de floresta Windows Server 2003 ou superior.
Clonagem de controladores de domínio virtuais	Permite a implantação de réplicas virtuais de controladores de domínio com segurança. Também ajuda a manter o estado dos controladores de domínio.	Um controlador de domínio com a função PDC Emulator deve executar o Windows Server 2012, e controladores de domínio virtuais também devem executar o Windows Server 2012.

Como trabalhar com estruturas de domínio

O Active Directory fornece estruturas lógicas e físicas para os componentes da rede. As estruturas lógicas ajudam a organizar os objetos de diretório e a gerenciar contas da rede e recursos compartilhados. As estruturas lógicas incluem as seguintes:

- **Unidades organizacionais** Subdivisão de domínios que frequentemente espelha a estrutura funcional ou empresarial da organização.
- **Domínios** Um grupo de computadores que compartilham um banco de dados de diretório em comum.
- **Árvores de domínios** Um ou mais domínios que compartilham um namespace contíguo.
- **Floresta de domínios** Uma ou mais árvores de domínio que compartilham informações de diretório em comum.

As estruturas físicas servem para melhorar a comunicação na rede e para definir limites físicos em relação aos recursos de rede. As estruturas físicas que ajudam a mapar a estrutura de rede física incluem as seguintes:

- **Sub-redes** Agrupamento de rede com um intervalo de endereços IP específico e com uma mesma máscara de rede.
- **Sites** Uma ou mais sub-redes. Os sites são utilizados para gerenciar o acesso e a replicação do diretório.

Noções básicas sobre domínios

Um domínio do Active Directory é, simplesmente, um grupo de computadores que compartilham um banco de dados de diretório em comum. Os nomes de domínio do Active Directory devem ser exclusivos. Por exemplo, não podem existir dois domínios chamados microsoft.com, mas pode haver um domínio-pai chamado microsoft.com com domínios-filho chamados seattle.microsoft.com e ny.microsoft.com. Se o domínio fizer parte de uma rede privada, o nome atribuído a um novo domínio não pode entrar em conflito com um nome de domínio existente na rede privada. Se o domínio fizer parte da Internet, o nome atribuído a um novo domínio não pode entrar em conflito com um nome de domínio existente na Internet. Para garantir a exclusividade na Internet, é preciso registrar o nome do domínio-pai antes de utilizá-lo. Você pode registrar um domínio por meio de qualquer registrador designado. Há uma lista atual de registradores designados na InterNIC (www.internic.net).

Cada domínio tem suas próprias políticas de segurança e relações de confiança com outros domínios. Os domínios também podem dividir-se em mais de um local físico, isso significa que um domínio pode consistir em múltiplos sites e que esses sites podem ter múltiplas sub-redes, como mostra a Figura 6-1. Dentro do banco de dados de diretório de um domínio, existem objetos que definem contas para usuários, grupos e computadores, assim como recursos compartilhados, como impressoras e pastas.

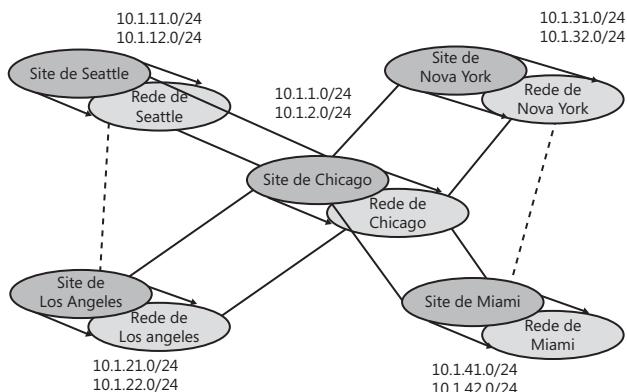


FIGURA 6-1 Esse diagrama de rede representa uma WAN (wide area network) com múltiplos sites e sub-redes.

OBSERVAÇÃO Contas de usuário e de grupo são discutidas no Capítulo 8. Contas de computador e os vários tipos de computadores utilizados nos domínios do Windows Server são discutidos em “Como trabalhar com domínios do Active Directory”, adiante neste capítulo.

As funções de domínio são limitadas e controladas pelo nível funcional de domínio. Há diversos níveis funcionais de domínio disponíveis, incluindo os seguintes:

- **Windows Server 2003** Dá suporte a controladores de domínio com Windows Server 2003 ou versão mais recente.
- **Windows Server 2008** Dá suporte a controladores de domínio com Windows Server 2008 ou versão mais recente.
- **Windows Server 2008 R2** Dá suporte a controladores de domínio com Windows Server 2008 R2 ou Windows Server 2012.
- **Windows Server 2012** Dá suporte a controladores de domínio com Windows Server 2012.

Para saber mais sobre níveis funcionais de domínio, consulte “Níveis funcionais de domínio”, adiante neste capítulo.

Noções básicas sobre floresta de domínio e árvores de domínios

Cada domínio do Active Directory possui um nome de domínio DNS, como em `microsoft.com`. Um ou mais domínios que compartilhem os mesmos dados de diretório são chamados de *floresta*. Os nomes de domínio nessa floresta podem ser não contíguos ou contíguos na hierarquia de nomenclatura DNS.

Quando os domínios possuem uma estrutura de nomenclatura contígua, diz-se que estão na mesma árvore de domínio. A Figura 6-2 mostra um exemplo de uma árvore de domínio. Neste exemplo, o domínio-raiz `msnbc.com` possui dois domínios-filho: `seattle.msnbc.com` e `ny.msnbc.com`. Cada um desses domínios, por sua vez, possui subdomínios. Todos os domínios fazem parte da mesma árvore porque possuem o mesmo domínio-raiz.

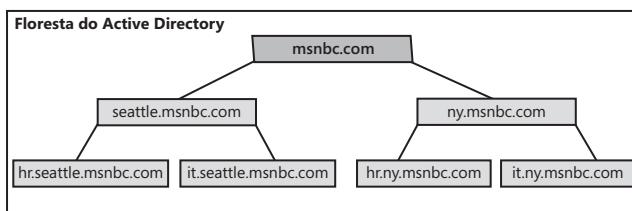


FIGURA 6-2 Os domínios de uma mesma árvore compartilham uma estrutura de nomenclatura contígua.

Se os domínios de uma floresta tiverem nomes DNS não contíguos, formam árvores de domínios separadas em uma mesma floresta. Como mostra a Figura 6-3, uma floresta de domínios pode ter uma ou mais árvores de domínios. Neste exemplo, os domínios `msnbc.com` e `microsoft.com` formam as raízes de árvores de domínios separadas em uma mesma floresta.

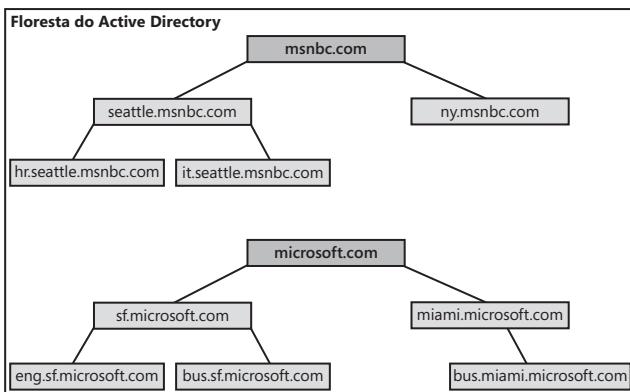


FIGURA 6-3 Múltiplas árvores em uma floresta com estruturas de nomenclatura não contíguas.

É possível acessar estruturas de domínio utilizando o Active Directory Domains And Trusts, mostrado na Figura 6-4. O Active Directory Domains And Trusts é um snap-in para o Microsoft Management Console (MMC). Você também pode iniciá-lo através do menu Tools no Server Manager. Haverá entradas separadas para cada domínio-raiz. Na Figura 6-4, o domínio ativo é o cpndl.com.

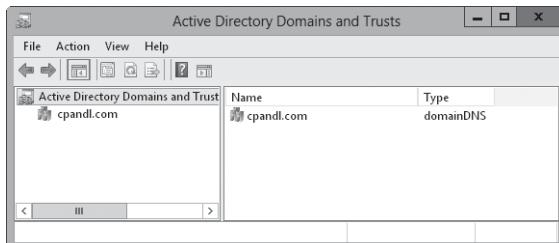


FIGURA 6-4 Use o Active Directory Domains And Trusts para trabalhar com domínios, árvores de domínios e floresta de domínios.

As funções de floresta são limitadas e controladas pelo nível funcional da floresta. Há diversos níveis funcionais de floresta disponíveis, incluindo os seguintes:

- **Windows Server 2003** Dá suporte a controladores de domínio com Windows Server 2003 ou versão mais recente.
- **Windows Server 2008** Dá suporte a controladores de domínio com Windows Server 2008 ou versão mais recente.
- **Windows Server 2008 R2** Dá suporte a controladores de domínio com Windows Server 2008 R2 ou Windows Server 2012.

- **Windows Server 2012** Dá suporte a controladores de domínio com Windows Server 2012.

Quando todos os domínios de uma floresta estiverem operando no nível funcional de floresta Windows Server 2003, você verá melhorias nas implementações de replicação de catálogo global e na eficiência de replicação. Como os valores de vínculo são replicados, também haverá melhorias na replicação entre sites. É possível desativar o esquema de classes de atributos e objetos; utilizar classes auxiliares dinâmicas; renomear domínios; e criar relações de confiança entre florestas unidirecionais, bidirecionais e transitivas.

O nível funcional de floresta Windows Server 2008 oferece ainda outras melhorias em relação ao nível funcional de floresta Windows Server 2003 no que diz respeito aos recursos e desempenho do Active Directory. Quando todos os domínios de uma floresta estiverem operando nesse modo, você verá melhorias tanto na replicação entre sites quanto dentro dos sites na organização. Os controladores de domínio também podem utilizar a replicação do Distributed File System (DFS, sistema de arquivos distribuído) em vez da replicação do File Replication Service (FRS, serviço de replicação de arquivos). Além disso, as entidades de segurança do Windows Server 2008 não são criadas até que o mestre de operações do emulador do controlador de domínio primário (PDC) no domínio-raiz da floresta esteja executando o Windows Server 2008.

O nível funcional de floresta Windows Server 2008 R2 possui diversos recursos adicionais. Esses recursos incluem a Lixeira do Active Directory, as contas de serviço gerenciado e o Authentication Mechanism Assurance (garantia de mecanismo de autenticação).

Embora o Active Directory do Windows Server 2012 possua várias melhorias, a maioria delas requer a utilização de somente controladores de domínio e esquema do Windows Server 2012. A principal exceção é para o Kerberos com proteção, que requer o nível funcional de domínio Windows Server 2012.

No geral, não é possível rebaixar o nível funcional de floresta após elevá-lo. Entretanto, quando você eleva o nível funcional de floresta para Windows Server 2012, você pode rebaixá-lo para Windows Server 2008 R2. Se a Lixeira do Active Directory não estiver habilitada, você também pode rebaixar o nível funcional do Windows Server 2012 para o Windows Server 2008 R2 ou Windows Server 2008 ou do Windows Server 2008 R2 de volta para o Windows Server 2008. Não é possível retornar o nível funcional de domínio para o Windows Server 2003 ou mais baixo.

Unidades Organizacionais

Unidades organizacionais (OUs, Organizational Units) são subdivisões dentro de domínios; normalmente espelham a estrutura empresarial ou funcional de uma empresa. Também podemos pensar em OUs como recipientes nos quais colocamos contas, recursos compartilhados e outras OUS. Por exemplo, você pode criar OUs dentro do domínio `microsoft.com` e dar a elas nomes como `RecursosHumanos`, `TI`, `Engenharia` e `Marketing`. Mais tarde, pode expandir esse esquema e incluir OUs-filha. Sub-OUs (OUs-filha) para `Marketing` poderiam incluir `VendasOnline`, `Ca-naldeVendas` e `FolhetosdeVendas`.

Objetos inseridos em uma OU só podem ser do domínio-pai. Por exemplo, OUs associadas a seattle.microsoft.com podem conter objetos somente para esse domínio. Não é possível adicionar objetos do ny.microsoft.com a esses recipientes, mas é possível criar OUs separadas para espelhar a estrutura empresarial de seattle.microsoft.com.

As OUs são úteis para organizar objetos de forma a representar uma estrutura empresarial ou funcional. Porém, essa não é a única razão para utilizar OUs. Outras razões incluem as seguintes:

- As OUs possibilitam que você atribua políticas de grupo a um conjunto pequeno de recursos em um domínio sem aplicar as políticas ao domínio inteiro. Isso ajuda a definir e gerenciar políticas de grupo no nível apropriado de uma empresa.
- As OUs criam visualizações menores e mais gerenciáveis dos objetos de diretório de um domínio. Isso ajuda a gerenciar recursos de maneira mais eficiente.
- As OUs possibilitam que você delegue autoridade e controle facilmente o acesso administrativo aos recursos de um domínio. Isso ajuda a controlar o escopo dos privilégios de administrador de um domínio. Você pode conceder a um usuário autoridade administrativa para apenas uma OU. Ao mesmo tempo, pode conceder a outro usuário autoridade administrativa para todas as OUs de um domínio.

As OUs são representadas por pastas no Active Directory Users and Computers, como mostra a Figura 6-5. Esse utilitário é um snap-in para o MMC que também pode ser iniciado a partir do menu Tools em Server Manager.

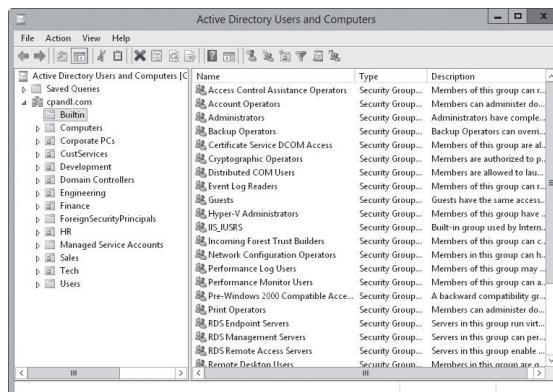


FIGURA 6-5 Utilize o Active Directory Users And Computers para gerenciar usuários, grupos, computadores e OUs.

Noções básicas sobre sites e sub-redes

Um *site* é um grupo de computadores em uma ou mais sub-redes IP. Os sites são usados para mapear a estrutura física da rede. Os mapeamentos de site são independentes da estrutura lógica do domínio, portanto não há, necessariamente, relação entre a estrutura física da rede e a estrutura lógica do domínio. Com o Active Directory, é possível criar vários sites dentro de um único domínio, ou criar um único site que contém diversos domínios. O intervalo de endereços IP utilizado por um site e o namespace de domínio também não têm relação.

Pode-se pensar em uma sub-rede como um grupo de endereços de rede. Diferente dos sites, que podem ter diversos intervalos de endereço IP, as sub-redes possuem uma máscara de rede e um intervalo de endereço IP específico. Os nomes de sub-redes são mostrados no formato *rede/bits-da-máscara*, como em 192.168.19.0/24. Aqui, o endereço de rede 192.168.19.9 e a máscara de rede 255.255.255.0 combinam-se para gerar o nome de sub-rede 192.168.19.0/24.

OBSERVAÇÃO Não se preocupe, você não precisa saber como criar um nome de sub-rede. Na maioria dos casos, você insere o endereço da rede e a máscara de sub-rede e o Windows Server gera o nome da sub-rede para você.

Os computadores são atribuídos a sites com base em sua localização em uma sub-rede ou em um conjunto de sub-redes. Se os computadores de uma sub-rede conseguem comunicar-se de maneira eficiente um com o outro através da rede, dizemos que estão *bem conectados*. Idealmente, sites consistem em sub-redes e computadores que estão bem conectados. Caso as sub-redes e os computadores não estejam bem conectados, talvez seja preciso estabelecer diversos sites. Há muitas vantagens em sites estarem bem conectados:

- Quando clientes fazem o logon em um domínio, o processo de autenticação primeiramente procura controladores de domínio que estejam no mesmo site que o cliente. Isso significa que os controladores de domínio locais são utilizados primeiro, se possível, o que mantém o tráfego na rede local e pode acelerar o processo de autenticação.
- As informações de diretório são replicadas com maior frequência dentro de sites do que entre sites. Isso reduz o tráfego de rede causado pela replicação, ao mesmo tempo que garante aos controladores de domínio locais obterem informações atualizadas rapidamente. Também é possível utilizar links de sites para personalizar a forma como as informações de diretório são replicadas entre sites. Um controlador de domínio designado para desempenhar replicação intersites é chamado de *servidor bridgehead*. Ao designar um servidor bridgehead para que trate da replicação entre sites, o peso da replicação intersites é colocado em um controlador de domínio específico em vez de em qualquer controlador disponível em um site.

O acesso a sites e sub-redes dá-se através do Active Directory Sites And Services, como mostra a Figura 6-6. Por tratar-se de um snap-in para o MMC, você pode adicioná-lo a qualquer console atualizável. Também pode abrir o Active Directory Sites And Services a partir do menu Tools em Server Manager.

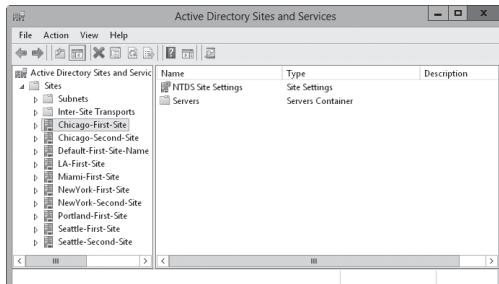


FIGURA 6-6 Utilize o Active Directory Sites And Services para gerenciar sites e sub-redes.

Como trabalhar com domínios do Active Directory

Embora seja necessário configurar tanto o Active Directory quanto o DNS em uma rede do Windows Server, os domínios do Active Directory e os domínios DNS têm fins diferentes. Os domínios do Active Directory ajudam a gerenciar contas, recursos e segurança. Os domínios DNS estabelecem uma hierarquia de domínios utilizada principalmente para resolução de nomes. O Windows Server utiliza o DNS para mapear nomes de host, como zeta.microsoft.com, para endereços TCP/IP numéricos, como 172.16.18.8. Para saber mais sobre o DNS e os domínios DNS, consulte o Capítulo 16.

Como utilizar computadores com o Active Directory

Computadores de usuários com edições profissionais do Windows podem utilizar plenamente o Active Directory. Esses computadores acessam a rede como clientes do Active Directory e têm acesso pleno aos recursos do Active Directory. Como clientes, esses sistemas podem utilizar relações de confiança transitivas que existem dentro da árvore de domínios ou da floresta. A confiança é transitiva quando não é estabelecida explicitamente. A confiança é estabelecida automaticamente com base na estrutura de floresta e na configuração de permissões na floresta. Essas relações permitem que usuários autorizados accessem recursos em qualquer domínio da floresta.

Computadores servidores fornecem serviços a outros sistemas e podem agir como controladores de domínio ou servidores membros. Um controlador de domínio distingue-se de um servidor membro por executar o Active Directory Domain Services. É possível promover servidores membros para controladores de domínio instalando o Active Directory Domain Services. É possível rebaixar controladores de domínio a servidores membros desinstalando o Active Directory Domain Services. É possível adicionar ou remover o Active Directory Domain Services utilizando os assistentes Add Roles And Features e Remove Role And Features. Para promover ou rebaixar um servidor, pode-se utilizar o Active Directory Installation Wizard (Dcpromo.exe).

Os domínios podem ter um ou mais controladores de domínio. Quando um domínio possui vários controladores de domínio, os controladores replicam automaticamente os dados de diretório entre eles utilizando um modelo de replicação multimestre. Esse modelo permite que qualquer controlador de domínio processe alterações de diretório e replique essas alterações para outros controladores de domínio.

Devido à estrutura de domínio multimestre, todos os controladores de domínio têm o mesmo nível de responsabilidade. Entretanto, é possível dar prioridade a alguns controladores de domínio em comparação a outros em algumas tarefas, como especificar que um servidor bridgehead tenha prioridade na replicação de informações de diretório para outros sites. Além disso, algumas tarefas são melhor desempenhadas por um único servidor. Um servidor que lida com esse tipo de tarefa é chamado de *mestre de operações*. Há cinco funções de mestre único (FSMO, Flexible Single Master Operation), e você pode atribuir cada uma delas a um controlador de domínio diferente. Para mais informações, consulte “Noções básicas sobre funções de mestre de operações” mais adiante neste capítulo.

Todo computador com Windows 2000 ou versão mais recente que ingresse em um domínio possui uma conta de computador. Como outros recursos, as contas de computadores são armazenadas no Active Directory como objetos. As contas de computadores são utilizadas para controlar o acesso à rede e seus recursos. Um computador acessa um domínio utilizando sua conta, que é autenticada antes que o computador possa acessar a rede.

MUNDO REAL Controladores de domínio utilizam o catálogo global do Active Directory para autenticar tanto os logons de computadores quanto de usuários. Se o catálogo global estiver indisponível, apenas os membros de grupo Domain Admins podem efetuar logon no domínio porque as informações dos membros de grupo universal estão armazenadas no catálogo global, e essas informações são necessárias para a autenticação. Em servidores com o Windows Server 2003 e versões mais recentes, existe a opção de armazenar as informações de membros de grupos universais localmente, o que resolve esse problema. Para mais informações, consulte “Para entender a estrutura de diretório” mais adiante neste capítulo.

Níveis funcionais de domínio

Para dar suporte a estruturas de domínio, o Active Directory inclui suporte para os seguintes níveis funcionais de domínio:

- **Modo Windows Server 2003** Quando o domínio estiver sendo operado no modo Windows Server 2003, o diretório suporta controladores de domínio com o Windows Server 2012, o Windows Server 2008 R2, Windows Server 2008 ou Windows Server 2003. Um domínio operando no modo Windows Server 2003 pode utilizar grupos universais, aninhamento de grupo, conversão de tipo de grupo, renomeação simples de controlador de domínio, carimbo de data/hora de logon e número de versão KDC do Kerberos.
- **Modo Windows Server 2008** Quando o domínio estiver sendo operado no modo Windows Server 2008, o diretório suporta controladores de domínio com o Windows Server 2012, o Windows Server 2008 R2 ou Windows Server 2008. Controladores de domínio com Windows Server 2003 não têm mais suporte. Um domínio operando no modo Windows Server 2008 pode utilizar recursos adicionais do Active Directory, incluindo o serviço de replicação do DFS para replicação intersite e intrasite.
- **Modo Windows Server 2008 R2** Quando o domínio estiver sendo operado no modo Windows Server 2008, o diretório suporta somente controladores de domínio com o Windows Server 2012, o Windows Server 2008 R2. Controladores de domínio com Windows Server 2003 e Windows Server 2008 não têm mais suporte. Um domínio operando no modo Windows Server 2008 R2 pode utilizar

a Lixeira do Active Directory, contas de serviço gerenciadas, Authentication Mechanism Assurance e outras melhorias importantes do Active Directory.

- **Modo Windows Server 2012** Quando o domínio estiver operando no modo Windows Server 2012, o diretório suporta somente controladores de domínio com o Windows Server 2012. Controladores de domínio com o Windows Server 2003, Windows Server 2008 ou Windows Server 2008 R2 não têm mais suporte. O esquema do Active Directory para Windows Server 2012 inclui diversas melhorias, mas somente o recurso Kerberos com proteção requer esse modo.

No geral, não é possível diminuir o nível funcional de domínio após elevá-lo. Entretanto, quando você eleva o nível funcional de domínio para Windows Server 2008 R2 ou Windows Server 2012 e o nível funcional de floresta é Windows Server 2008 ou mais baixo, pode reverter o nível funcional de domínio de volta para Windows Server 2008 ou Windows Server 2008 R2. Não é possível retornar o nível funcional de domínio para o Windows Server 2003 ou mais baixo.

Como utilizar o nível funcional de domínio Windows Server 2003

Todos os domínios de sua empresa devem ter nível funcional de domínio Windows Server 2003 ou mais alto, se possível, pois isso garantirá que os computadores do domínio aproveitem muitas das mais recentes melhorias do Active Directory. Após desativar as estruturas do Windows NT e atualizar as estruturas do Windows 2000 em sua empresa, você pode alterar o nível funcional de domínio para o modo de operações do Windows Server 2003.

Antes de atualizar os controladores de domínio do Windows 2000, é preciso preparar o domínio para atualizá-lo. Para isso, é necessário atualizar o esquema de floresta e o de domínio para que sejam compatíveis com os domínios do Windows Server 2003. Uma ferramenta chamada Adprep.exe é fornecida para realizar a atualização automaticamente. Tudo o que você precisa fazer é executar a ferramenta no mestre de operações de esquema na floresta e depois no mestre de operações de infraestrutura para cada domínio da floresta. Como sempre, é preciso testar qualquer procedimento em um laboratório antes de realizá-lo em um ambiente de produção.

Na mídia de instalação do Windows Server 2003, você encontrará o Adprep e arquivos relacionados na subpasta i386. Siga estas etapas para realizar a atualização:

1. No mestre de operações de esquema na floresta, execute `<cdrom>:\i386\adprep.exe /forestprep`. É preciso utilizar uma conta de administrador que seja membro do Enterprise Admins, Schema Admins ou Domain Admins no domínio-raiz da floresta.
2. No mestre de operações de infraestrutura para cada domínio da floresta, execute `<cdrom>:\i386\adprep.exe /domainprep`. É preciso utilizar uma conta que seja membro do grupo Domain Admins no domínio aplicável.

OBSERVAÇÃO Para saber qual servidor é o mestre de operações de esquema atual para a floresta, abra um prompt de comando e digite `dsquery server -hasfsmo schema`. Você recebe uma string com o caminho do serviço de diretório contendo o nome do servidor, como em "CN=CORPSERVER01,CN=Servers,CN=Default-First-Site-Name,CN=Sites, CN=Configuration, DC=microsoft,DC=com." Essa sequência informa que o mestre de operações de esquema é o CORPSERVER01 no domínio microsoft.com.

OBSERVAÇÃO Para saber qual servidor é o mestre de operações de infraestrutura para o domínio, abra um prompt de comando e digite **dsquery server -hasfsmo infr**.

MUNDO REAL De modo geral, tudo o que pode ser digitado em um prompt de comando também pode ser digitado no prompt do PowerShell. Isso é possível porque o PowerShell procura utilitários e comandos externos como parte de seu processamento normal. Contanto que o utilitário ou comando externo encontre-se em um diretório especificado pela variável de ambiente PATH, o utilitário ou comando será executado adequadamente. Entretanto, lembre-se de que a ordem de execução do PowerShell pode determinar se um comando é executado como esperado ou não. Para o PowerShell, a ordem de execução é 1) aliases alternativos internos ou definidos por perfil, 2) funções internas ou definidas por perfil, 3) palavras-chave de idiomas ou cmdlets, 4) scripts com a extensão .ps1, e 5) arquivos, utilitários e comandos externos. Assim, se qualquer elemento de 1 a 4 na ordem de execução tiver o mesmo nome que um comando, esse elemento será executado em vez do comando esperado.

Após atualizar seus servidores, você pode aumentar o nível funcional do domínio e da floresta para aproveitar os recursos adicionais do Active Directory do nível funcional Windows Server 2003. Lembre-se de que após fazer uma atualização, você só pode utilizar o Windows Server 2003 e versões mais recentes no domínio, e que não é possível retornar para qualquer outro modo. Deve-se utilizar o modo Windows Server 2003 somente quando houver certeza de que não precisará mais das estruturas de domínio do Windows NT, dos controladores de domínio de backup (BDCs) do Windows NT e das estruturas de domínio do Windows 2000.

Como utilizar o nível funcional de domínio Windows Server 2008

Após atualizar as estruturas do Windows 2000 e do Windows 2003 em sua empresa, você pode alterar o nível funcional de domínio para o modo de operações Windows Server 2008.

Antes de atualizar os controladores de domínio do Windows Server 2003, é preciso preparar o domínio para o Windows Server 2008. Para isso, você deve utilizar o Adprep.exe para atualizar o esquema de floresta e o de domínio para que sejam compatíveis com os domínios do Windows Server 2008. Siga estas etapas:

1. No mestre de operações de esquema na floresta, copie o conteúdo da pasta Sources\Adprep da mídia de instalação do Windows Server 2008 para uma pasta local, depois execute **adprep /forestprep**. Se você pretende instalar algum RODC, também deve executar **adprep /rodcprep**. É preciso utilizar uma conta de administrador que seja membro do Enterprise Admins, Schema Admins ou Domain Admins no domínio-raiz da floresta.
2. No mestre de operações de infraestrutura de cada domínio na floresta, copie o conteúdo da pasta Sources\Adprep da mídia de instalação do Windows Server 2008 para uma pasta local, depois execute **adprep /domainprep**. É preciso utilizar uma conta que seja membro do grupo Domain Admins no domínio aplicável.
3. Se você não tiver executado **adprep /domainprep /gpprep** em cada domínio, precisará realizar essa tarefa manualmente. O Server Manager para o Windows Server 2008 não preparará a Group Policy para você. Perceba que a Group Policy precisa ser preparada somente na primeira vez que você implantar controladores de domínio com Windows Server 2003 SP1 ou mais recente. **Adprep /gpprep** modifica as entradas de controle de acesso (ACEs) para todas as pastas da Group

Policy Object (GPO) no diretório SYSVOL para conceder acesso de leitura para todos os controladores de domínio da empresa. Esse nível de acesso é requerido para dar suporte ao Resultant Set of Policy (RSOP, conjunto de políticas resultantes) para políticas baseadas em site e faz com que o NT File Replication Service (NTFRS, Serviço de replicação de arquivos) reenvie todas as GPOs para todos os controladores de domínio.

Como sempre, é preciso testar qualquer procedimento em um laboratório antes de realizá-lo em um ambiente de produção.

OBSERVAÇÃO Para saber qual servidor é o mestre de operações de esquema atual para a floresta, abra um prompt de comando e digite **dsquery server –hasfsmo schema**. Para saber qual servidor é o mestre de operações de infraestrutura atual para o domínio, abra um prompt de comando e digite **dsquery server –hasfsmo infr**.

Após atualizar todos os controladores de domínio para o Windows Server 2008, você pode aumentar a funcionalidade de domínio e de floresta para utilizar recursos adicionais do Active Directory. Se fizer isso, você só pode utilizar o Windows Server 2008 e versões mais recentes no domínio, e não poderá retornar para qualquer outro modo. Você deve utilizar o modo Windows Server 2008 somente quando tiver certeza de que não precisará mais das estruturas de domínio do Windows NT, dos BDCs do Windows NT e das estruturas de domínio do Windows 2000 e do Windows Server 2003.

Como utilizar o nível funcional Windows Server 2008 R2

O Windows Server 2008 R2 e o Windows Server 2012 são executados somente em hardware de 64 bits. Provavelmente será necessário instalar o Windows Server 2008 R2 e o Windows Server 2012 em um novo hardware em vez de em um hardware projetado para versões anteriores do Windows Server.

Antes de atualizar os controladores de domínio do Windows Server 2008, é preciso preparar o domínio para o Windows Server 2008 R2. Para isso, você deve utilizar o Adprep.exe para atualizar o esquema da floresta e o domínio para que sejam compatíveis com os domínios do Windows Server 2008 R2. Siga estas etapas:

1. No mestre de operações de esquema na floresta, copie o conteúdo da pasta Support\Adprep da mídia de instalação do Windows Server 2008 R2 para uma pasta local, depois execute **adprep /forestprep**. Se você pretende instalar algum RODC, também deve executar **adprep /rodcprep**. É preciso utilizar uma conta de administrador que seja membro do Enterprise Admins, Schema Admins ou Domain Admins no domínio-raiz da floresta.
2. No mestre de operações de infraestrutura de cada domínio na floresta, copie o conteúdo da pasta Support\Adprep da mídia de instalação do Windows Server 2008 para uma pasta local, depois execute **adprep /domainprep**. É preciso utilizar uma conta que seja membro do grupo Domain Admins no domínio aplicável.

Como sempre, é preciso testar qualquer procedimento em um laboratório antes de realizá-lo em um ambiente de produção.

OBSERVAÇÃO Para saber qual servidor é o mestre de operações de esquema atual para a floresta, abra um prompt de comando e digite **dsquery server –hasfsmo schema**. Para saber qual servidor é o mestre de operações de infraestrutura atual para o domínio, abra um prompt de comando e digite **dsquery server –hasfsmo infr**.

Após atualizar todos os controladores de domínio para o Windows Server 2008 R2, você pode aumentar o nível funcional de domínio e de floresta para utilizar recursos mais recentes do Active Directory. Se fizer isso, poderá utilizar somente as versões do Windows Server 2008 R2 e Windows Server 2012 no domínio. Você deve utilizar o modo Windows Server 2008 R2 somente quando tiver certeza de que não precisará mais das estruturas de domínio do Windows NT, dos BDCs do Windows NT e das estruturas de domínio do Windows 2000; do Windows Server 2003 e do Windows Server 2008.

Como utilizar o nível funcional de domínio Windows Server 2012

Assim como o Windows Server 2008 R2, o Windows Server 2012 é executado somente em hardware de 64 bits e provavelmente será necessário instalar o Windows Server 2012 em um novo hardware em vez de em um hardware projetado para versões anteriores do Windows Server. Diferente das versões anteriores do Windows Server, os preparativos de domínio e floresta necessários para atualizar o esquema do Active Directory não precisam ser realizados manualmente. Em vez disso, quando você utiliza o Server Manager do Windows Server 2012 e o nível funcional de estrutura de floresta é Windows Server 2003 ou mais alto, qualquer preparação necessária é realizada automaticamente quando você implanta um controlador de domínio com o Windows Server 2012. Isso significa que o Configuration Wizard atualiza automaticamente o esquema de floresta e o de domínio.

Também é possível fazer a preparação para o Windows Server 2012 manualmente. Para isso, você deve utilizar o Adprep.exe para atualizar o esquema de floresta e o domínio para que sejam compatíveis com os domínios do Windows Server 2012. As etapas são parecidas com àquelas discutidas na seção anterior.

Após atualizar todos os controladores de domínio para o Windows Server 2012, você pode aumentar o nível funcional de domínio e de floresta para utilizar recursos mais recentes do Active Directory. Se fizer isso, poderá utilizar somente os recursos do Windows Server 2012 no domínio.

Como aumentar ou diminuir o nível funcional de domínio e de floresta

Um domínio operando no nível funcional Windows Server 2003 ou nível mais alto pode utilizar grupos universais, aninhamento de grupo, conversão de tipo de grupo, carimbo de data/hora de logon e número de versão KDC do Kerberos. Nesse modo ou em modo mais alto, os administradores podem fazer o seguinte:

- Renomear controladores de domínio sem ter que rebaixá-los primeiro.
- Renomear domínios com o Windows Server 2003 ou controladores de domínio mais atuais.
- Criar uma relação de confiança bidirecional entre duas florestas.
- Reestruturar domínios na hierarquia de domínio renomeando-os e colocando-os em níveis diferentes.
- Aproveitar as melhorias de replicação para membros de grupos individualmente e para catálogos globais.

Comparado a implementações anteriores, as florestas executadas no nível funcional Windows Server 2003 ou nível mais alto possuem replicação de catálogo global e replicação intrasite e intersite mais eficientes, além da habilidade de estabelecer confiança entre florestas unidirecionais, bidirecionais e transitivas.

MUNDO REAL O processo de atualização do domínio e da floresta pode gerar muito tráfego de rede devido à replicação de informações pela rede. Às vezes, o processo de atualização por inteiro pode levar 15 minutos ou mais. Durante esse intervalo de tempo, pode haver atraso na capacidade de resposta na comunicação entre servidores e pode haver latência mais alta na rede, portanto é recomendável programar a atualização para horário não comercial. Também é uma boa ideia testar a compatibilidade com aplicativos existentes (especialmente aplicativos herdados) antes de realizar essa operação.

Você pode aumentar o nível funcional de domínio seguindo estas etapas:

1. Abra o Active Directory Domains And Trusts (Domínios e Relações de Confiança do Active Directory). Na árvore de console, pressione e mantenha pressionado ou clique com o botão direito do mouse no domínio com o qual você deseja trabalhar e toque ou clique em Raise Domain Functional Level.

O nome de domínio e o nível funcional atuais são exibidos na caixa de diálogo Raise Domain Functional Level.

2. Para alterar o nível de domínio, selecione o novo nível funcional de domínio na lista fornecida e toque ou clique em Raise.
3. Toque ou clique em OK. O novo nível funcional de domínio é replicado para todos os controladores de domínio no domínio. Essa operação pode levar algum tempo em uma empresa de grande porte.

Você pode aumentar o nível funcional de floresta seguindo estas etapas:

1. Abra o Active Directory Domains And Trusts. Na árvore de console, pressione e mantenha pressionado ou clique com o botão direito do mouse no nó Active Directory Domains And Trusts e toque ou clique em Raise Forest Functional Level.

O nome da floresta e o nível funcional atuais são exibidos na caixa de diálogo Raise Forest Functional Level.

2. Para alterar o nível funcional de floresta, selecione o novo nível funcional de floresta na lista fornecida e toque ou clique em Raise.
3. Toque ou clique em OK. O novo nível funcional de floresta é replicado para todos os controladores de domínio na floresta. Essa operação pode levar algum tempo em uma empresa de grande porte.

Outra forma de aumentar o nível funcional de domínio ou de floresta é utilizando o Active Directory Administrative Center. Essa ferramenta está disponível como um item do menu Tools no Server Manager. Siga estas etapas para aumentar o nível funcional de domínio:

1. No Active Directory Administrative Center, por padrão, o domínio local é aberto para gerenciamento. Se quiser trabalhar com outro domínio, toque ou clique em Manage e depois em Add Navigation Nodes. Na caixa de diálogo Add Navigation Nodes, selecione o domínio desejado e toque ou clique em OK.
2. Selecione o domínio desejado tocando ou clicando nessa opção no painel esquerdo. No painel Tasks, toque ou clique em Raise Domain Functional Level.

O nome de domínio e o nível funcional atuais são exibidos na caixa de diálogo Raise Domain Functional Level.

3. Para alterar o nível funcional de domínio, selecione o novo nível funcional de domínio na lista fornecida e toque ou clique em Raise.
4. Toque ou clique em OK. O novo nível funcional de domínio é replicado para todos os controladores de domínio no domínio. Essa operação pode levar algum tempo em uma empresa de grande porte.

Siga estas etapas para aumentar o nível funcional da floresta:

1. No Active Directory Administrative Center, selecione o domínio desejado tocando ou clicando nessa opção no painel esquerdo. No painel Tasks, toque ou clique em Raise Forest Functional Level.
O nome da floresta e o nível funcional atuais são exibidos na caixa de diálogo Raise Forest Functional Level.
2. Para alterar o nível funcional de floresta, selecione o novo nível funcional de floresta na lista fornecida e toque ou clique em Raise.
3. Toque ou clique em OK. O novo nível funcional de floresta é replicado para todos os controladores de domínio na floresta. Essa operação pode levar algum tempo em uma empresa de grande porte.

No geral, não é possível diminuir o nível funcional de floresta após aumentá-lo. Entretanto, há exceções específicas como discutido anteriormente neste capítulo. Lembre-se de que se habilitar a Lixeira do Active Directory, você não poderá diminuir o nível funcional de floresta.

A estrutura de diretório

O Active Directory possui muitos componentes e utiliza várias tecnologias. Dados de diretório são disponibilizados para usuários e computadores através de armazenamentos de dados e catálogo global. Embora a maior parte das tarefas do Active Directory afete o armazenamento de dados, catálogo global têm igual importância porque são utilizados durante o logon e para buscas de informações. Na verdade, se o catálogo global estiver indisponível, usuários padrão não podem efetuar logon no domínio. A única forma de alterar esse comportamento é armazenando as informações de membros de grupos universais localmente. Como você deve imaginar, armazenar em cache as informações do grupo universal tem vantagens e desvantagens, as quais serão discutidas adiante.

O acesso e a distribuição de dados do Active Directory se dá utilizando protocolos de acesso ao diretório e replicação. Protocolos de acesso ao diretório possibilitam que clientes se comuniquem com computadores executando Active Directory. A replicação é necessária para garantir que as atualizações dos dados sejam distribuídas aos controladores de domínio. Embora a replicação multimestre seja a principal técnica utilizada para distribuir atualizações, algumas alterações nos dados só podem ser controladas por controladores de domínio individuais, chamados de mestres de operações. Um recurso do Windows Server 2008 e versões mais recentes, chamado de *partições de diretório de aplicativos*, também altera a forma como a replicação multimestre funciona.

Com partições de diretório de aplicativos, administradores corporativos (aqueles que pertencem ao grupo Enterprise Admins) podem criar partições de replicação na floresta do domínio. Essas partições são estruturas lógicas utilizadas para controlar a

replicação de dados dentro da floresta de um domínio. Por exemplo, é possível criar uma partição especialmente para controlar a replicação de informações de DNS dentro de um domínio, evitando, assim, que outros sistemas do domínio repliquem informações de DNS.

Uma partição de diretório de aplicativo também pode aparecer como filha de um domínio, filha de outra partição de aplicativo ou como uma nova árvore na floresta do domínio. Réplicas da partição de diretório de aplicativo podem ser disponibilizadas em qualquer controlador de domínio do Active Directory com Windows Server 2008 ou versão mais recente, incluindo servidores de catálogo global. Embora as partções de diretório de aplicativo sejam úteis em domínios e florestas grandes, elas representam uma sobrecarga em termos de planejamento, administração e manutenção.

O armazenamento de dados

O armazenamento de dados contém informações sobre objetos, como contas, recursos compartilhados, OUs e políticas de grupo. Outro nome para o armazenamento de dados é *diretório*, que faz referência ao próprio Active Directory.

Controladores de domínio armazenam o diretório em um arquivo chamado Ntds.dit. A localização desse arquivo é definida quando o Active Directory é instalado, e deve ser em uma unidade formatada com o sistema de arquivos NTFS para ser utilizada por um Windows Server 2008 ou versão mais recente. Também é possível armazenar dados de diretório separadamente do armazenamento de dados principal. Isso ocorre com políticas de grupo, scripts e outros tipos de informações públicas armazenadas em um volume de sistema compartilhado (SYSVOL).

Compartilhar informações de diretório chama-se *publicar*. Por exemplo, você publica informações sobre uma impressora ao compartilhar a impressora na rede. De maneira similar, você publica informações sobre uma pasta ao compartilhar a pasta na rede.

Os controladores de domínio replicam a maior parte das alterações no armazenamento de dados utilizando múltiplos mestres. Os administradores de empresas de pequeno e médio porte raramente precisam gerenciar replicação de armazenamento de dados. A replicação é realizada automaticamente, mas é possível personalizá-la e adequá-la às necessidades de empresas de grande porte e de empresas com requisitos especiais.

Nem todos os dados de diretório são replicados. Apenas as informações públicas que se encaixem em uma das seguintes categorias são replicadas:

- **Dados de domínio** São informações sobre objetos de um domínio. Incluem objetos de contas, recursos compartilhados, OUs e políticas de grupo.
- **Dados de configuração** Descrevem a topologia do diretório. Incluem uma lista de todos os domínios, árvores de domínios e floresta, assim como as localizações dos controladores de domínio e dos servidores de catálogo global.
- **Dados de esquema** Descrevem todos os tipos de dados e objetos que podem ser armazenados no diretório. O esquema padrão fornecido com o Windows Server descreve objetos de conta, objetos de recursos compartilhados, entre outros. Você pode estender o esquema padrão definindo novos objetos e atributos ou adicionando atributos a objetos existentes.

Os catálogos globais

Quando a associação de grupo universal não for armazenada localmente em cache, catálogos globais habilitam o logon de rede fornecendo informações de associação de grupo universal quando o processo de logon é iniciado. Catálogos globais também habilitam consultas ao diretório nos domínios em uma floresta. Um controlador de domínio designado como catálogo global armazena uma réplica completa de todos os objetos do diretório de seu domínio de origem e uma réplica parcial de todos os outros domínios em uma floresta de domínios.

OBSERVAÇÃO As réplicas parciais são utilizadas porque apenas algumas propriedades de objeto são necessárias para operações de consulta e logon. A replicação parcial também significa que menos informações precisam circular na rede, reduzindo o tráfego na rede.

Por padrão, o primeiro controlador de domínio instalado em um domínio é designado como o catálogo global. Se há apenas um controlador de domínio no domínio, o controlador de domínio e o catálogo global serão o mesmo servidor. Caso contrário, o catálogo global estará no controlador de domínio que você definiu. Você também pode adicionar catálogo global a um domínio para ajudar a melhorar o tempo de resposta para solicitações de consulta e logon. A recomendação é ter um catálogo global por site no domínio.

Controladores de domínio que estão hospedando o catálogo global devem estar bem conectados aos controladores de domínio que estão agindo como mestres de infraestrutura. A função do mestre de infraestrutura é uma das cinco funções de mestre de operações que podem ser atribuídas a um controlador de domínio. Em um domínio, o mestre de infraestrutura é o responsável por atualizar as referências de objeto. Para isso, o mestre de infraestrutura compara os dados dos objetos com os do catálogo global. Se o mestre de infraestrutura encontrar dados desatualizados, ele solicita dados atualizados a um catálogo global. Então, o mestre de infraestrutura replica as alterações para os outros controladores de domínio do domínio. Para mais informações sobre as funções de mestre de operações, consulte "Noções básicas sobre funções de mestre de operações", adiante neste capítulo.

Quando há apenas um controlador de domínio em um domínio, você pode atribuir a função de mestre de infraestrutura e o catálogo global ao mesmo controlador de domínio. Quando há dois ou mais controladores de domínio no domínio, o catálogo global e o mestre de infraestrutura devem estar em controladores de domínio distintos. Se não estiverem, o mestre de infraestrutura não encontrará dados desatualizados e nunca replicará alterações. A única exceção é quando todos os controladores de domínio no domínio hospedam o catálogo global. Nesse caso, não importa qual controlador de domínio atua como mestre de infraestrutura.

Uma das razões principais para configurar catálogos globais adicionais em um domínio é poder garantir que um catálogo esteja disponível para serviço de logon e solicitações de consulta ao diretório. Novamente, se o domínio tiver somente um catálogo global e o catálogo não estiver disponível, e se não houver cache de associação de grupo universal, os usuários padrão não poderão efetuar logon e os que estiverem logados não poderão fazer consultas ao diretório. Nesse cenário, os únicos usuários que podem efetuar logon no domínio quando o catálogo global estiver indisponível são os membros do grupo Domain Admins.

Buscas no catálogo global são muito eficientes. O catálogo contém informações sobre objetos de todos os domínios na floresta. Isso possibilita que as solicitações de

busca de diretório sejam resolvidas em um domínio local em vez de em um domínio em outra parte da rede. Resolver solicitações localmente reduz a carga na rede e possibilita respostas mais rápidas na maioria dos casos.

DICA Se você notar que os tempos de resposta de logon e solicitações estão lentos, pode configurar catálogos globais adicionais. Porém, um número maior de catálogos globais normalmente significa que mais dados de replicação estão sendo transferidos na rede.

Cache de Associação de Grupo Universal

Em uma empresa de grande porte, ter catálogos globais em cada escritório pode não ser prático. Porém, não ter catálogos globais em cada escritório representa um problema se um escritório remoto perder a conectividade com o escritório central ou com uma filial designada onde encontram-se os servidores de catálogo global. Se isso ocorrer, usuários padrão não conseguirão efetuar logon; apenas os membros do grupo Domain Admins conseguirão efetuar logon. Isso ocorre porque solicitações de logon devem ser encaminhadas pela rede para um servidor de catálogo global em um escritório diferente, e isso não é possível sem conectividade.

Como você deve imaginar, é possível solucionar esse problema de várias maneiras. Você pode definir um dos controladores de domínio em um escritório remoto como servidor de catálogo global, basta seguir os procedimentos discutidos em “Configuração de catálogos globais”, no Capítulo 7. A desvantagem dessa abordagem é que o servidor ou servidores designados terão mais uma responsabilidade e talvez requeiram recursos adicionais. Você também deve gerenciar com mais cuidado o tempo de ativação do servidor de catálogo global.

Outra forma de solucionar esse problema é armazenando associação de grupo universal em cache local. Dessa forma, qualquer controlador de domínio pode resolver solicitações de logon localmente sem ter que passar para um servidor de catálogo global. Isso possibilita logons mais rápidos e torna mais fácil o gerenciamento de paradas de servidor porque seu domínio não depende de um único servidor ou grupo de servidores para realizar logons. Essa solução também reduz o tráfego de replicação. Em vez de replicar o catálogo global inteiro periodicamente pela rede, somente as informações de associação de grupo universal no cache são atualizadas. Por padrão, uma atualização ocorre a cada oito horas em cada controlador de domínio que esteja armazenando associações em cache localmente.

O cache de associação de grupo universal é específico de site. Lembre-se, um site é uma estrutura de diretório física que consiste em uma ou mais sub-redes com um intervalo de endereços IP específico e com uma máscara de rede. Os controladores de domínio com o Windows Server e o catálogo global que estão contatando devem estar no mesmo site. Se você tiver diversos sites, precisa configurar o armazenamento em cache local em cada site. Além disso, usuários no site devem fazer parte de um domínio do Windows com modo funcional Windows Server 2003 ou superior. Para aprender a configurar o armazenamento em cache, consulte “Configuração de cache de associação de grupo universal” no Capítulo 7.

Replicação e o Active Directory

Independentemente de utilizar replicação do tipo FRS ou DFS, os três tipos de informação armazenados no diretório são: dados de domínio, dados de esquema e dados de configuração.

Os dados de domínio são replicados para todos os controladores de domínio de um domínio em especial. Os dados de esquema e de configuração são replicados para todos os domínios na árvore de domínios ou na floresta. Além disso, todos os objetos em um domínio individual e um subconjunto de propriedades de objeto na floresta do domínio são replicados para o catálogo global.

Isso significa que os controladores de domínio armazenam e replicam o seguinte:

- Informações de esquema para a árvore de domínios ou para a floresta
- Informações de configuração para todos os domínios em uma árvore de domínios ou floresta
- Todos os objetos do diretório e suas propriedades em seus respectivos domínios

Entretanto, controladores de domínio que estejam hospedando um catálogo global armazenam e replicam informações de esquema para a floresta e informações de configuração para todos os domínios na floresta. Além disso, eles também armazenam e replicam um subconjunto das propriedades de todos os objetos de diretório em uma floresta (esse subconjunto só é replicado entre servidores que estejam hospedando catálogos globais) e todos os objetos de diretório e suas propriedades para seus respectivos domínios:

- Informações de esquema para a floresta
- Informações de configuração para todos os domínios da floresta
- Um subconjunto das propriedades entre os servidores de catálogos globais
- Todos os objetos de diretório e suas propriedades para o domínio

Para um melhor entendimento de replicação, imagine o seguinte cenário, no qual você está instalando uma nova rede:

1. Comece instalando o primeiro controlador de domínio no domínio A. O servidor é o único controlador de domínio e também hospeda o catálogo global. Não ocorre replicação porque não há outro controlador de domínio na rede.
2. Instale um segundo controlador de domínio no domínio A. Como há dois controladores de domínio, a replicação começa. Para garantir que os dados sejam replicados de maneira apropriada, defina um controlador de domínio como o mestre de infraestrutura e o outro como o catálogo global. O mestre de infraestrutura busca atualizações para o catálogo global e solicita atualizações para os objetos alterados. Os dois controladores de domínio também replicam dados do esquema e da configuração.
3. Instale um terceiro controlador de domínio no domínio A. Esse servidor não é um catálogo global. O mestre de infraestrutura busca atualizações no catálogo global, solicita atualizações nos objetos modificados e então replica essas alterações para o terceiro controlador de domínio. Os três controladores de domínio também replicam dados do esquema e da configuração.
4. Configure um novo domínio, o domínio B, e adicione controladores de domínio nele. Os servidores do catálogo global no domínio A e no domínio B começam a replicar dados do esquema e da configuração assim como um subconjunto dos dados de domínio de cada domínio. A replicação no domínio A continua como foi descrito acima. A replicação no domínio B inicia.

O Active Directory e o LDAP

O Lightweight Directory Access Protocol (protocolo LDAP) é um protocolo de comunicação padrão na Internet para redes TCP/IP. O protocolo LDAP é projetado especificamente para acessar serviços de diretório com o mínimo de sobrecarga possível. O protocolo LDAP também define operações que podem ser utilizadas para consultar e modificar informações de diretório.

Cientes do Active Directory utilizam o protocolo LDAP para comunicar-se com computadores executando o Active Directory sempre que eles efetuam logon na rede ou buscam por recursos compartilhados. Você também pode utilizar o protocolo LDAP para gerenciar o Active Directory.

O protocolo LDAP é um padrão aberto utilizado por muitos serviços de diretório. Isso facilita a comunicação entre diretórios e fornece um caminho de migração mais claro de outros serviços de diretório para o Active Directory. Você também pode utilizar o Active Directory Service Interface (ADSI) para aprimorar a interoperabilidade. O ADSI dá suporte para as interfaces de programação de aplicativo (APIs) padrão para o protocolo LDAP; essas APIs estão especificadas na Request For Comments (RFC) 1823 padrão da Internet. Pode-se utilizar o ADSI com o Windows Script Host para criar e gerenciar objetos no Active Directory.

Noções básicas sobre funções de mestre de operações

As funções de mestre de operações realizam tarefas que não são praticáveis de serem realizadas utilizando múltiplos mestres. Existem cinco funções de mestre de operações, que podem ser atribuídas a um controlador de domínio. Embora algumas funções possam ser atribuídas apenas uma vez em uma floresta de domínio, outras funções devem ser atribuídas uma vez em cada domínio.

Todas as florestas do Active Directory devem ter as seguintes funções:

- **Mestre de esquema** Controla atualizações e modificações no esquema do diretório. Para atualizar o esquema do diretório, é preciso ter acesso ao mestre de esquema. Para saber qual servidor é o mestre de esquema atual para a floresta, abra um prompt de comando e digite **dsquery server -hasfsmo schema**.
- **Mestre de nomeação de domínios** Controla a adição ou remoção de domínios de uma floresta. Para adicionar ou remover domínios, é preciso ter acesso ao mestre de nomeação de domínios. Para saber qual servidor é o mestre de nomeação de domínios atual para a floresta, abra um prompt de comando e digite **dsquery server -hasfsmo name**.

Essas funções de floresta devem ser exclusivas na floresta. Isso significa que você pode atribuir apenas um mestre de esquema e um mestre de nomeação de domínios em uma floresta.

Todos os domínios do Active Directory devem ter as seguintes funções:

- **Mestre de RID (ID relativo)** Atribui IDs relativos a controladores de domínio. Sempre que um objeto de usuário, grupo ou computador for criado, os controladores de domínio atribuem um ID de segurança (SID) exclusivo ao objeto. Cada SID consiste no prefixo do ID de segurança do domínio e de um ID relativo exclusivo alocado pelo mestre de RID. Para saber qual servidor é o mestre de RID atual para o domínio, abra um prompt de comando e digite **dsquery server -hasfsmo rid**.

- **Emulador PDC** Quando você utiliza operações de modo misto ou provisório, o emulador de PDC age como um PDC do Windows NT. Sua incumbência é autenticar logons do Windows NT, processar alterações de senha e replicar atualizações aos BDCs. O emulador de PDC é o servidor de horário padrão e, como tal, também realiza a sincronização de horário em um domínio. Para saber qual servidor é o emulador de PDC atual para o domínio, abra um prompt de comando e digite **dsquery server -hasfsmo pdc**.
- **Mestre de infraestrutura** Atualiza referências de objeto comparando seus dados de diretório com os dados de um catálogo global. Se os dados estiverem desatualizados, o mestre de infraestrutura solicita dados atualizados de um catálogo global e então replica as alterações aos outros controladores de domínio no domínio. Para saber qual servidor é o mestre de operações de infraestrutura atual para o domínio, abra um prompt de comando e digite **dsquery server -hasfsmo infr**.

Essas funções de domínio devem ser exclusivas em cada domínio. Isso significa que você pode atribuir apenas um mestre de RID, um emulador de PDC e um mestre de infraestrutura em cada domínio.

Geralmente, as funções de mestre de operações são atribuídas automaticamente, mas é possível reatribuí-las. Quando uma nova rede é instalada, todas as funções de mestre de operações são atribuídas ao primeiro controlador de domínio no primeiro domínio. Se mais tarde você criar um domínio-filho ou um domínio-pai em uma nova árvore, ao primeiro controlador de domínio no novo domínio também são atribuídas as funções de mestre de operações. Em um novo domínio, ao primeiro controlador de domínio são atribuídas todas as funções de mestre de operações. Se o novo domínio pertencer a uma floresta existente, as funções atribuídas são: mestre de RID, emulador de PDC e mestre de infraestrutura. As funções mestres de esquema e mestre de nomeação de domínios permanecem no primeiro domínio da floresta.

Quando um domínio possui apenas um controlador de domínio, esse computador controla todas as funções de mestre de operações. Se estiver trabalhando com apenas um site, as localizações padrão dos mestres de operações deve ser suficiente. Entretanto, conforme a adição de controladores de domínio e domínios, é recomendável transferir as funções de mestre de operações para outros controladores de domínio.

Quando um domínio possui dois ou mais controladores de domínio, deve-se configurar dois controladores de domínio para controlarem as funções de mestre de operações. Define-se que um dos controladores de domínio será o mestre de operações e que o outro será o mestre de operações em espera. O mestre de operações em espera pode ser utilizado caso o mestre principal falhe. Certifique-se de que os controladores de domínio são parceiros diretos de replicação e de que estão bem conectados.

Conforme a estrutura de domínio cresce, é recomendável separar as funções de mestre de operações e colocá-las em controladores de domínio diferentes. Isso pode melhorar a capacidade de resposta dos mestres de operações. Preste atenção especial às responsabilidades atuais do controlador de domínio que pretende utilizar.

PRÁTICAS RECOMENDADAS Duas funções que não devem ser separadas são o mestre de esquema e o mestre de nomeação de domínios. Sempre atribua essas funções ao mesmo controlador. Para operações mais eficientes, também recomenda-se deixar o mestre de RID e o emulador de PDC no mesmo servidor. Mas é possível separar essas duas funções se necessário. Por exemplo, em uma rede grande na qual picos de carga estejam causando problemas de desempenho, é recomendável colocar o mestre de RID e o emulador de PDC em controladores de domínio diferentes. Além disso, não deve-se colocar o mestre de infraestrutura em um controlador de domínio que esteja hospedando um catálogo global. Consulte “Os catálogos globais” anteriormente neste capítulo para mais detalhes.

Como utilizar a Lixeira do Active Directory

Quando sua floresta do Active Directory está operando no modo Windows Server 2008 R2 ou em modo superior, é possível utilizar a Lixeira do Active Directory (Active Directory Recycle Bin). A Lixeira do Active Directory adiciona um recurso de recuperação para objetos do Active Directory que é fácil de usar. Quando você habilita esse recurso, tanto atributos de valor vinculado quanto de valor não vinculado de um objeto excluído são preservados, possibilitando que você restaure o objeto para o mesmo estado no qual se encontrava antes de ser excluído. Você também pode restaurar objetos da lixeira sem ter que iniciar uma restauração autoritativa. Isso difere bastante da técnica disponível anteriormente, que utilizava uma restauração autoritativa para recuperar objetos excluídos do contêiner de objetos excluídos. Anteriormente, quando se deletava um objeto, a maior parte de seus atributos de valor não vinculado eram apagados e todos os atributos de valor vinculado eram removidos, ou seja, mesmo que os objetos excluídos pudessem ser recuperados, eles não podiam ser restaurados para seu estado anterior.

Como preparar o esquema para a lixeira

Antes de disponibilizar a lixeira, é preciso atualizar o esquema do Active Directory com os atributos necessários para que a lixeira funcione. Isso é feito preparando a floresta e o domínio para o nível funcional Windows Server 2008 R2 ou superior. Ao fazer isso, o esquema é atualizado e todos os objetos da floresta são atualizados com os atributos da lixeira. Após iniciado, esse processo é irreversível.

Após preparar o Active Directory, é preciso atualizar todos os controladores de domínio na sua floresta do Active Directory para Windows Server 2008 R2 ou superior e então aumentar os níveis funcionais de domínio e floresta para Windows Server 2008 R2 ou superior. Opcionalmente, você pode atualizar o esquema do Active Directory em sua floresta e domínios para Windows Server 2012 para habilitar a lixeira aprimorada.

Após essas operações, você pode habilitar e acessar a lixeira. Uma vez que a lixeira tenha sido habilitada, ela não pode ser desabilitada. Agora, quando um objeto do Active Directory for excluído, ele é colocado em um estado que chamamos de *logicamente excluído* e movido para o contêiner Deleted Objects, como mostra a Figura 6-7. Além disso, seu nome distinto (distinguished name) é alterado. Um objeto excluído permanece no contêiner Deleted Objects pelo período de tempo definido como valor de tempo de vida do objeto excluído, que é, por padrão, 180 dias.

MUNDO REAL O atributo *msDS-deletedObjectLifetime* substitui o atributo *tombstoneLifetime*. Entretanto, quando *msDS-deletedObjectLifetime* é definido como *\$null*, o valor de tempo de vida origina-se de *tombstoneLifetime*. Se *tombstoneLifetime* também estiver definido como *\$null*, o valor padrão é 180 dias.

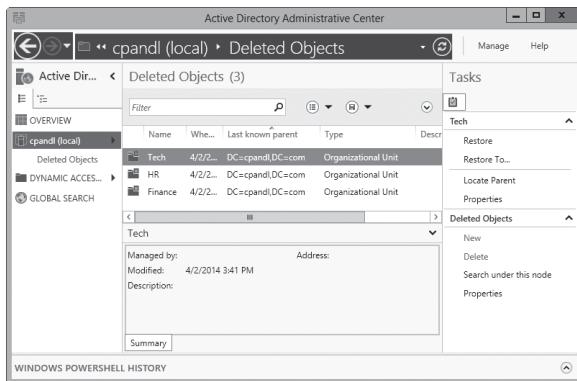


FIGURA 6-7 Objetos excluídos permanecem no contêiner Deleted Objects durante o tempo de vida do objeto.

Como recuperar objetos excluídos

Se escolher não utilizar a lixeira, você ainda pode recuperar objetos excluídos do contêiner Deleted Objects utilizando uma restauração autoritativa e outras técnicas que serão discutidas nesta seção. O procedimento é o mesmo das versões anteriores do Windows Server. A diferença é que os objetos são restaurados para seus estados anteriores com todos os atributos de valor vinculado e de valor não vinculado preservados. Para realizar uma restauração autoritativa, o controlador de domínio deve estar no Directory Services Restore Mode.

Em vez de utilizar uma restauração autoritativa e colocar um controlador de domínio offline, você pode recuperar objetos excluídos utilizando a ferramenta de administração Ldp.exe ou o cmdlets do Active Directory para o Windows PowerShell. Se tiver atualizado o esquema do Active Directory em sua floresta e domínios para Windows Server 2012, também pode habilitar a lixeira aprimorada, que possibilita a recuperação de objetos excluídos utilizando o Active Directory Administrative Center.

Lembre-se de que o Active Directory bloqueia o acesso a um objeto durante um curto intervalo de tempo após sua exclusão. Durante esse tempo, o Active Directory processa a tabela de valor vinculado do objeto para manter a integridade referencial no atributo de valor vinculado. Então, o Active Directory libera o acesso ao objeto excluído.

Como utilizar o Ldp.exe para recuperação básica

Pode-se utilizar o Ldp.exe para exibir o contêiner Deleted Objects e recuperar um objeto excluído seguindo estas etapas:

1. Digite **Ldp.exe** na caixa Apps Search e pressione Enter.
2. No menu Options, toque ou clique em Controls. Na caixa de diálogo Controls, selecione Return Deleted Objects na lista Load Predefined e toque ou clique em OK.
3. Conecte-se a um servidor que esteja no domínio-raiz da floresta escolhendo Bind a partir do menu Connection. Selecione o tipo de Bind e toque ou clique em OK.
4. No menu View, toque ou clique em Tree. Na caixa de diálogo Tree View, utilize a lista BaseDN para selecionar o nome de domínio-raiz da floresta adequado, como DC=Cpndl,DC=Com, e toque ou clique em OK.
5. Na árvore de console, dê um toque duplo ou clique duas vezes no nome distinto da raiz e localize o contêiner CN=Deleted Objects.
6. Localize, pressione e mantenha pressionado ou clique com o botão direito do mouse no objeto do Active Directory que deseja restaurar; toque ou clique em Modify. A caixa de diálogo Modify é exibida.
7. Na caixa de texto Edit Entry Attribute, digite **isDeleted**. Não digite nada na caixa de texto Values.
8. Sob Operation, toque ou clique em Delete depois em Enter.
9. Na caixa de texto Edit Entry Attribute, digite **distinguishedName**. Em Values, digite o nome distinto original deste objeto do Active Directory.
10. Sob Operation, toque ou clique em Replace. Selecione a caixa de seleção Extended, toque ou clique em Enter e depois em Run.

Como utilizar o Windows PowerShell para recuperação básica e avançada

Os cmdlets do Active Directory para o Windows PowerShell permitem que você recupere objetos excluídos utilizando scripts ou digitando comandos em um prompt do PowerShell. Use Get-ADObject para recuperar o objeto ou os objetos que deseja restaurar, passe este objeto ou objeto para Restore-ADObject e então o Restore-ADObject restaura o objeto ou objetos para o banco de dados do diretório.

OBSERVAÇÃO Por padrão, o módulo do Active Directory não é importado para o Windows PowerShell. Importe o módulo do Active Directory digitando **import-module activedirectory** no prompt do PowerShell. Para mais informações, consulte “Active Directory Administrative Center e Windows PowerShell” no Capítulo 7.

Para utilizar o cmdlet do Active Directory para recuperação, é preciso abrir um prompt do PowerShell elevado para administração pressionando e segurando ou clicando com o botão direito do mouse na entrada do Windows PowerShell no menu ou tocando ou clicando em Run As Administrator. A sintaxe básica para recuperar um objeto é a seguinte:

```
Get-ADObject -Filter {ObjectId} -IncludeDeletedObjects | Restore-ADObject
```

ObjectId é um valor de filtro que identifica o objeto que deseja restaurar. Por exemplo, você pode restaurar uma conta de usuário excluída através do nome de exibição ou nome de conta SAM como mostram estes exemplos:

```
Get-ADObject -Filter {DisplayName -eq "Rich Tuppy"}  
-IncludeDeletedObjects | Restore-ADObject
```

```
Get-ADObject -Filter {SamAccountName -eq "richt"}  
-IncludeDeletedObjects | Restore-ADObject
```

Observe que os objetos aninhados devem ser recuperados do mais alto nível da hierarquia excluída para um contêiner-pai ativo. Por exemplo, se você excluir acidentalmente uma OU e todas suas contas relacionadas, precisa restaurar a OU antes de restaurar as contas relacionadas.

A sintaxe básica para restaurar objetos contêineres como uma OU é a seguinte:

```
Get-ADObject -ldapFilter:"(msDS-LastKnownRDN=ContainerID)"  
-IncludeDeletedObjects | Restore-ADObject
```

ContainerID é um valor de filtro que identifica o objeto contêiner que deseja restaurar. Por exemplo, você pode restaurar a OU Corporate Services como mostra este exemplo:

```
Get-ADObject -ldapFilter:"(msDS-LastKnownRDN=Corporate_Services)"  
-IncludeDeletedObjects | Restore-ADObject
```

Se a OU contiver contas que você também deseja restaurar, é possível restaurar as contas utilizando a técnica discutida anteriormente, ou restaurar todas as contas ao mesmo tempo. A sintaxe básica exige que você estabeleça uma base de pesquisa e que associe as contas com seu último pai conhecido, como é mostrado a seguir:

```
Get-ADObject -SearchBase "CN=Deleted Objects,ForestRootDN" -Filter  
{lastKnownParent -eq "ContainerCN,ForestRootDN"} -IncludeDeletedObjects |  
Restore-ADObject
```

ForestRootDN é o nome distinto do domínio-raiz da floresta, como DC=Cpand1,DC=Com, e *ContainerCN* é o nome comum do contêiner, como OU=Corporate_Services ou CN=Users. O exemplo a seguir restaura todas as contas que estavam na OU Corporate Services quando ela foi excluída:

```
Get-ADObject -SearchBase "CN=Deleted Objects,DC=Cpand1,DC=com" -Filter  
{lastKnownParent -eq "OU=Corporate_Services,DC=Cpand1,DC=com"}  
-IncludeDeletedObjects | Restore-ADObject
```

Como utilizar a lixeira aprimorada para recuperação

A lixeira aprimorada torna a recuperação de objetos excluídos fácil a ponto de não precisar apenas um clique ou toque. Após ter atualizado o esquema do Active Directory em sua floresta e domínios para Windows Server 2012, é possível habilitar a lixeira aprimorada para uso seguindo estas etapas:

1. No Active Directory Administrative Center, por padrão, o domínio local é aberto para gerenciamento. Se quiser trabalhar com outro domínio, toque ou clique em Manage e depois em Add Navigation Nodes. Na caixa de diálogo Add Navigation Nodes, selecione o domínio desejado e toque ou clique em OK.

2. Selecione o domínio desejado tocando ou clicando nessa opção no painel esquerdo. No painel Task, toque ou clique em Enable Recycle Bin e depois em OK na caixa de diálogo para confirmação.
3. O Active Directory começará a replicar a alteração para todos os controladores de domínio na floresta. Quando a alteração tiver sido replicada, a lixeira aprimorada estará disponível para uso. Se você tocar ou clicar em Refresh no Active Directory Administrative Center, verá que um contêiner Deleted Objects está agora disponível para domínios que utilizem a lixeira aprimorada.

Lembre-se de que a lixeira aprimorada é uma opção para nível de floresta. Quando você habilita essa opção em um domínio da floresta, o Active Directory replica a alteração para todos os controladores de domínio em todos os domínios da floresta.

Com a lixeira aprimorada habilitada, é possível recuperar objetos excluídos com facilidade. No Active Directory Administrative Center, os domínios que estiverem utilizando a lixeira aprimorada terão um contêiner Deleted Objects. Nesse contêiner, há uma lista de objetos excluídos. Como discutido anteriormente, objetos excluídos permanecem nesse contêiner durante o tempo de vida do objeto, que é, por padrão, 180 dias.

Cada objeto excluído é listado por nome, momento de exclusão, último pai conhecido e tipo. Quando você seleciona um objeto excluído tocando ou clicando nele, pode utilizar as opções no painel Task para trabalhar com ele. A opção Restore restaura o objeto para seu contêiner original. Por exemplo, se o objeto tiver sido excluído do contêiner Users, será restaurado para esse contêiner.

A opção Restore To restaura o objeto para um contêiner diferente dentro do domínio original ou dentro de outro domínio da mesma floresta. Especifique o contêiner na caixa de diálogo Restore To. Por exemplo, se o objeto tiver sido excluído do contêiner Users no domínio tech.cpndl.com, você poderia restaurá-lo para a OU Devs no domínio eng.cpndl.com.

CAPÍTULO 7

Administração básica do Active Directory

- Ferramentas para o gerenciamento do Active Directory **247**
- Gerenciamento de contas de computador **257**
- Gerenciamento de controladores de domínio, funções e catálogo **268**
- Gerenciamento de unidades organizacionais **279**
- Gerenciamento de sites **280**
- Manutenção do Active Directory **287**
- Solução de problemas do Active Directory **290**

A administração básica do Active Directory concentra-se em tarefas-chave que você realiza rotineiramente no Active Directory Domain Services (AD DS, Serviços de Domínio do Active Directory), como a criação de contas de computador ou o ingresso de computadores em um domínio. Neste capítulo, você aprenderá sobre as ferramentas usadas no gerenciamento do Active Directory, bem como técnicas específicas para o gerenciamento de computadores, controladores de domínio e unidades organizacionais (OUs).

Ferramentas para o gerenciamento do Active Directory

Existem vários conjuntos de ferramentas disponíveis para o gerenciamento do Active Directory, incluindo ferramentas de administração gráfica, ferramentas de linha de comando, ferramentas de suporte e cmdlets do Microsoft Windows PowerShell.

Ferramentas administrativas do Active Directory

As ferramentas administrativas do Active Directory são oferecidas na forma de snap-ins para o Microsoft Management Console (MMC, Console de Gerenciamento Microsoft). Para gerenciar o Active Directory, utilizam-se as seguintes ferramentas-chave:

- **Active Directory Administrative Center** Para realizar tarefas de gerenciamento.
- **Active Directory Domains And Trusts** Para trabalhar com domínios, árvores de domínio e florestas.
- **Active Directory Module For Windows PowerShell** Para gerenciar o Active Directory trabalhando com o Windows PowerShell.
- **Active Directory Sites And Services** Para gerenciar sites e sub-redes.

- **Active Directory Users And Computers** Para gerenciar usuários, grupos, computadores e OUs.
- **Group Policy Management** Para gerenciar a forma como a Group Policy (Política de Grupo) é usada na organização. Dá acesso ao Resultant Set of Policy (RSOP, conjunto de políticas resultante) para planejamento e registro em log.

ALERTA DE SEGURANÇA O Windows Firewall pode afetar a administração remota com alguns snap-ins do MMC. Se o Windows Firewall estiver habilitado em um computador remoto e você receber uma mensagem de erro afirmado que você não tem a permissão adequada, que o caminho de rede não foi encontrado ou que o acesso foi negado, pode ser necessário configurar uma exceção no computador remoto para a entrada de porta TCP 445. Para solucionar esse problema, habilite a exceção Windows Firewall: Allow Remote Administration Exception em Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile. Outra opção é digitar em um prompt de comando no computador remoto: `netsh firewall set portopening tcp 445 smb enable`. Para mais detalhes, veja o artigo na Base de Dados de Conhecimento Microsoft (em Inglês) 840634 (support.microsoft.com/default.aspx?scid=kb;en-us;840634).

As ferramentas administrativas do Active Directory podem ser acessadas a partir do menu Tools no Server Manager ou adicionadas à qualquer MMC que possa ser atualizado. Caso esteja usando outro computador com acesso ao domínio do Windows Server, será preciso instalar as ferramentas para que elas fiquem disponíveis para uso. Uma técnica para realizar essa instalação é utilizar o Add Roles And Features Wizard (Assistente de Adição de Funções e Recursos) para adicionar Remote Server Administration Tools (Ferramentas de Administração de Servidor Remoto) para AD DS.

Ferramentas de linha de comando do Active Directory

Existem diversas ferramentas que permitem o gerenciamento do Active Directory a partir da linha de comando:

- **Adprep** Permite que você prepare manualmente uma floresta ou domínio do Windows para a instalação de controladores de domínio do Windows (DCs). Para preparar uma floresta ou um domínio, utilize **adprep /forestprep** e **adprep /domainprep**, respectivamente. Se você pretende instalar algum controlador de domínio somente leitura (RODC), também deve executar **adprep /rodcprep** para a floresta.

MUNDO REAL Como foi discutido no Capítulo 6, “Como utilizar o Active Directory,” o Server Manager para Windows Server 2012 prepara florestas e domínios automaticamente. Para isso, é necessário que você utilize uma conta com as permissões apropriadas. Para que a preparação de florestas e RODC seja bem-sucedida, é preciso usar uma conta de administrador que seja membro do grupo Enterprise Admins (Administradores de Empresa), Schema Admins (Administradores de Esquema) ou Domain Admins (Administradores de Domínio) no domínio-raiz da floresta. Para que a preparação de domínio seja bem-sucedida, é preciso usar uma conta que seja membro do grupo Domain Admins em um domínio aplicável.

Pode-se executar o Adprep em qualquer servidor com uma versão de 64 bits do Windows Server 2008 ou posterior. O servidor precisa de conectividade de rede ao mestre de esquema para a floresta e ao mestre de infraestrutura do domínio onde deseja adicionar o controlador de domínio. Se algum desses mestres de operação estiver com o Windows Server 2003, o servidor em que você está executando o Adprep deve estar conectado ao domínio e não será possível usar credenciais de cartão inteligente.

- **Dsadd** Adiciona computadores, contatos, grupos, OUs e usuários ao Active Directory. Digite **dsadd objectname /?** em um prompt de comando para exibir informações de ajuda sobre o uso do comando, como por exemplo: **dsadd computer /?**.
- **Dsget** Exibe propriedades de computadores, contatos, grupos, OUs, usuários, sites, sub-redes e servidores registrados no Active Directory. Digite **dsget objectname /?** em um prompt de comando para exibir informações de ajuda sobre o uso do comando, como por exemplo: **dsget subnet /?**.
- **Dsmod** Modifica propriedades de computadores, contatos, grupos, OUs, usuários e servidores existentes no Active Directory. Digite **dsmod objectname /?** em um prompt de comando para exibir informações de ajuda sobre o uso do comando, como por exemplo: **dsmod server /?**.
- **Dsmove** Move um único objeto para um novo local dentro de um único domínio ou renomeia o objeto sem movê-lo. Digite **dsmove /?** em um prompt de comando para exibir informações de ajuda sobre o uso do comando.
- **Dsquery** Utiliza critérios de busca para localizar computadores, contatos, grupos, OUs, usuários, sites, sub-redes e servidores no Active Directory. Digite **dsquery /?** em um prompt de comando para exibir informações de ajuda sobre o uso do comando.
- **Dsrm** Remove objetos do Active Directory. Digite **dsrm /?** em um prompt de comando para exibir informações de ajuda sobre o uso do comando.
- **Ntdsutil** Permite que o usuário visualize informações de site, domínio e servidor, gerencie mestres de operações e realize a manutenção do banco de dados do Active Directory. Digite **ntdsutil /?** em um prompt de comando para exibir informações de ajuda sobre o uso do comando.

O Adprep encontra-se na pasta \support\adprep da mídia de instalação do Windows Server 2012. As outras ferramentas são disponibilizadas quando você instala Remote Server Management Tools para AD DS.

Ferramentas de suporte do Active Directory

Diversas ferramentas de suporte para o Active Directory estão inclusas nas ferramentas de gerenciamento do AD DS. A Tabela 7-1 lista algumas das ferramentas de suporte mais úteis para configuração, gerenciamento e solução de problemas do Active Directory.

TABELA 7-1 Guia de Referência Rápida para ferramentas de suporte do Active Directory

FERRAMENTA DE SUPORTE	NOME DO EXECUTÁVEL	DESCRIÇÃO
ADSI Edit	Adsiedit.msc	Abre e edita a Active Directory Service Interface (Interface de Serviços do Active Directory) para os contêineres de domínio, esquema e configuração
Active Directory Administration Tool	Ldp.exe	Realiza operações do Lightweight Directory Access Protocol (protocolo LDAP) no Active Directory
Directory Services Access Control Lists Utility	Dsacls.exe	Gerencia listas de controle de acesso (ACLs) a objetos do Active Directory
Distributed File System Utility	Dfsutil.exe	Gerencia o Distributed File System (DFS, Sistema de Arquivos Distribuído) e exibe as informações do DFS
DNS Server Troubleshooting Tool	Dnscmd.exe	Gerencia propriedades de servidores, zonas e registros de recurso do Domain Name System (DNS, Sistema de Nomes de Domínio)
Replication Diagnostics Tool	Repadmin.exe	Gerencia e monitora a replicação usando a linha de comando
Windows Domain Manager	Netdom.exe	Permite o gerenciamento de domínios e relações de confiança na linha de comando

Como utilizar o Active Directory Users And Computers

Uma das principais ferramentas de administração que você utiliza para gerenciar o Active Directory é o utilitário Active Directory Users And Computers (Usuários e Computadores do Active Directory). Com esse utilitário, pode-se controlar e realizar tarefas em todos os usuários, grupos e computadores, além de gerenciar as OUs.

Para iniciar o Active Directory Users And Computers, selecione a opção referente no menu Tools do Server Manager. O Active Directory Users And Computers também pode ser adicionado como um snap-in em qualquer console que possa ser atualizado. Por padrão, o utilitário Active Directory Users And Computers trabalha com o domínio ao qual o seu computador está conectado no momento.

Pode-se acessar objetos de computador e usuário nesse domínio com a árvore de console, como mostra a Figura 7-1. Se você não encontrar um controlador de domínio ou se o domínio com o qual você deseja trabalhar não for exibido, pode ser preciso conectar-se a um controlador de domínio no domínio atual ou a um controlador de domínio em um domínio diferente. Entre as outras tarefas de alto nível realizadas com o Active Directory Users And Computers, podemos citar a visualização de opções avançadas e a consulta por objetos.

Ao acessar um domínio no Active Directory Users And Computers você verá as seguintes pastas padrão:

- **Builtin** A lista de contas de usuário e grupos internos.
- **Computers** O contêiner padrão para contas de computador.

- **Domain Controllers** O contêiner padrão para controladores de domínio.
- **ForeignSecurityPrincipals** Contém informações sobre objetos de um domínio externo confiável. Normalmente, esses objetos são criados quando um objeto de um domínio externo é adicionado a um grupo no domínio atual.
- **Managed Service Accounts** O contêiner padrão para contas de serviço gerenciado.
- **Microsoft Exchange Security Groups** O contêiner padrão para grupos usado pelo Microsoft Exchange Server. Essa pasta só é listada se o Exchange Server estiver sendo executado no ambiente.
- **Saved Queries** Contém critérios de pesquisas salvas para possibilitar a realização rápida de pesquisas feitas anteriormente no Active Directory.
- **Users** O contêiner padrão para usuários.

O Active Directory Users And Computers possui opções avançadas que por padrão não são exibidas. Para acessar essas opções, toque ou clique em View e selecione Advanced Features. Você verá as seguintes pastas adicionais:

- **LostAndFound** Contém objetos órfãos. Eles podem ser excluídos ou recuperados.
- **NTDS Quotas** Contém dados de cota do serviço de diretório.
- **Program Data** Contém dados armazenados no Active Directory para aplicativos Microsoft.
- **System** Contém configurações internas do sistema.
- **TPM Devices** Lista os dispositivos com informações de proprietário de Trusted Platform Module (TPM) armazenadas no Active Directory.

Também é possível adicionar pastas de OUs. A Figura 7-1 mostra várias OUs criadas pelo administrador no domínio cpandl.com. Isso inclui: Corporate PCs, CustServices, Development, Engineering, Finance, HR, LostAndfound, Managed Service Accounts, Program Data, System, Tech, Users, NTDS Quotas e TPM Devices.

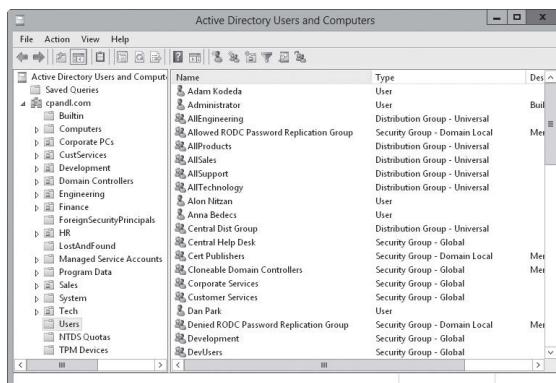


FIGURA 7-1 Ao trabalhar com o Active Directory Users And Computers, você pode acessar objetos de computador e de usuários na árvore de console.

Por padrão, você está conectado ao domínio local e ao primeiro controlador de domínio que responder à sua solicitação. Você pode trabalhar com qualquer domínio na floresta, desde que tenha as permissões de acesso apropriadas. Para isso, conecte-se ao domínio seguindo estas etapas:

1. Na árvore de console, pressione e mantenha pressionado ou clique com o botão direito do mouse em Active Directory Users And Computers e depois toque ou clique em Change Domain.
2. A caixa de diálogo Change Domain exibe o domínio atual (ou o domínio padrão). Digite um novo nome de domínio ou toque ou clique que em Browse, selecione um domínio na caixa de diálogo Browse For Domain e toque ou clique em OK.
3. Se deseja usar esse domínio sempre que estiver trabalhando com o Active Directory Users And Computers, selecione a caixa de seleção Save This Domain Setting For The Current Console e toque ou clique em OK. Caso contrário, apenas toque ou clique em OK.

Se não houver objeto disponível ao iniciar o Active Directory Users And Computers, pode ser que você não esteja conectado a um domínio ou que não foi possível encontrar um controlador de domínio. É preciso conectar-se a um controlador de domínio para acessar objetos de usuário, grupo e computador. Para se conectar a um controlador de domínio, siga as etapas:

1. Na árvore de console, pressione e mantenha pressionado ou clique com o botão direito do mouse em Active Directory Users And Computers e depois toque ou clique em Change Domain Controller. Você verá o domínio atual e o controlador de domínio com o qual você está trabalhando na caixa de diálogo Change Directory Server.
2. A lista Change To exibe os controladores disponíveis no domínio. A seleção padrão é Any Writable Domain Controller. Se você selecionar essa opção, será conectado ao primeiro controlador de domínio que responder à sua solicitação. Senão, escolha um controlador de domínio específico ao qual deseja se conectar.
3. Se deseja usar esse controlador de domínio sempre que estiver trabalhando com o Active Directory Users And Computers, selecione a caixa de seleção Save This Setting For The Current Console e toque ou clique em OK. Caso contrário, apenas toque ou clique em OK.

OBSERVAÇÃO A caixa de diálogo Change Directory Server também exibe o site associado com o controlador de domínio, bem como o tipo, a versão e o status do controlador de domínio. Se o tipo do controlador de domínio estiver classificado como GC, esse controlador de domínio também hospeda o catálogo global.

Você também pode se conectar a um controlador de domínio específico para solução de problemas. Se você desconfia que a replicação não está funcionando corretamente, por exemplo, pode inspecionar os objetos em um controlador específico. Uma vez conectado, procure por discrepâncias em objetos que foram atualizados recentemente.

O Active Directory Users And Computers possui um recurso de pesquisa interno para localizar contas, recursos compartilhados e outros objetos de diretório. Pode-se pesquisar facilmente no domínio atual, em um domínio específico ou em todo o diretório.

Para pesquisar por objetos de diretório, siga as etapas:

1. Na árvore de console, pressione e mantenha pressionado ou clique com o botão direito do mouse sobre o domínio atual ou sobre o contêiner específico no qual você quer pesquisar. Depois, toque ou clique em Find. Isso abrirá uma caixa de diálogo Find similar à mostrada na Figura 7-2.

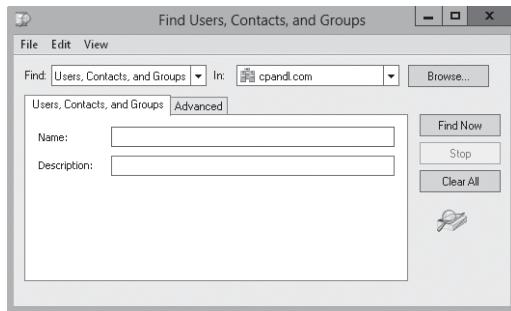


FIGURA 7-2 Na caixa de diálogo Find pode-se pesquisar por recursos do Active Directory.

2. Na lista Find, selecione o tipo de pesquisa desejado. As opções são as seguintes:
 - **Users, Contacts, And Groups** Pesquise por usuários e contas de grupo, bem como por contatos listados no serviço de diretório.
 - **Computers** Pesquise contas de computador por tipo, nome e proprietário.
 - **Printers** Pesquise impressoras por nome, modelo e recursos.
 - **Shared Folders** Procure pastas compartilhadas por nome ou palavra-chave.
 - **Organizational Units** Procure unidades organizacionais por nome.
 - **Custom Search** Realize uma pesquisa avançada ou consulta LDAP.
 - **Common Queries** Permite que você pesquise rapidamente por nomes de contas, descrições de contas, contas desativadas, senhas que nunca expiram e dias desde o último logon.
3. Utilizando a lista In, selecione o local em que deseja pesquisar. Caso tenha selecionado um contêiner na etapa 2, como por exemplo Computers, esse contêiner está selecionado por padrão. Para pesquisar todos os objetos no diretório, toque ou clique em Entire Directory.
4. Insira os seus parâmetros de pesquisa e toque ou clique em Find Now. Como mostra a Figura 7-3, qualquer entrada correspondente será exibida nos resultados da pesquisa. Dê um toque duplo ou clique duas vezes em um objeto para visualizar ou alterar as suas configurações de propriedade. Pressione e mantenha pressionado ou clique com o botão direito do mouse em um objeto para exibir um menu de atalho de opções de gerenciamento do objeto.

OBSERVAÇÃO O tipo de pesquisa determina quais caixas de texto e quais guias estarão disponíveis na caixa de diálogo Find. Na maioria dos casos, basta digitar o nome do objeto que você procura na caixa de texto Name, mas existem outras opções de pesquisa disponíveis. Com impressoras, por exemplo, pode-se pesquisar por uma impressora colorida, uma impressora que imprima frente e verso, uma impressora que grampeie folhas, entre outras.

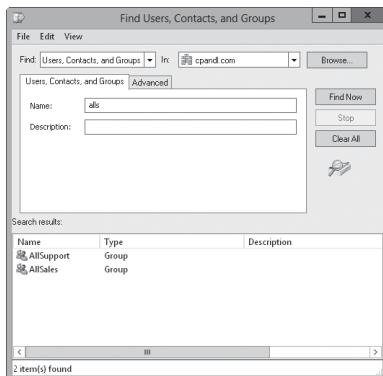


FIGURA 7-3 Os objetos que correspondem aos critérios de pesquisa são exibidos nos resultados da pesquisa. Para gerenciar os objetos, pressione e mantenha pressionadas ou clique com o botão direito do mouse nas entradas.

Active Directory Administrative Center e Windows PowerShell

O Active Directory Administrative Center (Centro Administrativo do Active Directory), mostrado na Figura 7-4, oferece uma interface orientada a tarefas para o gerenciamento do Active Directory. Para iniciar essa ferramenta, selecione a opção referente no menu Tools do Server Manager. Essa ferramenta pode ser usada para realizar muitas tarefas comuns, como:

- Conectar-se a um ou mais domínios
- Criar e gerenciar contas de usuário, grupos e OUs
- Criar e gerenciar objetos de configuração de senha
- Realizar pesquisas globais no Active Directory
- Elevar os níveis funcionais de floresta e domínio
- Recuperar objetos excluídos a partir da Lixeira do Active Directory (Recycle Bin)

O Active Directory Administrative Center está instalado por padrão no Windows Server 2012 e está disponível em computadores cliente ao instalar Remote Server Administration Tools (RSAT, Ferramentas de Administração de Servidor Remoto). Essa ferramenta utiliza o Windows PowerShell para realizar tarefas administrativas e depende do Microsoft .NET Framework. Ambos os recursos devem ser instalados e devidamente configurados para que você possa usar o Active Directory Administrative Center.

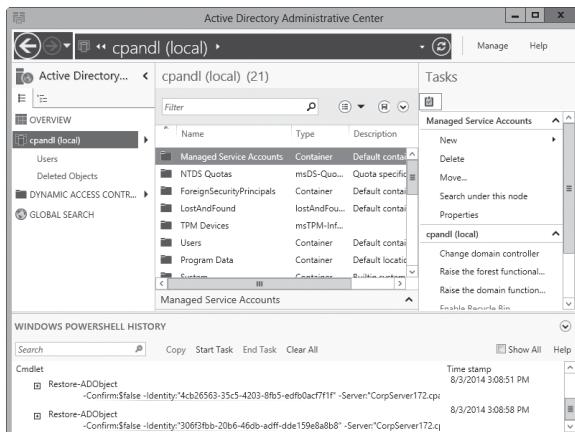


FIGURA 7-4 Realize o gerenciamento orientado a tarefas do Active Directory.

No Active Directory Administrative Center o domínio local é aberto para gerenciamento por padrão. Se quiser trabalhar com outro domínio, toque ou clique em Manage e depois em Add Navigation Nodes. Na caixa de diálogo Add Navigation Nodes, selecione o domínio desejado e toque ou clique em OK. Depois disso, pode-se tocar ou clicar em um domínio no painel esquerdo para selecioná-lo.

Por padrão, você está conectado ao primeiro controlador de domínio que respondeu à sua solicitação. Para a solução de problemas de replicação, pode ser desejável conectar-se a um controlador de domínio específico. Uma vez conectado, você pode inspecionar os objetos naquele controlador e procurar discrepâncias em objetos que foram atualizados recentemente. Para se conectar a um controlador de domínio específico, toque ou clique no nó de domínio no painel esquerdo e depois em Change Domain Controller.

Na caixa de diálogo Change Domain Controller você verá o domínio e o controlador de domínio com os quais você está trabalhando no momento, como mostra a Figura 7-5. Selecione o controlador de domínio a ser usado e toque ou clique em Change.

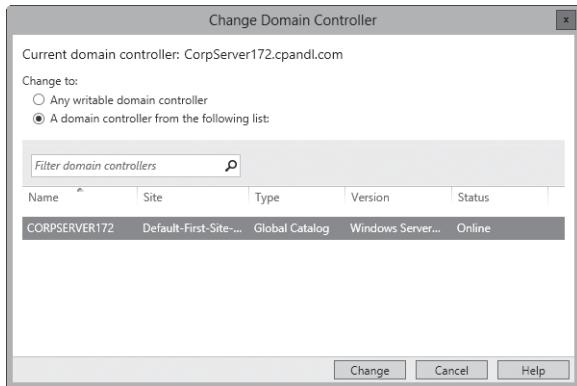


FIGURA 7-5 Altere o controlador de domínio.

Como o Active Directory Users And Computers, o Active Directory Administrative Center possui recursos de pesquisa internos que podem ser usados para localizar objetos no diretório. O mais básico deles é o filtro de pesquisa, que está disponível quando você seleciona um contêiner do diretório no painel esquerdo.

Com o filtro de pesquisa pode-se localizar rapidamente objetos de nível de contêiner dentro de um domínio ou uma OU filha dentro de uma OU selecionada. Ao selecionar um nó de domínio no painel esquerdo, pode-se usar o filtro para localizar rapidamente OUs de nível superior ou contêineres internos que iniciem com as letras ou palavras que você inseriu no filtro. Por exemplo: você poderia selecionar o nó de domínio no painel esquerdo e depois inserir **sa** na caixa Filter para encontrar OUs de nível superior que começem com as letras “sa”, como em *Sales*. Dessa maneira, uma pesquisa não incluiria OUs filhas ou sub-contêineres. Não seriam inclusas, portanto, as OUs *SalesVT* ou *SalesCA*, que são OUs filhas de *Sales*.

Ao selecionar um contêiner específico, pode-se pesquisar dentro daquele contêiner utilizando a mesma técnica de filtragem. Ao selecionar o nó Global Search, pode-se pesquisar os nomes de todos os objetos de nível de contêiner, bem como usuários, grupos, computadores e assim por diante, para o nó do contêiner selecionado no momento.

Em pesquisas globais, é possível alterar o nó do contêiner associado. Para isso, toque ou clique em Scope e depois selecione o nó que será usado. Selecione o Global Catalog Search como nó para pesquisar objetos não padrão, como atributos no esquema, especificadores de exibição, transportes entre sites e classes no esquema.

MUNDO REAL Tecnicamente, o filtro é baseado na cadeia inicial de qualquer parte do nome de um objeto. Para grupos, isso significa que o nome do grupo e o nome de conta Security Accounts Manager (SAM, Gerente de Contas de Segurança) do grupo estão inclusos. Para usuários, isso significa que o primeiro nome, o sobrenome, o nome completo, o universal principal name (nome UPN) e o nome de conta SAM do usuário estão inclusos.

Além disso, o Active Directory Administrative Center utiliza serviços Web fornecidos por Active Directory Web Services (ADWS, Serviços Web do Active Directory). Ao menos um dos controladores de domínio em cada um dos domínios do Active Directory que você quer gerenciar precisa ter instalado o ADWS e os serviços referentes. As conexões são feitas através da porta TCP 9389 por padrão e as políticas de firewall devem habilitar uma exceção nessa porta para ADWS.

Pode-se também trabalhar com o Active Directory usando o módulo Active Directory para o Windows PowerShell. Quando você seleciona a opção referente no menu Tools do Server Manager, o módulo é importado automaticamente. Caso contrário, esse módulo não é importado para o Windows PowerShell por padrão, sendo preciso importá-lo antes de trabalhar com os cmdlets do Active Directory.

No prompt do Windows PowerShell, digite **Import-Module ActiveDirectory** para importar o módulo Active Directory. Uma vez que o módulo tenha sido importado, ele pode ser usado na sessão sendo executada no Windows PowerShell no momento. Na próxima vez que você inicializar o Windows PowerShell, será preciso importar o módulo novamente se desejar usar os recursos que ele oferece. Uma outra forma é selecionar a opção Active Directory Module For Windows PowerShell no menu Tools do Server Manager para importar o módulo quando o Windows PowerShell for iniciado.

Para listar todos os cmdlets disponíveis, insira **get-command** no prompt do Windows PowerShell. Utilize Get-Help para mais informações sobre o uso de cmdlets. Insira **get-help *-*** para obter uma lista de todos os cmdlets, incluindo uma sinopse da finalidade de cada cmdlet. Para obter documentação de ajuda sobre um cmdlet específico, digite **get-help** seguido pelo nome do cmdlet. Estão disponíveis dezenas de cmdlets para o Active Directory. Para uma lista dos mais usados, digite **get-help *-ad*** no prompt do Windows PowerShell.

OBSERVAÇÃO O módulo Active Directory para o Windows PowerShell está instalado por padrão no Windows Server 2012. Para computadores cliente, ele está disponível quando se instala Remote Server Administration Tools e seleciona-se as opções referentes. O Windows PowerShell depende do .NET Framework e do Windows Remote Management (WinRM) para realizar tarefas administrativas.

Gerenciamento de contas de computador

As contas de computador são armazenadas como objetos no Active Directory, sendo utilizadas para controlar o acesso à rede e aos seus recursos. É possível adicionar contas de computador a qualquer contêiner padrão exibido em Active Directory Users And Computers. As pastas mais adequadas para esse caso são Computers, Domain Controllers e qualquer OU que você tenha criado.

Criação de contas de computador para uma estação de trabalho ou servidor

A maneira mais simples de criar uma conta de computador é realizar o logon no computador que deseja configurar e ingressar em um domínio, como será descrito mais adiante neste capítulo em "Como ingressar um computador em um domínio ou grupo de trabalho". Ao fazer isso, a conta de computador necessária é criada automaticamente e colocada na pasta Computers ou na pasta Domain Controllers, conforme for

apropriado. Você também pode criar uma conta de computador em Active Directory Users And Computers ou em Active Directory Administrative Center antes de tentar conectar o computador.

Criação de contas de computador no Active Directory Administrative Center

Com o Active Directory Administrative Center é possível criar uma conta de computador padrão, adicionar a conta como um membro de grupos específicos e definir propriedades quanto ao gerente do computador. Para isso, siga estas etapas:

1. Na árvore de console do Active Directory Administrative Center, pressione e mantenha pressionado ou clique com o botão direito do mouse sobre o contêiner em que você deseja colocar a conta de computador. Toque ou clique em New e depois em Computer. Isso abre a caixa de diálogo Create Computer, mostrada na Figura 7-6.



FIGURA 7-6 Crie novas contas de computador e defina as propriedades de gerentes e membros.

2. Insira o nome do computador.
3. Por padrão, apenas membros do Domain Admins podem ingressar este computador ao domínio. Para permitir que um usuário ou um grupo diferente ingresse o computador ao domínio, toque ou clique em Change e depois selecione um usuário ou conta de grupo na caixa de diálogo Select User Or Group.

OBSERVAÇÃO Pode-se selecionar qualquer usuário ou conta de grupo existente. Isso permite que você delegue a autoridade para ingressar esta conta de computador ao domínio.

4. Se esta conta será usada com aplicativos escritos para sistemas operacionais herdados, selecione Assign This Computer Account As A Pre-Windows 2000 Computer.
5. Opcionalmente, selecione Protect From Accidental Deletion para marcar a conta como protegida no Active Directory. As contas protegidas só podem ser excluídas se você remover o sinalizador Protect antes de tentar excluí-las.
6. Se desejar, designe uma entidade de segurança como gerente do computador. Para isso, toque ou clique em Edit sob Manage By e selecione um usuário ou grupo para ser designado gerente na caixa de diálogo Select User Or Group. A designação do gerente do computador depende de políticas corporativas, podendo incluir o usuário principal do computador, um gerente de uma filial em um escritório particular ou um contato de apoio.
7. A conta de computador é adicionada automaticamente ao grupo de computadores padrão apropriado. Normalmente, é o grupo Domain Computers. Para adicionar a conta de computador a outros grupos, toque ou clique em Add sob Member Of e depois utilize a caixa de diálogo Select Groups para definir os grupos aos quais deva pertencer a conta de computador.
8. Toque ou clique em OK para criar a conta de computador.

Criação de contas de computador no Active Directory Users And Computers

Dois tipos de contas de computadores podem ser criadas: contas de computador padrão e contas de computador gerenciado. As contas de computador gerenciado estão disponíveis quando você instala o Windows Deployment Services (Serviços de Implantação do Windows) no seu domínio.

Para criar uma conta de computador padrão através do Active Directory Users And Computers, siga as etapas:

1. Na árvore de console do Active Directory Users And Computers, pressione e mantenha pressionado ou clique com o botão direito do mouse no contêiner em que você deseja colocar a conta de computador. Toque ou clique em New e depois em Computer. Isso inicia o New Object – Computer Wizard, mostrado na Figura 7-7.

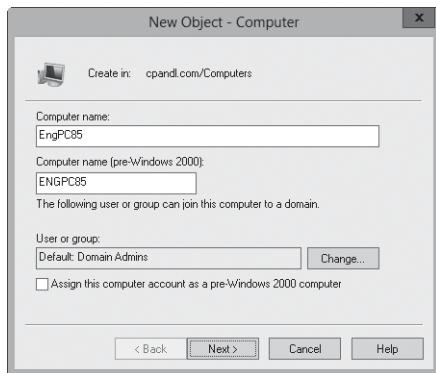


FIGURA 7-7 Crie novas contas de computador usando o New Object–Computer Wizard.

2. Insira o nome do computador.
 3. Por padrão, apenas membros do Domain Admins podem ingressar este computador ao domínio. Para permitir que um usuário ou um grupo diferente ingresse o computador ao domínio, toque ou clique em Change e depois selecione um usuário ou uma conta de grupo na caixa de diálogo Select User Or Group.
- OBSERVAÇÃO** Pode-se selecionar qualquer usuário ou conta de grupo existente. Isso permite que você delegue a autoridade para ingressar esta conta de computador ao domínio.
4. Se esta conta será usada com aplicativos escritos para sistemas operacionais herdados, selecione Assign This Computer Account As A Pre–Windows 2000 Computer.
 5. Se o Windows Deployment Services não estiver instalado, toque ou clique em OK para criar a conta de computador. Caso contrário, toque ou clique duas vezes em Next e depois em toque ou clique em Finish.

Ao trabalhar com o Windows Deployment Services, as contas de computador gerenciado são usadas para pré-configurar as contas de computador para que um computador possa ser instalado automaticamente. Para criar uma conta de computador gerenciado usando o Active Directory Users And Computers, siga as etapas:

1. Realize as etapas de 1 a 4 do procedimento anterior. Toque ou clique em Next para exibir a página Managed.
2. Selecione a caixa de seleção This Is A Managed Computer e insira o identificador global exclusivo/identificador universal exclusivo do computador (GUID/UUID). Toque ou clique em Next.
3. Na página Host Server há opções para determinar qual servidor host deve ser usado ou para permitir que qualquer servidor host disponível possa ser usado para a instalação remota. Para determinar um servidor host, selecione The Following Remote Installation Server. Na caixa de diálogo Find, toque ou clique em

Find Now para exibir uma lista de todos os servidores de instalação remota na organização. Toque ou clique no servidor host que você deseja usar e depois em OK para fechar a caixa de diálogo Find.

4. Toque ou clique em Next e em Finish.

MUNDO REAL Você pode localizar o GUID/UUID na BIOS do sistema ou no gabinete do computador. Se o Windows PowerShell estiver instalado, pode-se buscar o GUID/UUID usando a classe Win32_ComputerSystemProduct da interface Windows Management Instrumentation (WMI). O exemplo a seguir recupera o UUID do computador em que você está logado:

```
get-wmiobject -class win32_computersystemproduct | fl uuid
```

Neste outro, recupera-se o UUID de um computador remoto:

```
get-wmiobject -class win32_computersystemproduct -computername engpc24 | format-list pscomputername, uuid
```

Tendo criado uma conta de computador padrão ou gerenciado no Active Directory Users And Computers, pode ser que você queira marcar a conta como protegida. As contas protegidas só podem ser excluídas se você remover o sinalizador Protect antes de tentar excluí-las.

Para marcar uma conta de computador como protegida, siga as etapas:

1. Em Active Directory Users And Computers, certifique-se de que Advanced Features esteja selecionado no menu View.
2. Dê um clique duplo ou toque duas vezes na conta de computador para abrir a caixa de diálogo Properties.
3. Na guia Object, marque a caixa de seleção Protect Object From Accidental Deletion e toque ou clique em OK.

Visualização e edição das propriedades da conta de computador

Para visualizar e editar propriedades de contas de computador usando o Active Directory Users And Computers ou o Active Directory Administrative Center, siga as etapas:

1. Na árvore de console, expanda o nó de domínio.
2. Selecione o contêiner ou a OU em que está localizada a conta de computador.
3. Dê um toque duplo ou clique duas vezes na conta. Isso exibe a caixa de diálogo Properties, permitindo que você visualize e edite as configurações.

Em Active Directory Users And Computers, as guias e configurações avançadas só ficam disponíveis quando a opção Advanced Features estiver selecionada no menu View. Em Active Directory Administrative Center, a maioria das opções avançadas está disponível nas guias do painel Extensions.

Como excluir, desabilitar e habilitar contas de computador

Se você não precisa mais de uma conta de computador, ela pode ser excluída permanentemente do Active Directory. Pode também ser desabilitada temporariamente para mais tarde voltar a ser habilitada para uso.

Para excluir, desabilitar ou habilitar contas de computador, siga as etapas:

1. Abra o Active Directory Users And Computers ou o Active Directory Administrative Center. Na árvore de console, selecione o contêiner em que está localizada a conta de computador.
2. Pressione e mantenha pressionada ou clique com o botão direito na conta de computador e faça o seguinte:
 - Toque ou clique em Delete para excluir a conta permanentemente. Toque ou clique em Yes para confirmar a exclusão.
 - Toque ou clique em Disable Account para desabilitar a conta temporariamente. Toque ou clique em Yes para confirmar a ação. Um círculo vermelho com um X indica que a conta foi desabilitada.
 - Toque ou clique em Enable Account para habilitar a conta para que ela possa ser usada novamente.

Se a conta estiver protegida, é preciso remover o sinalizador Protect antes de excluí-la. Dê um toque duplo ou clique duas vezes na conta para abrir a sua caixa de diálogo Properties. Desmarque a caixa de seleção Protect Object From Accidental Deletion e toque ou clique em OK. Nas caixas de diálogo Properties do Active Directory Users And Computers, essa caixa de seleção fica na guia Object. No Active Directory Administrative Center, essa caixa de seleção fica no painel Computer.

DICA Se uma conta está em uso no momento, pode não ser possível desabilitá-la. Tente desligar o computador ou desconectar a sessão do computador na pasta Sessions do Computer Management.

Como redefinir contas de computador bloqueadas

Da mesma forma que as contas de usuário, as contas de computador possuem senhas. Entretanto, diferente do que acontece com contas de usuário, as senhas das contas de computador são gerenciadas e mantidas automaticamente. Para realizar este gerenciamento automatizado, os computadores no domínio armazenam uma senha de conta de computador, que é alterada a cada 30 dias por padrão, e uma senha de canal seguro para estabelecer uma comunicação segura com controladores de domínio. A senha do canal seguro também é atualizada a cada 30 dias por padrão, sendo que ambas as senhas devem estar sincronizadas. Se as senhas de canal seguro e de conta de computador perderem a sincronia, o computador não poderá fazer logon no domínio e uma mensagem de erro de autenticação do domínio será enviada para o serviço Netlogon com um ID do evento 3210 ou 5722.

Caso isso ocorra, será preciso redefinir a senha da conta de computador. Para isso, pressione e mantenha pressionada ou clique com o botão direito do mouse na conta de computador no Active Directory Users And Computers e selecione Reset Account. Será necessário remover o computador do domínio (tornando o computador membro

de um grupo de trabalho ou de outro domínio) e depois reingressar o computador no domínio.

MUNDO REAL Existem várias outras maneiras de redefinir a senha da conta de computador. No Active Directory Administrative Center, pressione e mantenha pressionada ou clique com o botão direito do mouse na conta de computador e depois selecione Reset Account. No prompt de comando, utilize Dsmod Computer -Reset para redefinir a senha da conta de computador. No Windows PowerShell, pode-se usar tanto Reset-ComputerMachinePassword quanto Set-ADAccountPassword com a opção -Reset para redefinir uma senha de conta de computador. O comando a seguir executa Reset-ComputerMachinePassword em um computador remoto:

```
Invoke-Command -ComputerName EngPC84 -ScriptBlock  
{Reset-ComputerMachinePassword}
```

Todas essas opções podem demandar etapas adicionais de remoção do computador do domínio (tornando o computador um membro de um grupo de trabalho ou de outro domínio) e de reingresso do computador ao domínio. As etapas adicionais podem ser necessárias porque a senha deve estar sincronizada entre o computador local e o domínio.

Várias ferramentas permitem que você redefina a senha de um computador e sincronize as alterações no domínio. Em computadores com o Windows PowerShell instalado, pode-se usar Test-ComputerSecureChannel para testar a conexão segura entre o computador local e o domínio. Para isso, faça o logon no computador localmente, abra o prompt do PowerShell e insira o comando:

```
test-computersecurechannel
```

Você pode usar a opção -Server para testar o canal de comunicação com um controlador de domínio específico. Se o comando retornar False, há um problema de comunicação. Use a opção -Repair para redefinir a senha da conta no computador local e escrever essa alteração para o objeto Computer relacionado em um controlador de domínio no domínio. A mudança de senha será replicada para outros controladores de domínio.

Outra ferramenta para redefinir a senha de um computador e sincronizar as alterações é o utilitário de linha de comando Netdom. Para mais detalhes, consulte o artigo 325850 na Base de Dados de Conhecimento da Microsoft (support.microsoft.com/default.aspx?scid=kb;en-us;325850).

Pode-se usar o Netdom Verify para testar a conexão segura entre um computador local e um domínio. Pode-se usar o Netdom Resetpwd para redefinir a senha da conta no computador local e escrever essa alteração para o objeto Computer relacionado em um controlador de domínio no domínio, isso garante que a mudança de senha seja replicada para outros controladores de domínio.

Para redefinir a senha de computador de um servidor membro, siga as etapas:

1. Faça o logon no computador localmente. Em um prompt de comando, digite **netdom resetpwd /s:*ServerName* /ud:*domain\UserName* /pd:*****, onde *ServerName* é o nome do controlador de domínio a ser usado para definir a senha, *domain\UserName* especifica uma conta de administrador com autoridade para alterar a senha e * indica que o Netdom deve solicitar a você a senha da conta antes de prosseguir.

2. Digite a sua senha quando solicitado. O Netdom altera a senha da conta de computador localmente e no controlador de domínio. O controlador de domínio distribui a mudança de senha para outros controladores de domínio no domínio.
3. Reinicie o computador.

Para controladores de domínio, é preciso realizar etapas adicionais. Depois de fazer o logon localmente, você deve parar o serviço Kerberos Key Distribution Center (KDC, Centro de Distribuição de Chaves Kerberos) e definir o seu tipo de inicialização como Manual. Após reiniciar o computador e verificar se a senha foi redefinida com sucesso, você pode reiniciar o serviço KDC e definir o seu tipo de inicialização de volta para Automatic.

Como mover contas de computador

Normalmente, as contas de computador são colocadas nos contêineres Computers ou Domain Controllers ou ainda em OUs personalizadas. Para mover uma conta para um outro contêiner, selecione a conta de computador no Active Directory Users And Computers e depois arraste a conta para o novo local. Não é possível clicar e arrastar contas no Active Directory Administrative Center.

Usando qualquer uma das ferramentas, utilize a seguinte técnica para mover contas de computador:

1. Na árvore de console, selecione o contêiner em que está localizada a conta de computador.
2. Pressione e mantenha pressionada ou clique com o botão direito do mouse na conta de computador que deseja mover e depois toque ou clique em Move. Isso abre a caixa de diálogo Move, mostrada na Figura 7-8.

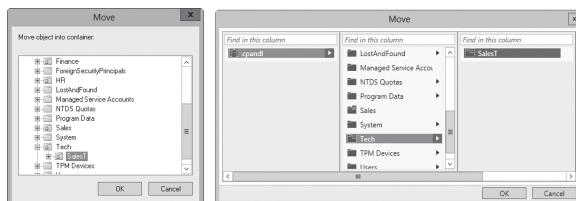


FIGURA 7-8 Na caixa de diálogo Move pode-se mover contas de computador para outros contêineres.

3. Na caixa de diálogo Move, utilize as opções oferecidas para selecionar o contêiner para o qual deseja mover o computador. Navegue até sub-contêineres ou OUs filhas conforme for necessário. Toque ou clique em OK.

Gerenciamento de computadores

Como o nome sugere, você utiliza o Computer Management (Gerenciamento de Computadores) para gerenciar computadores. Você pode abrir o Computer Management e conectar-se a um determinado computador se estiver trabalhando com o Active Directory Users And Computers ou com o Active Directory Administrative Center. Para isso, pressione e mantenha pressionada ou clique com o botão direito do mouse na entrada do computador e depois selecione Manage no menu de atalhos. Isso inicializará o Computer Management e conectará automaticamente ao computador selecionado.

Como ingressar um computador a um domínio ou grupo de trabalho

Um computador ingressado a um domínio ou grupo de trabalho pode fazer logon e acessar a rede. Antes de começar, certifique-se de que os componentes de rede estejam instalados adequadamente no computador. Eles devem ter sido instalados durante a instalação do sistema operacional. Para mais detalhes sobre a configuração de conexões TCP/IP, você pode consultar o Capítulo 14, "Gerenciamento de redes TCP/IP". As configurações de TCP/IP devem estar corretas e permitir a comunicação entre o computador que você está configurando e um controlador no domínio. Se o Dynamic Host Configuration Protocol (Protocolo DHCP), o Windows Internet Name Service (WINS, Serviço de cadastramento na Internet do Windows), e o DNS estiverem instalados corretamente na rede, não é necessário designar um endereço IP estático ou ter uma configuração especial para as estações de trabalho. Os únicos requisitos são um nome de computador e um nome de domínio, que podem ser determinados ao ingressar o computador ao domínio.

MUNDO REAL O Windows Server 2012 concede automaticamente o direito de usuário Add Workstations To The Domain ao grupo interno Authenticated Users. Ou seja, o usuário que fizer logon no domínio como User e for autenticado pode adicionar estações de trabalho ao domínio, sem precisar de privilégios de administração. Entretanto, como medida de segurança, o número de estações de trabalho que um usuário desse tipo pode adicionar ao domínio é limitado a 10. Se um usuário autenticado exceder esse limite, uma mensagem de erro será exibida.

Ainda que você possa usar a ferramenta Ldp.exe do Windows Server 2012 Support Tools para substituir o limite padrão do número de computadores que um usuário autenticado pode ingressar a um domínio (como definido pelo atributo *ms-DS-MachineAccountQuota*), essa não é uma boa prática de segurança. Uma técnica melhor e mais adequada no que diz respeito à segurança é criar com antecedência a conta de computador necessária em uma determinada OU ou conceder ao usuário o privilégio de segurança avançada Create Account Objects para o contêiner Computers. Pode-se também conceder a certos usuários o privilégio Delete Account Objects para o contêiner Computers. Assim, os usuários designados podem remover contas de computador do domínio.

Durante a instalação do sistema operacional, é provável que uma conexão de rede tenha sido configurada para o computador ou que você tenha ingressado o computador ao domínio ou ao grupo de trabalho anteriormente. Se esse for o caso, pode-se ingressar o computador a um novo domínio ou grupo de trabalho. Para ingressar um computador com Windows Vista ou posterior (bem como com Windows Server 2008 ou posterior) a um domínio, consulte "A guia Computer Name" no Capítulo 2, "Gerenciamento de servidores com o Microsoft Windows Server 2012." O processo é quase idêntico para configuração de computadores com Windows 2000 Professio-

nal, Windows 2000 Server, Windows XP Professional e Windows Server 2003. Uma diferença-chave é que ao tocar ou clicar em System And Security, System no Control Panel abre diretamente a caixa de diálogo System Properties.

Se a alteração de nome não for bem-sucedida, você verá uma mensagem informando que a alteração foi malsucedida ou então que as credenciais da conta já existem. Esse problema pode ocorrer quando você estiver alterando o nome de um computador que já está conectado a um domínio e quando o computador tiver sessões ativas naquele domínio. Feche os aplicativos que possam estar conectados ao domínio, como o File Explorer, acessando uma pasta compartilhada através da rede. Depois, repita o processo para alterar o nome do computador.

Se você enfrentar outros problemas ao ingressar em um domínio, certifique-se de que o computador que você está configurando tenha as configurações de rede apropriadas. O computador deve ter instalado o Networking Services e as propriedades TCP/IP devem ter as configurações de servidor DNS corretas, como será discutido no Capítulo 14.

Todos os usuários autenticados possuem por padrão o direito de usuário Add Workstations To The Domain, podendo criar até 10 contas de computador ao ingressar computadores a um domínio. Não há restrições nesse sentido para os usuários que possuem o privilégio Create Account Objects para o contêiner Computers. Eles podem criar um número ilimitado de contas de computador no domínio. A diferença é que as contas de computador criadas por usuários autenticados têm como proprietário da conta o Domain Admins, enquanto contas de computador criadas por usuários com o privilégio Create Account Objects têm como proprietário o criador. Se você conceder o privilégio Create Account Objects, pode ser desejável conceder também o privilégio Delete Account Objects para que certos usuários possam remover contas de computador do domínio.

Para conceder o privilégio Create Account Objects, o privilégio Delete Account Objects ou ambos os privilégios para o contêiner Computers, siga as etapas:

1. Abra o Active Directory Users And Computers ou o Active Directory Administrative Center. No Active Directory Users And Computers, certifique-se de que Advanced Features estejam habilitados no menu View.
2. Pressione e mantenha pressionado ou clique com o botão direito do mouse no contêiner Computers e depois toque ou clique em Properties.
3. Na guia Security, toque ou clique em Advanced. Na caixa de diálogo Advanced Security Settings For Computers, toque ou clique em Add para abrir a caixa de diálogo Permission Entry For Computers.
4. Toque ou clique em Select A Principal. Na caixa de diálogo Select User, Computer, Service Account, Or Group, digite o nome do usuário ou grupo para o qual você deseja conceder os privilégios e toque ou clique em OK. Clique em OK novamente.

Como usar o ingresso offline ao domínio

Os computadores com edições do Windows 7 e Windows 8 projetadas para uso em local de trabalho suportam o ingresso offline ao domínio, da mesma forma que o Windows Server 2008 R2 ou versão posterior. O utilitário referente (Djoin.exe) está incluso nessas edições do Windows. Qualquer membro do Domain Admins pode realizar ingressos offline ao domínio (bem como qualquer pessoa a quem tenham sido concedidos os direitos do usuário apropriados).

As etapas básicas para realizar uma operação de ingresso offline ao domínio são:

1. Criar uma conta de computador no Active Directory e forçar a replicação dos segredos compartilhados do computador que deve ingressar ao domínio.
2. Gravar em um arquivo de texto as informações de estado relevantes que o computador precisa para ingressar ao domínio e disponibilizar essas informações de estado para o computador.
3. Quando o computador iniciar, o Windows lerá os dados de provisionamento e o computador será ingressado ao domínio.

OBSERVAÇÃO Computadores clientes devem estar conectados à rede corporativa para ingressar em um domínio ou receber configurações de domínio. Com o novo recurso de ingresso remoto no domínio, o Windows Server 2012 possibilita que computadores com o Windows 8 ingressem em um domínio e recebam configurações de domínio remotamente através da Internet.

Para provisionar os metadados da conta de computador, execute Djoin.exe em um prompt de comando elevado para administração. Os metadados da conta de computador serão gravados em um arquivo .txt. Depois de provisionar o computador, você pode executar novamente o Djoin.exe para solicitar os metadados da conta de computador e inseri-los no diretório do Windows do computador de destino. Como opção, pode-se salvar os metadados da conta de computador em um arquivo Unattend.xml e depois especificar o arquivo Unattend.xml durante uma instalação autônoma de sistema operacional.

Para usar um arquivo .txt para provisionamento, siga as etapas:

1. Usando uma conta com permissão para ingressar computadores ao domínio, faça o logon em um computador que seja membro do domínio.
2. Utilize o Djoin.exe para criar um arquivo de texto contendo os metadados da conta de computador. Para isso, digite **djoin /provision /domain DomainName /machine MachineName /savefile FileName** em um prompt de comando elevado para administração, onde *DomainName* é o nome do domínio ao qual se quer ingressar, *MachineName* é o nome do computador e *FileName* é o nome do arquivo .txt onde os metadados devem ser salvos, como por exemplo:

```
djoin /provision /domain cpandl /machine HrComputer15 /savefile  
Hrcomputer15.txt
```

DICA Por padrão, contas de computador são criadas no contêiner Computers. Se quiser utilizar um outro contêiner, adicione o parâmetro */Machineou* e depois especifique o contêiner a ser utilizado. Se o objeto da conta de computador já tiver sido criado, ainda assim você pode gerar os metadados necessários. Para isso, adicione o parâmetro */reuse*. Se o seu controlador de domínio ainda não estiver com o Windows Server 2008 R2 ou Windows Server 2012, adicione o comando */downlevel*.

3. No novo computador, utilize Djoin.exe para importar o arquivo .txt. Em um prompt de comando elevado para administração, digite **djoin /requestODJ /loadfile FileName /windowspath %SystemRoot% /localosCaution**, onde *FileName* é o nome do arquivo de metadados, como por exemplo:

```
djoin /requestODJ /loadfile HrComputer15.txt /windowspath  
%SystemRoot% /localos
```

4. Certifique-se de que o novo computador esteja conectado à rede e depois faça a reinicialização. Durante a inicialização, o computador será ingressado ao domínio.

Para usar um arquivo Unattend.xml para provisionamento, crie uma seção no arquivo Unattend.xml e adicione o conteúdo do arquivo de metadados .txt ao elemento *AccountData*, como mostra o exemplo:

```
<Component>
<Component name=Microsoft-Windows-UnattendedJoin>
    <Identification>
        <Provisioning>
            <AccountData> Insert metadata here! </AccountData>
        </Provisioning>
    </Identification>
</Component>
```

Após criar o arquivo Unattend.xml, inicie o novo computador no modo de segurança ou no Windows Preinstallation Environment (Windows PE, Ambiente de Pré-Instalação do Windows) e execute o comando Setup com um arquivo de resposta, como mostra o exemplo a seguir:

```
setup /unattend: FullPathToAnswerFile
```

Aqui, *FullPathToAnswerFile* é o caminho completo de arquivo para o arquivo Unattend.xml.

Gerenciamento de controladores de domínio, funções e catálogo

Os controladores de domínio desempenham muitas tarefas importantes nos domínios do Active Directory. Várias dessas tarefas foram discutidas no Capítulo 6.

Como instalar e rebaixar controladores de domínio

Para instalar um controlador de domínio, configura-se o Active Directory Domain Services (AD DS) em um servidor. Mais tarde, se não quiser que o servidor tenha tarefas de controlador, você pode rebaixar o servidor. Assim, ele voltará a atuar como um servidor membro. O procedimento é parecido para instalar e rebaixar servidores. Mas antes que você o faça, reflita sobre o impacto na rede e leia "A estrutura de diretório" no Capítulo 6.

Como explica a referida seção, ao instalar um controlador de domínio pode ser preciso transferir funções de mestre de operações e reconfigurar a estrutura do catálogo global. Além disso, o DNS deve estar em funcionamento na rede para que você possa instalar o AD DS. Ao instalar o AD DS, pode-se incluir a instalação de servidor DNS se isso for necessário. Ao criar um novo domínio, uma delegação de DNS é criada automaticamente durante o processo de instalação. Para isso, são necessárias credenciais que tenham permissões para atualizar zonas DNS pai.

Para adicionar o primeiro controlador de domínio que execute o Windows Server 2012 a uma infraestrutura de Active Directory existente, o Active Directory Installation Wizard (Assistente para instalação do Active Directory) executa automaticamente o Adprep.exe para floresta e domínio, conforme for necessário. A preparação da floresta e do domínio inclui a atualização do esquema do Active Directory, a criação de novos

objetos e contêineres e a modificação de descritores de segurança e listas de controle de acesso, conforme for necessário. Para a preparação da floresta, a conta utilizada deve ser um membro dos grupos Schema Admins, Enterprise Admins e Domain Admins do domínio que hospeda o mestre de esquema, que é, por padrão, o domínio-raiz da floresta. Para a preparação do domínio, utiliza-se uma conta que possa fazer logon no mestre de infraestrutura e seja membro do grupo Domain Admins. Para a preparação para o RODC, deve ser usada uma conta membro do grupo Enterprise Admins.

Antes de rebaixar um controlador de domínio, você deve transferir qualquer responsabilidade-chave para outros controladores de domínio. Isso significa retirar o catálogo global do servidor e transferir as funções de mestre de operações, se for necessário. Também é preciso remover qualquer partição de diretório de aplicativos que estejam no servidor.

MUNDO REAL Observe que com o Windows Server 2012 e versões posteriores, todas as tarefas de instalação e configuração de AD DS são realizadas via Server Manager. Você não precisa mais executar um assistente de instalação e uma tarefa de promoção de linha de comando separada. Também pode ser que você não precise preparar manualmente o Active Directory para o Windows Server 2012.

Repare que no Windows Server 2003 e em versões posteriores não é mais necessário rebaixar um controlador de domínio para poder renomeá-lo, sendo possível renomear um controlador de domínio a qualquer momento. O único problema é que o servidor fica indisponível para os usuários durante o processo de renomeação e pode ser preciso forçar uma atualização de diretório para reestabelecer a comunicação com o servidor. Entretanto, não é possível mover um controlador de domínio para outro domínio. Para isso, é necessário rebaixar o controlador de domínio, atualizar as configurações de domínio para o servidor e para a sua conta de computador e depois promover o servidor a controlador de domínio mais uma vez.

Para instalar um controlador de domínio, siga as etapas:

1. No Server Manager, o servidor local é automaticamente adicionado para gerenciamento. Se você desejar instalar o AD DS em outro servidor, precisa adicionar o servidor para gerenciamento usando a opção Add Servers. Para usar o Server Manager para gerenciamento remoto, é necessária a configuração discutida no Capítulo 2 e um conjunto mínimo de permissões. Normalmente, é preciso ter Domain Admin ou outra permissão explícita para adicionar um servidor e gerenciá-lo remotamente. Para criar uma nova floresta do Active Directory, você precisa estar logado como o Administrador local do computador. Para instalar um novo domínio-filho ou uma nova árvore de domínio, você precisa estar logado como membro do grupo Enterprise Admins. Para instalar um controlador de domínio adicional em um domínio existente, você precisa estar logado como membro do grupo Domain Admins.
2. Em Server Manager, toque ou clique em Manage e depois em Add Roles And Features. Isso iniciará o Add Roles And Features Wizard. Se o Assistente exibir a página Before You Begin, leia a mensagem de boas-vindas e depois toque ou clique em Next.
3. Na página Select Installation Type, selecione Role-Based Or Feature-Based Installation e toque ou clique em Next.
4. Na página Select Destination Server, o pool de servidores exibe os servidores que você adicionou para gerenciamento. Toque ou clique no servidor que você está configurando e depois em Next.

5. Na página Select Server Roles, selecione Active Directory Domain Services e toque ou clique em Next duas vezes. Toque ou clique em Install. Isso executa o Active Directory Domain Services Installation Wizard.
6. Quando terminar a tarefa de instalação inicial, você deve tocar ou clicar em Promote This Server To A Domain Controller para iniciar o Active Directory Domain Services Configuration Wizard. Caso tenha fechado a janela Add Roles And Features Wizard, toque ou clique no ícone Notifications e depois em Promote This Server To A Domain Controller.

MAIS INFORMAÇÕES Se a instalação falhar, verifique o erro e realize a ação corretiva apropriada antes de recomeçar o procedimento. Os erros típicos de instalação estão relacionados com permissões, como aquelas necessárias para a preparação da floresta ou do domínio para adicionar o Windows Server 2012 a primeira vez. Nesse caso, faça logoff e depois faça logon novamente usando uma conta que tenha as permissões apropriadas.

7. Se o computador for um servidor membro no momento, o assistente leva você às etapas necessárias para instalar o Active Directory. Isso pode incluir a preparação automática do esquema do diretório na floresta e no domínio para o Windows Server 2012. É preciso definir se este é um controlador de domínio para um novo domínio ou um controlador de domínio adicional para um domínio existente. Para verificar se um controlador de domínio está instalado adequadamente, proceda da seguinte maneira: confira se há erros no log de eventos do Directory Service, certifique-se de que a pasta SYSVOL esteja acessível para os clientes, verifique se a resolução de nomes está usando o DNS e confira a replicação de alterações para o Active Directory.

Para rebaixar um controlador de domínio, siga as etapas:

1. Em Server Manager, toque ou clique em Manage e depois em Remove Roles And Features. Isso iniciará o Remove Roles And Features Wizard. Se o Assistente exibir a página Before You Begin, leia a mensagem de boas-vindas e depois toque ou clique em Next.
2. Na página Select Destination Server, o pool de servidores exibe os servidores que você adicionou para gerenciamento. Toque ou clique no servidor que você está configurando e depois em Next.
3. Na página Select Server Roles, desmarque a caixa de seleção do Active Directory Domain Services para definir que essa é a função que você quer remover.
4. Uma nova caixa de diálogo é aberta. Aqui, é desejável desmarcar a caixa de seleção Remove Management Tools para garantir que as ferramentas de gerenciamento do AD DS não sejam desinstaladas e clicar em Continue. Caso contrário, clique em Remove Features. Clique em Next duas vezes.
5. Na página Credentials, observe a sua conta de logon atual. Se for necessário, forneça credenciais alternativas com permissões para remover o controlador de domínio. Clique em Next.
6. Se a página Warnings for exibida, veja os avisos, selecione Proceed With Removal e clique em Next.

7. Insira e confirme uma nova senha para a conta de Administrador local do servidor. As senhas inseridas devem ser iguais. Clique em Next.
8. Na página Confirm Removal Selections, você tem a opção de marcar a caixa de seleção Restart The Destination Server Automatically If Required. Como é necessário reiniciar o servidor para concluir a remoção, pode-se escolher essa opção e tocar ou clicar em Yes para confirmar. Quando estiver pronto para continuar, clique em Remove.

ATENÇÃO Normalmente, o rebaixamento de um servidor transfere as funções mantidas pelo servidor. Porém, se tentativas anteriores de rebaixar o controlador de domínio falharam, pode-se repetir esse procedimento e marcar a caixa de seleção Force The Removal Of This Domain Controller como parte do processo de remoção. Nesse caso, as funções FSMO (flexible single master operation) do controlador de domínio podem ser deixadas em um estado inválido até que sejam reatribuídas por um administrador. Os dados do domínio também podem ficar em um estado inconsistente.

MUNDO REAL Uma técnica alternativa para a instalação de controladores de domínio é o uso de mídia de backup. Essa opção foi introduzida no Windows Server 2003. Para instalar um controlador de domínio a partir da mídia de backup, crie um backup dos dados do estado do sistema de um controlador de domínio e restaure-o em um outro servidor com o Windows Server 2003 ou versão posterior. Ao criar um controlador de domínio a partir da mídia de backup, você elimina a necessidade de replicar todo o banco de dados do diretório através da rede para o novo controlador de domínio. Isso é muito útil se houverem limitações de largura de banda ou se o banco de dados do diretório possuir milhares de entradas.

Visualização e transferência de funções de domínio

Para visualizar e alterar o local de funções de mestre de operações do domínio, pode-se usar o Active Directory Users And Computers. No nível do domínio, pode-se trabalhar com funções para mestres de RID (relative ID), mestres de emulador de PDC (primary domain controller emulator) e mestres de infraestrutura.

OBSERVAÇÃO As funções de mestre de operações são discutidas no Capítulo 6 em “Nóções básicas sobre funções de mestre de operações”. Utiliza-se o Active Directory Domains And Trusts (Domínios e Relações de Confiança do Active Directory) para definir a função de mestre de nomeação de domínios e o Active Directory Schema (Esquema do Active Directory) para alterar a função de mestre do esquema. A maneira mais rápida de determinar o FSMO atual para todas as funções é digitando `netdom query fsmo` em um prompt de comando.

Para visualizar as funções de mestre de operações atuais, siga as etapas:

1. Em Active Directory Users And Computers, pressione e mantenha pressionado ou clique com o botão direito do mouse em Active Directory Users And Computers na árvore de console. No menu de atalhos, aponte o cursor para All Tasks e toque ou clique em Operations Masters. Isso abre a caixa de diálogo Operations Masters, mostrada na Figura 7-9.

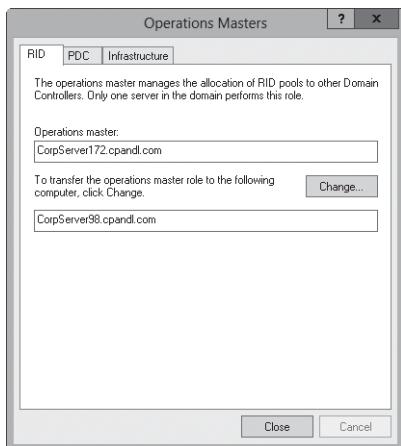


FIGURA 7-9 Na caixa de diálogo Operations Masters você pode transferir mestres de operações para novos locais ou apenas visualizar seus locais atuais.

2. A caixa de diálogo Operations Masters possui três guias. A guia RID mostra o local do mestre de RID atual. A guia PDC mostra o local do mestre de emulador de PDC atual. A guia Infraestructure mostra o local do mestre de infraestrutura atual.

Para transferir as funções de mestre de operações atuais, siga as etapas:

1. Inicie o Active Directory Users And Computers. Na árvore de console, pressione e mantenha pressionado ou clique com o botão direito do mouse em Active Directory Users And Computers e depois toque ou clique em Change Domain Controller.
2. Na caixa de diálogo Change Directory Server, toque ou clique em This Domain Controller Or AD LDS Instance, selecione o controlador de domínio para o qual deseja transferir uma função de mestre de operações e toque ou clique em OK.
3. Na árvore de console, pressione e mantenha pressionado ou clique com o botão direito do mouse em Active Directory Users And Computers. No menu de atalhos, aponte o cursor para All Tasks e toque ou clique em Operations Masters.
4. Na caixa de diálogo Operations Masters, toque ou clique na guia RID, PDC ou Infraestructure, dependendo do tipo de função a ser transferida.
5. Toque ou clique em Change para transferir a função para o controlador de domínio selecionado anteriormente. Toque ou clique em OK.

Visualização e transferência da função mestre de nomeação de domínios

Para visualizar e alterar o local da função mestre de nomeação de domínios (domain naming master role) na floresta, pode-se usar o Active Directory Domains And Trusts. Em Active Directory Domains And Trusts, o nível de raiz da árvore de controle mostra o domínio selecionado no momento.

DICA Caso precise se conectar a um domínio diferente, conecte-se a um controlador de domínio seguindo etapas similares àquelas descritas em “Como utilizar o Active Directory Users And Computers” anteriormente neste capítulo. A diferença é que você pressiona e mantém pressionado ou clica com o botão direito do mouse em Active Directory Domains And Trusts na árvore de console.

Para transferir a função mestre de nomeação de domínios, siga estas etapas:

1. Abra o Active Directory Domains And Trusts. Na árvore de console, pressione e mantenha pressionado ou clique com o botão direito do mouse em Active Directory Domains And Trusts e depois toque ou clique em Change Active Directory Domain Controller.
2. Na caixa de diálogo Change Directory Server, selecione a opção This Domain Controller Or AD LDS Instance e depois selecione o controlador de domínio para o qual deseja transferir a função mestre de nomeação de domínios. Toque ou clique em OK.
3. Na árvore de console, pressione e mantenha pressionado ou clique com o botão direito do mouse em Active Directory Domains And Trusts e depois toque ou clique em Operations Masters. Isso abre a caixa de diálogo Operations Masters.
4. A caixa Domain Naming Operations Master exibe o mestre de nomeação de domínios atual. Toque ou clique em Change para transferir a função para o controlador de domínio selecionado anteriormente.
5. Toque ou clique em Close.

Visualização e transferência da função de mestre de esquema

Para visualizar ou alterar o local do mestre de esquema, utiliza-se o Active Directory Schema (Esquema do Active Directory). Insira **regsvr32 schmmgmt.dll** em um prompt de comando elevado para administração para registrar o Active Directory Schema. Depois disso, pode-se transferir a função de mestre de esquema seguindo as etapas:

1. Adicione o snap-in Active Directory Schema a um MMC.
2. Na árvore de console, pressione e mantenha pressionado ou clique com o botão direito do mouse em Active Directory Schema e depois toque ou clique em Change Active Directory Domain Controller.
3. Selecione Any Writable Domain Controller para deixar que o Active Directory escolha o novo mestre de esquema, ou então selecione This Domain Controller Or AD LDS Instance e escolha o novo mestre de esquema.
4. Toque ou clique em OK. Na árvore de console, pressione e mantenha pressionado ou clique com o botão direito do mouse em Active Directory Schema e depois toque ou clique em Operations Master.
5. Na caixa de diálogo Change Schema Master, toque ou clique em Change. Toque ou clique em OK e depois em Close.

Como transferir funções usando a linha de comando

Outra maneira de transferir funções é utilizar o Netdom para listar os atuais proprietários de função FSMO e depois o Ntdsutil.exe para transferir as funções. O Ntdsutil é uma ferramenta de linha de comando para o gerenciamento do Active Directory. Siga as etapas para transferir funções na linha de comando:

1. Para obter uma lista dos atuais proprietários de função FSMO, digite **netdom query fsmo** em um prompt de comando.
2. É recomendável (mas não é necessário) que você faça logon no console do servidor que você quer designar como o novo mestre de operações. Você pode fazer o logon localmente ou usar Remote Desktop Connection (Conexão de Área de Trabalho Remota).
3. Abra um prompt. Uma maneira de fazê-lo é pressionar a tecla Windows, digitar **cmd.exe** e pressionar Enter.
4. No prompt, digite **ntdsutil**. Isso inicia Directory Services Management Tool.
5. No prompt ntdsutil, digite **roles**. Isso coloca o utilitário no modo Operations Master Maintenance.
6. No prompt de manutenção fsmo, digite **connections**. No prompt de conexões do servidor, digite **connect to server** seguido pelo nome de domínio totalmente qualificado do controlador de domínio para o qual será designada a função FSMO role, da seguinte forma:
`connect to server engdc01.technology.adatum.com`
7. Depois de estabelecer uma conexão bem-sucedida, digite **quit** para sair do prompt de conexões do servidor. No prompt de manutenção fsmo, digite **transfer** e depois digite o identificador da função que será transferida. Os identificadores são os seguintes:
 - **pdc** Para a função emulador de PDC
 - **rid master** Para a função mestre de RID
 - **infrastructure master** Para a função mestre de infraestrutura
 - **schema master** Para a função mestre de esquema
 - **domain naming master** Para a função mestre de nomeação de domínios
8. Digite **quit** no prompt de manutenção fsmo e depois digite **quit** no prompt ntdsutil.

Como capturar funções usando a linha de comando

Às vezes, pode ser que você se encontre em uma situação em que não consiga transferir normalmente as funções de servidor. Um controlador de domínio atuando como um mestre de RID pode sofrer uma falha na unidade que derrube todo o servidor, por exemplo. Se não for possível deixar o servidor online novamente, pode ser necessário executar (capturar) a função mestre de RID e designar essa função a outro controlador de domínio.

OBSERVAÇÃO Só execute uma função de servidor se o controlador de domínio que gerencia a função atual não estiver operando. Quando o servidor original estiver online novamente, ele reconhecerá e aceitará a alteração.

Não execute uma função sem antes determinar o quanto atualizado está o controlador de domínio que assumirá a função no que diz respeito ao proprietário anterior da função. O Active Directory rastreia as alterações de replicação usando números de sequência de atualização (USNs). Como a replicação demanda tempo, nem todos os controladores de domínio estarão necessariamente atualizados. Se você comparar o USN de um controlador de domínio aos de outros controladores no domínio, pode determinar se o controlador de domínio é o mais atualizado no que diz respeito às alterações do proprietário anterior da função. Se o controlador de domínio estiver atualizado, você pode transferir a função com segurança. Já se o controlador de domínio não estiver atualizado, você pode esperar pela replicação e depois transferir a função para o controlador de domínio.

O Windows Server 2012 inclui diversas ferramentas para trabalhar com a replicação do Active Directory. Uma delas é a Repadmin.

Para exibir o status da última replicação de entrada para um controlador de domínio, utilize Repadmin /ShowRepl. A sintaxe é:

```
repadmin /showrep1 DomainControllerName NamingContext
```

Aqui, *DomainControllerName* é o nome de domínio totalmente qualificado do controlador de domínio e *NamingContext* é o nome distinto do domínio onde está localizado o servidor. Neste exemplo, examina-se a partição padrão para Server252 no domínio Cpndl.com:

```
repadmin /showrep1 server252.cpndl.com dc=cpndl,dc=com
```

OBSERVAÇÃO O PowerShell e o prompt de comando analisam diferentemente os comandos. Em geral, pode-se inserir comandos no prompt do PowerShell da mesma forma que você o faz em um prompt de comando. Nesse caso, porém, o PowerShell interpretará dc=cpndl,dc=com da forma errada, como se fossem dois parâmetros separados. Para evitar que isso aconteça, insira o valor entre aspas: "dc=cpndl,dc=com".

Para exibir o número de sequência mais alto para um determinado contexto de nomenclatura em cada parceiro de replicação de um controlador de domínio, digite em um prompt de comando:

```
repadmin /showutdvec DomainControllerName NamingContext
```

Nesse exemplo, é exibido o número de sequência mais alto para a partição de configuração padrão no Server252 no domínio Cpndl.com:

```
repadmin /showutdvec server252.cpndl.com dc=cpndl,dc=com
```

A saída mostra o mais alto USN (número de atualização de sequência) em parceiros de replicação para a partição de configuração padrão:

```
Default-First-Site-Name\SERVER252 @ USN 45164 @ Time 2014-03-30 11:35:24
```

```
Default-First-Site-Name\SERVER147 @ USN 45414 @ Time 2014-03-30 11:42:16
```

Se o Server252 era o proprietário de função anterior e o controlador de domínio que você está examinando tiver um USN igual ou mais alto do que o Server252, isso significa que o controlador de domínio está atualizado. Porém, se o Server252 era o proprietário de função anterior e o controlador de domínio que você está examinando tiver um USN mais baixo do que o Server252, o controlador não está atualizado. Espere que ocorra a replicação para depois executar (capturar) a função.

Pode-se também usar Repadmin /Syncall para forçar o controlador de domínio mais atualizado em relação ao proprietário de função anterior a replicar com todos os seus parceiros de replicação.

No PowerShell, utilize cmdlets de gerenciamento de replicação para visualizar e solucionar problemas de replicação do Active Directory. Os cmdlets relacionados incluem:

- **Get-ADReplicationAttributeMetadata** Obtém metadados de replicação para os atributos do nome distinto especificado
- **Get-ADReplicationFailure** Obtém informações sobre falhas na replicação para um determinado servidor, site, domínio ou floresta, quando aplicável
- **Get-ADReplicationPartnerMetadata** Obtém metadados de replicação para um determinado servidor, site, domínio ou floresta
- **Get-ADReplicationQueueOperation** Obtém operações pendentes em uma fila de replicação de um servidor
- **Get-ADReplicationUpToDateNessVectorTable** Obtém o USN mais alto para um determinado servidor, site, domínio ou floresta
- **Sync-ADObject** Replica o objeto de diretório especificado

Utilize Get-ADReplicationPartnerMetadata para obter informações sobre replicações de entrada para um servidor, com a seguinte sintaxe:

```
Get-ADReplicationPartnerMetadata -Target Object  
[-Scope Server|Site|Domain|Forest]  
[-Partition Domain|Schema|Configuration|*]
```

Acima, *-Target* define o nome do servidor, site, domínio ou floresta com que se trabalhará. A definição do escopo é exigida quando se trabalha com objetos que não sejam servidores. A definição da partição é exigida quando se quer trabalhar com partições que não sejam a partição padrão. Neste exemplo, examina-se a partição padrão no CorpServer98:

```
Get-ADReplicationPartnerMetadata -target corpserver98
```

Também é possível examinar todas as partições no servidor, usando a seguinte sintaxe:

```
Get-ADReplicationPartnerMetadata -target corpserver98 -partition *
```

Da mesma forma que Repadmin /Showudvec, Get-ADReplicationUpToDateNessVectorTable exibe o número de sequência mais alto para as partições replicadas, podendo ajudar você na solução de problemas de replicação. Aqui está a sintaxe básica:

```
Get-ADReplicationUpToDateNessVectorTable -Target Object  
[-Scope Server|Site|Domain|Forest]  
[-Partition Domain|Schema|Configuration|*]
```

Nesse exemplo, é exibido o número de sequência mais alto para a partição padrão (a partição de configuração de domínio) no CorpServer98:

```
Get-ADReplicationUpToDateNessVectorTable -target corpserver98
```

A saída mostra o mais alto USN em parceiros de replicação para a partição de configuração padrão:

```
LastReplicationSuccess : 3/30/2014 1:45:57 PM
Partition           : DC=cpandl,DC=com
PartitionGuid       : c39cfdbd-e1a1-4c4c-9355-85d7ea05c10a
Partner             : CN=NTDS Settings,CN=CORPSERVER172,CN=Servers,
CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=cpandl,DC=com
PartnerInvocationId : fb32931c-e319-473a-8069-d781f980057b
Server              : CorpServer98.cpandl.com
UsnFilter          : 82656

LastReplicationSuccess : 3/30/2014 1:48:44 PM
Partition           : DC=cpandl,DC=com
PartitionGuid       : c39cfdbd-e1a1-4c4c-9355-85d7ea05c10a
Partner             : CN=NTDS Settings,CN=CORPSERVER98,CN=Servers,
CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=cpandl,DC=com
PartnerInvocationId : d8bf2da2-b08d-4d36-bc53-1b7f62643437
Server              : CorpServer98.cpandl.com
UsnFilter          : 12593
```

Interpreta-se a saída como se interpretaria uma saída de Repadmin /Showutdvec. Se você desconfiar que há algum problema, utilize Get-ADReplicationFailure para examinar problemas de replicação. Aqui está a sintaxe básica:

```
Get-ADReplicationFailure -Target Object [-Scope Server|Site|Domain|Forest]
```

Com essa informação, pode-se exibir informações sobre todos os problemas de replicação no domínio Cpandl.com, inserindo o seguinte:

```
Get-ADReplicationFailure -Target "cpandl.com" -Scope Domain
```

Pode-se exibir informações para um determinado site, inserindo o seguinte:

```
Get-ADReplicationFailure -Target "NewYork-FirstSite" -Scope Site
```

Ou pode-se ainda exibir informações para um determinado servidor, inserindo o seguinte:

```
Get-ADReplicationFailure -Target CorpServer172
```

Para capturar uma função de servidor, siga as etapas:

1. Digite **netdom query fsmo** em um prompt de comando para obter uma lista dos proprietários de função FSMO atuais.
2. Certifique-se de que o atual controlador de domínio com a função que você deseja executar esteja permanentemente offline. Se o servidor pode voltar a ficar online, não realize este procedimento a menos que pretenda reinstalar esse servidor por completo.
3. É recomendável que você faça logon no console do servidor que você quer designar como o novo mestre de operações. Você pode fazer o logon localmente ou usar Remote Desktop Connection.
4. Abra uma janela de prompt de comando.
5. No prompt de comando, digite **ntdsutil**. Isso inicia Directory Services Management Tool.

6. No prompt ntdsutil, digite **roles**. Isso coloca o utilitário no modo Operations Master Maintenance.
7. No prompt de manutenção fsmo, digite **connections**. No prompt de conexões do servidor, digite **connect to server** seguido pelo nome de domínio totalmente qualificado do controlador de domínio para o qual será designada a função FSMO role, da seguinte forma:
`connect to server engdc01.technology.adatum.com`
8. Depois de estabelecer uma conexão bem-sucedida, digite **quit** para sair do prompt de conexões do servidor. No prompt de manutenção fsmo, digite **seize** e depois digite o identificador da função que será executada. Os identificadores são os seguintes:
 - **pdc** Para a função emulador de PDC
 - **rid master** Para a função mestre de RID
 - **infrastructure master** Para a função mestre de infraestrutura
 - **schema master** Para a função mestre de esquema
 - **domain naming master** Para a função mestre de nomeação de domínios
9. Digite **quit** no prompt de manutenção fsmo e depois digite **quit** no prompt ntdsutil.

Configuração de catálogos globais

Os catálogos globais desempenham uma função importante na rede. Essa função é discutida no Capítulo 6, em “A estrutura de diretório”. Para configurar catálogos globais adicionais, habilitam-se controladores de domínio para hospedarem o catálogo global. Além disso, se você tiver dois ou mais catálogos globais em um local, pode querer que um controlador de domínio pare de hospedar o catálogo global, o que é feito desabilitando-se o catálogo global no controlador de domínio.

Para habilitar ou desabilitar um catálogo global, siga as etapas:

1. Em Active Directory Sites And Services, expanda o site na árvore de console em que deseja trabalhar.
2. Expanda a pasta Servers para aquele site e depois selecione o servidor que será configurado como servidor do catálogo global.
3. Na painel de detalhes, pressione e mantenha pressionado ou clique com o botão direito do mouse em NTDS Settings e depois toque ou clique em Properties.
4. Para habilitar o servidor para hospedar um catálogo global, marque a caixa de seleção Global Catalog, na guia General.
5. Para desabilitar o catálogo global, desmarque a caixa de seleção Global Catalog, na guia General.

ATENÇÃO Não habilite ou desabilite catálogos globais sem antes fazer adequadamente o planejamento e a análise do impacto na rede. Em um grande ambiente empresarial, a designação de um controlador de domínio como um servidor de catálogo global pode fazer os dados relacionados a milhares de objetos do Active Directory serem replicados por toda a rede.

Configuração de cache de associação de grupo universal

O cache de associação de grupo universal elimina a dependência da disponibilidade de um servidor de catálogo global durante o logon. Ao habilitar esse recurso em um domínio operando com o Windows Server 2003 ou com um nível funcional mais alto, qualquer controlador de domínio pode resolver solicitações de logon localmente, sem precisar passar pelo servidor de catálogo global. Como foi discutido em "Cache de Associação de Grupo Universal" no Capítulo 6, há vantagens e desvantagens.

Você pode habilitar ou desabilitar o cache de associação de um grupo universal seguindo estas etapas:

1. Em Active Directory Sites And Services, expanda e selecione o site com o qual você deseja trabalhar.
2. Na painel de detalhes, pressione e mantenha pressionado ou clique com o botão direito do mouse em NTDS Site Settings e depois toque ou clique em Properties.
3. Para habilitar o cache de associação de grupo universal, marque a caixa de seleção Enable Universal Group Membership Caching na guia Site Settings. Depois, na lista Refresh Cache From, escolha o site que será usado para fazer o cache das associações de grupo universal. O site selecionado precisa ter um servidor de catálogo global operante.
4. Para desabilitar o cache de associação de grupo universal, desmarque a caixa de seleção Enable Universal Group Membership Caching na guia Site Settings.
5. Toque ou clique em OK.

Gerenciamento de unidades organizacionais

Como foi discutido no Capítulo 6, as unidades organizacionais (OUs, organizational units) ajudam você a organizar objetos, definir Group Policy de escopo limitado, entre outros. Nesta seção, você aprenderá a criar e gerenciar OUs.

Como criar unidades organizacionais

Normalmente, as OUs são criadas para espelhar a estrutura funcional ou de negócio da sua organização. Pode-se também criá-las por razões administrativas, como a delegação de direitos para usuários e administradores. As OUs podem ser criadas como subdivisões de um domínio ou como unidades filhas dentro de uma OU existente.

Para criar uma OU, siga estas etapas:

1. No Active Directory Users And Computers ou no Active Directory Administrative Center, pressione e mantenha pressionado ou clique com o botão direito do mouse no nó de domínio ou em uma OU existente em que deseje adicionar a nova OU. Toque ou clique em New no menu de atalhos e depois em Organizational Unit.
2. Insira o nome da OU e toque ou clique em OK.
3. Agora você já pode mover contas e recursos compartilhados para a OU. Para ver um exemplo, consulte a seção "Como mover contas de computador", abordada anteriormente neste capítulo.

Visualização e edição de propriedades de unidade organizacional

Para visualizar e editar as propriedades de uma OU, siga as etapas:

1. Abra o Active Directory Users And Computers ou o Active Directory Administrative Center.
2. Pressione e mantenha pressionada ou clique com o botão direito do mouse na OU com a qual você deseja trabalhar e toque ou clique em Properties. Isso exibirá a caixa de diálogo Properties, que permite a você visualizar e editar as configurações.

Como renomear ou excluir unidades organizacionais

Para renomear ou excluir uma OU, siga as etapas:

1. Em Active Directory Users And Computers, pressione e mantenha pressionada ou clique com o botão direito do mouse na OU com a qual você quer trabalhar.
2. Para excluir a OU, toque ou clique em Delete. Em seguida, toque ou clique em Yes para confirmar a ação.
3. Para renomear a OU, toque ou clique em Rename. Insira um novo nome para a OU e pressione a tecla Enter.

Para excluir uma OU no Active Directory Administrative Center, proceda da mesma maneira. Já para renomear uma OU, abra a sua caixa de diálogo Properties, insira o novo nome e toque ou clique em OK.

Como mover unidades organizacionais

As OUs podem ser movidas a qualquer momento para outros locais dentro de um domínio. Em Active Directory Users And Computers, basta selecionar a OU e arrastá-la para o local desejado.

Tanto no Active Directory Users And Computers quanto no Active Directory Administrative Center, siga estas etapas para mover OUs:

1. Pressione e mantenha pressionada ou clique com o botão direito do mouse na pasta da OU que deseja mover e depois toque ou clique em Move.
2. Na caixa de diálogo Move, expanda o domínio e selecione o contêiner para o qual deseja mover a OU. Toque ou clique em OK.

Gerenciamento de sites

O Active Directory Domain Services Installation Wizard (Assistente de Instalação dos Serviços de Domínio Active Directory) cria um site padrão e um link de site padrão quando você instala o Active Directory Domain Services no primeiro controlador de domínio em um site. O site padrão chama-se Default-First-Site-Name, enquanto o link de site padrão chama-se DEFAULTTIPSITELINK. Você pode renomear o site e o link de site padrão como você preferir. Sites e links de site subsequentes precisam ser criados manualmente.

A configuração de um site é um processo de várias partes que envolve as seguintes etapas:

1. Criação do site
2. Criação de uma ou mais sub-redes e associação delas ao site
3. Associação de um controlador de domínio ao site
4. Vinculação do site a outros sites usando links de sites e, se necessário, criação de pontes de link de site.

Estas tarefas serão abordadas na seção seguinte.

Criação de sites

Qualquer administrador que seja membro do Domain Admins ou do Enterprise Admins pode criar sites. Para criar um site, siga estas etapas:

1. Em Active Directory Sites And Services, pressione e mantenha pressionado ou clique com o botão direito do mouse no contêiner Sites, na raiz do console, e depois toque ou clique em New Site.
2. Na caixa de diálogo New Object–Site, mostrada na Figura 7-10, insira um nome para o site, como **Chicago-First-Site**. Nomes de sites não podem conter espaços ou caracteres especiais, apenas traços.

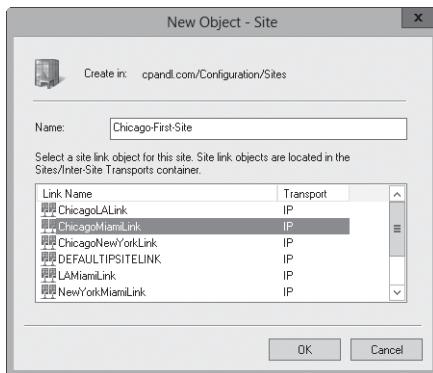


FIGURA 7-10 Para criar o site, configure o nome do site e um link de site relacionado.

3. Toque ou clique no link de site que será usado para conectar este site a outros sites. Se o link de site que você quer utilizar não existe, selecione o link de site padrão e altere as configurações de link de site depois.
4. Toque ou clique em OK. Um prompt é exibido, detalhando as etapas que você deve cumprir para concluir a configuração do site. Toque ou clique novamente em OK.
5. Para concluir a configuração do site, realize as tarefas de configuração que ainda faltam.

DICA Pode-se renomear um site a qualquer momento. Em Active Directory Sites And Services, pressione e mantenha pressionado ou clique com o botão direito do mouse no site e selecione Rename. Digite o novo nome para o site e pressione Enter.

Criação de sub-redes

Cada site que você define deve possuir sub-redes associadas que detalhem os segmentos de rede que pertencem ao site. Qualquer computador com um endereço IP em um segmento de rede associado a um site é considerado como sendo localizado nesse site. Se por um lado um único site pode ter várias sub-redes associadas a ele, por outro uma sub-rede pode ser associada a apenas um site.

Para criar uma sub-rede e associá-la a um site, siga as etapas:

1. Em Active Directory Sites And Services, pressione e mantenha pressionado ou clique com o botão direito do mouse no contêiner Subnets na árvore de console. Depois toque ou clique em New Subnet. Isso exibe a caixa de diálogo New Object–Subnet, mostrada na Figura 7-11.

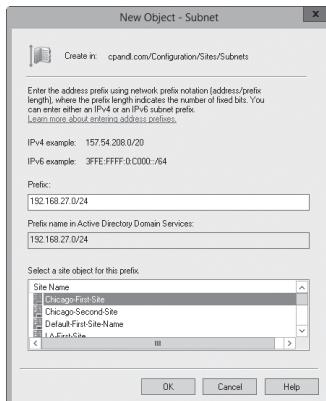


FIGURA 7-11 Para criar a sub-rede, insira o prefixo da rede e selecione um site associado.

2. Na caixa de texto Prefix, digite o prefixo do endereço de rede IPv4 ou IPv6, usando a notação de prefixo de rede. Na notação de prefixo de rede, digite o ID da rede e depois uma barra “/”, especificando em seguida quantos bits são usados para o ID da rede. Por exemplo: se o ID da rede é 192.168.27.0 e os primeiros 24 bits identificam o ID da rede, insira **192.168.27.0/24** como a notação de prefixo de rede.
3. Selecione o site a que deve ser associada a sub-rede e toque ou clique em OK.

DICA Você pode alterar a associação de site para uma sub-rede a qualquer momento. Em Active Directory Sites And Services, dê um toque duplo ou clique duas vezes na pasta Subnets. Na guia General, altere a associação de site na lista Site.

Associação de controladores de domínio a sites

Todo site deve ter ao menos um controlador de domínio associado a ele. Ao adicionar um segundo controlador de domínio a um site, você cria redundância e tolerância a falhas. Se ao menos um controlador de domínio no site também for um servidor de catálogo global, pode-se garantir que as pesquisas de diretório e o tráfego de autenticação sejam restritos ao site.

Os controladores de domínios e os sites podem ser adicionados manual ou automaticamente. Quando você associa sub-redes a um site, qualquer novo controlador de domínio que você instalar e que tenha o endereço IP dentro do intervalo válido de endereços IP para a sub-rede é automaticamente colocado no site. Porém, os controladores de domínio existentes não são associados automaticamente a sites. É preciso associá-los manualmente, movendo o objeto controlador de domínio para o novo site.

Para que você possa mover um controlador de domínio de um site a outro, é preciso primeiro determinar em qual site o controlador de domínio se encontra no momento. Uma maneira rápida de fazê-lo é digitar o seguinte comando em um prompt de comando:

```
dsquery server -s DomainControllerName | dsget server -site
```

Aqui, *DomainControllerName* é o nome de domínio totalmente qualificado do controlador de domínio, como em:

```
dsquery server -s server241.cpandl.com | dsget server -site
```

A saída desse comando é o nome do site em que está localizado o controlador de domínio designado.

Para mover um controlador de domínio de um site para outro, siga as etapas:

1. Em Active Directory Sites And Services, qualquer controlador de domínio associado a um site está listado no nó Servers do site. Selecione o site em que está localizado o controlador de domínio no momento.
2. Pressione e mantenha pressionado ou clique com o botão direito do mouse no controlador de domínio e toque ou clique em Move. Na caixa de diálogo Move Server, toque ou clique no site que deve conter o servidor. Depois, toque ou clique em OK.

OBSERVAÇÃO Não move um controlador de domínio para um site se ele não estiver em uma sub-rede associada ao site. Se você alterar associações de site e sub-rede, é preciso mover os controladores de domínio que estão nas sub-redes afetadas para os conteineres de site apropriados.

Configuração de links de site

Os sites são grupos de sub-redes IP conectados por links confiáveis de alta velocidade. Na maior parte do tempo, todas as sub-redes em uma rede local fazem parte do mesmo site. As redes com vários sites são conectadas por links de site. Os links de site são conexões transitivas lógicas entre dois ou mais sites. Cada link de site tem uma agenda de replicação, um intervalo de replicação, um custo de link e um transporte de replicação.

Como os links de site são usados em conexões de rede de longa distância, a disponibilidade e o uso da largura de banda são pontos importantes a serem considera-

dos quando se está configurando links de site. Por padrão, links de site são agendados para replicar dados 24 horas por dia, sete dias por semana e em um intervalo mínimo de 180 minutos. Se você sabe que um link possui limitações de largura de banda, é preciso alterar o agendamento para permitir que o tráfego de usuário tenha prioridade durante horários de pico.

Quando se tem vários links entre sites, deve-se considerar a prioridade relativa de cada link. A prioridade é determinada com base na disponibilidade e confiabilidade da conexão. O valor padrão do link está definido em 100. Se houverem várias rotas possíveis para um site, aquela com o menor custo de link de site será usada primeiro. Portanto, os caminhos mais confiáveis, com a maior largura de banda entre os sites devem ser configurados, na maioria dos casos, para terem o menor custo de link de site.

Os links de site podem ser configurados para usar como protocolo de transporte RPC sobre IP ou Simple Mail Transfer Protocol (protocolo SMTP). Com o IP como transporte, os controladores de domínio estabelecem uma conexão RPC sobre IP com apenas um parceiro de replicação por vez e replicam as alterações do Active Directory de forma síncrona. Como o RPC sobre IP é síncrono, ambos os parceiros de replicação precisam estar disponíveis no momento em que a conexão for estabelecida. O RPC sobre IP deve ser usado quando houverem conexões dedicadas confiáveis entre sites.

Com o protocolo SMTP como transporte, os controladores de domínio convertem todo o tráfego de replicação em mensagens de email que são enviadas entre os sites de forma assíncrona. Tendo em vista que a replicação SMTP é assíncrona, não é preciso que ambos os parceiros de replicação estejam disponíveis no momento em que a conexão for estabelecida. As transações de replicação podem ser armazenadas até que um servidor de destino esteja disponível. O SMTP deve ser usado quando os links não forem confiáveis ou não estiverem sempre disponíveis.

OBSERVAÇÃO Se você pretende usar o SMTP, é preciso configurar uma certificate authority (CA, Autoridade de Certificação). Os certificados da CA são usados para assinar digitalmente e criptografar mensagens de SMTP enviadas entre os sites. As CAs não são exigidas por padrão para IP.

Para criar um link de site entre dois ou mais sites, siga estas etapas:

1. Em Active Directory Sites And Services, expanda o contêiner Sites e depois expanda o contêiner Inter-Site Transports.
2. Pressione e mantenha pressionado ou clique com o botão direito do mouse no contêiner para o protocolo de transporte que você deseja usar (IP ou SMTP) e depois toque ou clique em New Site Link.
3. Na caixa de diálogo New Object–Site Link, mostrada na Figura 7-12, insira um nome para o link de site, como **ChicagotoSeattleLink**. Nomes de links de site não podem conter espaços ou caracteres especiais, apenas traços.
4. Na lista Sites Not In This Site Link, toque ou clique no primeiro site a ser incluso no link. Depois, toque ou clique em Add para adicionar o site à lista Sites In This Site Link. Repita esse processo para cada um dos sites que você deseja adicionar ao link. É preciso incluir ao menos dois sites. Toque ou clique em OK.

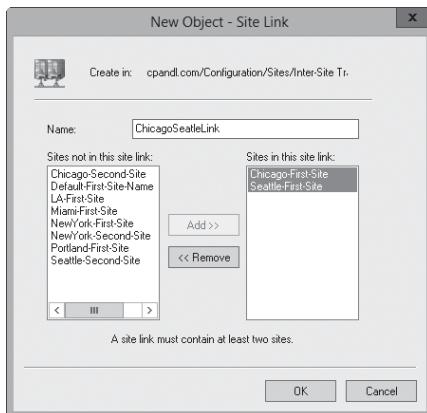


FIGURA 7-12 Para criar o link de site, insira um nome para o link e selecione os sites associados.

Após concluir a criação do link de site, você deve configurar as propriedades do link. Isso permite que você determine o custo do link, a agenda de replicação e o intervalo de replicação. Para configurar as propriedades de um link de site, siga as etapas:

1. Em Active Directory Sites And Services, pressione e mantenha pressionado ou clique com o botão direito do mouse no link de site no painel de detalhes. Depois, toque ou clique em Properties.
2. Na caixa de diálogo Properties, a guia General está selecionada por padrão. Na caixa Cost, defina o custo relativo do link. O custo padrão é 100.
3. Na caixa Replicate Every, defina o intervalo de replicação. O intervalo padrão é 180 minutos.
4. A agenda de replicação padrão é 24 horas por dia, sete dias por semana. Para definir uma agenda diferente, toque ou clique em Change Schedule e defina a agenda de replicação na caixa de diálogo Schedule For. Toque ou clique em OK.

Você pode alterar os sites associados a um link de site a qualquer momento, seguindo as etapas:

1. Em Active Directory Sites And Services, pressione e mantenha pressionado ou clique com o botão direito do mouse no link de site no painel de detalhes. Depois, toque ou clique em Properties.
2. Na caixa de diálogo Properties, a guia General está selecionada por padrão. Na lista Sites Not In This Site Link, toque ou clique no primeiro site a ser incluso no link. Depois, toque ou clique em Add para adicionar o site à lista Sites In This Site Link. Repita esse processo para cada um dos sites que você deseja adicionar ao link.

3. Na lista Sites In This Site Link, toque ou clique no primeiro site que não deve ser incluso no link. Depois, toque ou clique em Remove para adicionar o site à lista Sites Not In This Site Link. Repita esse processo para cada um dos sites que você deseja remover do link. Toque ou clique em OK.

Configuração de pontes de link de site

Todos os links de site são transitivos por padrão. Isso significa que quando mais de dois sites estão vinculados para replicação e utilizam o mesmo transporte, é feita uma ponte entre os links de site automaticamente, permitindo que os links sejam transitivos entre sites. Devido à transitividade, qualquer par de controladores de domínio pode fazer uma conexão por qualquer série de links consecutivos. Por exemplo: um controlador de domínio no site A poderia conectar-se a um controlador de domínio no site C, através do site B.

O caminho de link que os controladores de domínio escolhem para fazer conexões pelos sites é amplamente determinado pelo custo da ponte de link de site. O custo da ponte de link de site é a soma de todos os links inclusos na ponte. Normalmente, é utilizado o caminho com o custo total de ponte de link de site mais baixo.

Sabendo os custos de links e pontes de link, você pode calcular os efeitos de uma falha de rede e determinar os caminhos a serem usados quando uma conexão estiver inoperante. Por exemplo: normalmente, um controlador de domínio no site A se conectararia a um controlador de domínio no site C através do site B. Porém, se a conexão do site B estiver inoperante, os dois controladores de domínio escolheriam automaticamente um caminho alternativo que estivesse disponível, como usar o site D e o site E para estabelecer uma conexão.

Por padrão, a topologia de replicação entre sites é otimizada para um máximo de três saltos. Em configurações de sites grandes, isso pode ter consequências não planejadas, como o mesmo tráfego de replicação passando pelo mesmo link várias vezes. Nesse caso, desabilite a ponte de link de site automática e configure manualmente as pontes de link de sites. Em outros casos não é desejável desabilitar a ponte de link de site automática.

Dentro de uma floresta do Active Directory, pode-se habilitar ou desabilitar a transitividade de link de site por protocolo de transporte. Isso significa que todos os links de sites que utilizam um determinado transporte utilizam ou não a transitividade de link de site. Para configurar a transitividade para um protocolo de transporte, siga as etapas:

1. Em Active Directory Sites And Services, expanda o contêiner Sites e depois expanda o contêiner Inter-Site Transports.
2. Pressione e mantenha pressionado ou clique com o botão direito do mouse no contêiner para o protocolo de transporte que você deseja usar (IP ou SMTP) e depois toque ou clique em Properties.
3. Para habilitar a transitividade de link de site, selecione Bridge All Site Links. Em seguida, toque ou clique em OK. Com a transitividade de link de site habilitada, qualquer ponte de link de site que você tenha criado para um protocolo de transporte em especial será ignorada.
4. Para desabilitar a transitividade de link de site, desmarque a caixa de seleção Bridge All Site Links. Em seguida, toque ou clique em OK. Com a transitividade de link de site desabilitada, é preciso configurar pontes de link de site para o protocolo afetado.

Uma vez que você tenha desabilitado os links transitivos, você pode criar manualmente uma ponte de link de site entre dois ou mais sites. Para isso, siga estas etapas:

1. Em Active Directory Sites And Services, expanda o contêiner Sites e depois expanda o contêiner Inter-Site Transports.
2. Pressione e mantenha pressionado ou clique com o botão direito do mouse no contêiner para o protocolo de transporte que você deseja usar (IP ou SMTP) e depois toque ou clique em New Site Link Bridge.
3. Na caixa de diálogo New Object–Site Link Bridge, insira um nome para a ponte de link de site. Nomes de pontes não podem conter espaços ou caracteres especiais, apenas traços.
4. Na lista Site Links Not In This Site Link Bridge, selecione um link de site para ser incluso na ponte. Toque ou clique em Add para adicioná-lo à lista Site Links In This Site Link Bridge. Repita esse processo para cada um dos links de site que você deseja adicionar à ponte. Uma ponte precisa incluir ao menos dois links de site. Toque ou clique em OK.

Você pode alterar os links de site associados a uma ponte de link de site a qualquer momento, seguindo as etapas:

1. Em Active Directory Sites And Services, pressione e mantenha pressionado ou clique com o botão direito do mouse no contêiner do protocolo de transporte com o qual deseja trabalhar. Depois, toque ou clique em Properties.
2. Na caixa de diálogo Properties, a guia General está selecionada por padrão. Na lista Site Links Not In This Site Link Bridge, toque ou clique no primeiro link de site que deve ser incluso na ponte. Toque ou clique em Add para adicioná-lo à lista Site Links In This Site Link Bridge. Repita esse processo para cada um dos links de site que você deseja adicionar à ponte.
3. Na lista Site Links In This Site Link Bridge, toque ou clique no primeiro link de site que não deve ser incluso na ponte. Toque ou clique em Remove para adicioná-lo à lista Site Links Not In This Site Link Bridge. Repita esse processo para cada um dos links de site que você deseja remover da ponte. Toque ou clique em OK.

Manutenção do Active Directory

Para garantir que as operações do Active Directory sejam adequadas, é preciso realizar monitoramento e manutenção periódicos. No seu trabalho de monitoramento e manutenção, você verá que algumas ferramentas são fundamentais para o seu sucesso. Nesta seção, essas ferramentas serão apresentadas, bem como algumas tarefas de manutenção geral.

Como usar o ADSI Edit

A ferramenta de administração do Active Directory que você deve usar para diagnosticar e solucionar problemas é o ADSI Edit (Editor ADSI). O ADSI Edit pode ser usado para gerenciar as definições de classes de objetos e dos seus atributos no esquema e para trabalhar com outros contextos de nomenclatura, incluindo o contexto de nomenclatura padrão, o contexto de nomenclatura de Configuração e o contexto

de nomenclatura RootDSE. Se quiser criar atributos personalizados para usuários ou grupos, utilize o ADSI Edit. Para iniciá-lo, utilize a opção relacionada no menu Tools do Server Manager.

Para utilizar o snap-in do ADSI Edit para conectar-se a um contexto de nomenclatura, siga as etapas:

1. Pressione e mantenha pressionado ou clique com o botão direito do mouse no nó ADSI Edit na árvore de console. Depois, toque ou clique em Connect To. Isso exibe a caixa de diálogo Connection Settings, mostrada na Figura 7-13.



FIGURA 7-13 Conecte-se a um contexto de nomenclatura no ADSI Edit.

2. Na caixa de diálogo Connection Settings, a lista Select A Well Known Naming Context está habilitada por padrão. Selecione o contexto de nomenclatura com o qual você deseja trabalhar.
3. Ao tocar ou clicar em OK, você estará conectado a qualquer controlador de domínio disponível no seu domínio de logon. Para se conectar a outro domínio ou servidor, selecione Select Or Type A Domain Or Server. Em seguida, escolha o servidor ou o domínio com o qual você quer trabalhar, juntamente com um número de porta opcional para a conexão, como FileServer252.cpndl.com:389. A porta 389 é a porta padrão para LDAP.

Uma vez que você tenha selecionado um contexto de nomenclatura, um domínio e um servidor, você estará conectado ao contexto de nomenclatura e poderá trabalhar com ele. Como mostra a Figura 7-14, ao conectar-se a diversos contextos de nomenclatura você tem nós separados para gerenciar cada um dos contextos. Para a solução de problemas, você também pode se conectar ao mesmo contexto de nomenclatura em servidores diferentes no mesmo domínio. Para identificar um problema de replicação, compare os valores associados às propriedades em um servidor com os de outro servidor.

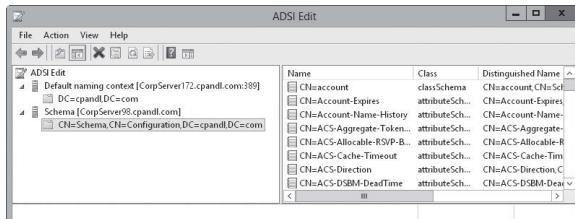


FIGURA 7-14 Navegue nos contextos de nomenclatura para examinar contêineres e propriedades relacionadas.

Como examinar a topologia entre sites

O Inter-Site Topology Generator (ISTG, Gerador de Topologia entre Sites) em um site é responsável pela geração da topologia de replicação entre sites. Ao calcular a topologia de replicação, o ISTG pode usar um poder de processamento considerável, especialmente conforme vá crescendo o tamanho da rede. Por esse motivo você deve monitorar de perto o ISTG em cada site para garantir que ele não seja sobrecarregado.

Para determinar qual controlador de domínio controla o ISTG, siga estas etapas:

1. Em Active Directory Sites And Services, expanda o contêiner Sites e expanda o site para o ISTG que você deseja localizar na árvore de console.
2. No painel de detalhes, dê um toque duplo ou clique duas vezes em NTDS Site Settings. Na caixa de diálogo NTDS Site Settings, o ISTG atual está listado no painel Inter-Site Topology Generator.

A replicação entre os sites é realizada normalmente por *bridgehead servers* (servidores bridgehead). Um servidor bridgehead é um controlador de domínio designado pelo ISTG para realizar a replicação entre sites. O ISTG configura um servidor bridgehead para cada partição do Active Directory que precisa ser replicada e mantém uma topologia de replicação separada para cada tipo de partição. Ainda que um único servidor bridgehead possa ser responsável pela replicação de várias partições de diretório, a topologia de replicação para cada partição é mantida separadamente.

Os controladores de domínio que são designados como servidores bridgehead possuem uma carga de trabalho adicional, que vai aumentando com o número e a frequência das alterações a serem replicadas. Da mesma forma que você deve fazer com o ISTG, monitore periodicamente os servidores bridgehead para garantir que não sejam sobrecarregados. Para listar os servidores bridgehead em um site, insira o seguinte comando em um prompt de comando:

```
repadmin /bridgeheads site:SiteName
```

Onde *SiteName* é o nome do site, como:

```
repadmin /bridgeheads site:SacramentoSite
```

Se os servidores bridgehead atuais ficaram sobrecarregados ou se você tem controladores de domínio que preferiria que fossem servidores bridgehead, pode desig-

nar os servidores bridgehead preferenciais a serem usados. Uma vez que você tenha designado um servidor bridgehead preferencial para um site, o ISTG utiliza-o para a replicação entre sites. Caso o servidor bridgehead preferencial fique offline ou seja incapaz de replicar por algum motivo qualquer, a replicação entre sites é parada até que o servidor esteja disponível novamente ou até que você tenha alterado a configuração de servidor bridgehead preferencial.

Ao designar bridgeheads preferenciais, sempre configure doversos servidores bridgehead preferencias em cada site. O ISTG escolherá um dos servidores que você designou como o servidor bridgehead preferencial. Se o servidor falhar, o ISTG escolherá outro servidor da lista de servidores bridgehead preferenciais.

É necessário configurar um servidor bridgehead para cada partição que precisa ser replicada. Isso significa que você deve configurar ao menos um controlador de domínio com uma réplica de cada partição de diretório como um servidor bridgehead. Se você não proceder dessa forma, a replicação da partição falhará e o ISTG fará o log de um evento detalhando a falha no log de eventos do Directory Services.

Para configurar um controlador de domínio como o servidor bridgehead preferencial, siga estas etapas:

1. Em Active Directory Sites And Services, os controladores de domínio associados a um site estão listados no nó Servers do site. Pressione e mantenha pressionado ou clique com o botão direito do mouse no servidor que você quer designar como um bridgehead preferencial e toque ou clique em Properties.
2. Na caixa de diálogo Properties, selecione o protocolo de transporte entre sites para o qual o servidor deve ser um bridgehead preferencial na lista Transports Available For Inter-Site Data Transfer. Depois, toque ou clique em Add. Repita conforme for necessário para determinar tanto IP quanto SMTP. Toque ou clique em OK.

Tendo designado servidores bridgehead preferenciais, há diversas maneiras de se recuperar de uma falha na replicação. Você pode remover os servidores falhos da condição de servidores bridgehead preferenciais e designar outros servidores bridgehead preferenciais. Pode também remover todos os servidores da condição de servidores bridgehead preferenciais e permitir que o ISTG selecione os servidores bridgehead que devem ser usados. Para que um servidor deixe de ser o bridgehead preferencial para um determinado protocolo de transporte, siga as etapas:

1. Em Active Directory Sites And Services, os controladores de domínio associados a um site estão listados no nó Servers do site. Pressione e mantenha pressionado ou clique com o botão direito do mouse no servidor que você quer deixar de utilizar como bridgehead preferencial e toque ou clique em Properties.
2. Selecione o protocolo de transporte na lista This Server Is A Preferred Bridgehead Server For The Following Transports e toque ou clique em Remove. Toque ou clique em OK.

Solução de problemas do Active Directory

Como parte da manutenção de rotina, é preciso monitorar controladores de domínio, servidores de catálogo global, servidores bridgehead e links de sites. Na maioria dos casos, se você desconfiar que há problemas com o Active Directory, veja a replicação como ponto de partida para o diagnóstico e solução de problemas. Ao configurar o

monitoramento da replicação intrassite e entre sites do Active Directory, é possível diagnosticar e solucionar a maioria dos problemas de replicação. Porém, lembre-se que a replicação de Active Directory possui diversas dependências de serviços, incluindo: LDAP, Domain Name System (DNS), Kerberos version 5 authentication e Remote Procedure Call (RPC).

Esses serviços importantes devem estar funcionando corretamente para permitir que atualizações de diretório sejam replicadas. Durante a replicação, o Active Directory depende de várias portas TCP e UDP estarem abertas entre os controladores de domínio. Por padrão, as portas utilizadas são as seguintes:

- O LDAP utiliza TCP e UDP na porta 389 para tráfego padrão e TCP na porta 686 para tráfego seguro.
- Os catálogos globais utilizam TCP na porta 3268. O Kerberos versão 5 utiliza TCP e UDP na porta 88.
- O DNS utiliza TCP e UDP na porta 53.
- O SMB sobre IP utiliza TCP e UDP na porta 445.

Além disso, para a replicação de arquivos nas pastas compartilhadas do System Volume (SYSVOL) em controladores de domínio, o Active Directory utiliza ou o File Replication Service (FRS) ou o DFS Replication Service. O serviço de replicação apropriado deve ser executado e configurado corretamente para replicar o SYSVOL.

O Active Directory rastreia as alterações usando USNs. Toda a vez que é feita uma alteração no diretório, o controlador de domínio que está processando a alteração atribui um USN a ela. Cada controlador de domínio mantém seus próprios USNs locais e incrementa o valor toda a vez que ocorre uma alteração. O controlador de domínio também atribui o USN local ao atributo de objeto que foi alterado. Cada objeto possui um atributo relacionado, chamado *uSNChanged*, que é armazenado com o objeto e identifica o USN mais alto que tenha sido atribuído a qualquer um dos atributos do objeto.

Cada controlador de domínio acompanha o seu USN local e também os USNs locais dos outros controladores de domínio. Durante a replicação, os controladores de domínio comparam os valores de USN recebidos com os que estão armazenados. Se o valor de USN atual de um determinado controlador de domínio for mais alto que o valor armazenado, as alterações associadas com aquele controlador de domínio precisam ser replicadas. Se o valor de USN atual de um determinado controlador de domínio for igual ao valor armazenado, as alterações associadas com aquele controlador de domínio não precisam ser replicadas.

A replicação pode ser monitorada pela linha de comando, utilizando o Repadmin. Com o Repadmin, a maioria dos parâmetros de linha de comando aceitam uma lista dos controladores de domínio com os quais você deseja trabalhar, chamada DCList. Os valores para DCList podem ser especificados da seguinte maneira:

- * Um curinga que inclui todos os controladores de domínio da organização
- **PartialName** Um nome de servidor parcial, seguido pelo caractere * curinga para corresponder ao restante do nome do servidor
- **Site:SiteName** O nome do site do qual você quer incluir controladores de domínio
- **Gc** Incluir todos os servidores de catálogo global da organização

Ainda que o Repadmin possua vários parâmetros e você possa utilizá-lo de diversas maneiras, algumas tarefas serão mais usadas que outras. A Tabela 7-2 apresenta algumas dessas tarefas.

TABELA 7-2 Comandos e tarefas de replicação comuns

TAREFA	COMANDO
Forçar o Knowledge Consistency Checker (KCC) a recalcular a topologia de replicação intra-site para um determinado controlador de domínio.	repadmin /kcc DCList [/async]
Listar servidores bridgehead que correspondam à DCList.	repadmin /bridgeheads [DCList] [/verbose]
Listar as chamadas feitas e ainda não respondidas pelo servidor especificado para outros servidores.	repadmin /showoutcalls [DCList]
Listar os domínios em que um determinado domínio confia.	repadmin /showtrust [DCList]
Listar eventos com falha na replicação detectados pelo KCC.	repadmin /failcache [DCList]
Listar objetos de conexão para os controladores de domínio especificados. O padrão é o site local.	repadmin /showconn [DCList]
Listar os computadores que tenham sessões abertas com um determinado controlador de domínio.	repadmin /showctx [DCList]
Listar o nome do ISTG para um determinado site.	repadmin istg [DCList] [/verbose]
Listar parceiros de replicação para cada partição de diretório no controlador de domínio especificado.	repadmin /showrepl [DCList]
Listar um resumo do estado de replicação.	repadmin /replsummary [DCList]
Listar os certificados do servidor carregados nos controladores de domínio especificados.	repadmin /showcert [DCList]
Listar tarefas em espera na fila de replicação.	repadmin /queue [DCList]
Listar o intervalo de replicações entre sites usando o carimbo de hora ISTG Keep Alive.	repadmin /latency [DCList] [/verbose]

CAPÍTULO 8

Como criar contas de usuário e de grupo

- Modelo de segurança do Windows Server **294**
- Diferenças entre contas de usuário e de grupo **299**
- Contas de usuário e grupos padrão **304**
- Capacidades de conta **307**
- Uso de contas de grupo padrão **313**
- Configuração e organização da conta de usuário **316**
- Configuração das políticas de conta **320**
- Configuração das políticas de direitos do usuário **325**
- Como adicionar uma conta de usuário **328**
- Como adicionar uma conta de grupo **333**
- Manipulação de associação de grupo **336**
- Implementação de contas gerenciadas **339**

O gerenciamento de contas é uma das tarefas primárias de um administrador do Microsoft Windows. O Capítulo 7, "Administração básica do Active Directory", aborda as contas de computador. Este capítulo examina as contas de usuário e de grupo. Com as contas de usuário, você pode permitir que usuários individuais se conectem à rede e acessem os recursos da rede. Com as contas de grupo, você gerencia recursos para vários usuários. As permissões e privilégios que você atribui a contas de usuário e de grupo determinam quais ações os usuários podem executar, bem como quais sistemas de computador e recursos eles podem acessar.

Embora você possa ficar tentado a conceder aos usuários um amplo acesso, é preciso equilibrar a necessidade de um usuário acessar recursos relacionados ao trabalho com sua necessidade de proteger recursos confidenciais ou informações privilegiadas. Por exemplo, você certamente não quer que todas as pessoas da empresa tenham acesso aos dados de folha de pagamento. Consequentemente, você deve se certificar de que apenas quem precisa dessas informações tenha acesso a elas.

Neste capítulo, você aprenderá como gerenciar contas de domínio. Embora as contas do computador local sejam discutidas, elas não são o assunto principal. Para obter mais informações sobre a configuração de contas do computador local, consulte o Capítulo 7, "Managing User Access and Security", no livro *Microsoft Windows 8 Administration Pocket Consultant* (Microsoft Press, 2012). Lembre-se de que o Windows 8 inclui um tipo especial de conta local, a *conta da Microsoft*. As contas da Microsoft podem ser consideradas contas locais sincronizadas. Embora as contas da Microsoft não estejam disponíveis em domínios, os usuários podem acessar a Windows Store usando

credenciais armazenadas no Windows e também podem usar *apps*. Uso aqui o termo *apps* apenas para ajudar a distinguir *apps* de área de trabalho e programas de área de trabalho. Para ler uma discussão mais profunda sobre o gerenciamento de *apps* e do acesso à Windows Store, consulte o Capítulo 8, "Installing and Maintaining Programs", do livro *Microsoft Windows 8 Administration Pocket Consultant*.

Modelo de segurança do Windows Server

O acesso aos recursos de rede é controlado por meio dos componentes do modelo de segurança do Windows Server. Os principais componentes que você precisa conhecer são os usados para o controle de autenticação e de acesso.

Protocolos de autenticação

A autenticação do Windows Server é implementada como um processo de duas etapas que consiste em um logon interativo e na autenticação de rede. Quando um usuário efetua logon em um computador com uma conta de domínio, o processo de logon interativo autentica as credenciais de logon do usuário, o que confirma a identidade do usuário ao computador local e concede acesso ao Active Directory Domain Services (AD DS, Serviços de Domínio do Active Directory). Após, sempre que o usuário tentar acessar recurso da rede, a autenticação de rede é usada para determinar se o usuário tem permissão para isso.

O Windows Server 2012 é compatível com muitos protocolos de autenticação de rede. O Active Directory usa o Kerberos versão 5 como o protocolo de autenticação padrão. A autenticação NTLM é mantida apenas para fins de compatibilidade com versões anteriores. Na Group Policy (política de grupo), você pode controlar como o NTLM é usado com a opção de segurança Network Security: LAN Manager Authentication Level. O nível padrão de autenticação é, na maioria dos casos, Send NTLMv2 Response Only. Com esse nível de autenticação, os clientes usam o NTLM versão 2 para autenticação e segurança de sessão se o servidor for compatível. O Active Directory também pode usar certificados de cliente para prover autenticação.

Um recurso-chave do modelo de autenticação do Windows Server é que ele comporta logon único, que funciona conforme descrito a seguir:

1. Um usuário efetua logon no domínio com um nome de logon e uma senha ou inserindo um cartão inteligente em um leitor de cartão.
2. O processo de logon interativo autentica o acesso do usuário. Com uma conta local, as credenciais são autenticadas localmente e o usuário recebe acesso ao computador local. Com uma conta de domínio, as credenciais são autenticadas no Active Directory, e o usuário tem acesso aos recursos locais e da rede.
3. A partir desse ponto, o usuário pode autenticar-se em qualquer computador no domínio por meio do processo de autenticação de rede.

Com contas de domínio, o processo de autenticação de rede normalmente é automático (por meio de logon único). Com contas locais, por outro lado, os usuários devem fornecer um nome de usuário e senha todas as vezes que acessarem um recurso de rede.

O Windows Server inclui o Active Directory Federation Services (AD FS, Serviços de Federação do Active Directory), que estende o logon único a recursos confiáveis da

Internet. Com o AD FS, as organizações podem estender sua infraestrutura existente do Active Directory para fornecer acesso a recursos confiáveis da Internet, que podem incluir recursos de terceiros, bem como de unidades geograficamente separadas da mesma organização. Após a configuração de servidores federados, os usuários localizados na organização podem efetuar logon uma vez na rede da organização e serem automaticamente conectados a aplicativos Web confiáveis hospedados na Internet por parceiros. O Single Sign-On federado da Web usa autorização federada para fornecer acesso transparente. Além da identidade do usuário e das informações da conta, os tokens de segurança usados na autorização federada incluem declarações (claims) de autorização que fornecem detalhes da autorização do usuário e de características específicas do aplicativo.

Controles de acesso

O Active Directory é baseado em objeto. Usuários, computadores, grupos, recursos compartilhados e muitas outras entidades são definidas como objetos. Os controles de acesso são aplicados a esses objetos com descritores de segurança. Os descritores de segurança:

- Listam os usuários e grupos que recebem acesso a objetos
- Especificam as permissões atribuídas a usuários e grupos
- Rastreiam eventos que devem receber auditoria por objetos
- Definem a posse de objetos

As entradas individuais do descritor de segurança são chamadas de access control entries (ACEs, entradas de controle de acesso). Objetos do Active Directory podem herdar ACEs de seus objetos-pai. Isso significa que as permissões de um objeto-pai podem ser aplicadas a um objeto-filho. Por exemplo, todos os membros do grupo Domain Admins herdam permissões concedidas a esse grupo.

Ao trabalhar com ACEs, lembre-se:

- As ACEs são criadas com a herança habilitada por padrão.
- A herança começa a operar imediatamente após a ACE ser criada e salva.
- Todas as ACEs contêm informações especificando se a permissão é herdada ou atribuída explicitamente ao objeto relacionado.

Controles de acesso baseados em declarações

O Windows Server 2012 adiciona aos controles de acesso padrão a blindagem Kerberos, identidades compostas e controles de acesso baseados em declarações (*claims-based*). O Kerberos com a blindagem aumenta a segurança do domínio permitindo aos clientes que ingressaram em um domínio e os controladores de domínio se comunicarem por canais seguros e criptografados. As identidades compostas incorporam não apenas os grupos dos quais um usuário é membro, mas também as declarações do usuário, declarações do dispositivo e propriedades do recurso.

Os controles de acesso baseados em declarações (*claims-based*) podem ser configurados de diversas maneiras. A abordagem mais simples é definir as condições que limitam o acesso como parte das permissões de segurança avançadas de um recurso. Normalmente, essas condições adicionam declarações do dispositivo e do usuário aos controles de acesso. As declarações do usuário identificam usuários, enquanto as declarações do dispositivo identificam dispositivos. Por exemplo, para acessar o

compartilhamento de Recursos Humanos, você pode adicionar uma declaração de dispositivo para garantir que o computador que está sendo usado para acessar um recurso é membro de RH Computadores e uma declaração de usuário que assegure que o usuário é membro do grupo RH Gerentes.

A blindagem Kerberos, as identidades compostas e os controles de acesso baseados em declarações também podem trabalhar em conjunto como parte de uma nova plataforma de autorização que permite acesso dinâmico a recursos por meio de políticas de acesso central. Com essas políticas, definem-se regras de acesso central no Active Directory que são aplicadas dinamicamente em toda a empresa. As regras de acesso central usam expressões condicionais que requerem que você determine as propriedades do recurso, os tipos de declaração e os grupos de segurança exigidos para a política e os servidores em que a política deve ser aplicada.

Antes de poder definir e aplicar uma regra de acesso, você provavelmente terá que definir as propriedades do recurso e os tipos de declaração:

- As propriedades do recurso criam definições de propriedade para recursos. Por exemplo, você pode adicionar as propriedades Department e Country a arquivos para controlar dinamicamente o acesso por departamento e país.
- Os tipos de declaração criam definições de declaração para recursos. Por exemplo, você pode criar uma declaração do usuário para adicionar as propriedades Department e Country a objetos de usuário com a finalidade de controlar dinamicamente o acesso por departamento e país.

Após criar propriedades do recurso e tipos de declaração e determinar os locais em que a política deve ser aplicada, é possível criar uma regra de acesso e adicioná-la a uma política de acesso central. A inclusão da regra em uma política a torna disponível para controle dinâmico. Agora, você precisa aplicar a política em servidores de arquivos por meio da Group Policy.

A política baseada em declarações deve estar habilitada para a política Default Domain Controllers. Isso é feito por meio da habilitação e da configuração da diretiva KDC Support For Claims, Compound Authentication And Kerberos Armoring nas políticas em Administrative Templates para Computer Configuration sob System\KDC. A política deve ser configurada para usar um modo específico. Os modos disponíveis são:

- **Supported** Os controladores de domínio são compatíveis com declarações, identidades compostas e blindagem Kerberos. Os computadores clientes que não comportam a blindagem Kerberos podem ser autenticados.
- **Always Provide Claims** Este modo é igual ao Supported, mas os controladores de domínio sempre retornam declarações para contas.
- **Fail Unarmored Authentication Requests** A blindagem Kerberos é obrigatória. Os computadores clientes que não comportam a blindagem Kerberos não podem ser autenticados.

A política Kerberos Client Support For Claims, Compound Authentication And Kerberos Armoring nas políticas em Administrative Templates para Computer Configuration sob System\Kerberos controla se o cliente Kerberos com Windows 8 e Windows Server 2012 solicita declarações e autenticação composta. A política deve ser habilitada para clientes Kerberos compatíveis para solicitar diretivas e autenticação composta para Dynamic Access Control e blindagem Kerberos.

MUNDO REAL A política baseada em declarações deve ser habilitada para todos os controladores de domínio de um domínio para garantir uma aplicação consistente. Um domínio deve ter, no mínimo, um controlador de domínio com Windows Server 2012, e os servidores de arquivos devem executar o Windows Server 2012. Por padrão, os controladores de domínio são posicionados na unidade organizacional (OU, organizational unit) Domain Controllers e a política Default Domain Controllers tem a precedência mais alta entre as Group Policy Objects (GPOs, objetos de Group Policy) vinculadas à OU Domain Controllers. Se sua organização usa uma abordagem diferente, você precisa assegurar que a GPO com a precedência mais alta para a OU apropriada tem a política baseada em declarações habilitada e configurada adequadamente.

Políticas de acesso central

As políticas de acesso central não substituem os controles de acesso tradicionais. Em vez disso, elas são projetadas para aprimorar os controles de acesso existentes definindo de maneira muito precisa os atributos específicos que usuários e dispositivos devem apresentar para acessar recursos. O modo mais fácil de gerenciar uma política de acesso central é por meio do Active Directory Administrative Center.

A seguir, é apresentada uma visão geral do processo de criação e implantação da política:

1. Abra o Active Directory Administrative Center. No painel esquerdo, a opção List View está selecionada por padrão. Toque ou clique em Tree View para escolher o modo de exibição de árvore. Em seguida, expanda Dynamic Access Control no painel esquerdo e selecione Claim Types.
2. Use o nó Claim Types para criar e gerenciar os tipos de declaração. Por exemplo, clique com o botão direito do mouse no nó Claim Types, clique em New e selecione Claim Type para iniciar a criação de um novo tipo de declaração.
3. Use o nó Resource Properties para criar e gerenciar propriedades do recurso. Por exemplo, clique com o botão direito do mouse no nó Resource Properties, clique em New e selecione Resource Property para iniciar a criação de uma nova propriedade do recurso.

OBSERVAÇÃO As propriedades do recurso são adicionadas como propriedades de definição de classificação em servidores de arquivos também.

4. Use o nó Central Access Rules para criar e gerenciar regras de acesso central. Por exemplo, clique com o botão direito do mouse no nó Central Access Rules, clique em New e selecione Central Access Rule para iniciar a criação de uma nova regra de acesso.
5. Use o nó Central Access Policies para criar e gerenciar políticas de acesso central. Por exemplo, clique com o botão direito do mouse no nó Central Access Policies, clique em New e selecione Central Access Policy para iniciar a criação de uma nova política de acesso.

Para concluir a implantação, é necessário editar a GPO de precedência mais alta vinculada à OU em que você coloca servidores de arquivos e habilitar as políticas de acesso central. Para isso, siga estas etapas:

1. Em Group Policy Management, abra a GPO a ser editada.

2. Navegue pelas políticas de Computer Configuration até Windows Settings\Security Settings\File System.
3. Pressione e mantenha pressionado ou clique com o botão direito do mouse em Central Access Policy e toque ou clique em Manage Central Access Policies. A caixa de diálogo Central Access Policies Configuration será aberta.
4. Na caixa de diálogo Central Access Policies Configuration, as políticas disponíveis estão listadas no painel esquerdo e as políticas que estão sendo aplicadas no momento estão listadas no painel direito. Para aplicar uma política, clique na política a partir do painel esquerdo e clique em Add. Para remover uma política, clique na política a partir do painel direito e clique em Remove. Clique em OK.

Após as alterações de Group Policy entrarem em vigor em seus servidores, os controles dinâmicos são disponibilizados. Você pode acelerar a atualização inserindo **gpupdate /force** em um prompt de comando elevado com privilégios de administrador.

Os servidores para os quais você deseja aplicar controles dinâmicos devem ter, no mínimo, a função File And Storage Services com os serviços de função File Server, Storage Services e File Server Resource Manager. Você precisa do serviço de função File Server Resource Manager e as ferramentas relacionadas para aplicar definições de propriedades de classificação a pastas.

Após habilitar a política de acesso central e todas as vezes que você atualizar as definições de propriedades de classificação, será necessário esperar que as Global Resource Properties do Active Directory atualizem também seus servidores de arquivos. Esse processo pode ser acelerado abrindo o Windows PowerShell e inserindo **update-fsrmclassificationpropertydefinition**. Faça isso em cada servidor de arquivos no qual você quer configurar políticas de acesso central.

Para concluir a implantação de políticas de acesso central, você precisa editar as propriedades de cada pasta em que uma política de acesso central será aplicada e seguir estas etapas:

1. Adicione as definições de classificação apropriadas na guia Classification da pasta. Na guia Classification estarão listadas todas as propriedades do recurso criadas. Selecione uma propriedade por vez e configure seu valor conforme apropriado.
2. Habilite a política adequada por meio das configurações de segurança avançadas para a pasta. Na guia Security, toque ou clique em Advanced e selecione a guia Central Policy. Qualquer política que estiver selecionada ou sendo aplicada no momento estará listada juntamente com uma descrição que permite a você analisar as regras dessa política. Ao tocar ou clicar em Change, você pode usar a lista de seleção fornecida para selecionar uma política para ser aplicada ou pode escolher No Central Access Policy para interromper o uso da política. Toque ou clique em OK.

Repeta esse processo para cada pasta de nível superior ou outra pasta cujo acesso você quer limitar. Os arquivos e as pastas que estiverem na pasta selecionada herdarão automaticamente a regra de acesso a menos que você especifique o contrário. Por exemplo, se você criar uma regra de acesso chamada "Gerentes de RH nos EUA" e estabelecer definições do recurso Department e Country, poderá editar as propriedades da pasta RH, selecionar a guia Classification e usar as opções disponíveis para configurar Department para RH e Country para EUA. Então, você poderia aplicar a política "Gerentes de RH nos EUA" com as configurações de segurança avançadas para a pasta.

Diferenças entre contas de usuário e de grupo

O Windows Server 2012 fornece contas de usuário e contas de grupo (das quais os usuários podem ser membros). As contas de usuário são projetadas para pessoas. Por sua vez, as contas de grupo são projetadas para facilitar a administração de vários usuários. Embora você possa efetuar logon com contas de usuário, não é possível efetuar logon com uma conta de grupo. As contas de grupo são normalmente chamadas simplesmente de *grupos*.

MUNDO REAL O Windows Server dá suporte ao objeto *InetOrgPerson*. Essencialmente, esse objeto é igual a um objeto de usuário, e você pode usá-lo como tal. No entanto, a real finalidade do objeto *InetOrgPerson* é permitir a compatibilidade e a transição de serviços de diretório de terceiros X.500 e Lightweight Directory Access Protocol (LDAP) que usam esse objeto para representar usuários. Se você estiver migrando de um serviço de diretório de terceiros e acabar com muitos objetos *InetOrgPerson*, não se preocupe. Você pode usá-los como entidades de segurança assim como as contas de usuário. O objeto *InetOrgPerson* estará completamente habilitado apenas em modo funcional de domínio Windows Server 2003 ou superior. Nesse modo, é possível configurar senhas para objetos *InetOrgPerson* e alterar a classe de objeto se desejado. Quando você alterar a classe de objeto, o objeto *InetOrgPerson* será convertido a um objeto de usuário e, a partir de então, ele estará listado como tipo User no Active Directory Users And Computers (Usuários e Computadores do Active Directory).

Contas de usuário

Há dois tipos de contas de usuário definidos no Windows Server:

- Contas de usuário definidas no Active Directory são chamadas de *contas de usuário de domínio*. Por meio de logon único, as contas de usuário de domínio podem acessar recursos de todo o domínio. As contas de usuário de domínio são criadas no Active Directory Users And Computers.
- Contas de usuário definidas em um computador local são chamadas de *contas de usuário locais*. As contas de usuário locais têm acesso apenas ao computador local e devem autenticar a si mesmas antes de poderem acessar recursos de rede. As contas de usuário locais são criadas com o utilitário Local Users And Groups.

OBSERVAÇÃO Em um domínio, apenas os servidores membros e as estações de trabalho apresentam contas de usuário e de grupo local. No primeiro controlador de domínio de um novo domínio, essas contas são movidas do banco de dados local do Security Account Manager (SAM) para o Active Directory e, então, tornam-se contas de domínio.

Nomes de logon, senhas e certificados públicos

Todas as contas de usuário são identificadas com um nome de logon. No Windows Server, esse nome de logon tem duas partes:

- **Nome de usuário** O rótulo de texto para a conta
- **Domínio ou grupo de trabalho do usuário** O grupo de trabalho ou domínio em que está a conta de usuário

Para o usuário wrstanek, cuja conta está criada no domínio cpndl.com, o nome completo de logon é wrstanek@cpndl.com. O nome de logon anterior ao Windows 2000 seria CPANDL\wrstanek.

Ao trabalhar com o Active Directory, talvez você também precise especificar o *fully qualified domain name* (FQDN, nome de domínio totalmente qualificado) de um usuário. O FQDN de um usuário é a combinação do nome de domínio Domain Name System (DNS, Sistema de Nomes de Domínio), do contêiner ou OU que contém o usuário e do nome de usuário. Para o usuário *cpndl.com\users\wrstanek*, *cpndl.com* é o nome de domínio DNS, *users* é o local do contêiner ou da OU e *wrstanek* é o nome de usuário.

As contas de usuário também podem ser associadas a senhas e certificados públicos. As senhas são cadeias de caracteres para autenticação de uma conta. Os certificados públicos combinam uma chave pública e uma chave privada para identificar um usuário. Com uma senha, o logon é efetuado interativamente. Com um certificado público, o logon é efetuado por meio de um cartão inteligente e de um leitor de cartão inteligente.

Security identifiers e contas de usuário

Embora o Windows Server exiba nomes de usuário para descrever privilégios e permissões, as chaves de identificação para contas são os *security identifiers* (IDs, identificadores de segurança). Os IDs são identificadores exclusivos gerados quando contas são criadas. Cada SID de conta consiste no prefixo do ID de segurança do domínio e de um ID relativo exclusivo, que é alocado pelo mestre de RID.

O Windows Server usa esses identificadores para rastrear contas independentemente dos nomes de usuário. Os IDs apresentam várias finalidades. As duas finalidades mais importantes são permitir a alteração fácil de nomes de usuário e também a exclusão de contas sem a preocupação de que alguém possa ganhar acesso a recursos simplesmente recriando uma conta com o mesmo nome.

Ao alterar um nome de usuário, você diz ao Windows Server para mapear um determinado SID para um novo nome. Ao excluir uma conta, você diz ao Windows Server que um determinado SID deixou de ser válido. Depois disso, mesmo se você criar uma conta com o mesmo nome de usuário, a nova conta não terá os mesmos privilégios e permissões que a anterior. Isso acontecerá porque a nova conta terá um novo SID.

Contas de grupo

Além das contas de usuário, o Windows Server fornece grupos. De maneira geral, os grupos são usados para conceder permissões a tipos similares de usuários e simplificar a administração de contas. Se um usuário for membro de um grupo que pode acessar um recurso, esse usuário pode acessar o mesmo recurso. Portanto, é possível fornecer a um usuário acesso a vários recursos relacionados ao trabalho apenas tornando-o membro do grupo correto. Observe que embora você possa efetuar logon em um computador com uma conta de usuário, isso não pode ser feito com uma conta de grupo.

Como diferentes domínios do Active Directory podem ter grupos com o mesmo nome, a referência aos grupos frequentemente é feita com o padrão *domínio\nomedogrupo*, como *cpndl\gmarketing* para o grupo *Gmarketing* do domínio *cpndl*. Ao trabalhar com o Active Directory, talvez você também precise especificar o FQDN de um grupo. O FQDN de um grupo é a concatenação do nome de domínio DNS, do posicionamento do contêiner ou OU e do nome de grupo. Para o grupo *cpndl.com\users\gmarketing*, *cpndl.com* é o nome de domínio DNS, *users* é o contêiner ou OU que o grupo está contido e *gmarketing* é o nome de grupo.

MUNDO REAL Os funcionários de um departamento de marketing provavelmente precisam de acesso a todos os recursos relacionados a marketing. Em vez de conceder a cada funcionário individual acesso a esses recursos, você poderia tornar os usuários membros de um grupo de marketing. Assim, eles automaticamente obtêm os privilégios do grupo. Depois, se um usuário for transferido para outro departamento, basta remover o usuário do grupo revogando, assim, todas as permissões de acesso. Se compararmos essa técnica com ter que revogar acesso a cada recurso individual, poderemos perceber que ela é bem fácil, de modo que será melhor usar os grupos sempre que possível.

Tipos de grupo

O Windows Server é compatível com três tipos de grupos:

- **Grupos locais** Grupos que são definidos em um computador local. Os grupos locais são usados apenas no computador local. Os grupos locais são criados com o utilitário Local Users And Groups.
- **Grupos de segurança** Grupos que podem ser associados a descritores de segurança. Os grupos de segurança são definidos em domínios por meio do Active Directory Users And Computers.
- **Grupos de distribuição** Grupos usados como listas de distribuição de emails. Eles não podem ser associados a descritores de segurança. Os grupos de distribuição são definidos em domínios por meio do Active Directory Users And Computers.

OBSERVAÇÃO A maioria das abordagens gerais sobre grupos enfocam os grupos locais e os grupos de segurança em vez dos grupos de distribuição. Os grupos de distribuição apresentam como única finalidade a distribuição de emails, não proporcionando a atribuição e o gerenciamento de acesso.

Escopo do grupo

No Active Directory, os grupos podem ter diferentes escopos: local de domínio, local interno, global e universal. Ou seja, os grupos são válidos em áreas diferentes, conforme descrito a seguir:

- **Grupos domínio local** Grupos usados principalmente para atribuir permissões de acesso a recursos dentro de um domínio único. Os grupos domínio local podem incluir membros de qualquer domínio da floresta e de domínios confiáveis de outras florestas. Normalmente, os grupos globais e universais são membros de grupos domínio local.
- **Grupos locais internos** Grupos com um escopo de grupo especial que apresentam permissões locais no domínio e que, para fins de simplicidade, são frequentemente incluídos no termo *grupos domínio local*. A diferença entre os grupos locais internos e os outros grupos é que você não pode criar ou excluir grupos locais internos, pode apenas modificá-los. As referências feitas aos grupos domínio local aplicam-se aos grupos locais internos a menos que avisado do contrário.
- **Grupos globais** Grupos usados principalmente para definir conjuntos de usuários ou computadores do mesmo domínio que compartilham uma função, funcionalidade ou trabalho similar. Os membros dos grupos globais podem incluir apenas contas e grupos do domínio em que são definidos.

- Grupos universais** Grupos usados principalmente para definir conjuntos de usuários ou computadores que devem ter amplas permissões em todo um domínio ou floresta. Os membros de grupos universais incluem contas, grupos globais e outros grupos universais de qualquer domínio da árvore de domínios ou da floresta.

PRÁTICAS RECOMENDADAS Os grupos universais são muito úteis em empresas de grande porte com vários domínios. Com o planejamento adequado, você pode usar os grupos universais para simplificar a administração do sistema. Não é recomendável que membros de grupos universais sejam alterados com frequência. Cada vez que você altera os membros de um grupo universal, é necessário replicar essas alterações a todos os servidores de catálogo global da árvore de domínios ou da floresta. Para reduzir as alterações, atribua outros grupos em vez de contas de usuário ao grupo universal. Para obter mais informações, consulte “Quando usar grupos domínio local, globais e universais” mais adiante neste capítulo.

Quando você trabalha com grupos, o escopo do grupo restringe o que você pode ou não pode fazer. A Tabela 8-1 fornece um breve resumo desses itens. Para obter os detalhes completos sobre a criação de grupos, consulte “Como adicionar uma conta de grupo” mais adiante neste capítulo.

TABELA 8-1 Como o escopo do grupo afeta as capacidades do grupo

CAPACIDADE DO GRUPO	ESCOPO DOMÍNIO LOCAL	ESCOPO GLOBAL	ESCOPO UNIVERSAL
Membros	Usuários, grupos globais e grupos universais de qualquer domínio; grupos domínio apenas do mesmo domínio	Usuários e grupos globais apenas do mesmo domínio	Usuários de qualquer domínio, bem como grupos globais e universais de qualquer domínio
Membro do	Pode ser inserido em outros grupos domínio local e receber permissões apenas no mesmo domínio	Pode ser inserido em outros grupos e receber permissões em qualquer domínio	Pode ser colocado em outros grupos e receber permissões em qualquer domínio
Conversão do escopo	Pode ser convertido para o escopo universal desde que não tenha como membro outro grupo com escopo domínio local	Pode ser convertido para o escopo universal desde que não seja membro de qualquer outro grupo com escopo global	Pode ser convertido a qualquer outro escopo de grupo, dependendo dos seus membros

Security identifiers e contas de grupo

Assim como ocorre com as contas de usuário, o Windows Server configura as contas de grupo com SIDs exclusivos. Isso significa que você não pode excluir uma conta de grupo, recriá-la e esperar que todas as permissões e os privilégios continuem os mesmos. O novo grupo terá um novo SID e todas as permissões e privilégios do grupo antigo serão perdidos.

O Windows Server cria um token de segurança para cada logon de usuário. O token de segurança especifica o ID da conta de usuário e os SIDs de todos os grupos de segurança aos quais o usuário pertence. O tamanho do token aumenta à medida que o usuário é adicionado a mais grupos de segurança, o que gera as seguintes consequências:

- O token de segurança deve ser passado no processo de logon do usuário antes que o logon possa ser concluído. À medida que o número de associações de grupo de segurança aumenta, o processo de logon se torna mais demorado.
- Para determinar permissões de acesso, o token de segurança é enviado a cada computador que o usuário acessa. Portanto, o tamanho do token de segurança gera um impacto direto na carga de tráfego de rede.

OBSERVAÇÃO As associações de grupo de distribuição não são distribuídas com tokens de segurança. Portanto, associações de grupo de distribuição não afetam o tamanho do token.

Quando usar grupos domínio local, globais e universais

Os grupos domínio local, os grupos globais e os grupos universais fornecem muitas opções para a configuração dos grupos em uma empresa. Embora esses escopos de grupo sejam projetados para simplificar a administração, um planejamento insuficiente pode transformá-los em seu maior pesadelo de administração. Idealmente, os escopos de grupo são usados para ajudar a criar hierarquias de grupo que sejam similares à estrutura de sua organização e que abranjam as responsabilidades de determinados grupos de usuários. Os melhores usos de grupos domínio local, grupos globais e grupos universais são:

- **Grupos domínio local** Os grupos com escopo domínio local apresentam a menor extensão. Use grupos com escopo domínio local para ajudá-lo a gerenciar o acesso a recursos como impressoras e pastas compartilhadas.
- **Grupos globais** Use grupos com escopo global para ajudá-lo a gerenciar contas de usuário e computador em um determinado domínio. Assim, você poderá conceder permissões de acesso a um recurso tornando o grupo com escopo global um membro do grupo com escopo domínio local.
- **Grupos universais** Os grupos com escopo universal apresentam a maior extensão.

Use grupos com escopo universal para consolidar grupos que se estendam por múltiplos domínios. Normalmente, isso é feito adicionando grupos globais como membros. Assim, ao alterar a associação dos grupos globais, as alterações não são replicadas a todos os servidores de catálogos global, pois a associação do grupo universal não foi alterada.

DICA Se sua organização não possui mais de um domínio, não há a necessidade de usar grupos universais. Em vez disso, elabore sua estrutura de grupo com grupos domínio local e globais. Assim, se algum dia outro domínio for adicionado em sua árvore de domínios ou floresta, você poderá facilmente estender a hierarquia de grupo para acomodar a integração.

Para colocar isso em perspectiva, considere o cenário a seguir. Suponhamos que você tenha filiais em Seattle, Chicago e Nova York. Cada filial tem seu próprio domínio, que é parte da mesma árvore de domínios ou floresta. Esses domínios são chamados de Seattle, Chicago e NY. Você quer facilitar o gerenciamento de recursos de rede

para todos os administradores (de todas as filiais), então você cria uma estrutura de grupo que é muito similar em cada local. Embora a empresa tenha departamentos de marketing, TI e engenharia, vamos focar na estrutura do departamento de marketing. Em cada filial, os membros do departamento de marketing precisam acessar uma impressora compartilhada chamada MarketingImpressora e uma pasta de dados compartilhada chamada MarketingDados. Além disso, você quer que os usuários possam compartilhar e imprimir documentos. Por exemplo, o Bob em Seattle deve ser capaz de imprimir documentos para que o Ralph em Nova York possa pegá-los em sua impressora local. O Bob também deve conseguir acessar o relatório trimestral na pasta compartilhada na filial de Nova York.

Para configurar os grupos para os departamentos de marketing nas três filiais, você deve cumprir estas etapas:

1. Comece criando grupos globais para cada grupo de marketing. No domínio Seattle, crie um grupo chamado GMarketing e adicione os membros do departamento de marketing de Seattle a ele. No domínio Chicago, crie um grupo chamado GMarketing e adicione os membros do departamento de marketing de Chicago a ele. No domínio NY, crie um grupo chamado GMarketing e adicione os membros do departamento de marketing de Nova York a ele.
2. Em cada local, crie grupos domínio local que atribuam acesso às impressoras e pastas compartilhadas. Chame o grupo da impressora de MarketingImpressoraLocal. Chame o grupo da pasta compartilhada MarketingDadosLocal. Os domínios Seattle, Chicago e NY devem ter, cada um, seus próprios grupos domínio local.
3. Crie um grupo com escopo universal no catálogo global para todas as filiais. Chame o grupo de UMarketing. Adicione Seattle\GMarketing, Chicago\GMarketing e NY\GMarketing a esse grupo.
4. Adicione UMarketing aos grupos MarketingImpressoraLocal e MarketingDadosLocal em cada filial. Agora, os usuários de marketing devem conseguir compartilhar dados e impressoras.

Contas de usuário e grupos padrão

Ao instalar o Windows Server 2012, o sistema operacional instala usuários e grupos padrão. Essas contas são projetadas para fornecer a configuração básica necessária para expandir sua rede. Há três tipos de contas padrão disponíveis:

- **Interna** Contas de usuário e de grupo instaladas com o sistema operacional, aplicativos e serviços
- **Predefinida** Contas de usuário e de grupo instaladas com o sistema operacional
- **Implícita** Grupos especiais, também conhecidos como *identidades especiais*, criados implicitamente para acessar recursos de rede

OBSERVAÇÃO Embora seja possível modificar usuários e grupos padrão, você não pode excluir usuários e grupos padrão criados pelo sistema operacional, pois não conseguiria recriá-los. Os SIDs das contas antigas e novas não seriam correspondentes e as permissões e os privilégios dessas contas seriam perdidos.

Contas de usuário internas

As contas de usuário internas apresentam finalidades especiais no Windows Server. Todos os sistemas do Windows Server têm diversas contas de usuário internas, incluindo:

- **LocalSystem** LocalSystem é uma pseudoconta para executar processos do sistema e manipular tarefas em nível de sistema. Essa conta é parte do grupo Administrators do servidor e tem todos os direitos de usuário no servidor. Se você configurar aplicativos ou serviços para usar essa conta, os processos relacionados apresentarão acesso completo ao sistema do servidor. Muitos serviços são executados sob a conta LocalSystem. Em alguns casos, esses serviços têm o privilégio de interagirem também com a área de trabalho. Os serviços que precisam de privilégios ou direitos de logon alternativos são executados sob a conta LocalService ou NetworkService.
- **LocalService** LocalService é uma pseudoconta com privilégios limitados. Essa conta concede acesso apenas ao sistema local. A LocalService é parte do grupo Users do servidor e tem os mesmos direitos que a conta NetworkService, exceto que ela é limitada ao computador local. Configure aplicativos ou serviços para usarem essa conta quando processos relacionados não precisarem acessar outros servidores.
- **NetworkService** NetworkService é uma pseudoconta para executar serviços que precisem de privilégios adicionais e direitos de logon no sistema local e na rede. Essa conta é parte do grupo Users do servidor e fornece menos permissões e privilégios que a conta LocalSystem (mas fornece mais que a conta LocalService). Especificamente, os processos em execução sob essa conta podem interagir com toda a rede usando as credenciais da conta do computador.

Ao instalar add-ons ou outros aplicativos em um servidor, outras contas padrão podem ser instaladas.

Contas de usuário predefinidas

Várias contas de usuário predefinidas são instaladas com o Windows Server, inclusive as contas Administrator e Guest. Com servidores membros, as contas predefinidas são locais ao sistema individual em que estão instaladas.

As contas predefinidas têm correspondentes no Active Directory. Essas contas apresentam acesso em nível de domínio e são completamente separadas das contas locais em sistemas individuais.

Conta Administrator

Administrator é uma conta predefinida que fornece acesso completo a arquivos, diretórios, serviços e outros recursos. No Active Directory, a conta Administrator tem acesso e privilégios em nível de domínio. Em outros casos, a conta Administrator normalmente tem acesso apenas ao sistema local. Embora arquivos e diretórios possam ser protegidos da conta Administrator temporariamente, a conta Administrator pode assumir o controle desses recursos a qualquer momento alterando as permissões de acesso. Por padrão, a conta Administrator está habilitada para uso, mas você pode desabilitá-la ou renomeá-la para aumentar a segurança.

ALERTA DE SEGURANÇA Para impedir acesso não autorizado ao sistema ou domínio, certifique-se de conceder à conta Administrator uma senha especialmente segura. Além disso, como essa é uma conta conhecida do Windows, talvez seja recomendável que você renomeie a conta como mais uma precaução de segurança. Se optar por renomear a conta Administrator original, é provável que também seja interessante criar uma conta Administrador fictícia. Essa conta fictícia deve ser mantida sem permissões, direitos ou privilégios e você deve desabilitá-la.

Normalmente, não é preciso que as configurações básicas da conta Administrator sejam alteradas. No entanto, talvez haja a necessidade de alterar as configurações avançadas, como a associação a grupos específicos. Por padrão, a conta Administrator de um domínio é membro dos grupos: Administrators, Domain Admins, Domain Users, Enterprise Admins, Group Policy Creator Owners e Schema Admins. Na próxima seção, serão apresentadas mais informações sobre esses grupos.

MUNDO REAL Em um ambiente de domínio, a conta Administrator local é usada principalmente para gerenciar o sistema quando você acaba de instalá-lo. Isso permite que você configure o sistema sem ser bloqueado. Provavelmente, a conta não será usada depois que o sistema tiver sido instalado. Em vez disso, você deve tornar seus administradores membros do grupo Administrators. Isso garante que você possa revogar privilégios de administrador sem a necessidade de alterar as senhas de contas Administrator.

Para um sistema que é parte de um grupo de trabalho em que cada computador individual é gerenciado separadamente, em geral você recorre a essa conta toda vez que precisa realizar suas tarefas de administração do sistema. Nesse caso, você provavelmente não quer configurar contas individuais para cada pessoa que tem acesso administrativo a um sistema. Em vez disso, use uma conta de administrador separada em cada computador.

Conta Guest

A conta Guest é projetada para usuários que precisam de apenas um acesso ou um acesso ocasional. Embora os convidados que usarem a conta Guest tenham privilégios limitados do sistema, é necessário muito cuidado ao usar essa conta. Sempre que a conta Guest é usada, o sistema é aberto a possíveis problemas de segurança. O risco é tão grande que a conta é inicialmente desabilitada ao instalar o Windows Server.

Por padrão, a conta Guest é membro dos grupos Domain Guests e Guests. Observe que a conta Guest – como todas as outras contas nomeadas – também é membro do grupo implícito chamado Everyone. O grupo Everyone normalmente tem acesso a arquivos e pastas por padrão. Além disso, o grupo Everyone tem um conjunto padrão de direitos do usuário.

ALERTA DE SEGURANÇA Se você decidir habilitar a conta Guest, certifique-se de restringir seu uso e alterar a senha regularmente. Assim como na conta Administrator, talvez seja recomendável renomear a conta como mais uma precaução de segurança.

Grupos internos e predefinidos

Os grupos internos são instalados com todos os sistemas Windows Server. Use os grupos internos e predefinidos para conceder a um usuário os privilégios e as permissões do grupo. Isso é feito tornando o usuário um membro do grupo. Por exemplo, você fornece a um usuário acesso administrativo ao sistema tornando-o membro do grupo local Administrators. Para fornecer a um usuário acesso administrativo ao domínio, por sua vez, você deve torná-lo membro do grupo Domain Admins no Active Directory.

Grupos implícitos e identidades especiais

No Windows NT, os grupos implícitos eram atribuídos implicitamente durante o logon e eram baseados em como um usuário acessava um recurso de rede. Por exemplo, se um usuário acessasse um recurso por meio de um logon interativo, o usuário era automaticamente um membro do grupo implícito chamado Interactive. No Windows 2000 e em versões superiores, a abordagem baseada em objeto da estrutura de diretórios alterou as regras originais para grupos implícitos. Embora ainda não seja possível visualizar a associação de identidades especiais, a associação a grupos implícitos pode ser concedida a usuários, grupos e computadores.

Para refletir a função modificada, os grupos implícitos também são chamados de *identidades especiais*. Uma identidade especial é um grupo cuja associação pode ser configurada implicitamente, como durante o logon, ou explicitamente por meio de permissões de acesso de segurança. Como ocorre com outros grupos padrão, a disponibilidade de um grupo implícito específico depende da configuração do momento. Os grupos implícitos são abordados mais adiante neste capítulo.

Capacidades de conta

Ao configurar uma conta de usuário, você pode atribuir ao usuário capacidades específicas. Normalmente, essas capacidades são atribuídas tornando o usuário um membro de um ou mais grupos, fornecendo, assim, as capacidades desses grupos a ele. Para retirar capacidades, você deve remover a associação de grupo.

No Windows Server, é possível atribuir os seguintes tipos de capacidades a uma conta:

- **Privilégios** Um tipo de direito do usuário que concede permissões para realizar determinadas tarefas administrativas. Os privilégios podem ser atribuídos tanto a contas de usuário quanto a contas de grupo. Um exemplo de um privilégio é a capacidade de desligar o sistema.
- **Direitos de logon** Um tipo de direito do usuário que concede permissões de logon. Os direitos de logon podem ser atribuídos tanto a contas de usuário quanto a contas de grupo. Um exemplo de direito de logon é a capacidade de efetuar logon localmente.
- **Capacidades internas** Um tipo de direito do usuário que é atribuído a grupos e inclui as capacidades automáticas do grupo. As capacidades internas são predefinidas e não podem ser alteradas, mas podem ser delegadas a usuários com permissão para gerenciar objetos, OUs e outros contêineres. São exemplos de capacidades internas as ações de criar, excluir e gerenciar contas de usuário. Essa capacidade é atribuída a administradores e operadores de conta. Assim, se um usuário for um membro do grupo Administrators, ele pode criar, excluir e gerenciar contas de usuário.
- **Permissões de acesso** Um tipo de direito do usuário que define as operações que podem ser realizadas em recursos de rede. As permissões de acesso podem ser atribuídas a usuários, computadores e grupos. Um exemplo de permissão de acesso é a capacidade de criar um arquivo em um diretório. As permissões de acesso são abordadas no Capítulo 12, "Compartilhamento de dados, segurança e auditoria".

Como administrador, você lida com capacidades de conta diariamente. Para um melhor acompanhamento das capacidades internas, consulte as seções a seguir. Lembre-se de que apesar de não ser possível alterar as capacidades internas de um grupo, você pode alterar os direitos padrão dele. Por exemplo, um administrador poderia revogar o acesso a um computador através da rede removendo o direito de um grupo acessar o computador a partir da rede.

Privilégios

Um privilégio é uma atribuição de direito do usuário que concede permissões para realizar uma determinada tarefa administrativa. Você atribui privilégios por meio de Group Policies, que podem ser aplicadas individualmente a computadores, OUs ou domínios. Embora você possa atribuir privilégios tanto a usuários quanto a grupos, normalmente é mais indicado atribuir privilégios a grupos. Assim, os usuários recebem automaticamente os privilégios apropriados ao se tornarem membros de um grupo. A atribuição de privilégios a grupos também facilita o gerenciamento de contas de usuário.

A Tabela 8-2 fornece um breve resumo de cada privilégio que pode ser atribuído a usuários e grupos. Para aprender a atribuir privilégios, consulte “Configuração das políticas de direitos do usuário” mais adiante neste capítulo.

TABELA 8-2 Privilégios do Windows Server 2012 para usuários e grupos

PRIVILÉGIO	DESCRIÇÃO
Act As Part Of The Operating System	Permite que um processo seja autenticado e receba acesso a recursos como qualquer usuário. Os processos que requerem esse privilégio devem usar a conta LocalSystem, que já possui esse privilégio.
Add Workstations To Domain	Permite que os usuários adicionem computadores ao domínio.
Adjust Memory Quotas For A Process	Permite que os usuários ajustem as cotas de uso de memória com base em processo.
Back Up Files And Directories	Permite que os usuários façam backup do sistema independentemente das permissões configuradas nos arquivos e diretórios.
Bypass Traverse Checking	Permite que os usuários passem por diretórios ao navegar por um caminho de objeto independentemente das permissões configuradas nos diretórios. Esse privilégio não permite que o usuário liste o conteúdo dos diretórios.
Change The System Time	Permite que os usuários configurem o horário do relógio do sistema.
Change The Time Zone	Permite que os usuários configurem o fuso horário do relógio do sistema. Por padrão, todos os usuários apresentam esse privilégio.
Create A Pagefile	Permite que os usuários criem e alterem o tamanho do arquivo de paginação da memória virtual.

PRIVILÉGIO	DESCRIÇÃO
Create A Token Object	Permite que processos criem objetos de token que possam ser usados para obter acesso a recursos locais. Os processos que requerem esse privilégio devem usar a conta LocalSystem, que já possui esse privilégio.
Create Global Objects	Permite que processos criem objetos globais. Por padrão, as contas LocalService e NetworkService apresentam esse privilégio.
Create Permanent Shared Objects	Permite que processos criem objetos de diretório no gerenciador de objetos. A maioria dos componentes já apresenta esse privilégio; não é necessário atribuí-lo especificamente.
Create Symbolic Links	Permite que um aplicativo que esteja sendo executado por um usuário crie links simbólicos. Os links simbólicos fazem com que documentos ou pastas pareçam estar em um determinado local quando, na verdade, eles residem em outro. Por padrão, o uso de links simbólicos é restrito para aumentar a segurança.
Debug Programs	Permite que os usuários realizem depuração.
Enable Computer And User Accounts To Be Trusted For Delegation	Permite que computadores e usuários alterem ou apliquem a configuração de ser confiável para delegação, desde que eles tenham acesso para gravação ao objeto.
Force Shutdown From A Remote System	Permite que os usuários desliguem um computador a partir de um local remoto na rede.
Generate Security Audits	Permite que processos gerem entradas em log de segurança para auditoria do acesso a objetos.
Impersonate A Client After Authentication	Permite que aplicativos Web atuem como clientes durante o processamento de solicitações. Serviços e usuários também podem atuar como clientes.
Increase A Process Working Set	Permite que um aplicativo que esteja sendo executado por um usuário aumente a memória que o conjunto de trabalho do processo relacionado usa. Um <i>conjunto de trabalho de processo</i> é o conjunto de páginas de memória visíveis no momento a um processo na memória física. Permitir o aumento nas páginas de memória reduz as falhas de página e melhora o desempenho.
Increase Scheduling Priority	Permite que processos aumentem a prioridade de agendamento atribuída a outro processo, desde que eles tenham acesso para gravação no processo.
Load And Unload Device Drivers	Permite que os usuários instalem e desinstalem drivers de dispositivos Plug and Play. Isso não afeta os drivers de dispositivos que não são Plug and Play, que podem ser instalados apenas por administradores.

Continua

TABELA 8-2 Privilégios do Windows Server 2012 para usuários e grupos (*continuação*)

PRIVILÉGIO	DESCRIÇÃO
Lock Pages In Memory	Permite que processos mantenham dados na memória física, impedindo que o sistema efetue a paginação de dados para a memória virtual do disco.
Manage Auditing And Security Log	Permite que os usuários especifiquem as opções de auditoria e acessem o log de segurança. Antes disso, você deve ativar a auditoria na Group Policy.
Modify An Object Label	Permite que um processo de usuário modifique o rótulo de integridade de objetos, como arquivos, chaves de registro ou processos de outros usuários. Esse privilégio pode ser usado para diminuir a prioridade de outros processos. Os processos em execução sob uma conta de usuário podem modificar o rótulo de qualquer objeto de propriedade desse usuário sem exigir esse privilégio.
Modify Firmware Environment Values	Permite que os usuários e os processos modifiquem variáveis de ambiente do sistema.
Perform Volume Maintenance Tasks	Permite a administração do armazenamento removível, o gerenciamento de disco e disponibiliza o desfragmentador de disco.
Profile A Single Process	Permite que os usuários monitorem o desempenho de processos que não são do sistema.
Profile System Performance	Permite que os usuários monitorem o desempenho de processos do sistema.
Remove Computer From Docking Station	Permite que um laptop seja desencaixado e removido da rede.
Replace A Process Level Token	Permite que processos substituam o token padrão para subprocessos.
Restore Files And Directories	Permite que os usuários restaurem arquivos e diretórios armazenados em backup independentemente das permissões configuradas nos arquivos e diretórios.
Shut Down The System	Permite que os usuários desliguem o computador local.
Synchronize Directory Service Data	Permite que os usuários sincronizem os dados do serviço de diretório em controladores de domínio.
Take Ownership Of Files Or Other Objects	Permite que os usuários assumam a posse de arquivos e de qualquer outro objeto do Active Directory.

Direitos de logon

Um *direito de logon* é a atribuição de direitos do usuário que concede permissões de logon. Os direitos de logon podem ser atribuídos tanto a contas de usuário quanto a contas de grupo. Assim como ocorre com os privilégios, você atribui direitos de logon por meio de Group Policies e, normalmente, é recomendável que se atribua direitos de logon a grupos e não a usuários individuais.

A Tabela 8-3 fornece um breve resumo de cada direito de logon que pode ser atribuído a usuários e grupos. A atribuição de direitos de logon é abordada em “Configuração das políticas de direitos do usuário”.

TABELA 8-3 Direitos de logon do Windows Server 2012 para usuários e grupos

DIREITO DE LOGON	DESCRIÇÃO
Access Credential Manager As A Trusted Caller	Concede permissão para estabelecer uma conexão confiável com o Credential Manager. As credenciais, como o nome de usuário e senha ou cartão inteligente, fornecem identificação e prova de identificação.
Access This Computer From The Network	Concede acesso remoto ao computador.
Allow Log On Locally	Concede permissão de efetuar logon usando o teclado do computador. Em controladores de domínio, esse direito é restrito por padrão e apenas membros dos grupos a seguir podem efetuar logon localmente: Administrators, Account Operators, Backup Operators, Print Operators e Server Operators.
Allow Log On Through Remote Desktop Services	Concede acesso por meio do Remote Desktop Services. Esse direito é necessário para assistência remota e uso de área de trabalho remota.
Deny Access To This Computer From The Network	Nega acesso remoto ao computador por meio dos serviços de rede.
Deny Logon As Batch Job	Nega o direito de efetuar logon por meio de um arquivo em lote ou script.
Deny Logon As Service	Nega o direito de efetuar logon como um serviço.
Deny Logon Locally	Nega o direito de efetuar logon usando o teclado do computador.
Deny Logon Through Remote Desktop Services	Nega o direito de efetuar logon por meio do Remote Desktop Services.
Log On As A Batch Job	Concede permissão para efetuar logon como um arquivo em lote ou script.
Log On As A Service	Concede permissão para efetuar logon como um serviço. A conta LocalSystem tem esse direito. Uma conta que deva ser usada para iniciar um serviço deve receber esse direito.

Capacidades internas para grupos no Active Directory

As capacidades internas que são atribuídas a grupos no Active Directory dependem da configuração de um computador. Com o Local Group Policy Editor, mostrado na Figura 8-1, você pode exibir as capacidades atribuídas a cada grupo expandindo Computer Configuration\Windows Settings\Security Settings\Local Policies e selecionando o nó User Rights Assignment.

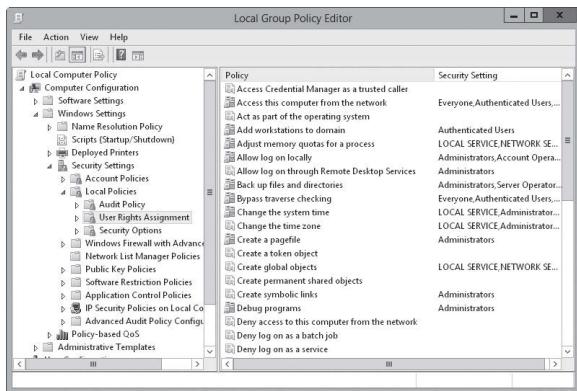


FIGURA 8-1 Visualize as capacidades internas que são atribuídas para os grupos.

Observe que todas as ações disponíveis ao grupo Everyone estão disponíveis a todos os grupos, inclusive ao grupo Guests. Isso significa que, apesar do grupo Guests não apresentar permissão explícita para acessar o computador através da rede, um membro do grupo Guests ainda pode acessar o sistema porque o grupo Everyone tem esse direito.

A Tabela 8-4 resume as capacidades que você pode delegar a outros usuários e grupos. Ao estudar a tabela, observe que as contas restritas abrangem a conta de usuário Administrator, as contas de usuário de administradores e as contas de grupo para Administrators, Server Operators, Account Operators, Backup Operators e Print Operators. Como essas contas são restritas, o Account Operators não pode criá-las ou modificá-las.

TABELA 8-4 Outras capacidades para grupos internos e locais

TAREFA	DESCRIÇÃO	GRUPO QUE NORMALMENTE RECEBE A ATRIBUIÇÃO
Assign User Rights	Permite que os usuários atribuam direitos de usuário a outros usuários	Administrators
Create And Delete Groups	Permite que os usuários criem novos grupos e excluam grupos existentes	Administrators, Account Operators
Create And Delete Printers	Permite que os usuários criem e excluam impressoras	Administrators, Server Operators, Print Operators
Create, Delete, And Manage User Accounts	Permite que os usuários administrem contas de usuário de domínio	Administrators, Account Operators

TAREFA	DESCRIÇÃO	GRUPO QUE NORMALMENTE RECEBE A ATRIBUIÇÃO
Manage Group Policy Links	Permite que usuários apliquem Group Policies existentes a sites, domínios e OUs para os quais eles apresentam permissão de escrita nos objetos relacionados	Administrators
Manage Network Configuration	Permite que os usuários configurem a rede	Administrators, Network Configuration Operators
Manage Performance Logs	Permite que os usuários configurem o registro em log de desempenho	Administrators, Performance Log Users
Manage Printers	Permite que os usuários modifiquem as configurações de impressora e gerenciem as filas de impressão	Administrators, Server Operators, Printer Operators
Modify The Membership Of A Group	Permite que os usuários adicionem e removam usuários a grupos no domínio	Administrators, Account Operators
Monitor Performance Logs	Permite que os usuários monitorem o registro em log de desempenho	Administrators, Performance Monitor Users
Perform Cryptographic Operations	Permite que os usuários gerenciem opções de criptografia	Administrators, Cryptographic Operators
Read All User Information	Permite que os usuários visualizem informações de contas de usuário	Administrators, Server Operators, Account Operators
Read Event Logs	Permite que os usuários leiam logs de eventos	Administrators, Event Log Readers
Reset Passwords On User Accounts	Permite que os usuários redefinam senhas de contas de usuário	Administrators, Account Operators

Uso de contas de grupo padrão

As contas de grupo padrão são projetadas para serem versáteis. Com a atribuição dos usuários aos grupos corretos, você pode facilitar muito o gerenciamento de seu grupo de trabalho ou domínio do Windows Server 2012. Infelizmente, com a grande quantidade de grupos, entender a finalidade de cada um não é fácil. Para ajudá-lo, vamos analisar os grupos usados por administradores e os grupos que são criados implicitamente.

Grupos usados por administradores

Um administrador é alguém com amplo acesso aos recursos da rede. Os administradores podem criar contas, modificar direitos do usuário, instalar impressoras, gerenciar recursos compartilhados, entre outras ações. Os principais grupos de administração são Administrators, Domain Admins e Enterprise Admins. A Tabela 8-5 compara os grupos de administração.

TABELA 8-5 Visão geral dos grupos de administração

TIPO DO GRUPO DE ADMINISTRAÇÃO	AMBIENTE DE REDE	ESCOPO DO GRUPO	ASSOCIAÇÃO
Administrators	Domínios do Active Directory	Domínio local	Administrator, Domain Admins, Enterprise Admins
Administrators	Grupos de trabalho, computadores que não fazem parte de um domínio	Local	Administrator
Domain Admins	Domínios do Active Directory	Global	Administrator
Enterprise Admins	Domínios do Active Directory	Global ou universal	Administrator
Schema Admins	Domínios do Active Directory	Universal	Administrator

DICA A conta Administrator e os grupos globais Domain Admins e Enterprise Admins são membros do grupo Administrators. A conta Administrator é usada para acessar o computador local. A associação do Domain Admins permite que outros administradores acessem o sistema de qualquer lugar do domínio. A associação do Enterprise Admins permite que outros administradores acessem o sistema a partir de outros domínios da árvore de domínios ou da floresta atuais. Para impedir o acesso em nível de empresa a um domínio, você pode remover o Enterprise Admins desse grupo.

Administrators é um grupo local que fornece acesso administrativo completo a um computador individual ou um domínio único, dependendo da sua localização. Como essa conta tem acesso completo, você deve ter cuidado quanto a adicionar usuários a esse grupo.

Para tornar uma pessoa um administrador de um computador local ou domínio, basta fazer com que ela seja membro desse grupo. Somente os membros do grupo Administrators podem modificar essa conta.

Domain Admins é um grupo global projetado para ajudá-lo a gerenciar recursos em um domínio. Os membros desse grupo têm controle total em um domínio. Esse grupo apresenta controle administrativo sobre todos os computadores de um domínio, pois é membro do grupo Administrators por padrão em todos os controladores de domínio, em todas as estações de trabalho do domínio e em todos os servidores membros do domínio no momento em que ingressaram no domínio. Para tornar uma pessoa um administrador de um domínio, faça com que ela seja membro desse grupo.

DICA Por padrão, a conta Administrator é membro de Domain Admins. Isso significa que se um usuário efetuar logon em um computador como administrador e o computador for membro do domínio, o usuário terá acesso completo a todos os recursos do domínio.

Enterprise Admins é um grupo universal projetado para ajudá-lo a gerenciar recursos em uma floresta. Os membros desse grupo têm controle total de todos os domínios de uma floresta. Esse grupo apresenta controle administrativo sobre todos os controladores de domínio de uma empresa, pois é membro do grupo Administrators por padrão em todos os controladores de domínio de uma floresta. Para tornar uma pessoa um administrador da empresa, faça com que ela seja membro desse grupo.

DICA Por padrão, a conta Administrator é membro de Enterprise Admins. Isso significa que se alguém efetuar logon em um computador como administrador e o computador for membro do domínio, o usuário terá acesso completo à árvore de domínios ou à floresta.

Schema Admins é um grupo universal projetado para ajudá-lo a gerenciar o esquema do Active Directory. Os membros desse grupo podem trabalhar com o esquema e gerenciá-lo no domínio. Para que uma pessoa possa editar o esquema, ela precisa ser membro desse grupo.

Grupos implícitos e identidades

O Windows Server define um conjunto de identidades especiais que você pode usar para atribuir permissões em certas situações. Normalmente, as permissões são atribuídas implicitamente a identidades especiais. No entanto, você pode atribuir permissões a identidades especiais de maneira direta ao modificar objetos do Active Directory. São identidades especiais:

- **Anonymous Logon** Qualquer usuário que estiver acessando o sistema por meio de um logon anônimo tem a identidade Anonymous Logon. Essa identidade permite acesso anônimo a recursos, como uma página da Web publicada nos servidores de presença na web corporativos.
- **Authenticated Users** Qualquer usuário que estiver acessando o sistema por meio de um processo de logon tem a identidade Authenticated Users. Essa identidade permite o acesso a recursos compartilhados dentro do domínio, como arquivos de uma pasta compartilhada que deve estar acessível a todos os funcionários da organização.
- **Batch** Qualquer usuário ou processo que estiver acessando o sistema como um arquivo em lote (ou por meio da fila de trabalhos em lotes) tem a identidade Batch. Essa identidade permite que trabalhos em lotes executem tarefas agendadas, como uma limpeza noturna que exclua arquivos temporários.
- **Creator Group** O Windows Server usa esse grupo de identidade especial para conceder automaticamente permissões de acesso a usuários membros do mesmo grupo ou dos mesmos grupos que o criador de um arquivo ou diretório.
- **Creator Owner** A pessoa que criou o arquivo ou o diretório é membro desse grupo de identidade especial. O Windows Server usa a identidade Creator Owner para conceder automaticamente permissões de acesso ao criador de um arquivo ou diretório.
- **Dial-Up** Qualquer usuário que estiver acessando o sistema por meio de uma conexão discada tem a identidade Dial-Up. Essa identidade diferencia os usuários de conexão discada dos outros tipos de usuários autenticados.
- **Enterprise Domain Controllers** Os controladores de domínio com funções e responsabilidades em nível de empresa têm a identidade Enterprise Domain Con-

trollers. Essa identidade permite que eles realizem certas tarefas na empresa por meio de relações de confiança transitivas.

- **Everyone** Todos os usuários interativos, autenticados, de rede e de conexão discada são membros do grupo Everyone. Esse grupo de identidade especial fornece amplo acesso a um recurso do sistema.
- **Interactive** Qualquer usuário conectado ao sistema local tem a identidade Interactive. Essa identidade permite que apenas usuários locais acessem um recurso.
- **Network** Qualquer usuário que estiver acessando o sistema por meio de uma rede tem a identidade Network. Essa identidade permite que apenas usuários remotos acessem um recurso.
- **Proxy** Os usuários e computadores que estiverem acessando recursos por meio de um proxy têm a identidade Proxy. Essa identidade é usada quando os proxies são implementados na rede.
- **Remote Desktop Services User** Qualquer usuário que estiver acessando o sistema por meio do Remote Desktop Services tem a identidade Remote Desktop Services User. Essa identidade permite que usuários do Remote Desktop Services acessem aplicativos do Remote Desktop Services e realizem outras tarefas necessárias com esses serviços.
- **Restricted** Os usuários e computadores com capacidades restritas têm a identidade Restricted.
- **Self** A identidade Self se refere ao próprio objeto e permite que ele modifique a si mesmo.
- **Service** Qualquer serviço que estiver acessando o sistema tem a identidade Service. Essa identidade concede acesso aos processos que estão sendo executados pelos serviços do Windows Server.
- **System** O próprio sistema operacional do Windows Server tem a identidade System. Essa identidade é usada quando o sistema operacional precisa executar uma função em nível de sistema.

Configuração e organização da conta de usuário

Uma parte importante de seu trabalho como administrador é criar contas. Este capítulo mostra como fazer isso. As contas de usuário e de grupo permitem que o Windows Server 2012 rastreie e gerencie informações sobre usuários, inclusive permissões e privilégios. Para criar contas de usuário, são utilizadas principalmente as duas ferramentas de administração de contas a seguir:

- Active Directory Users And Computers, ferramenta projetada para administrar contas em todo um domínio do Active Directory Domain Services
- Local Users And Groups, ferramenta projetada para administrar contas em um computador local

Os aspectos mais importantes da criação de contas são a configuração e a organização das contas. Sem as diretrizes e políticas adequadas, talvez você perceba em pouco tempo que precisa trabalhar novamente com todas as suas contas de usuário. Antes de criar contas, determine as políticas a serem usadas para configuração e organização.

Políticas de nomeação de contas

Uma política importante que você precisa configurar é o esquema de nomes para as contas. As contas de usuário apresentam nomes de exibição e nomes de logon. O *nome de exibição* (ou nome completo) é o nome exibido a usuários e o nome que aparece em sessões do usuário. O *nome de logon* é o nome usado para efetuar logon no domínio. Os nomes de logon foram abordados brevemente em “Nomes de logon, senhas e certificados públicos” neste capítulo.

Regras para nomes de exibição

Para contas de domínio, o nome de exibição é normalmente a concatenação do primeiro nome do usuário, a inicial do nome do meio e o sobrenome, mas você pode configura-lo para qualquer valor de cadeia de caracteres. Os nomes de exibição devem seguir a estas regras:

- Os nomes de exibição locais devem ser exclusivos em um computador individual.
- Os nomes de exibição devem ser exclusivos em todo o domínio.
- Os nomes de exibição não devem ter mais de 64 caracteres.
- Os nomes de exibição podem conter caracteres alfanuméricos e caracteres especiais.

Regras para nomes de logon

Os nomes de logon devem seguir estas regras:

- Os nomes de logon locais devem ser exclusivos em um computador individual, enquanto os nomes de logon globais devem ser exclusivos em todo o domínio.
- Os nomes de logon podem conter até 256 caracteres. No entanto, não é prático usar nomes de logon com mais de 64 caracteres.
- Um nome de logon anterior ao Windows 2000 é dado a todas as contas. Por padrão, esse nome de logon é configurado com os primeiros 20 caracteres do nome de logon do Windows. O nome de logon anterior ao Windows 2000 deve ser exclusivo em todo o domínio.
- Os usuários que efetuam logon no domínio com um computador com Windows 2000 ou uma versão superior podem usar seus nomes de logon padrão ou seus nomes de logon anterior ao Windows 2000, independentemente do modo operacional do domínio.
- Os nomes de logon não podem conter determinados caracteres. Os caracteres a seguir são inválidos:
" / \ [] ; | =, + * ? < >
- Os nomes de logon podem conter todos os outros caracteres especiais, inclusive espaços, pontos finais, traços e sublinhados. No entanto, normalmente não é recomendável utilizar espaços em nomes de contas.

OBSERVAÇÃO Embora o Windows Server armazene nomes de usuário com as maiúsculas e minúsculas que você inserir, os nomes de usuário não diferenciam maiúsculas de minúsculas. Por exemplo, você pode acessar a conta Administrator com o nome de usuário Administrator, administrador ou ADMINISTRATOR. Portanto, os nomes de usuário reconhecem maiúsculas e minúsculas, mas não as diferenciam.

Esquemas de nomenclatura

A maioria das organizações de pequeno porte tende a atribuir nomes de logon que usem o primeiro nome e o último sobrenome do usuário. Porém, é possível que haja mais de uma pessoa com o mesmo nome em uma organização de qualquer porte. Em vez de ter que refazer seu esquema de nomeação para nomes de logon ao enfrentar problemas, selecione um bom esquema de nomeação agora e certifique-se de que outros administradores o usem. Você deve usar um procedimento consistente para nomear contas – permitindo que sua base de usuários cresça, limite a possibilidade de conflito entre nomes e garanta que suas contas tenham nomes seguros que não sejam facilmente explorados. Se você seguir essas diretrizes, os tipos de esquemas de nomeação que talvez você queira usar são:

- Primeiro nome e última inicial do usuário
- Primeira inicial e sobrenome do usuário
- Primeira inicial, inicial do nome do meio e sobrenome do usuário
- Primeira inicial, inicial do nome do meio e primeiros cinco caracteres do sobrenome do usuário
- Primeiro nome e sobrenome do usuário

ALERTA DE SEGURANÇA Em ambientes com segurança restrita, um código numérico pode ser atribuído para o nome de logon. Esse código numérico deve ter no mínimo 20 caracteres. Combine esse método de nomeação restrito com cartões inteligentes e leitores de cartão inteligente para permitir que usuários efetuem logon rapidamente no domínio sem ter que digitar todos os caracteres. Não se preocupe, os usuários ainda terão um nome de exibição que possa ser lido.

Políticas de senha e conta

As contas de domínio usam senhas ou chaves privadas de certificados para autenticar o acesso a recursos de rede. Esta seção tem como foco as senhas.

Uso de senhas seguras

Uma senha é uma cadeia de caracteres que diferencia maiúsculas de minúsculas que pode conter mais de 127 caracteres com o Active Directory e até 14 caracteres com o Windows NT Security Manager. Letras, números e símbolos são caracteres válidos para senhas. Quando uma senha é configurada para uma conta, o Windows Server a armazena em um formato criptografado no banco de dados de conta.

Porém, apenas ter uma senha não é suficiente. Para impedir o acesso não autorizado a recursos de rede é essencial usar senhas seguras. A diferença entre uma senha comum e uma senha segura é que as senhas seguras são difíceis de serem adivinhadas e quebradas. Para criar senhas assim, use combinações de todos os tipos de caracteres disponíveis, inclusive letras minúsculas, letras maiúsculas, números e símbolos. Por exemplo, em vez de usar happydays como senha, use haPPy2Days&, Ha**y!day5 ou até mesmo h*99Y%d*ys.

Também é possível usar frases como senha. Com uma frase como senha, a senha contém várias palavras e pontuação, como uma frase completa. Por exemplo, você pode usar a frase de senha *This problem is 99 times ten!* Uma frase de senha que inclui pontuação e números atende a todos os requisitos de complexidade e é incrivelmente difícil de ser quebrada.

Infelizmente, não importa quão segura você configure uma senha de usuário inicialmente, o usuário em algum momento escolherá sua própria senha. Portanto, você deve configurar políticas de conta que definam uma senha segura para seus sistemas. As políticas de conta são um subconjunto das políticas configuráveis em Group Policy.

Configuração de políticas de conta

Como mencionado em capítulos anteriores, as Group Policies podem ser aplicadas em vários níveis dentro da estrutura de rede. As Group Policies locais são gerenciadas conforme discutido em "Gerenciamento de Group Policies locais" no Capítulo 4, "Automatização de tarefas administrativas, políticas e procedimentos". Por sua vez, as Group Policies globais são gerenciadas conforme explicado em "Gerenciamento de políticas de site, domínio e unidade organizacional", também no Capítulo 4.

As políticas de conta devem ser configuradas na GPO de precedência mais alta vinculada a um domínio. Por padrão, a GPO de precedência mais alta vinculada a um domínio é a GPO Default Domain Policy. Ao acessar a GPO Default Domain Policy ou outra GPO apropriada, você pode configurar políticas de conta seguindo estas etapas:

1. No Group Policy Management Editor, mostrado na Figura 8-2, abra o nó Account Policies expandindo Computer Configuration, Windows Settings e Security Settings. A árvore de console exibe o nome do computador ou domínio que está sendo configurado. Certifique-se de que esse é o recurso de rede apropriado para ser configurado.

OBSERVAÇÃO As políticas de domínio têm precedência sobre as políticas locais. A GPO com a ordem de vinculação 1 no domínio sempre tem a precedência mais alta.

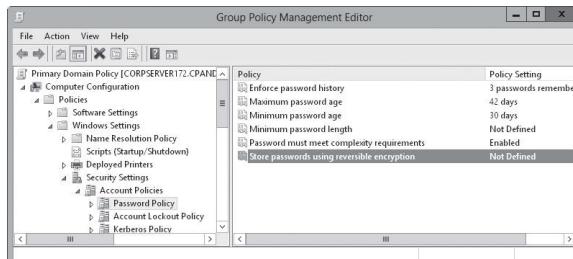


FIGURA 8-2 Use o nó Account Policies para configurar políticas para senhas e para o uso geral de contas.

2. Agora você pode gerenciar políticas de conta por meio dos nós Password Policy, Account Lockout Policy e Kerberos Policy. Para configurar uma política, dê um toque duplo ou clique duas vezes em sua entrada. Outra opção é pressionar e manter pressionado ou clicar com o botão direito do mouse e tocar ou clicar em Properties. Isso abre uma caixa de diálogo Properties para a política, mostrada na Figura 8-3.

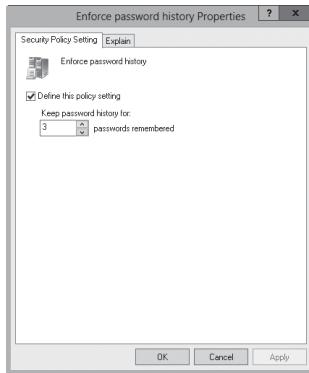


FIGURA 8-3 Defina e configure Group Policies globais na caixa de diálogo Properties.

Todas as políticas são definidas ou não definidas. Isso é, ou elas estão configuradas para uso ou não estão configuradas para uso. Uma política que não é definida no contêiner atual pode ser herdada de outro contêiner.

OBSERVAÇÃO As políticas Kerberos não são usadas com computadores locais. As políticas Kerberos estão disponíveis apenas com Group Policies que afetam domínios. Para servidores autônomos, você pode alterar as configurações das políticas locais. No entanto, você não pode alterar as configurações de políticas locais para controladores de domínio ou servidores membros.

3. Marque ou desmarque a caixa de seleção Define This Policy Setting para especificar se uma política está definida.

DICA As políticas podem ter mais opções de configuração. Frequentemente, essas opções são botões chamados Enabled ou Disabled. Tocar ou clicar em Enabled ativa a restrição da política. Tocar ou clicar em Disabled desativa a restrição da política. Algumas políticas são negações, ou seja, se você habilitá-las estará na verdade negando o item. Por exemplo, Disable Log On As A Service é a negação do item Log On As A Service.

Procedimentos específicos para trabalhar com políticas de conta são discutidos nas seções a seguir: “Configuração de políticas de senha”, “Configuração de políticas de bloqueio de conta” e “Configuração de políticas Kerberos”.

Configuração das políticas de conta

Como você aprendeu na seção anterior, há três tipos de políticas de conta: políticas de senha, políticas de bloqueio de conta e políticas Kerberos. As seções a seguir mostram como configurar cada uma dessas políticas.

Configuração de políticas de senha

As políticas de senha, listadas aqui, controlam a segurança de senhas:

- Enforce Password History
- Maximum Password Age
- Minimum Password Age
- Minimum Password Length
- Passwords Must Meet Complexity Requirements
- Store Password Using Reversible Encryption For All Users In The Domain

Os usos dessas políticas são abordados nas seções a seguir.

Enforce Password History

A política Enforce Password History configura com que frequência senhas antigas podem ser reutilizadas. Com essa política, você pode desencorajar os usuários a alternarem entre diversas senhas comuns. O Windows Server pode armazenar até 24 senhas para cada usuário no histórico de senhas.

Para desabilitar esse recurso, configure o valor do histórico de senhas para 0. Para habilitar esse recurso, configure o valor do histórico de senhas usando a caixa Passwords Remembered. Dessa maneira, o Windows Server rastreia as senhas antigas por meio de um histórico de senhas que é exclusivo para cada usuário, e os usuários não têm permissão para usar novamente as senhas armazenadas.

OBSERVAÇÃO Para evitar que usuários contornem as configurações de Enforce Password History, não permita que eles alterem senhas imediatamente. Isso impede que os usuários alterem suas senhas diversas vezes para retornar para uma senha antiga. Você pode configurar o tempo necessário para manter uma senha com a política Minimum Password Age, conforme abordado mais adiante neste capítulo.

Maximum Password Age

A diretiva Maximum Password Age determina por quanto tempo um usuário pode manter uma senha antes de ter que alterá-la. O objetivo é forçar os usuários a alterarem suas senhas periodicamente. Ao usar esse recurso, configure um valor que seja condizente com sua rede. Normalmente, opta-se por um período mais curto quando a segurança é muito importante e um período mais longo quando a segurança é menos importante.

O tempo máximo da senha pode ser configurado com qualquer valor de 0 a 999. Um valor 0 especifica que as senhas não expiram. Embora seja tentador não estabelecer uma data de expiração, os usuários devem alterar suas senhas regularmente para assegurar a segurança da rede. Quando a segurança for uma preocupação, 30, 60 ou 90 dias são bons valores. Quando a segurança for menos importante, 120, 150 ou 180 dias são bons valores.

OBSERVAÇÃO O Windows Server notifica os usuários quando a data de expiração da senha estiver se aproximando. Todas as vezes em que faltar menos de 30 dias para a data de expiração, os usuários verão um aviso ao efetuarem logon informando que eles devem alterar sua senha dentro de um determinado número de dias.

Minimum Password Age

A diretiva Minimum Password Age determina por quanto tempo um usuário deve manter uma senha antes de poder alterá-la. Você pode usar essa caixa para impedir que os usuários contornem o sistema de senhas inserindo uma nova senha e alterando-a logo após para a senha antiga.

Se o tempo mínimo da senha for configurado para 0, os usuários podem alterar suas senhas imediatamente. Para que isso seja impeditido, determine um certo tempo mínimo. Uma configuração razoável é de 3 a 7 dias. Assim, você garante que os usuários estejam menos propensos a trocar de volta suas senhas para senhas antigas, mas permite que eles possam alternar suas senhas em um período razoável se quiserem. Lembre-se de que o tempo mínimo da senha pode impedir que um usuário altere uma senha comprometida. Se um usuário não puder alterar a senha, um administrador terá de fazê-lo.

Minimum Password Length

A diretiva Minimum Password Length configura um número mínimo de caracteres para uma senha. Se você ainda não alterou a configuração padrão, deveria fazer isso imediatamente. O padrão em alguns casos permite senhas vazias (senhas com zero caracteres), o que com certeza não é bom.

Por razões de segurança, são recomendáveis senhas de no mínimo oito caracteres, pois senhas longas normalmente são mais difíceis de serem quebradas que as curtas. Se você desejar uma segurança maior, configure o comprimento mínimo de senha para 14 caracteres.

Passwords Must Meet Complexity Requirements

Além das políticas básicas de senha e de conta, o Windows Server inclui recursos para criar mais controles de senha. Esses recursos impõem o uso de senhas seguras que sigam a estas diretrizes:

- As senhas devem ter no mínimo seis caracteres.
- As senhas não podem conter o nome de usuário, como stevew ou partes do nome completo do usuário, como steve.
- As senhas devem usar ao menos três dos quatro tipos de caracteres disponíveis: letras minúsculas, letras maiúsculas, números e símbolos.

Para impor essas regras, habilite Passwords Must Meet Complexity Requirements.

Store Password Using Reversible Encryption For All Users

As senhas são criptografadas no banco de dados de senhas. Normalmente, essa criptografia não pode ser revertida. A única situação em que você poderia considerar alterar essa configuração seria se sua organização usasse aplicativos que precisassem ler a senha. Se esse for o caso, habilite Store Password Using Reversible Encryption For All Users.

Com essa política habilitada, as senhas poderiam também ser armazenadas como texto sem formatação – os riscos de segurança são os mesmos. Portanto, uma técnica muito melhor é habilitar a opção por usuário, apenas conforme for preciso para atender às necessidades reais do usuário.

Configuração de política de bloqueio de conta

As políticas de bloqueio de conta, listadas aqui, controlam como e quando as contas são bloqueadas no domínio ou no sistema local:

- Account Lockout Threshold
- Account Lockout Duration
- Reset Account Lockout Counter After

Essas políticas são abordadas nas seções a seguir.

Account Lockout Threshold

A diretiva Account Lockout Threshold configura o número de tentativas de logon permitidas antes que uma conta seja bloqueada. Se você decidir usar controles de bloqueio, deve usar um valor que equilibre a necessidade de evitar a invasão de contas com a necessidade dos usuários que estão tendo dificuldades para acessar suas contas.

O principal motivo para os usuários não conseguirem acessar suas contas corretamente na primeira vez é terem esquecido a senha. Se esse for o caso, talvez eles precisem de várias tentativas para efetuarem logon adequadamente. Os usuários de grupos de trabalho também podem ter problemas para acessar um sistema remoto se suas senhas atuais não corresponderem às senhas que o sistema remoto espera. Por exemplo, o sistema remoto pode registrar várias tentativas falhas de efetuar logon antes do usuário receber um prompt para inserir a senha correta, pois o Windows Server tentou efetuar logon automaticamente no sistema remoto. Em um ambiente de domínio, isso normalmente não acontece devido ao recurso de logon único.

O limite para bloqueio pode ser configurado com qualquer valor de 0 a 999. Por padrão, o limite para bloqueio é configurado como 0, e isso significa que as contas não serão bloqueadas por tentativas de logon inválidas. Qualquer outro valor determina um limite para bloqueio específico. Lembre-se de que quanto mais alto o valor de bloqueio, maior o risco de um hacker invadir seu sistema. Uma variação razoável de valores para esse limite é de 7 a 15. Esse intervalo é alto o bastante para descartar erros dos usuários e baixo o bastante para deter hackers.

Account Lockout Duration

Se alguém violar os controles de bloqueio, a diretiva Account Lockout Duration configura o período de tempo em que a conta permanece bloqueada. A duração do bloqueio pode ser configurada para um período específico com um valor entre 1 e 99.999 minutos ou para um período indeterminado com a duração do bloqueio de 0.

A melhor política de segurança é bloquear a conta indefinidamente. Ao fazer isso, apenas um administrador pode desbloquear a conta. Isso impede que hackers tentem acessar o sistema novamente e force os usuários que estão bloqueados a procurarem a ajuda de um administrador, o que normalmente é uma boa ideia. Conversando com o usuário, você pode determinar o que ele está fazendo errado e ajudá-lo a evitar problemas futuros.

DICA Quando uma conta estiver bloqueada, abra a caixa de diálogo Properties para a conta no Active Directory Users And Computers. Toque ou clique na guia Account e selecione a caixa de seleção Unlock Account.

Reset Account Lockout Counter After

Todas as vezes que uma tentativa de logon falhar, o Windows Server aumenta o valor de um limite que rastreia o número de tentativas de logon falhas. Para manter o equilíbrio entre possíveis bloqueios oriundos de questões de segurança válidas e bloqueios que poderiam ocorrer devido a um simples erro humano, outra política determina por quanto tempo as informações sobre tentativas de logon falhas devem ser mantidas. Essa política é chamada de Reset Account Lockout Counter After e é usada para zerar as tentativas de logon falhas após um determinado tempo de espera. O modo com que a política funciona é simples: se o tempo de espera do Reset Account Lockout Counter After tiver decorrido desde a última tentativa de logon falha, o contador de tentativas de logon falhas é zerado. O contador também é reiniciado quando um usuário efetua logon com êxito.

Se a política Reset Account Lockout Counter After estiver habilitada, você pode defini-la para qualquer valor de 1 a 99.999 minutos. Assim como ocorre com a política Account Lockout Threshold, você precisa selecionar um valor que equilibre as necessidades de segurança e as necessidades de acesso dos usuários. Um bom valor é de 1 a 2 horas. Esse período de espera deve ser longo o suficiente para forçar os hackers a esperarem mais tempo do que eles querem antes de tentar acessar a conta novamente.

Se a política Reset Account Lockout Counter After não estiver configurada ou estiver desabilitada, o contador de tentativas de logon falhas é zerado apenas quando um usuário efetuar logon com êxito.

OBSERVAÇÃO As tentativas de logon falhas feitas em uma proteção de tela protegida com senha de uma estação de trabalho não aumentam o contador para bloqueio. Da mesma forma, se você pressionar Ctrl+Alt+Delete para bloquear um servidor ou uma estação de trabalho, as tentativas de logon falhas na caixa de diálogo Unlock não contarão.

Configuração de políticas do Kerberos

O Kerberos v5 é o principal mecanismo de autenticação usado em um domínio do Active Directory. O protocolo Kerberos usa tíquetes para verificar a identificação de usuários e serviços de rede. Os tíquetes contêm dados criptografados que confirmam a identidade para fins de autenticação e autorização.

É possível controlar a duração, a renovação e a imposição dos tíquetes com as políticas:

- Enforce User Logon Restrictions
- Maximum Lifetime For Service Ticket
- Maximum Lifetime For User Ticket
- Maximum Lifetime For User Ticket Renewal
- Maximum Tolerance For Computer Clock Synchronization

Essas políticas são abordadas nas seções a seguir.

ALERTA DE SEGURANÇA Somente administradores com um profundo conhecimento da segurança do Kerberos devem alterar essas políticas. Se você alterar essas políticas para configurações inefficientes, poderá causar sérios problemas na rede. As configurações padrão da política do Kerberos normalmente funcionam bem.

Enforce User Logon Restrictions

A diretiva Enforce User Logon Restrictions garante que qualquer restrição submetida a uma conta de usuário seja imposta. Por exemplo, se as horas de logon de um usuário são restritas, essa política impõe a restrição. Por padrão, a política está habilitada e somente deve ser desabilitada em raras circunstâncias.

Maximum Lifetime

As diretivas Maximum Lifetime For Service Ticket e Maximum Lifetime For User Ticket configuram o tempo máximo no qual um tíquete de serviço ou usuário permanece válido. Por padrão, os tíquetes de serviço têm uma duração máxima de 600 minutos, enquanto os tíquetes de usuário têm uma duração máxima de 10 horas.

Você pode alterar a duração de tíquetes. Para tíquetes de serviço, o intervalo válido é de 0 a 99.999 minutos. Para tíquetes de usuário, o intervalo válido é de 0 a 99.999 horas. O valor 0 desativa a expiração efetivamente. Qualquer outro valor determina um tempo de validade específico de tíquetes.

Um tíquete de usuário que expirar pode ser renovado, desde que a renovação ocorra dentro do tempo configurado para Maximum Lifetime For User Ticket Renewal. Por padrão, o período máximo de renovação é de sete dias. O período de renovação pode ser alterado para qualquer valor de 0 a 99.999 dias. O valor 0 desativa o período máximo de renovação efetivamente, e qualquer outro valor determina um período de renovação específico.

Maximum Tolerance

A diretiva Maximum Tolerance For Computer Clock Synchronization é uma das novas políticas do Kerberos que talvez você precise alterar. Por padrão, os computadores no domínio devem estar sincronizados dentro de um intervalo de cinco minutos entre um e outro. Se isso não acontecer, a autenticação falha.

Se você tiver usuários remotos que conectam-se ao domínio sem sincronizar seus relógios com o servidor de horário da rede, talvez esse valor deva ser ajustado. Você pode definir qualquer valor entre 0 e 99.999. O valor 0 indica que não há tolerância para um diferença de horário, ou seja, o sistema do usuário remoto deve estar com seu horário sincronizado de forma precisa ou a autenticação falhará.

Configuração das políticas de direitos do usuário

As contas de usuário apresentam capacidades internas e direitos do usuário. Embora não possa alterar as capacidades internas de contas, você pode gerenciar seus direitos do usuário. Normalmente, aplicam-se direitos do usuário a usuários tornando-os membros de grupo ou grupos apropriados. Também é possível aplicar direitos diretamente gerenciando os direitos do usuário para a conta do usuário.

ALERTA DE SEGURANÇA Qualquer usuário que for membro de um grupo que tem certo direito, também recebe esse direito. Por exemplo, se o grupo Backup Operators tiver o direito e jsmith for membro desse grupo, jsmith também terá esse direito. Lembre-se de que as mudanças que você fizer quanto aos direitos do usuário podem ter um efeito muito abrangente. Por isso, apenas administradores experientes devem fazer alterações na política dos direitos do usuário.

Os direitos do usuário são atribuídos por meio do nó Local Policies da Group Policy. Como o nome sugere, as políticas locais pertencem a um computador local. No entanto, você pode configurar políticas locais e importá-las para o Active Directory. Você também pode configurar essas políticas locais como parte de uma GPO existente para um site, domínio ou OU. Ao fazer isso, as políticas locais são aplicadas a contas de computador no site, domínio ou OU.

Para administrar políticas de direitos do usuário, siga estas etapas:

1. Abra a GPO com a qual você deseja trabalhar e o nó Local Policies percorrendo a árvore de console. Para isso, expanda Computer Configuration, Windows Settings, Security Settings e Local Policies.
2. Selecione User Rights Assignment para gerenciar os direitos do usuário. Para configurar uma atribuição de direitos do usuário, dê um toque duplo ou clique duas vezes em um direito do usuário. Outra opção é pressionar e manter pressionado ou clicar com o botão direito do mouse e tocar ou clicar em Properties. Uma caixa de diálogo Properties é aberta.
3. Agora você pode configurar os direitos do usuário. Para configurar direitos locais do usuário, siga as etapas de 1 a 3 em “Configuração de direitos locais do usuário”, mais adiante neste capítulo. Para configurar direitos globais do usuário, siga as etapas de 1 a 6 na seção a seguir.

Direitos globais do usuário

Para um site, domínio ou OU, os direitos individuais do usuário são configurados seguindo estas etapas:

1. Abra a caixa de diálogo Properties para o direito do usuário. Ela é similar à mostrada na Figura 8-4. Se a política não estiver definida, clique em Define These Policy Settings.

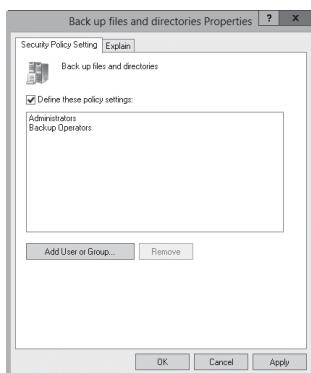


FIGURA 8-4 Na caixa de diálogo Properties, defina o direito do usuário e aplique-o a usuários e grupos.

- Para aplicar o direito a um usuário ou grupo, toque ou clique em Add User Or Group. Na caixa de diálogo Add User Or Group, toque ou clique em Browse. A caixa de diálogo Select Users, Computers, Service Accounts, Or Groups, mostrada na Figura 8-5, será aberta.

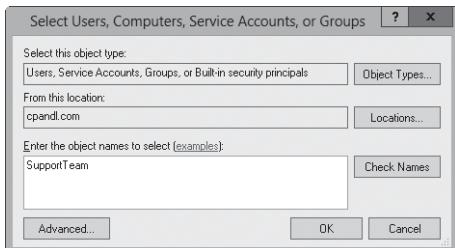


FIGURA 8-5 Na caixa de diálogo Select Users, Computers, Service Accounts, Or Groups, aplique o direito do usuário a usuários e grupos.

ALERTA DE SEGURANÇA O Windows Firewall em execução em um controlador de domínio pode impedir que você use a caixa de diálogo Select Users, Computers, Service Accounts, Or Groups. Isso pode ocorrer quando você não estiver conectado localmente no controlador de domínio e, em vez disso, estiver trabalhando remotamente. Talvez você precise configurar uma exceção no controlador de domínio para a porta TCP 445 de entrada. Para isso, expanda Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile. No painel de detalhes, dê um toque duplo ou clique duas vezes na política Windows Firewall: Allow Inbound Remote Administration Exception e selecione Enabled. Uma exceção também pode ser configurada digitando o comando a seguir em um prompt de comando no computador remoto: **netsh firewall set portopening tcp 445 smb enable**. Para mais detalhes, consulte o artigo 840634 da Microsoft Knowledge Base (support.microsoft.com/default.aspx?scid=kb;en-us;840634).

- Digite o nome do usuário ou grupo que você quer usar na caixa de texto fornecida e toque ou clique em Check Names. Por padrão, a pesquisa está configurada para encontrar entidades de segurança e contas de usuário integradas. Para adicionar grupos à pesquisa, toque ou clique em Object Types, selecione Groups na caixa de listagem e toque ou clique em OK.
- Após selecionar os nomes dos usuários ou grupos a serem adicionados, toque ou clique em OK. A caixa de diálogo Add User Or Group deve mostrar as contas selecionadas. Toque ou clique novamente em OK.
- A caixa de diálogo Properties é atualizada para corresponder a suas seleções. Caso tenha se enganado em alguma seleção, selecione um nome e remova-o tocando ou clicando em Remove.
- Após concluir a atribuição do direito a usuários e grupos, toque ou clique em OK.

Direitos locais do usuário

Para computadores locais, aplique os direitos do usuário seguindo estas etapas:

1. Abra a caixa de diálogo Properties para o direito do usuário. Ela é similar à mostrada na Figura 8-6. Lembre-se de que políticas de site, domínio ou OU têm precedência sobre as políticas locais.

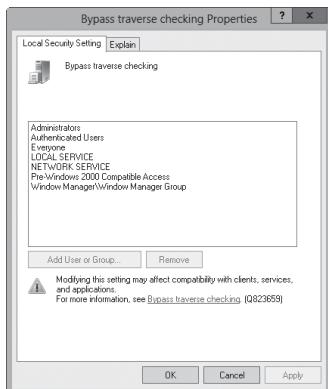


FIGURA 8-6 Na caixa de diálogo Properties, defina o direito do usuário e aplique-o a usuários e grupos. Se não puder editar direitos locais do usuário, talvez você esteja trabalhando em um controlador de domínio.

2. A caixa de diálogo Properties exibe os usuários e grupos que, no momento, já tiverem recebido o direito do usuário. Para remover o direito do usuário, selecione o usuário ou grupo e toque ou clique em Remove.
3. O direito do usuário pode ser aplicado a mais usuários e grupos tocando ou clicando em Add User Or Group. A caixa de diálogo Select Users, Computers, Service Accounts, Or Groups, mostrada anteriormente na Figura 8-5, será aberta. Agora, é possível adicionar usuários e grupos.

Como adicionar uma conta de usuário

Você precisa criar uma conta de usuário para cada usuário que quiser usar seus recursos de rede. As contas de usuário de domínio são criadas com o Active Directory Users And Computers. As contas de usuário locais, por sua vez, são criadas com o Local Users And Groups.

Como criar contas de usuário de domínio

Normalmente, novas contas de domínio são criadas de duas maneiras:

- **Criar uma conta de usuário totalmente nova** Pressione e mantenha pressionado ou clique com o botão direito do mouse no contêiner em que você pretende colocar a conta de usuário, toque ou clique em New e, após, em User. A caixa

de diálogo New Object–User Wizard, mostrada na Figura 8-7, será aberta. Ao criar uma nova conta, as configurações padrão do sistema são usadas.

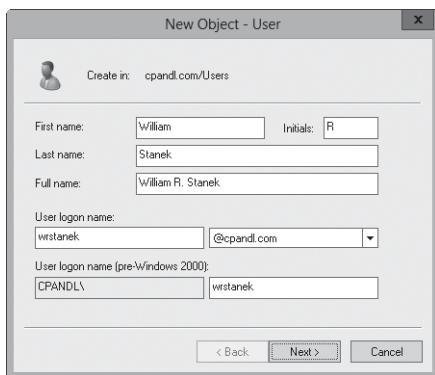


FIGURA 8-7 Configure o nome de exibição e o nome de logon do usuário.

- **Basear uma conta nova em uma conta já existente** Pressione e mantenha pressionado ou clique com o botão direito do mouse na conta de usuário que você quer copiar no Active Directory Users And Computers e toque ou clique em Copy. O Copy Object–User Wizard, que é essencialmente igual ao New Object–User Wizard, será iniciado. No entanto, ao criar uma cópia de uma conta, a nova conta recebe a maioria de suas configurações de ambiente da conta existente. Para mais informações sobre a cópia de contas, consulte “Como copiar contas de usuário de domínio” no Capítulo 9, “Gerenciamento de contas de usuário e de grupo”.

Tanto com o New Object–User Wizard quanto com o Copy Object–User Wizard, uma conta pode ser criada seguindo estas etapas:

1. Como mostrado na Figura 8-7, a primeira página do assistente deixa você configurar o nome de exibição e o nome de logon do usuário. Digite o primeiro nome do usuário, a inicial do nome do meio e o sobrenome nas caixas de texto fornecidas. Essas caixas são usadas para criar o nome completo, que é o nome de exibição do usuário.
2. Se necessário, faça alterações no campo Full Name. Por exemplo, talvez você queira digitar o nome no formato Sobrenome PrimeiroNome InicialDoNomeDoMeio ou ainda no formato PrimeiroNome InicialDoNomeDoMeio Sobrenome. O nome completo deve ser exclusivo no domínio e ter no máximo 64 caracteres.
3. Na caixa User Logon Name, digite o nome de logon do usuário. Use a lista suspensa para selecionar o domínio a ser associado com a conta. Isso configura o nome de logon totalmente qualificado.
4. Os primeiros 20 caracteres do nome de logon são usados para determinar o nome de logon anterior ao Windows 2000. Esse nome de logon deve ser exclusivo no domínio. Se necessário, altere o nome de logon anterior ao Windows 2000.

5. Toque ou clique em Next e configure a senha do usuário na página mostrada na Figura 8-8.

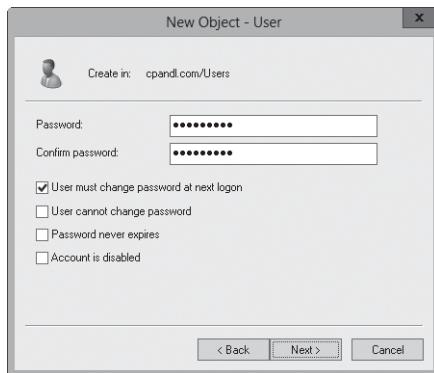


FIGURA 8-8 Use o New Object–User Wizard para configurar a senha do usuário.

As opções dessa página são:

- **Password** A senha da conta. Essa senha deve seguir as convenções de sua política de senha.
- **Confirm Password** Uma caixa de texto para garantir que você atribua a senha da conta corretamente. Basta reinserir a senha para confirmá-la.
- **User Must Change Password At Next Logon** Se selecionada, o usuário deve alterar a senha no logon.
- **User Cannot Change Password** Se selecionada, o usuário não tem permissão para alterar a senha.
- **Password Never Expires** Se selecionada, a senha dessa conta nunca será expirada. Essa configuração substitui a política de conta do domínio. Normalmente, não é recomendável determinar que uma senha não expire, pois isso, antes de tudo, diminui o propósito de ter senhas.
- **Account Is Disabled** Se selecionada, a conta é desabilitada e não pode ser usada. Use essa caixa de seleção para impedir temporariamente que alguém use uma conta.

6. Toque ou clique em Next e em Finish para criar a conta. Se houver problemas para criar a conta, você verá um aviso e precisará usar o botão Back para digitar novamente as informações nas páginas de nome de usuário e senha, conforme necessário.

Após criar a conta, é possível configurar as propriedades avançadas para a conta como discutido mais adiante neste capítulo.

Você também pode criar contas de usuário com o Active Directory Administrative Center. Para isso, siga estas etapas:

- Na árvore de console Active Directory Administrative Center, pressione e mantenha pressionado ou clique com o botão direito do mouse no contêiner em que você pretende colocar a conta de usuário, toque ou clique em New no painel do contêiner e, após, em User. A caixa de diálogo Create User, mostrada na Figura 8-9, será aberta.

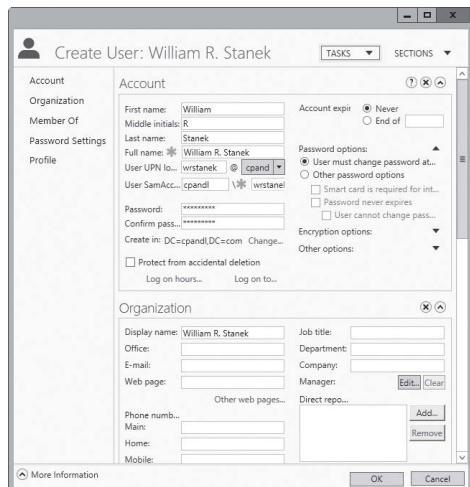


FIGURA 8-9 Criação de uma nova conta de usuário no Active Directory Administrative Center.

- Digite o primeiro nome do usuário, a inicial do nome do meio e o sobrenome nas caixas de texto fornecidas. Essas caixas de texto são usadas para criar o nome completo, que é o nome de exibição do usuário.
- Se necessário, faça alterações na caixa Full Name. O nome completo deve ser exclusivo no domínio e ter no máximo 64 caracteres.
- Na caixa User UPN Logon, digite o nome de logon do usuário. Use a lista suspenso para selecionar o domínio a ser associado com a conta. Isso configura o nome de logon totalmente qualificado.
- Os primeiros 20 caracteres do nome de logon são usados para configurar a caixa User SamAccountName Logon. O conteúdo dessa caixa é o nome de logon anterior ao Windows 2000 do usuário, que deve ser exclusivo no domínio.

6. Todas as outras caixas de texto da caixa de diálogo são opcionais. Configure e confirme a senha do usuário, se desejado. Opcionalmente, selecione Protect From Accidental Deletion para marcar a conta como protegida no Active Directory. As contas protegidas só podem ser excluídas se você remover o sinalizador Protect antes de tentar excluí-las.
7. Toque ou clique em OK para criar a conta de usuário.

Como criar contas de usuário locais

As contas de usuário locais são criadas com o Local Users And Groups. Você pode abrir esse utilitário e criar uma conta seguindo estas etapas:

1. Em Server Manager, toque ou clique em Tools e depois em Computer Management. Outra opção é pressionar Windows+X e clicar em Computer Management.
2. Pressione e mantenha pressionado ou clique com o botão direito do mouse na entrada do Computer Management na árvore de console e toque ou clique em Connect To Another Computer. Assim você pode escolher o sistema com as contas locais a serem gerenciadas. Os controladores de domínio não apresentam usuários e grupos locais.
3. Sob System Tools, escolha Local Users And Groups.
4. Pressione e mantenha pressionado ou clique com o botão direito do mouse em Users e toque ou clique em New User. A caixa de diálogo New User, mostrada na Figura 8-10, será aberta. Cada caixa de texto da caixa de diálogo é usada como apresentado a seguir:
 - **User Name** O nome de logon para a conta de usuário. Esse nome deve seguir as convenções da política de nomes para o usuário local.
 - **Full Name** O nome completo do usuário, como William R. Stanek.
 - **Description** Uma descrição do usuário. Normalmente, aqui insere-se o cargo do usuário, como Webmaster. Outra opção é digitar o cargo e o departamento do usuário.
 - **Password** A senha da conta. Essa senha deve seguir as convenções de sua política de senha.
 - **Confirm Password** Uma segunda entrada para garantir que você atribua a senha da conta corretamente. Basta reinserir a senha para confirmá-la.
 - **User Must Change Password At Next Logon** Se selecionada, o usuário deve alterar a senha no logon.
 - **User Cannot Change Password** Se selecionada, o usuário não tem permissão para alterar a senha.
 - **Password Never Expires** Se selecionada, a senha dessa conta nunca será expirada. Essa configuração substitui a política de conta local.
 - **Account Is Disabled** Se selecionada, a conta é desabilitada e não pode ser usada. Use essa caixa de seleção para impedir temporariamente que alguém use uma conta.

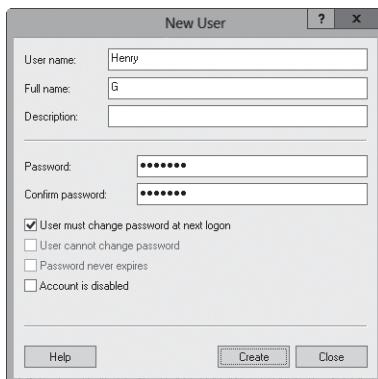


FIGURA 8-10 A configuração de uma conta de usuário local é diferente da configuração de uma conta de usuário de domínio.

5. Toque ou clique em Create após concluir a configuração da nova conta.

Como adicionar uma conta de grupo

As contas de grupo são usadas para gerenciar os privilégios para vários usuários. As contas de grupo global são criadas no Active Directory Users And Computers. As contas de grupo local, por sua vez, são criadas no Local Users And Groups.

Durante as definições para a criação de contas de grupo, lembre-se de que elas são criadas para tipos semelhantes de usuários. Os tipos de grupos que talvez você queira criar incluem:

- **Grupos por departamento da organização** Normalmente, os usuários que trabalham no mesmo departamento precisam de acesso a recursos similares. Você criará frequentemente grupos organizados por departamento, como Desenvolvimento de Negócios, Vendas, Marketing e Engenharia.
- **Grupos para usuários de aplicativos específicos** Os usuários muitas vezes precisam de acesso a um aplicativo e a recursos relacionados a esse aplicativo. Se você criar grupos para aplicativos específicos, pode ter certeza que os usuários têm o acesso adequado aos recursos e arquivos do aplicativo necessários.
- **Grupos para funções dentro da organização** Também é possível organizar grupos por funções de usuário dentro da organização. Por exemplo, os executivos provavelmente precisam acessar recursos diferentes dos supervisores e usuários em geral. Com a criação de grupos feitos com base nas funções dentro da organização, você pode assegurar que o acesso adequado é dado aos usuários que precisam dele.

Como criar um grupo global

Para criar um grupo no domínio, siga estas etapas:

1. Inicie o Active Directory Users And Computers. Pressione e mantenha pressionado ou clique com o botão direito do mouse no contêiner em que você pretende colocar a conta do grupo, toque ou clique em New e, após, em Group. A caixa de diálogo New Object–Group, mostrada na Figura 8-11, será aberta.

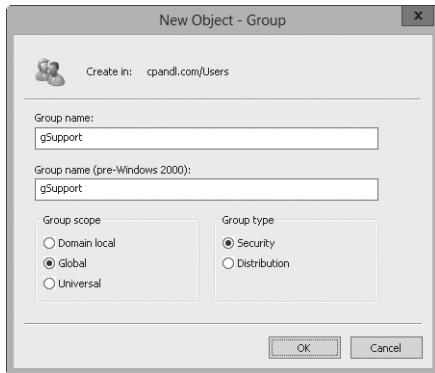


FIGURA 8-11 A caixa de diálogo New Object–Group permite que você adicione um novo grupo ao domínio.

2. Digite um nome para o grupo. Os nomes das contas de grupo seguem as mesmas regras de nomeação dos nomes de exibição de contas de usuário. Eles não diferenciam maiúsculas de minúsculas e podem ser formados por até 64 caracteres.
3. Os primeiros 20 caracteres do nome de grupo são usados para determinar o nome do grupo anterior ao Windows 2000. Esse nome de grupo deve ser exclusivo no domínio. Se necessário, altere o nome de grupo anterior ao Windows 2000.
4. Selecione um escopo de grupo (Domain Local, Global ou Universal).
5. Selecione um tipo de grupo (Security ou Distribution).
6. Toque ou clique em OK para criar o grupo. Após criar a conta, é possível adicionar membros e configurar as propriedades adicionais, como discutido mais adiante neste capítulo.

Você também pode criar grupos com o Active Directory Administrative Center. Para isso, siga estas etapas:

1. Na árvore de console do Active Directory Administrative Center, pressione e mantenha pressionado ou clique com o botão direito do mouse no contêiner em que você pretende colocar o grupo, toque ou clique em New no painel do contêiner e, após, em Group. A caixa de diálogo Create Group, mostrada na Figura 8-12, será aberta.

2. Digite um nome para o grupo. Os nomes das contas de grupo seguem as mesmas regras de nomeação dos nomes de exibição de contas de usuário. Eles não diferenciam maiúsculas e podem ser formados por até 64 caracteres.
3. Os primeiros 20 caracteres do nome de grupo são usados para configurar o nome de grupo SAMAccountName do grupo. O conteúdo dessa caixa é o nome de grupo anterior ao Windows 2000, que deve ser exclusivo no domínio.
4. Selecione um tipo de grupo (Security ou Distribution).
5. Selecione um escopo de grupo (Domain Local, Global ou Universal).
6. Todas as outras configurações da caixa de diálogo não são obrigatórias. Como opção, selecione Protect From Accidental Deletion para marcar a conta como protegida no Active Directory. As contas protegidas só podem ser excluídas se você remover o sinalizador Protect antes de tentar excluí-las.
7. Toque ou clique em OK para criar o grupo.



FIGURA 8-12 Criação de um novo grupo no Active Directory Administrative Center.

Como criar um grupo local e atribuir membros

Os grupos locais são criados com o Local Users And Groups. Você pode abrir esse utilitário e criar um grupo seguindo estas etapas:

1. Em Server Manager, toque ou clique em Tools e depois em Computer Management. Pressione e mantenha pressionado ou clique com o botão direito do mouse na entrada do Computer Management na árvore de console e toque ou clique em Connect To Another Computer. Assim você pode escolher o sistema com as contas locais a serem gerenciadas. Os controladores de domínio não apresentam usuários e grupos locais.

2. Sob System Tools, escolha Local Users And Groups.
3. Pressione e mantenha pressionado ou clique com o botão direito do mouse em Groups e toque ou clique em New Group. A caixa de diálogo New Group, mostrada na Figura 8-13, será aberta.

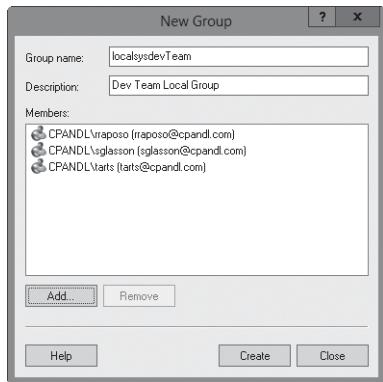


FIGURA 8-13 Na caixa de diálogo New Group, você pode adicionar um novo grupo local a um computador.

4. Após digitar um nome e uma descrição para o grupo, toque ou clique no botão Add para adicionar usuários ao grupo. A caixa de diálogo Select Users será aberta.
5. Na caixa de diálogo Select Users, digite o nome de um usuário que você queira usar na caixa Name e toque ou clique em Check Names. Se forem encontradas correspondências, selecione a conta que queira usar e toque ou clique em OK. Se nenhuma correspondência for encontrada, atualize o nome digitado e faça uma nova pesquisa. Repita esta etapa conforme necessário e toque ou clique em OK.
6. A caixa de diálogo New Group é atualizada para corresponder a suas seleções. Caso tenha se enganado em alguma seleção, selecione o nome e toque ou clique em Remove.
7. Toque ou clique em Create após terminar de adicionar ou remover membros do grupo.

Manipulação de associação de grupo

Para configurar a associação de grupo, use o Active Directory Users And Computers ou o Active Directory Administrative Center. Ao trabalhar com grupos, lembre-se do seguinte:

- Todos os novos usuários de um domínio são membros do grupo Domain Users e o grupo primário deles é especificado como Domain Users.
- Todas as novas estações de trabalho e servidores membros de um domínio são membros de Domain Computers e o grupo primário deles é Domain Computers.

- Todos os novos controladores de domínio são membros de Domain Controllers e o grupo primário deles é Domain Controllers.

As associações de grupo são gerenciadas de diversas maneiras:

- Gerenciar associação individual
- Gerenciar várias associações
- Determinar a associação de grupo primária de cada usuário e computador

Gerenciamento de associação individual

Você pode adicionar um usuário ou grupo a um ou mais grupos rapidamente pressionando e mantendo pressionada ou clicando com o botão direito do mouse na conta e selecionando Add To Group. A caixa de diálogo Select Groups será aberta. Nessa caixa, você pode escolher os grupos dos quais a conta selecionada no momento deve ser membro.

Você pode gerenciar a associação de grupo de qualquer tipo de conta seguindo estas etapas:

1. Dê um toque duplo ou clique duas vezes na entrada do usuário, grupo ou computador no Active Directory Users And Computers ou no Active Directory Administrative Center. A caixa de diálogo Properties da conta será aberta.
2. Na guia ou no painel Member Of, encontram-se listados os grupos dos quais o usuário é membro no momento. Toque ou clique em Add para tornar a conta membro de um grupo adicional. A caixa de diálogo Select Groups será aberta. Nessa caixa, você pode escolher os grupos dos quais a conta selecionada no momento deve ser membro.
3. Para remover a conta de um grupo, selecione o grupo e toque ou clique em Remove.
4. Toque ou clique em OK.

Se você estiver trabalhando exclusivamente com contas de usuário, pode adicionar usuários a grupos seguindo estas etapas:

1. Selecione as contas de usuário com as quais você deseja trabalhar no Active Directory Users And Computers ou no Active Directory Administrative Center.
DICA Para selecionar vários usuários individualmente, mantenha a tecla Ctrl pressionada e toque ou clique em cada conta de usuário que deseja selecionar. Para selecionar uma sequência de contas, mantenha a tecla Shift pressionada, selecione a primeira conta de usuário e, depois, a última conta de usuário.
2. Pressione e mantenha pressionado ou clique com o botão direito do mouse em uma das seleções e toque ou clique em Add To A Group ou Add To Group, conforme apropriado. A caixa de diálogo Select Groups será aberta. Nessa caixa, você pode escolher os grupos dos quais as contas selecionadas no momento devem ser membros.
3. Toque ou clique em OK.

Gerenciamento de várias associações a um grupo

Outra maneira de gerenciar a associação de grupo é com a caixa de diálogo Properties de um grupo para adicionar ou remover várias contas. Para isso, siga estas etapas:

1. Dê um toque duplo ou clique duas vezes na entrada do grupo no Active Directory Users And Computers ou no Active Directory Administrative Center. A caixa de diálogo Properties do grupo será aberta.
2. Na guia ou painel Members, encontram-se listados os membros atuais do grupo em ordem alfabética. Para adicionar contas ao grupo, toque ou clique em Add. A caixa de diálogo Select Users, Contacts, Computers, Service Accounts, Or Groups será aberta. Você pode escolher usuários, computadores, contas de serviço e grupos que devem ser membros do grupo selecionado no momento.
3. Para remover membros de um grupo, selecione a conta e toque ou clique em Remove.
4. Toque ou clique em OK.

Configuração do grupo primário para usuários e computadores

Os usuários que acessam o Windows Server por meio do Services for Macintosh usam grupos primários. Quando um usuário de Macintosh cria arquivos ou diretórios em um sistema com Windows Server, o grupo primário é atribuído a esses arquivos e diretórios.

OBSERVAÇÃO O Windows Server 2008 e as versões superiores não incluem o Services for Macintosh. O Services for Macintosh estão incluídos apenas em versões anteriores do Windows Server. Todas as contas de usuário e computador devem ter um grupo primário independentemente se as contas acessem ou não os sistemas Windows Server por meio de Macintosh. Esse grupo dever ter um escopo global ou universal, como os grupos globais Domain Users ou Domain Computers.

Para configurar o grupo primário, siga estas etapas:

1. Dê um toque duplo ou clique duas vezes na entrada do usuário ou computador no Active Directory Users And Computers ou no Active Directory Administrative Center. A caixa de diálogo Properties da conta será aberta.
2. Na guia ou no painel Member Of, selecione um grupo com escopo global ou universal da lista Member Of.
3. Toque ou clique em Set Primary Group.

Todos os usuários devem ser membros de pelo menos um grupo primário. Não é possível revogar a associação a um grupo primário sem antes atribuir o usuário a outro grupo primário. Para isso, siga estas etapas:

1. Selecione um grupo diferente com escopo global ou universal na lista Member Of e toque ou clique em Set Primary Group.
2. Na lista Member Of, toque ou clique no grupo primário anterior e, depois, em Remove. Assim, a associação de grupo é revogada.

Implementação de contas gerenciadas

O Microsoft Exchange Server, o Internet Information Services, o SQL Server e outros tipos de aplicativos usam frequentemente contas de serviço. Em um computador local, é possível configurar o aplicativo para que ele execute como uma conta de usuário interna, como Local Service, Network Service ou Local System. Embora essas contas de serviço sejam fáceis de configurar e usar, elas normalmente são compartilhadas entre vários aplicativos e serviços e não podem ser gerenciadas em nível de domínio. Se você configurar o aplicativo para usar uma conta de domínio, pode isolar os privilégios para o aplicativo, mas, nesse caso, deve gerenciar manualmente a senha da conta e qualquer Service Principal Name (SPN, nome da entidade de serviço) requisitado pela autenticação do Kerberos.

O Windows 7 e todas as versões superiores do Windows são compatíveis com dois tipos de conta adicionais:

- Contas de serviço gerenciado
- Contas virtuais gerenciadas

As contas de serviço gerenciado são um tipo especial de conta de usuário de domínio para serviços gerenciados. Essas contas reduzem as interrupções de serviços e outros problemas encarregando o Windows de gerenciar automaticamente a senha da conta e os SPNs.

As contas virtuais gerenciadas são um tipo especial de conta de computador local para serviços gerenciados. Essas contas fornecem a possibilidade de acessar a rede com uma identidade de computador em um ambiente de domínio. Como a identidade do computador é usada, não há a necessidade de gerenciamento de senha.

Você pode gerenciar essas contas com o módulo do Active Directory para Windows PowerShell. O módulo do Active Directory não é importado para o Windows PowerShell por padrão. Por isso, você precisa importar o módulo antes de poder usar os cmdlets que ele fornece. Embora não estejam disponíveis originalmente no Windows 7 e no Windows Server 2008 R2, o Windows 8 e o Windows Server 2012 comportam contas de serviço gerenciado de grupo. As contas de serviço gerenciado de grupo fornecem a mesma funcionalidade que as contas de serviço gerenciado padrão, mas estendem essa funcionalidade para vários servidores. Por exemplo, quando um computador cliente se conecta a um serviço hospedado por um farm de servidores, a autenticação mútua não tem sucesso a menos que todas as instâncias dos serviços usem a mesma entidade. Com o uso de uma conta de serviço gerenciado de grupo, você permite que cada servidor do farm use a mesma entidade de serviço, que é gerenciada pelo próprio Windows em vez de individualmente pelo administrador.

As contas de serviço gerenciado de grupo são, na verdade, o tipo padrão de conta de serviço do Windows 8 e do Windows Server 2012. Por isso, as contas de serviço gerenciado podem abranger vários computadores por padrão. Isso significa que você pode adicionar a conta a mais de um computador por vez conforme necessário para dar suporte a nós de cluster, farms de servidores com平衡amento de carga de rede e assim por diante. Se desejar restringir uma conta de serviço gerenciado a um computador único, você deve configurar a opção *-RestrictToSingleComputer* ao criar a conta. Não se esqueça que um computador único também pode ter várias contas de serviço gerenciado.

No esquema do Active Directory, as contas de serviço gerenciado são representadas por *msDSManagedServiceAccounts*. Essa classe de objeto herda seus atributos

da classe de objeto *Computer*, mas os objetos também são usuários. As contas de serviço gerenciado usam o mesmo mecanismo de atualização de senha que as contas de computador comuns. Isso significa que a senha da conta é atualizada sempre que o computador atualizar sua senha, o que ocorre a cada 30 dias por padrão. Além disso, as contas de serviço gerenciado podem manter seu SPN Kerberos e dar suporte à delegação automaticamente.

DICA Alguns aplicativos, como o SQL Server e o IIS, usam muito o Kerberos e sabem como registrarem a si mesmos com SPNs. Se um aplicativo consegue gravar seus próprios SPNs, as contas de serviço gerenciado trabalharão para o gerenciamento automático de SPN.

OBSERVAÇÃO Por padrão, todas as contas de serviço gerenciado são criadas no contêiner Managed Service Accounts no Active Directory. Esse contêiner torna-se visível no Active Directory Users And Computers quando os recursos avançados são exibidos.

Como as contas de computador, as contas de serviço gerenciado não usam políticas de senha de domínio ou de bloqueio refinado. Em vez disso, elas usam uma senha de 240 bytes (120 caracteres) gerada aleatoriamente. As contas de serviço gerenciado não podem executar logons interativos e nem serem bloqueadas como as contas de usuário. Você pode adicionar contas de serviço gerenciado a grupos com o Active Directory Users And Computers ou com o Add-ADGroupMember.

Como criar e usar as contas de serviço gerenciado

Com as contas de serviço gerenciado, você pode criar uma conta real, que é armazenada por padrão no contêiner Managed Service Accounts do Active Directory. Em seguida, você deve associar a conta com um computador no Active Directory e instalar a conta de serviço gerenciado em um servidor local para adicionar a conta como um usuário local. Por fim, o serviço local deve ser configurado para usar a conta. Em outras palavras, você precisa:

1. Criar a conta de serviço gerenciado.
2. Associar a conta com um computador no Active Directory.
3. Instalar a conta de serviço gerenciado no computador que foi associado.
4. Configurar o serviço local para usar a conta.

Os cmdlets do Windows PowerShell podem ser usados para instalar, desinstalar e redefinir senhas para contas de serviço gerenciado. Após a instalação de uma conta de serviço gerenciado, você poderá configurar um serviço ou aplicativo para usar a conta e não precisará mais especificar ou alterar senhas, pois a manutenção da senha da conta é feita pelo computador. Você também pode configurar o SPN na conta de serviço sem a necessidade de ter privilégios de administrador no domínio.

Uma conta de serviço gerenciado é criada com o New-ADServiceAccount. A sintaxe básica é a seguinte:

```
New-ADServiceAccount -DisplayName DisplayName -SamAccountName  
SAMName -Name Name [-RestrictToSingleComputer]
```

DisplayName é o nome de exibição da conta, *SAMName* é o nome anterior ao Windows 2000 da conta e *Name* é o nome efetivamente da conta, como:

```
New-ADServiceAccount -DisplayName "SQL Agent Account"  
-SamAccountName sqlagent -Name "SQL Agent"
```

A conta será criada como uma conta de grupo por padrão. Ela terá uma senha de 240 bytes (120 caracteres) gerada aleatoriamente e será criada no contêiner Managed Service Accounts. Por padrão, a conta também está habilitada, mas você pode criar a conta de maneira que ela permaneça em estado desabilitado adicionando *-Enabled \$false*. Se for necessário passar as credenciais para criar a conta, use o parâmetro *-Credential* como mostrado no exemplo a seguir:

```
$cred = Get-Credential  
New-ADServiceAccount -DisplayName "IIS App Pool 1"  
-SamAccountName pool1 -Name "IIS Pool 1" -Credential $cred
```

Embora a conta esteja listada no Active Directory Users And Computers, você não deve usar essa ferramenta de gerenciamento para trabalhar com a conta. Em vez disso, use os seguintes cmdlets do Windows PowerShell:

- `Get-ADServiceAccount`, para obter informações sobre uma ou mais contas de serviço gerenciado.
- `Set-ADServiceAccount`, para configurar as propriedades de uma conta de serviço gerenciado.
- `Remove-ADServiceAccount`, para remover uma conta de serviço gerenciado do Active Directory.

Após criar uma conta de serviço gerenciado no Active Directory, você deve associá-la a um computador de destino no Active Directory por meio do `Add-ADComputerServiceAccount`. O `Remove-ADComputerServiceAccount` é usado para remover uma associação de computador do Active Directory.

A sintaxe básica do `Add-ADComputerServiceAccount` é a seguinte:

```
Add-ADComputerServiceAccount [-Identity] ComputerName  
[-ServiceAccount] MSAName
```

ComputerName é o nome do computador de destino e *MSAName* é o nome da conta de serviço gerenciado, como:

```
Add-ADComputerServiceAccount IISServer84 WebServicesAccount
```

Se for necessário passar as credenciais para criar a conta, use o parâmetro *-Credential* como mostrado no exemplo a seguir:

```
$cred = Get-Credential  
Add-ADComputerServiceAccount IISServer32 FarmFourServicesAccount
```

Você pode instalar a conta em um computador local com o `Install-ADServiceAccount`. A sintaxe básica é a seguinte:

```
Install-ADServiceAccount [-Identity] ServiceAccountId
```

ServiceAccountId é o nome de exibição ou o nome SAM da conta de serviço, como:

```
Install-ADServiceAccount sqlagent
```

Se for necessário passar as credenciais para criar a conta, use o parâmetro *-Credential*. Use o Uninstall-ADServiceAccount para desinstalar uma conta.

Configuração de serviços para o uso de contas de serviço gerenciado

Você pode configurar um serviço para executar com a conta de serviço gerenciado seguindo estas etapas:

1. Em Server Manager, toque ou clique em Tools e depois em Computer Management.
2. Conforme necessário, conecte-se ao computador a ser gerenciado. No painel esquerdo, pressione e mantenha pressionado ou clique com o botão direito do mouse no nó Computer Management e toque ou clique em Connect To Another Computer. Insira o nome do host, o FQDN ou o endereço IP do servidor remoto e toque ou clique em OK.
3. No painel esquerdo, expanda o nó Services And Applications e selecione o nó Services.
4. Pressione e mantenha pressionado ou clique com o botão direito do mouse no nome do serviço com o qual você deseja trabalhar e toque ou clique em Properties.
5. Na guia Log On, selecione This Account e digite o nome da conta de serviço gerenciado no formato *NomeDoDomínio\NomeDaConta* ou toque ou clique em Browse para procurar a conta.
6. Verifique se a caixa de senha está em branco e toque ou clique em OK.
7. Selecione o nome do serviço e toque ou clique em Start para iniciar o serviço. Se for o caso, outra opção é tocar ou clicar em Restart para reiniciar o serviço. Verifique se o nome da conta recém-configurado aparece na coluna Log On As para o serviço.

OBSERVAÇÃO Um cífrão (\$) aparece no final do nome da conta no console do snap-in Services. Ao usar o console do snap-in Services para configurar o logon de uma conta para um serviço, o direito de logon Service Logon Right é atribuído automaticamente à conta. Se você usar uma ferramenta diferente, esse direito deve ser concedido à conta explicitamente.

Como remover contas de serviço gerenciado

Se uma conta de serviço gerenciado deixou de ser usada em um computador, talvez você queira desinstalar essa conta. No entanto, antes disso você deve verificar o snap-in Services para assegurar que a conta não está sendo usada. Para desinstalar uma conta de serviço gerenciado de um computador local, use o Uninstall-ADServiceAccount. A sintaxe básica é a seguinte:

```
Uninstall-ADServiceAccount -Identity ServiceAccountId
```

ServiceAccountId é o nome de exibição ou o nome SAM da conta de serviço, como:

```
Uninstall-ADServiceAccount -Identity sqlagent
```

Se for necessário passar as credenciais para desinstalar a conta, use o parâmetro *-Credential*.

As senhas das contas de serviço gerenciado são redefinidas regularmente de acordo com os requisitos de redefinição de senha do domínio, mas você pode redefinir a senha manualmente se necessário. Para redefinir a senha de uma conta de serviço gerenciado, use o Reset-ADServiceAccountPassword. A sintaxe básica é a seguinte:

```
Reset-ADServiceAccountPassword -Identity ServiceAccountId
```

ServiceAccountId é o nome de exibição ou o nome SAM da conta de serviço, como:

```
Reset-ADServiceAccountPassword -Identity sqlagent
```

Se for necessário passar as credenciais para redefinir a senha, use o parâmetro *-Credential*. O intervalo padrão para alteração da senha pode ser modificado para as contas de serviço gerenciado com a política de domínio Domain Member: Maximum Machine Account Password Age sob Local Policy\Security Options. As configurações de Group Policy sob Account Policies\Password Policy não são usadas para modificar os intervalos de redefinição de senha de contas de serviço gerenciado, bem como o comando NLTEST /SC_CHANGE_PWD não pode ser usado para redefinir senhas de contas de serviço gerenciado.

Como mover contas de serviço gerenciado

Para mover uma conta de serviço gerenciado de um computador de origem a um novo computador de destino, você precisa seguir estas etapas:

1. No computador de origem, configure todos os serviços que estiverem usando a conta gerenciada de modo que eles usem uma conta diferente. Após, execute o Uninstall-ADServiceAccount.
2. No computador de destino, execute o Install-ADServiceAccount e use o console do snap-in Services para configurar o serviço a ser executado com a conta de serviço gerenciado.

Para migrar um serviço de uma conta de usuário para uma conta de serviço gerenciado, você precisa seguir estas etapas:

1. Crie uma nova conta de serviço gerenciado no Active Directory com o New-ADServiceAccount.
2. Instale a conta de serviço gerenciado no computador adequado com o Install-ADServiceAccount e use o console do snap-in Services para configurar o serviço a ser executado com a conta de serviço gerenciado.
3. Você também precisa configurar as listas de controle de acesso nos recursos do serviço para a conta de serviço gerenciado.

Uso de contas virtuais

As contas virtuais requerem pouco gerenciamento. Além de elas não poderem ser criadas ou excluídas, essas contas não exigem qualquer tipo de gerenciamento de senha. Em vez disso, elas existem automaticamente e são representadas pela identidade da máquina do computador local.

Com as contas virtuais, você pode configurar um serviço local para que ele acesse a rede com a identidade do computador em um ambiente de domínio. Como a identidade do computador é usada, não é necessária a criação de uma conta, bem como o gerenciamento de senha não é exigido.

Você pode configurar um serviço para executar com uma conta virtual seguindo estas etapas:

1. Em Server Manager, toque ou clique em Tools e depois em Computer Management.
2. Conforme necessário, conecte-se ao computador a ser gerenciado. No painel esquerdo, pressione e mantenha pressionado ou clique com o botão direito do mouse no nó Computer Management e toque ou clique em Connect To Another Computer. Insira o nome de host, o FQDN ou o endereço IP do servidor remoto e toque ou clique em OK.
3. No painel esquerdo, expanda o nó Services And Applications e selecione o nó Services.
4. Pressione e mantenha pressionado ou clique com o botão direito do mouse no nome do serviço com o qual você deseja trabalhar e toque ou clique em Properties.
5. Na guia Log On, selecione This Account e digite o nome da conta de serviço no formato *SERVIÇO\NomeDoComputador*.
6. Verifique se a caixa de senha está em branco e toque ou clique em OK.
7. Selecione o nome do serviço e toque ou clique em Start para iniciar o serviço. Se for o caso, toque ou clique em Restart para reiniciar o serviço. Verifique se o nome da conta recém-configurado aparece na coluna Log On As para o serviço.

OBSERVAÇÃO Um cífrão (\$) aparece no final do nome da conta no console do snap-in Services. Ao usar o console do snap-in Services para configurar o logon de uma conta para um serviço, o direito de logon Logon Right é atribuído automaticamente à conta. Se você usar uma ferramenta diferente, esse direito deve ser concedido à conta explicitamente.

CAPÍTULO 9

Gerenciamento de contas de usuário e de grupo

- Gerenciamento das informações de contato do usuário **345**
- Configurações do ambiente do usuário **349**
- Configuração de opções e restrições de conta **353**
- Gerenciamento de perfis de usuário **359**
- Atualização de contas de usuário e de grupo **366**
- Gerenciamento de várias contas de usuário **373**
- Solução de problemas de logon **376**
- Visualização e configuração de permissões no Active Directory **378**

Em um mundo perfeito, criariamos contas de usuário e de grupo e esqueceríamos delas. Infelizmente, vivemos no mundo real; depois de criar as contas, você passará um bom tempo gerenciando-as. Este capítulo oferece orientações e dicas para facilitar essa tarefa.

Gerenciamento das informações de contato do usuário

O Active Directory é um serviço de diretório. Ao criar contas de usuário, elas podem conter informações de contato detalhadas associadas a elas. Assim, as informações de contato ficarão disponíveis para qualquer um na árvore de domínios ou na floresta e poderão ser usadas como critério de busca por usuários e para criar entradas no catálogo de endereços.

Configuração das informações de contato

Para configurar as informações de contato de um usuário no Active Directory Users And Computers (Usuários e Computadores do Active Directory), siga estas etapas:

1. Dê um toque duplo ou clique duas vezes no nome do usuário no Active Directory Users And Computers. A caixa de diálogo Properties da conta será aberta.

2. Toque ou clique na guia General, mostrada na Figura 9-1. Configure as informações gerais do contato nas seguintes caixas de texto:

- **First Name, Initials, Last Name** Define o nome completo do usuário.
- **Display Name** Define o nome de exibição do usuário, como ele é visto nas sessões de logon e no Active Directory Domain Services (AD DS, Serviços de Domínio do Active Directory).
- **Description** Define uma descrição do usuário.
- **Office** Define o local do escritório do usuário.
- **Telephone Number** Define o número de telefone comercial principal do usuário. Caso o usuário tenha outros números de telefone comercial que você queira incluir, toque ou clique em Other e depois insira os números de telefone adicionais na caixa de diálogo Phone Number (Others).
- **E-Mail** Define o endereço de email comercial do usuário.
- **Web Page** Define a URL da home page do usuário na Internet ou na intranet da empresa. Caso o usuário tenha outras páginas da Web que você queira incluir, toque ou clique em Other e depois insira os endereços das páginas adicionais na caixa de diálogo Web Page Address (Others).

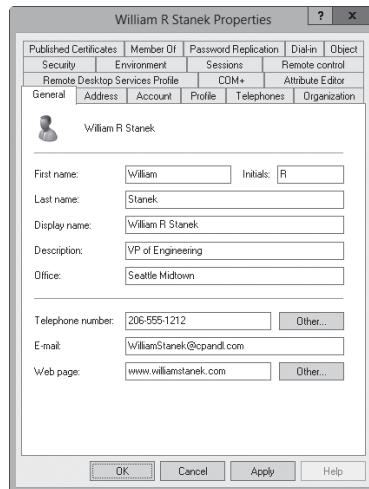


FIGURA 9-1 Configure informações gerais de contato para o usuário na guia General.

DICA É necessário preencher as caixas de texto de E-Mail e Web Page para utilizar os recursos Send Mail (Enviar Email) e Open Home Page (Abrir Home Page) do Active Directory Users And Computers. Para mais informações, consulte “Atualização de contas de usuário e de grupo” mais adiante neste capítulo.

3. Toque ou clique na guia Address. Configure o endereço comercial ou residencial do usuário nas caixas oferecidas. Normalmente, insere-se o endereço comercial do usuário. Assim, pode-se encontrar localizações comerciais e endereços para correspondência de usuários de vários escritórios.

OBSERVAÇÃO É preciso levar em consideração questões relativas à privacidade antes de inserir endereços residenciais de usuários. Fale sobre isso com o departamento jurídico e de recursos humanos. Também pode ser desejável obter o consentimento do usuário antes de disponibilizar endereços residenciais.

4. Toque ou clique na guia Telephones. Insira os principais números de telefone que devem ser usados para entrar em contato com o usuário, como: residencial, pager, celular, fax e telefone IP.
5. Pode-se configurar outros números para cada um dos tipos de número de telefone. Toque ou clique no botão Other referente e depois insira os números adicionais na caixa de diálogo que aparece.
6. Toque ou clique na guia Organization. Conforme for adequado, insira o cargo, o departamento e a empresa do usuário.
7. Para especificar o gerente do usuário, toque ou clique em Change e selecione o gerente do usuário na caixa de diálogo Select User Or Contact. Ao especificar um gerente, o usuário aparecerá como um subordinado direto na conta do gerente.
8. Toque ou clique em Apply ou em OK para aplicar as alterações.

Também é possível definir as informações de contato usando o Active Directory Administrative Center (Centro Administrativo do Active Directory). Dê um toque duplo ou clique duas vezes no nome do usuário. Na caixa de diálogo Properties da conta, toque ou clique em Organization para exibir o painel Organization. Como mostra a Figura 9-2, esse painel permite configurar detalhes gerais, endereços, telefones e ainda detalhes da organização em um só lugar.

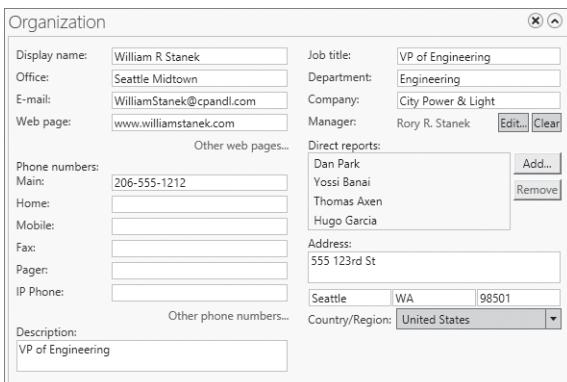


FIGURA 9-2 O painel Organization permite configurar detalhes gerais, endereços, telefones e detalhes da organização em um só lugar.

A caixa Web Page define a URL da home page do usuário na Internet ou na intranet da empresa. Caso o usuário tenha outras páginas da Web que você queira incluir, toque ou clique em Other Web Pages e depois insira os endereços das páginas da Web adicionais na caixa de diálogo Web Page Address (Others).

Sob Phone Numbers, insira os principais números de telefone que devem ser usados para entrar em contato com o usuário, como: residencial, pager, celular, fax e telefone IP. Pode-se configurar outros números para cada um dos tipos de número de telefone. Toque ou clique em Other Phone Numbers e depois insira os números de telefone adicionais na caixa de diálogo que aparece.

Se o usuário possuir um gerente definido, isso estará listado na caixa de texto Manager. Caso não tenha um gerente definido ou queira alterar o gerente, toque ou clique no botão Edit ao lado de Manager e determine o gerente do usuário na caixa de diálogo Select User Or Contact. Ao especificar um gerente, o usuário aparecerá como um subordinado direto na conta do gerente.

Se o usuário possui subordinados diretos, aparecerão listados sob Direct Reports. Para adicionar ou remover subordinados diretos, utilize os botões Add e Remove, respectivamente. Para adicionar um subordinado direto, toque ou clique em Add e especifique o subordinado direto na caixa de diálogo Select User Or Contact. Depois, toque ou clique em OK. Para remover um subordinado direto, toque ou clique no seu nome na lista e depois em Remove.

Como pesquisar usuários e grupos no Active Directory

O Active Directory facilita a busca por usuários e grupos no diretório, o que pode ser feito seguindo estas etapas:

1. Em Active Directory Users And Computers, pressione e mantenha pressionado ou clique com o botão direito do mouse no domínio ou no contêiner. Depois, toque ou clique em Find.
2. Na caixa de diálogo Find Users, Contacts, And Groups, a lista In exibe o domínio ou contêiner selecionado anteriormente. Se em vez disso você quiser pesquisar em todo o diretório, selecione Entire Directory ou toque ou clique em Browse para selecionar o domínio ou contêiner a ser pesquisado.
3. Na guia Users, Contacts, And Groups, insira o nome do usuário, contato ou grupo pelo qual quer procurar.
4. Toque ou clique em Find Now para iniciar a pesquisa. Se forem encontradas ocorrências, os resultados da pesquisa serão exibidos como mostra a Figura 9-3. Caso contrário, insira novos parâmetros de pesquisa e tente novamente.
5. Para gerenciar uma conta, pressione e mantenha pressionada ou clique com o botão direito do mouse na entrada correspondente. Se você pressionar e manter pressionada ou clicar com o botão direito do mouse em uma entrada de conta e selecionar Properties, abrirá a caixa de diálogo Properties da conta.

Você também pode pesquisar por usuários e grupos usando os recursos de pesquisa global e filtrada do Active Directory Administrative Center. Para mais informações, consulte "Active Directory Administrative Center e Windows PowerShell" no Capítulo 7, "Administração básica do Active Directory".

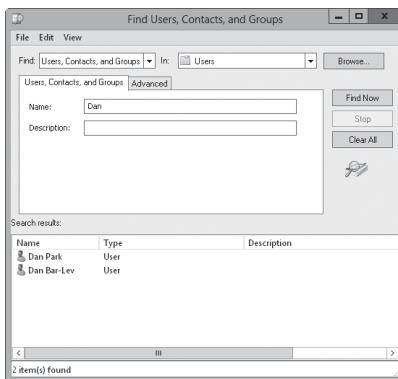


FIGURA 9-3 Pesquise por usuários no Active Directory e utilize os resultados para criar entradas do catálogo de endereços.

Configurações do ambiente do usuário

As contas de usuário também podem ter perfis, scripts de logon e pastas base associados a elas. Para realizar essas configurações adicionais, dê um toque duplo ou clique duas vezes em um nome de exibição no Active Directory Users And Computers e depois toque ou clique na guia Profile, mostrada na Figura 9-4. Na guia Profile pode-se definir as seguintes configurações:

- **Profile Path** O caminho para o perfil móvel do usuário. Os perfis fornecem as configurações de ambiente para usuários. Toda vez que um usuário faz logon em um computador, o perfil daquele usuário é usado para determinar configurações de área de trabalho e de Control Panel (Painel de Controle), disponibilidade de opções e aplicativos no menu, entre outras. A configuração do caminho do perfil será abordada mais tarde neste capítulo, em "Gerenciamento de perfis de usuário".
- **Logon Script** O caminho para o script de logon do usuário. Os scripts de logon são arquivos em lotes que são executados sempre que um usuário faz logon. Você pode utilizar os scripts de logon para definir comandos a serem executados toda vez que o usuário fizer logon. O Capítulo 4 "Automatização de tarefas administrativas, políticas e procedimentos" aborda em detalhes os scripts de logon.
- **Home Folder** O diretório que o usuário deve utilizar para armazenar arquivos. Aqui, você determina um diretório específico para os arquivos do usuário, como um caminho local no sistema do usuário ou em uma unidade de rede conectada. Se a pasta estiver disponível na rede, o usuário pode acessar a pasta de qualquer computador na rede, o que é uma grande vantagem.

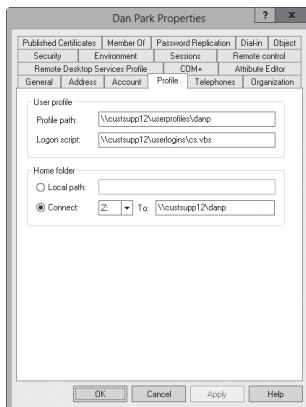


FIGURA 9-4 A guia Profile permite que você crie um perfil móvel de usuário e, desse modo, configure o ambiente na rede para um usuário.

Para definir as configurações do ambiente de um usuário no Active Directory Administrative Center, utilize as opções no painel Profile. Para realizar essas configurações, dê um toque duplo ou clique duas vezes em um nome de exibição no Active Directory Administrative Center e depois toque ou clique em Profile para exibir o painel Profile, mostrado na Figura 9-5.

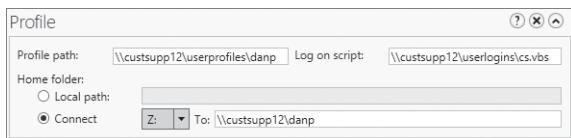


FIGURA 9-5 Realize as configurações de ambiente do usuário usando as opções no painel Profile.

Variáveis de ambiente do sistema

As variáveis de ambiente do sistema são bastante úteis na configuração do ambiente do usuário, especialmente quando você trabalha com scripts de logon. Utilizam-se as variáveis de ambiente para especificar informações de caminho que possam ser atribuídas dinamicamente. As variáveis de ambiente usadas com mais frequência são:

- **%SystemRoot%** A pasta base para o sistema operacional, como C:\Windows. Utilize-a com a guia Profile da caixa de diálogo Properties do usuário e com scripts de logon.
- **%UserName%** O nome da conta de usuário, como wrstanek. Utilize-a com a guia Profile da caixa de diálogo Properties do usuário e com scripts de logon.
- **%HomeDrive%** A letra da unidade da pasta base do usuário seguida por dois pontos, como em C:. Utilize-a com scripts de logon.

- **%HomePath%** O caminho completo para a pasta base do usuário na respectiva unidade base, como `\Users\{User}\Georgej`. Utilize-a com scripts de logon.
- **%Processor_Architecture%** A arquitetura do processador do computador do usuário, como `x86`, por exemplo. Utilize-a com scripts de logon.

A Figura 9-6 mostra como você pode utilizar as variáveis de ambiente ao criar contas de usuário. Observe que ao usar a variável `%UserName%`, você permite que o sistema determine a informação completa de caminho usuário por usuário. Se você utilizar essa técnica, pode usar a mesma informação de caminho para vários usuários e todos eles terão configurações exclusivas.

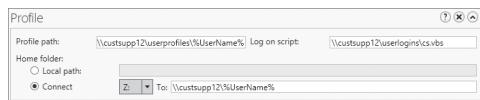


FIGURA 9-6 Ao usar a guia Profile, as variáveis de ambiente podem reduzir a quantidade de informação que você precisa digitar, especialmente ao criar uma conta baseada em outra.

Scripts de logon

Os scripts de logon definem comandos que devem ser executados sempre que um usuário fizer logon. Esses scripts podem ser usados para configurar hora do sistema, caminhos de unidade de rede, impressoras de rede, entre outros. Ainda que os scripts de logon possam ser usados para executar comandos uma só vez, eles não devem ser usados para configurar variáveis de ambiente. Qualquer configuração de ambiente usada por scripts não será mantida para os processos de usuário subsequentes. Além disso, não se deve usar scripts de logon para determinar os aplicativos que devem ser executados ao inicializar. Para determinar os aplicativos de inicialização, insira os atalhos apropriados na pasta Startup do usuário.

Normalmente, os scripts de logon contêm comandos do Microsoft Windows, mas eles podem ser qualquer um dos seguintes:

- Scripts do PowerShell com uma extensão `.ps1` ou outra extensão válida
- Arquivos do Windows Script Host com `.vbs`, `.js` ou outra extensão de script válida
- Arquivos em lotes com a extensão `.bat`
- Linhas de comando com a extensão `.cmd`
- Programas executáveis com a extensão `.exe`

Um ou vários usuários podem usar um só script de logon. Como administrador, você controla quais usuários utilizam quais scripts. Como indica o nome, os scripts de logon podem ser acessados quando os usuários fizerem logon nas suas contas. Para determinar um script de logon, siga as etapas:

1. Abra a caixa de diálogo Properties do usuário no Active Directory Users And Computers e toque ou clique na guia Profile.
2. Digite o caminho para o script de logon na caixa de texto Logon Script. Certifique-se de inserir o caminho completo para o script de logon, como em `\Zeta\User_Logon\Eng.vbs`.

OBSERVAÇÃO Existem outras técnicas para determinar os scripts de logon e logoff. Para mais detalhes, consulte “Gerenciamento de scripts de usuário e computador” no Capítulo 4.

Criar scripts de logon é mais simples do que você pensa, especialmente quando se utiliza a linguagem de comandos do Windows. Quase todos os comandos que podem ser digitados em um prompt de comando podem ser configurados para serem executados em um script de logon. As configurações de impressoras padrão e de caminhos de rede para usuários são as tarefas mais comuns a serem controladas por scripts de logon. Essas informações podem ser configuradas com o comando NET USE. Os comandos NET USE a seguir definem uma impressora de rede e uma unidade de rede:

```
net use lpt1: \\zeta\techmain  
net use G: \\gamma\corpfiles
```

Se esses comandos estivessem no script de logon do usuário, ele teria uma impressora de rede na LPT1 e uma unidade de rede no G. Pode-se criar conexões semelhantes em um script. Com o VBScript, é preciso inicializar as variáveis e objetos que você pretende usar e depois chamar os métodos apropriados do objeto *Network* para adicionar as conexões. Veja o exemplo a seguir:

```
Option Explicit  
Dim wNetwork, printerPath  
Set wNetwork = WScript.CreateObject("WScript.Network")  
  
printerPath = "\\zeta\techmain"  
wNetwork.AddWindowsPrinterConnection printerPath  
wNetwork.SetDefaultPrinter printerPath  
  
wNetwork.MapNetworkDrive "G:", "\\gamma\corpfiles"  
  
Set wNetwork = vbEmpty  
Set printerPath = vbEmpty
```

Aqui, utiliza-se o método *AddWindowsPrinterConnection* para adicionar uma conexão à impressora TechMain no Zeta e o método *SetDefaultPrinter* para definir a impressora como padrão para o usuário. Depois, você utiliza o método *MapNetworkDrive* para definir uma unidade de rede no G.

Atribuição de pastas base

O Windows Server 2012 permite que você atribua uma pasta base para cada conta de usuário, onde os usuários podem armazenar e recuperar os seus arquivos pessoais. Muitos aplicativos utilizam a pasta base como padrão para as operações File Open e File Save As, o que ajuda os usuários a encontrarem os recursos com facilidade. O prompt de comando também utiliza a pasta base como o diretório atual inicial.

As pastas base podem estar localizados na unidade de disco rígido local de um usuário ou em uma unidade de rede compartilhada. Em uma unidade local, a pasta está acessível em uma só estação de trabalho. Por outro lado, as unidades de rede compartilhadas podem ser acessadas de qualquer computador na rede, o que torna o ambiente do usuário mais versátil.

DICA Embora os usuários possam compartilhar pastas base, essa não é uma boa ideia. É desejável que cada usuário tenha uma pasta base exclusiva.

Não é necessário criar a pasta base do usuário com antecedência. O Active Directory Users And Computers cria a pasta automaticamente. Se ocorrer um problema na criação da pasta, o Active Directory Users And Computers instruirá você a criá-la manualmente.

Para especificar uma pasta base local, siga estas etapas:

1. Abra a caixa de diálogo Properties do usuário no Active Directory Users And Computers e toque ou clique na guia Profile.
2. Na seção Home Folder, selecione Local Path e insira o caminho para a pasta base na caixa de texto referente, como **C:\Home\%UserName%**.

Para especificar uma pasta base na rede, siga estas etapas:

1. Abra a caixa de diálogo Properties do usuário no Active Directory Users And Computers e toque ou clique na guia Profile.
2. Na seção Home Folder, selecione a opção Connect e depois selecione uma letra de unidade para a pasta base. Para ficar coerente, utilize a mesma letra de unidade para todos os usuários. Além disso, certifique-se de selecionar uma letra de unidade que não esteja em conflito com outras unidades físicas ou mapeadas configuradas no momento. Para evitar qualquer problema, você pode utilizar Z como a letra de unidade.
3. Insira o caminho completo para a pasta base utilizando a notação Universal Naming Convention (UNC, Convenção de Nomenclatura Universal), como **\\\Gammama\User_Dirs\%UserName%**. O nome do servidor é incluso no caminho da unidade para garantir que o usuário possa acessar a pasta em qualquer computador na rede.

OBSERVAÇÃO Se você não atribuir uma pasta base, o Windows Server 2012 utilizará a pasta base local padrão.

Configuração de opções e restrições de conta

O Windows Server 2012 oferece diversas formas de controle das contas de usuário e do acesso à rede. Você pode definir horário de logon, estações de trabalho permitidas para logon, privilégios de discagem, entre outras.

Gerenciamento do horário de logon

O Windows Server 2012 permite que você controle quando os usuários podem fazer logon na rede. Para isso, você configura um horário de logon válido para os usuários. As restrições de horário de logon podem ser utilizadas para reforçar a segurança e evitar quebras no sistema ou qualquer conduta maliciosa após o horário comercial regular.

Durante o horário de logon válido, os usuários trabalham normalmente, podendo fazer logon na rede e acessar os recursos de rede. Durante o horário de logon restrito, os usuários não podem trabalhar. Eles não poderão fazer logon na rede ou conectarem-se aos recursos de rede. Se os usuários estiverem logados quando o horário de

logon terminar, o que acontece depende da política de conta que você configurar para eles. Normalmente, acontecerá uma destas duas coisas:

- **Forcibly disconnected** Você pode configurar uma política que diz ao Windows Server para desconectar os usuários forçosamente ao terminar o horário de logon. Se essa política estiver configurada, os usuários remotos serão desconectados de todos os recursos de rede e do sistema ao término do horário.
- **Not disconnected** Os usuários não são desconectados da rede quando termina o horário do logon. Em vez disso, o Windows Server não permite que os usuários façam novas conexões de rede.

Configuração do horário de logon

Para configurar o horário de logon, siga as etapas:

1. Abra a caixa de diálogo Properties do usuário. Em Active Directory Users And Computers, toque ou clique na guia Account e depois em Logon Hours. Em Active Directory Administrative Center, toque ou clique em Log On Hours, no painel Account.
2. Agora, defina os horários de logon válido e inválido na caixa de diálogo Log On Hours, mostrada na Figura 9-7. Nessa caixa de diálogo, pode-se ativar ou desativar cada hora do dia e da noite.
 - As horas permitidas aparecem preenchidas por uma barra escura. Pense nelas como horas ativadas.
 - As horas proibidas aparecem vazias. Pense nelas como horas desativadas.

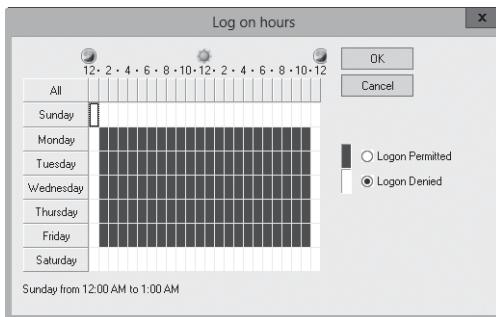


FIGURA 9-7 Configure o horário de logon para os usuários.

3. Para alterar a configuração de uma hora, toque ou clique nela e selecione Logon Permitted (Logon permitido) ou Logon Denied (Logon negado).

A Tabela 9-1 lista as opções da caixa de diálogo Log On Hours.

TABELA 9-1 Opções da caixa de diálogo Log On Hours

RECURSO	FUNÇÃO
All	Permite que você selecione todos os períodos de tempo
Botões Days of the week	Permitem que você selecione todas as horas de um determinado dia
Botões Hourly	Permitem que você selecione uma determinada hora para todos os dias da semana
Logon Permitted	Define o horário de logon permitido
Logon Denied	Define o horário de logon não permitido

DICA Ao definir horários de logon, você economizará bastante tempo a longo prazo se conceder aos usuários uma janela de tempo com restrições moderadas. Por exemplo: em vez de um horário explícito das 9h às 17h, é aconselhável permitir algumas horas antes ou depois do horário de trabalho normal. Assim, os que cedo madrugam têm acesso ao sistema e, também, permite-se que aqueles que ficam até mais tarde continuem trabalhando até que tenham encerrado o dia de trabalho.

Imposição do horário de logon

Para desconectar forçosamente os usuários no término do horário de logon, siga estas etapas:

1. Acesse a Group Policy Object (GPO) com a qual deseja trabalhar, como foi mostrado em "Gerenciamento de políticas de site, domínio e unidade organizacional" no Capítulo 4.
2. Abra o nó Security Options, descendo pela árvore de console. Expanda Computer Configuration, Windows Settings e Security Settings. Em Security Settings, expanda Local Policies e selecione Security Options.
3. Dê um toque duplo ou clique duas vezes em Network Security: Force Logoff When Logon Hours Expire. Será aberta uma caixa de diálogo Properties para a política.
4. Marque a caixa de seleção Define This Policy Setting e toque ou clique em Enabled. Isso ativa a restrição de política e impõe o horário de logon. Toque ou clique em OK.

Configuração de estações de trabalho com logon permitido

O Windows Server 2012 possui uma política formal que permite aos usuários fazerem logon nos sistemas localmente. Essa política controla se um usuário que se senta em frente ao computador é capaz de fazer logon. Por padrão, você pode usar qualquer conta de usuário válida, até mesmo uma conta Guest (Convidado), para fazer logon localmente em uma estação de trabalho.

Como se pode imaginar, permitir que usuários façam logon a qualquer estação de trabalho oferece um risco à segurança. A menos que você restrinja o uso das estações de trabalho, alguém que tenha acesso a um nome de usuário e senha pode usá-los para fazer logon em qualquer estação de trabalho no domínio. Ao definir uma lista de estações de trabalho permitidas, você fecha a abertura do seu domínio e diminui os riscos à segurança. Dessa forma, os hackers precisariam não apenas ter um nome de usuário e senha mas também localizar as estação de trabalho permitidas para a conta.

Para definir uma estação de trabalho de logon permitido para usuários de domínio, siga estas etapas:

1. Abra a caixa de diálogo Properties do usuário. Em Active Directory Users And Computers, toque ou clique na guia Account e depois em Log On To. Em Active Directory Administrative Center, toque ou clique em Log On To, no painel Account.
2. Na opção This User Can Log On To, selecione The Following Computers, como mostra a Figura 9-8.

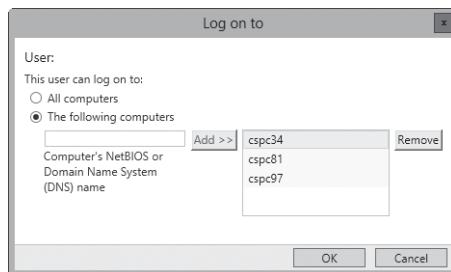


FIGURA 9-8 Para restringir o acesso a estações de trabalho, especifique as estações de trabalho de logon permitido.

3. Insira o nome de uma estação de trabalho permitida e clique ou toque em Add. Repita esse procedimento para especificar estações de trabalho adicionais.
4. Se cometer um engano, selecione a entrada incorreta e clique ou toque em Remove.

Configuração de privilégios de discagem e VPN

O Windows Server 2012 permite que você defina os privilégios de acesso remoto para contas na guia Dial-In (Discagem) da caixa de diálogo Properties do usuário. Essas configurações controlam o acesso para redes virtuais privadas (VPNs) e de discagem. Os privilégios de acesso remoto são controlados através da política de acesso à rede do Network Policy Server (NPS, Servidor de Políticas de Rede) por padrão. Esse é o método preferencial para o controle do acesso remoto. Você pode conceder ou negar explicitamente privilégios de discagem. Para isso, selecione Allow Access ou Deny Access. De qualquer maneira, antes que os usuários possam acessar a rede remotamente, é preciso seguir estas etapas:

1. No Server Manager, adicione a função Network Policy And Access Services (Serviços de Acesso e Política de Rede).
2. Para habilitar conexões de acesso remoto, acesse a GPO para o site, domínio ou OU com o qual deseja trabalhar, como foi explicado em "Gerenciamento de políticas de site, domínio e unidade organizacional", no Capítulo 4. No editor de políticas, expanda User Configuration, Administrative Templates e depois Network. Selecione Network Connections e configure as políticas Network Connections para o site, domínio ou OU adequadamente.

3. Configure o acesso remoto utilizando Routing And Remote Access (Roteamento e Acesso Remoto). Em Computer Management, expanda Services And Applications e depois selecione Routing And Remote Access. Configure o Routing And Remote Access da maneira apropriada.

MUNDO REAL Os binários necessários para a instalação de funções e recursos são chamados de payloads. No Windows Server 2012, os payloads para funções e recursos que estão sendo desinstalados são removidos utilizando-se o parâmetro *-Remove* do cmdlet Uninstall-WindowsFeature. É possível restaurar um payload removido utilizando o cmdlet Install-WindowsFeature. Por padrão, payloads são restaurados via Windows Update. Utilize o parâmetro *-Source* para restaurar um payload a partir de um ponto de montagem de um WIM. O exemplo a seguir mostra como restaurar os binários NPS e RRAS por meio do Windows Update:

```
install-windowsfeature -name npas-policy-server -includemanagementtools  
install-windowsfeature -name remoteaccess -includeallsubfeature  
-includemanagementtools
```

Após conceder a um usuário permissão para acessar a rede remotamente, siga estas etapas para configurar parâmetros de discagem adicionais na guia Dial-In da caixa de diálogo Properties do usuário (como mostra a Figura 9-9):

1. Se o usuário precisa discar a partir de um número de telefone específico, selecione Verify Caller-ID e insira o número de telefone do qual o usuário deve efetuar a discagem. O seu sistema telefônico deve suportar Caller ID (identificador de chamada) para que este recurso funcione.

OBSERVAÇÃO No Active Directory Administrative Center a guia Dial-In é acessada no painel Extensions. Toque ou clique em Extensions e depois toque ou clique em Dial-In.

2. Defina os parâmetros de retorno de chamada usando as seguintes opções:

- **No Callback** Permite ao usuário discar diretamente e permanecer conectado. O usuário paga pelas taxas de ligação de longa distância, se aplicáveis.
- **Set By Caller** Permite ao usuário discar diretamente. Depois, o servidor solicita ao usuário um número para retorno de chamada. Uma vez que o número tenha sido inserido, o usuário é desconectado e o servidor retorna para o usuário no número especificado para reestabelecer a conexão. A empresa paga pelas taxas de ligação de longa distância, se aplicáveis.
- **Always Callback To** Permite que você determine um número pré-definido para retorno de chamada por questões de segurança. Quando um usuário discar, o servidor retorna a chamada para o número pré-definido. A empresa paga pelas taxas de ligação de longa distância, se aplicáveis, e o risco de uma pessoa sem autorização acessar a rede é reduzido.

OBSERVAÇÃO Não é aconselhável atribuir números para retorno de chamada para usuários que discam usando o quadro de distribuição. O quadro de distribuição pode não permitir que o usuário conecte-se à rede corretamente. Também não é aconselhável utilizar números predefinidos para retorno de chamada com linhas com múltiplas ligações. As linhas com múltiplas ligações não terão o funcionamento adequado.

Se for necessário, você também pode atribuir endereços IP estáticos e rotas estáticas para conexões discadas. Para isso, selecione Assign Static IP Addresses e Apply Static Routes respectivamente.

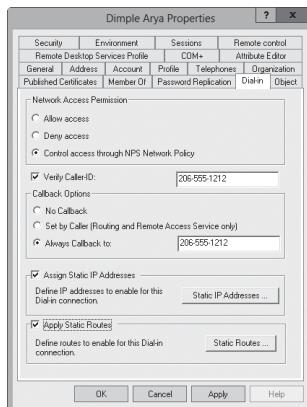


FIGURA 9-9 As configurações de discagem controlam o acesso remoto à rede.

Configuração das opções de segurança da conta

Para ajudá-lo a manter um ambiente de rede seguro e controlar como as contas de usuário são utilizadas, a guia/painel Account da caixa de diálogo Properties do usuário apresenta as seguintes opções:

- **User Must Change Password At Next Logon** Obriga o usuário a alterar a senha no seu próximo logon.
 - **User Cannot Change Password** Não permite que o usuário altere a senha da conta.
 - **Password Never Expires** Garante que a senha da conta nunca expire, o que substitui o período normal de data de validade da senha.
- ATENÇÃO** A seleção dessa opção cria um risco à segurança na rede. Ainda que você queira definir a opção Password Never Expires para contas de administrador, não é recomendável usá-la para contas de usuário normais.
- **Store Password Using Reversible Encryption** Salva a senha na forma de texto não criptografado.
 - **Account Is Disabled** Desabilita a conta, evitando que o usuário acesse a rede e faça logon (apenas para Active Directory Users And Computers).
 - **Smart Card Is Required For Interactive Logon** Exige que o usuário faça logon em uma estação de trabalho utilizando o smart card. O usuário não conseguirá fazer logon na estação de trabalho ao inserir o nome e a senha usando o teclado.

- **Account Is Sensitive And Cannot Be Delegated** Determina que as credenciais da conta de usuário não possam ser delegadas usando o Kerberos. Utilize essa opção para contas confidenciais que devem ser controladas com cuidado.
- **Use Kerberos DES Encryption Types For This Account** Determina que a conta de usuário utilize a criptografia Data Encryption Standard (DES).
- **This Account Supports Kerberos AES 128 Bit Encryption** Determina que a conta suporte criptografia Advanced Encryption Standard (AES) de 128 bits.
- **This Account Supports Kerberos AES 256 Bit Encryption** Determina que a conta suporte criptografia AES de 256 bits.
- **Do Not Require Kerberos Preauthentication** Determina que a conta de usuário não precise de pré-autenticação Kerberos para acessar os recursos de rede. A pré-autenticação faz parte do procedimento de segurança do Kerberos versão 5. A opção de fazer logon sem ela permite a autenticação de clientes utilizando uma versão anterior ou não padrão do Kerberos.

MUNDO REAL O AES é um de vários padrões de criptografia. Outro padrão é o Data Encryption Standard (DES). A maioria dos computadores com versões mais antigas do Windows suporta DES.

Já computadores com versões atuais do Windows suportam AES, que fornece uma criptografia mais segura em comparação ao DES. Enquanto as versões norte-americanas suportam tanto versões do AES de 128 bits quanto de 256 bits, as versões exportadas para uso fora dos Estados Unidos normalmente suportam apenas a criptografia de 128 bits.

Gerenciamento de perfis de usuário

Os perfis de usuário contêm definições para o ambiente de rede, como configurações da área de trabalho e opções de menu. Às vezes, a existência de problemas em um perfil pode impedir que um usuário consiga fazer logon. Por exemplo, se a configuração de vídeo definida no perfil não estiver disponível no sistema que está sendo utilizado, o usuário pode não conseguir fazer o logon corretamente. Na verdade, o usuário pode se deparar com uma tela em branco. Nesse caso, você poderia reiniciar o computador, entrar no modo Video Graphics Adapter (VGA) e redefinir a exibição manualmente. Entretanto, nem sempre as soluções para os problemas de perfil são simples assim, podendo ser necessário atualizar o próprio perfil.

O Windows Server 2012 oferece diversas formas de gerenciar os perfis de usuário:

- Determine caminhos de perfil no Active Directory Users And Computers ou no Active Directory Administrative Center.
- Copie, exclua ou altere o tipo de perfil local existente localmente, com o utilitário System no Control Panel.
- Defina políticas de sistema que evitem que os usuários manipulem certos aspectos do ambiente.

Perfis locais, móveis e obrigatórios

No Windows Server 2012, todo usuário possui um perfil. Os perfis controlam recursos de inicialização para a sessão do usuário, tipos de programa e aplicativos disponíveis, definições da área de trabalho e muito mais. Cada computador em que um usuário faz logon tem uma cópia do perfil do usuário. Como o perfil é armazenado no disco rígido do computador, os usuários que acessam diversos computadores possuem um perfil em cada um deles. Um outro computador da rede não pode acessar um perfil armazenado localmente (*local profile* ou perfil local). Como se pode imaginar, isso tem algumas desvantagens. Por exemplo: se um usuário fizesse logon em três estações de trabalho distintas, ele poderia ter três perfis bem diferentes (um para cada sistema). Como resultado, o usuário poderia se confundir em relação a quais recursos de rede estariam disponíveis em um determinado sistema.

Como trabalhar com o perfil móvel e com o perfil obrigatório

Para diminuir a confusão causada por vários perfis, cria-se um perfil que possa ser acessado a partir de outros computadores. Esse tipo de perfil é chamado *roaming profile* ou perfil móvel. Por padrão, com um perfil móvel um usuário pode acessar o mesmo perfil independentemente de qual computador estiver usando dentro do domínio. Os perfis móveis são baseados em servidor e podem ser armazenados em qualquer servidor com Windows. Quando um usuário com um perfil móvel faz o logon, o perfil é baixado e cria-se uma cópia local no computador do usuário. Quando o usuário faz o logoff, as alterações no perfil são atualizadas na cópia local e no servidor.

MUNDO REAL Se uma organização utiliza o Encrypting File System (EFS) para tornar mais seguros os acessos aos arquivos, o uso de perfis móveis é muito importante para aqueles usuários que fazem logon em vários computadores. Isso porque os certificados de criptografia são armazenados em perfis de usuário e são necessários para acessar e trabalhar com os arquivos criptografados do usuário. Se um usuário possui arquivos criptografados e não tem um perfil móvel, ele não poderá trabalhar com esses arquivos em outro computador a menos que utilize a mobilidade de credenciais com Digital ID Management Service (DIMS).

No papel de administrador, você pode controlar os perfis de usuário ou deixar que os usuários controlem os seus próprios perfis. Uma razão para que você mesmo os controle é garantir que todos os usuários possuam a mesma configuração de rede, o que diminui o número de problemas relacionados ao ambiente.

Os perfis controlados por administradores são chamados *mandatory profiles* ou perfis obrigatórios. Os usuários com perfis obrigatórios só podem realizar alterações temporárias no ambiente. As alterações que o usuário fizer no ambiente local não serão salvas e no próximo logon ele voltará ao perfil original. A ideia aqui é que se os usuários não puderem alterar permanentemente o ambiente na rede, não farão alterações que causem problemas. Uma grande desvantagem dos perfis obrigatórios é que o usuário só pode fazer logon se o perfil estiver acessível. Se por algum motivo o servidor que armazena o perfil estiver inacessível e se um perfil armazenado em cache não estiver acessível, o usuário não poderá fazer logon. Se o servidor estiver inacessível mas um perfil armazenado em cache estiver acessível, o usuário receberá uma mensagem de aviso e fará o logon no sistema local usando o perfil armazenado em cache do sistema.

MUNDO REAL Quando um usuário tem um perfil obrigatório, um perfil temporário (ou seja, que esteja logado como convidado) ou um perfil do sistema, o Windows 8 e o Windows Server 2012 bloqueiam a implantação de pacotes de aplicativos por padrão. Para permitir a implantação de aplicativos usando um desses perfis, pode-se habilitar a opção Allow Deployment Operation In Special Profiles nas políticas de Administrative Templates para Computer Configuration sob o caminho Windows Components\App Package Deployment.

Restrições de perfis móveis

Normalmente, os usuários podem acessar seus perfis móveis independentemente de qual computador estiverem usando dentro do domínio. O Windows 8 e o Windows Server 2012 permitem a modificação desse comportamento por meio da especificação de quais computadores um usuário pode usar para acessar os perfis móveis e as pastas redirecionadas. Para realizar essa ação, determina-se que certos computadores sejam computadores primários e configura-se a política de domínio para restringir aos computadores primários o download de perfis, de pastas redirecionadas ou de ambos.

Um *primary computer* (computador primário) é um computador designado especificamente como permitido para uso com dados redirecionados. Para isso, edita-se as propriedades avançadas de um usuário ou de um grupo no Active Directory, configurando-se a propriedade *msDS-PrimaryComputer* com o nome dos computadores permitidos. Depois, ativa-se a restrição do computador primário para perfis móveis. Para isso, habilite a política Download Roaming Profiles On Primary Computers Only que se encontra nas políticas de Administrative Templates para Computer Configuration sob o caminho System\User Profiles. Você também pode ativar a restrição do computador primário para pastas redirecionadas. Para isso, habilite a política Redirect Folders On Primary Computers Only que se encontra nas políticas de Administrative Templates para Computer Configuration sob o caminho System\Folder Redirection.

O objetivo dessas políticas é proteger dados pessoais e corporativos quando os usuários fizerem logon em computadores que não sejam os que eles utilizam regularmente. Ao não baixar e armazenar em cache nos computadores que o usuário não usa normalmente, a segurança dos dados é ampliada. Para definir o *msDS-PrimaryComputer* para um usuário ou grupo, siga estas etapas:

1. Em Active Directory Administrative Center, abra a caixa de diálogo Properties do usuário ou do grupo e toque ou clique em Extensions. Como opção, em Active Directory Users And Computers, certifique-se de que Advanced Features esteja selecionado no menu View e abra a caixa de diálogo Properties do usuário ou do grupo.
2. Na guia Attribute Editor, role a lista de atributos. Toque ou clique em *msDS-PrimaryComputer* e depois em Edit.
3. Na caixa de diálogo Multi-Valued String Editor, insira o nome do primeiro computador primário e depois clique em Add. Repita esse procedimento até que tenha adicionado todos os computadores primários. Toque ou clique em OK duas vezes.

Criação de perfis locais

Os perfis do usuário são mantidos na pasta padrão ou no local definido na caixa de texto Profile Path, na caixa de diálogo Properties do usuário. Para o Windows 7 ou versão posterior, o local padrão para perfis é %SystemDrive%\Users%\%UserName%. Uma parte fundamental do perfil é o arquivo Ntuser.dat nesse local, como em C:\Users\wrstanek\Ntuser.dat. Se você não alterar o local padrão, o usuário terá um perfil local.

Criação de perfis móveis

Os perfis móveis são armazenados em servidores do Windows. Quando o usuário faz logon em vários computadores e utiliza o EFS, é preciso um perfil móvel para garantir que os certificados necessários para ler e trabalhar com arquivos criptografados estejam disponíveis em computadores que não sejam o seu computador principal de trabalho.

Se você deseja que um usuário tenha um perfil móvel, você deve definir um local baseado em servidor para o diretório de perfil. Siga estas etapas:

1. Crie uma pasta compartilhada em um servidor com Windows Server e certifique-se de que o grupo Everyone tenha acesso ao menos a Change and Read.
2. Em Active Directory Users And Computers ou Active Directory Administrative Center, abra a caixa de diálogo Properties do usuário e acesse a guia/painel Profile. Digite o caminho para a pasta compartilhada na caixa de texto Profile Path. O caminho deve ter a forma `\server name\profile folder name\user name`. Um exemplo é `\Zeta\User_Profiles\Georgej`, onde Zeta é o nome do servidor, User_Profiles é a pasta compartilhada e Georgej é o nome do usuário.

O perfil móvel será armazenado no arquivo Ntuser.dat na pasta designada, como em `\Zeta\User_Profiles\Georgej\Ntuser.dat`.

OBSERVAÇÃO Normalmente, não é preciso criar a pasta de perfil. Ele é criado automaticamente quando o usuário faz logon e as permissões NTFS são definidas para que apenas o usuário tenha acesso. Pode-se selecionar várias contas de usuário para edição conjunta. Uma forma de fazê-lo é manter pressionada a tecla Shift ou a tecla Ctrl ao tocar ou clicar em nomes de usuário. Assim, quando você clicar com o botão direito do mouse em um dos usuários selecionados e depois tocar ou clicar em Properties, poderá editar as propriedades para todos eles. Certifique-se de utilizar %UserName% no caminho de perfil, como em `\Zeta\User_Profiles%\UserName%`.

3. Como etapa adicional, pode-se criar um perfil para o usuário ou copiar um perfil existente para a pasta de perfil do usuário. Se você não criar um perfil para o usuário, ele utilizará o perfil local padrão na próxima vez que fizer logon. Qualquer alteração que o usuário fizer neste perfil será salva quando ele fizer logoff. No seu próximo logon, o usuário terá um perfil pessoal.

Criação de perfis obrigatórios

Os perfis obrigatórios são armazenados em servidores com o Windows Server. Se deseja que um usuário tenha um perfil obrigatório, defina o perfil da seguinte maneira:

1. Siga as etapas 1 e 2 da seção anterior, "Criação de perfis móveis".
2. Crie um perfil obrigatório, renomeando o arquivo Ntuser.dat como `%UserName%\Ntuser.man`. No seu próximo logon, o usuário terá um perfil obrigatório.

OBSERVAÇÃO O arquivo Ntuser.dat contém as configurações de registro do usuário. Ao alterar a extensão do arquivo para Ntuser.man, você diz ao Windows Server que ele deve criar um perfil obrigatório.

Como usar o utilitário System para gerenciar perfis locais

Para gerenciar perfis locais, é preciso fazer logon no computador do usuário. Dessa forma, você poderá usar o utilitário System no Control Panel para gerenciar os perfis locais. Para visualizar as informações do perfil atual, toque ou clique em System And Security no Control Panel e depois toque ou clique em System. Na página System no Control Panel, toque ou clique em Advanced System Settings. Na caixa de diálogo System Properties, sob User Profiles, toque ou clique em Settings.

Como mostra a Figura 9-10, a caixa de diálogo User Profiles exibe informações sobre os perfis armazenados no sistema local. Utilize essas informações para ajudá-lo no gerenciamento dos perfis. A caixa de diálogo lista as seguintes informações:

- **Name** O nome do perfil local, que geralmente inclui o nome do domínio ou computador de origem e o nome da conta de usuário. Por exemplo: o nome ADATUM\Wrstanek indica que o perfil original é do domínio adatum e que a conta de usuário é wrstanek.

OBSERVAÇÃO Se você excluir uma conta mas não excluir o perfil associado a ela, pode ser que você veja uma entrada que diz Account Deleted ou Account Unknown. Não se preocupe. O perfil ainda está disponível para ser copiado se você precisar. Senão, você pode excluir o perfil aqui mesmo.

- **Size** O tamanho do perfil. Normalmente, quanto maior o perfil mais o ambiente foi personalizado pelo usuário.
- **Type** O tipo de perfil, que é local ou móvel.
- **Status** O status atual do perfil, como, por exemplo, se ele é de um cache local.
- **Modified** A data da última modificação no perfil.



FIGURA 9-10 A caixa de diálogo User Profiles permite que você gerencie os perfis locais existentes.

Criação manual de um perfil

Às vezes, você pode querer criar o perfil manualmente. Para isso, faça logon na conta de usuário, configure o ambiente e depois faça logoff. Como se pode imaginar, a criação de contas dessa forma demanda bastante tempo. Uma maneira melhor de abordar a criação de contas é criar uma conta de usuário base, configurar o ambiente dessa conta e depois usá-la como ponto de partida para outras contas.

Como copiar um perfil existente para uma nova conta de usuário

Se você tiver uma conta de usuário base ou uma conta de usuário que deseja utilizar de forma semelhante, você pode copiar um perfil existente para a nova conta de usuário. Siga estas etapas para usar o utilitário System Control Panel:

1. Inicie o utilitário System no Control Panel. Na página System, toque ou clique em Advanced System Settings. Na caixa de diálogo System Properties, sob User Profiles, toque ou clique em Settings.
2. Selecione o perfil que deseja copiar na lista Profiles Stored On This Computer. (Veja a Figura 9-10.)
3. Toque ou clique em Copy To para copiar o perfil para a nova conta de usuário. Na caixa Copy Profile To, mostrada na Figura 9-11, insira o caminho para o diretório do novo perfil de usuário. Se você estivesse criando o perfil para georgej, por exemplo, inseriria \\Zeta\User_Profiles\Georgej.

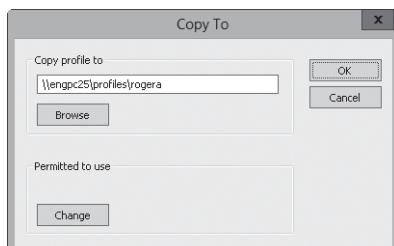


FIGURA 9-11 Na caixa de diálogo Copy To digite o local da pasta do perfil e atribua permissões de acesso ao usuário.

4. Agora, você precisa dar permissão ao usuário para acessar o perfil. Na área Permitted To Use, toque ou clique em Change. Use a caixa de diálogo Select User Or Group para conceder o acesso à nova conta de usuário.
5. Toque ou clique em OK para fechar a caixa de diálogo Copy To. O Windows copiará o perfil para o novo local.

DICA Se você souber o nome do usuário ou do grupo que deseja utilizar, pode inseri-lo diretamente na caixa Name, economizando tempo.

Como copiar ou restaurar um perfil

Quando se trabalha com grupos de trabalho em que cada computador é gerenciado separadamente, muitas vezes é preciso copiar um perfil local de usuário de um computador para outro. A cópia de um perfil permite que os usuários mantenham as configurações de ambiente ao usarem outros computadores. É claro que em um domínio do Windows Server pode-se utilizar um perfil móvel para criar um único perfil acessível de qualquer local dentro do domínio. O problema é que às vezes é preciso copiar um perfil local existente para substituir o perfil móvel de um usuário (quando o perfil móvel é corrompido), ou ainda copiar um perfil local existente para criar um perfil móvel em outro domínio.

Para copiar um perfil para um novo local, siga estas etapas:

1. Faça logon no computador do usuário e inicie o utilitário System Control Panel. Na página System, toque ou clique em Advanced System Settings. Na caixa de diálogo System Properties, sob User Profiles, toque ou clique em Settings.
2. Na lista Profiles Stored On This Computer, selecione o perfil que você deseja copiar.
3. Toque ou clique em Copy To para copiar o perfil para o novo local. Depois, insira o caminho para o novo diretório de perfil na caixa Copy Profile To. Se você estivesse criando um perfil para janew, por exemplo, poderia inserir **\\\Gammama\>User_Profiles\Janew**.
4. Para dar permissão ao usuário para acessar o perfil, clique no botão Change na área Permitted To Use e depois conceda o acesso à conta de usuário apropriada na caixa de diálogo Select User Or Group.
5. Ao terminar, toque ou clique em OK para fechar a caixa de diálogo Copy To. O Windows copiará o perfil para o novo local.

Como excluir um perfil local e atribuir um novo

Os perfis são acessados quando um usuário faz logon em um computador. O Windows Server utiliza perfis locais para todos os usuários que não tenham perfis móveis. Geralmente, os perfis locais também são usados se o perfil local possuir uma data de modificação mais recente que o perfil móvel do usuário. Sendo assim, às vezes é necessário excluir um perfil local de usuário. Se o perfil local de um usuário for corrompido, por exemplo, pode-se excluir esse perfil e atribuir um novo. Lembre-se que se você excluir um perfil local que não esteja armazenado em outro lugar no domínio, não será possível recuperar as configurações de ambiente originais do usuário.

Para excluir um perfil local de usuário, siga estas etapas:

1. Faça logon no computador do usuário utilizando uma conta com privilégios de administrador e depois inicie o utilitário System.
2. Toque ou clique em Advanced System Settings. Na caixa de diálogo System Properties, sob User Profiles, toque ou clique em Settings.
3. Selecione o perfil que você deseja excluir e toque ou clique em Delete. Quando for solicitado que você confirme se deseja excluir o perfil, toque ou clique em Yes.

OBSERVAÇÃO Não é possível excluir um perfil em uso. Se o usuário estiver logado no sistema local (ou seja, no computador do qual você está excluindo o perfil), o usuário precisa fazer logoff antes que seja possível excluir o perfil. Em alguns casos, o Windows Server sinaliza os perfis como estando em uso quando eles não estão. Isso normalmente é decorrência de uma alteração de ambiente do usuário que não foi aplicada corretamente. Para resolver, pode ser preciso reiniciar o computador.

Na próxima vez que o usuário fizer logon, o Windows Server procederá de uma das seguintes maneiras: ou o sistema operacional dará ao usuário o perfil local padrão para aquele sistema ou ele recuperará o perfil móvel do usuário armazenado em outro computador. Para impedir o uso de um desses perfis, é preciso atribuir um novo perfil ao usuário. Para tanto, siga um destes procedimentos:

- Copie um perfil existente para o diretório de perfil do usuário. A cópia de perfis foi abordada anteriormente neste capítulo em “Criação de perfis móveis”.
- Atualize as configurações de perfil para o usuário em Active Directory Users And Computers. A configuração do caminho de perfil foi abordada em “Criação de perfis móveis”.

Alteração do tipo de perfil

Com perfis móveis, o utilitário System permite que você altere o tipo de perfil no computador do usuário. Para isso, selecione o perfil e toque ou clique em Change Type. As opções nessa caixa de diálogo possibilitam as seguintes ações:

- **Change a roaming profile to a local profile** Se você quiser que o usuário sempre trabalhe com o perfil local neste computador, determine que o perfil é para uso local. Todas as alterações no perfil são feitas localmente e o perfil móvel original permanece intocado.
- **Change a local profile (that was defined originally as a roaming profile) to a roaming profile** O usuário utiliza o perfil móvel original para o próximo logon. O Windows Server trata o perfil como qualquer outro perfil móvel, ou seja, qualquer alteração feita no perfil local é copiada para o perfil móvel.

OBSERVAÇÃO Se essas opções não estiverem disponíveis, o perfil original do usuário está definido como local.

Atualização de contas de usuário e de grupo

O Active Directory Administrative Center e o Active Directory Users And Computers são as ferramentas utilizadas quando se quer atualizar uma conta de usuário ou de grupo do domínio. Caso queira atualizar uma conta de usuário ou de grupo local, utilize Local Users And Groups.

Ao trabalhar com o Active Directory, frequentemente você irá querer uma lista das contas para depois fazer algo com elas. Você pode, por exemplo, obter uma lista de todas as contas de usuário na organização e depois desabilitar as contas dos usuários que tenham saído da empresa. Uma forma de fazê-lo é através destas etapas:

1. Em Active Directory Users And Computers, pressione e mantenha pressionado ou clique com o botão direito do mouse no nome do domínio. Depois, toque ou clique em Find.

2. Na lista Find, selecione Custom Search. Isso atualiza a caixa de diálogo Find para que exiba a guia Custom Search.
3. Na lista In, selecione a área em que deseja procurar. Para procurar na empresa, selecione Entire Directory.
4. Na guia Custom Search, toque ou clique em Field para exibir um menu. Selecione User. Em seguida, selecione Logon Name (Pre–Windows 2000).

DICA Certifique-se de selecionar Logon Name (Pre–Windows 2000). Não utilize Logon Name. As contas de usuário não são obrigadas a ter um nome de logon mas sim a ter um nome de logon pre–Windows 2000.

5. Na lista Condition, selecione Present e toque ou clique em Add. Se for solicitado que você confirme, toque ou clique em Yes.
6. Toque ou clique em Find Now. O Active Directory Users And Computers compila uma lista de todos os usuários na área designada.
7. Agora você pode trabalhar com as contas uma a uma ou com várias contas ao mesmo tempo. Uma forma de selecionar vários elementos que não estejam em sequência é segurar e pressionar a tecla Ctrl e depois clicar em cada um dos objetos que você quer selecionar. Uma forma de selecionar uma série de elementos de uma só vez é segurar e pressionar a tecla Shift, clicar no primeiro objeto e depois no último.
8. Pressione e mantenha pressionada ou clique com o botão direito do mouse em uma conta de usuário e depois selecione uma ação no menu de atalhos que é exibido, como Disable Account, por exemplo.

DICA As ações que podem ser feitas em várias contas incluem: Add To Group (utilizada para adicionar as contas selecionadas a um grupo designado), Enable Account, Disable Account, Delete, Move e Send Mail. Escolha Properties para editar as propriedades de várias contas.

Utilize o mesmo procedimento para obter uma lista de computadores, grupos ou outros elementos do Active Directory. Com os computadores, faça uma pesquisa personalizada. Toque ou clique em Field, escolha Computer e depois selecione Computer Name (Pre–Windows 2000). Com os grupos, faça uma pesquisa personalizada. Toque ou clique em Field, escolha Group e depois selecione Group Name (Pre–Windows 2000).

A seção a seguir analisa outras técnicas que podem ser usadas para atualizar (renomear, copiar, excluir e habilitar) contas, bem como para alterar e redefinir senhas. Você também aprenderá como solucionar problemas de logon da conta.

Como renomear contas de usuário e de grupo

Ao renomear uma conta de usuário, você confere à conta um novo rótulo. Como foi discutido no Capítulo 8, “Como criar contas de usuário e de grupo”, os nomes de usuário têm o objetivo de tornar mais fáceis o gerenciamento e o uso das contas. Internamente, o Windows Server utiliza identificadores de segurança (SIDs) para identificar, acompanhar e controlar as contas, independentemente dos nomes de usuário. Os SIDs são identificadores exclusivos gerados quando as contas são criadas.

Como os SIDs são mapeados internamente para os nomes das contas, não é necessário alterar os privilégios ou permissões em contas renomeadas. O Windows Server mapeará os SIDs para os novos nomes de conta conforme for necessário.

Uma ocasião comum que leva à alteração do nome de uma conta de usuário é quando um usuário se casa e opta por mudar o seu sobrenome. Por exemplo: se Heidi Steen (heidis) casar-se, ela pode querer que o nome de usuário seja alterado para Heidi Jensen (heidij). Ao alterar o nome de usuário de heidis para heidij, todos os privilégios e permissões associadas refletirão a mudança de nome. Se você visualizar as permissões em um arquivo ao qual heidis tinha acesso, agora será heidij que terá acesso (e heidis não será mais listado).

Para simplificar o processo de renomeação de contas de usuário, o Active Directory Users And Computers oferece uma caixa de diálogo Rename User. Utilize-a para renomear uma conta de usuário e todos os componentes de nome relacionados. Como essa caixa de diálogo não está no Active Directory Administrative Center no momento, é preciso abrir a caixa de diálogo Properties e inserir as propriedades do novo nome em cada uma das caixas de texto referentes.

Para renomear uma conta, siga as etapas:

1. Localize a conta de usuário que você deseja renomear no Active Directory Users And Computers.
2. Pressione e mantenha pressionada ou clique com o botão direito do mouse na conta de usuário e toque ou clique em Rename. O Active Directory Users And Computers destaca o nome da conta para edição. Pressione a tecla Backspace ou Delete para apagar o nome existente. Em seguida, pressione a tecla Enter para abrir a caixa de diálogo Rename User, mostrada na Figura 9-12.

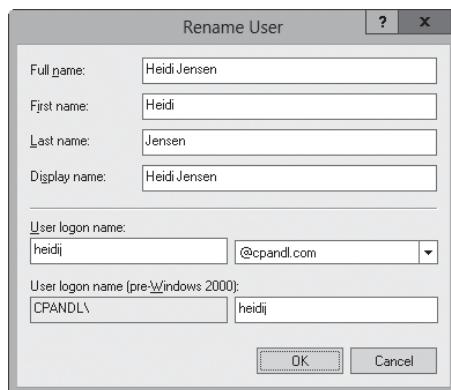


FIGURA 9-12 Renomeie completamente uma conta.

3. Faça as alterações necessárias nas informações do nome do usuário e toque ou clique em OK. Se o usuário estiver logado, você verá um prompt de aviso informando que o usuário deve fazer logoff e depois fazer logon novamente com o novo nome de logon da conta.
4. A conta é renomeada, mas o SID para permissões de acesso permanece o mesmo. Ainda pode ser necessário modificar outros dados para o usuário na caixa de diálogo Properties da conta, incluindo:

- **User Profile Path** Altere o Profile Path em Active Directory Users And Computers. Depois, renomeie a pasta correspondente no disco.
- **Logon Script Name** Se você utiliza scripts de logon individuais para cada usuário, altere o Logon Script Name no Active Directory Users And Computers. Depois, renomeie o script de logon no disco.
- **Home Directory** Altere o caminho da pasta base no Active Directory Users And Computers. Depois, renomeie a pasta correspondente no disco.

OBSERVAÇÃO Alterar informações de pasta e arquivo para uma conta quando o usuário estiver logado pode causar problemas. Atualize essas informações após o expediente ou peça para o usuário fazer logoff por alguns minutos e depois voltar a fazer logon. Normalmente, pode-se gravar um script de Windows simples que realize essas tarefas por você de forma automática.

Como copiar contas de usuário de domínio

Criar contas de usuário de domínio do zero pode ser uma tarefa entediante. Em vez de começar uma nova conta toda a vez, utilize uma conta existente como ponto de partida. Essa opção não se encontra no Active Directory Administrative Center no momento. Para fazê-lo no Active Directory Users And Computers, siga estas etapas:

1. Pressione e mantenha pressionada ou clique com o botão direito do mouse na conta que deseja copiar e depois toque ou clique em Copy. Isso abre a caixa de diálogo Copy Object–User.
2. Crie a conta da mesma maneira que criaria qualquer nova conta de usuário de domínio. Depois, atualize as propriedades da conta adequadamente.

Como é de se esperar, ao criar uma cópia de uma conta o Active Directory Users And Computers não retém todas as informações da conta existente. Em vez disso, o Active Directory Users And Computers tenta copiar apenas as informações de que você necessita e descartar informações que precisem ser atualizadas. As propriedades a seguir são retidas:

- Valores de cidade, Estado, CEP e país definidos na guia Address
- Departamento e empresa definidos na guia Organization
- Opções de conta definidas nas caixas Account Options na guia Account
- Horário de logon e estações de trabalho de logon permitido
- Data de validade da conta
- Associações a contas de grupo
- Configurações de perfil
- Privilégios de discagem

OBSERVAÇÃO Se você usou variáveis de ambiente para determinar as configurações de perfil na conta original, as variáveis de ambiente serão usadas para a cópia da conta também. Se a conta original utilizou a variável %UserName%, por exemplo, a cópia da conta também usará essa variável.

Importação e exportação de contas

O Windows Server 2012 conta com o utilitário de linha de comando Comma-Separated Value Directory Exchange (CSVDE) para a importação e exportação de objetos do Active Directory. Para operações de importação, o CSVDE utiliza um arquivo de texto delimitado por vírgula como a fonte de importação. Você pode executar o CSVDE com os seguintes parâmetros gerais:

- **-i** Ativa o modo de importação (em vez do modo de exportação, que é o padrão)
- **-f filename** Define a fonte para uma importação ou o arquivo de saída para uma exportação
- **-s servername** Define o servidor a ser usado para importar e exportar (em vez do controlador de domínio padrão para o domínio)
- **-v** Ativa o modo detalhado

Para operações de importação, a primeira linha do arquivo de origem define a lista de atributos Lightweight Directory Access Protocol (LDAP) para cada objeto definido. Cada linha sucessiva de dados fornece os detalhes para a importação de um objeto específico e deve conter exatamente os atributos listados. Veja o exemplo:

```
DN,objectClass,sAMAccoutName,sn,givenName,userPrincipalName  
"CN=William Stanek,OU=Eng,DC=cpand1,DC=com",user,williams,William,  
Stanek,williams@cpand1.com
```

Dada essa lista, se o arquivo de origem da importação se chamassem newusers.csv, você poderia importar o arquivo para o Active Directory inserindo o seguinte comando em um prompt de comando elevado:

```
csvde -i -f newusers.csv
```

Para operações de exportação, o CSVDE grava os objetos exportados para um arquivo de texto delimitado por vírgula. Você pode executar o CSVDE usando os parâmetros gerais listados anteriormente ou então usando parâmetros específicos para exportação, incluindo:

- **-d RootDN** Define o ponto de partida para a exportação, como `-d "OU=Sales,DC=domain,DC=local"`, por exemplo. O padrão é o contexto de nomenclatura atual.
- **-l list** Fornece uma lista de atributos delimitados por vírgula para saída.
- **-r Filter** Define o filtro de pesquisa LDAP, como em `-r "(objectClass=user)"`.
- **-m** Configura a saída para o Security Accounts Manager (SAM, Gerenciador de Contas de Segurança) e não para o Active Directory.

Para criar um arquivo de exportação para o contexto de nomenclatura atual (domínio padrão), você poderia inserir em um prompt de comando elevado o seguinte:

```
csvde -f newusers.csv
```

Porém, isso poderia resultar em um arquivo com uma quantidade enorme de dados exportados. Sendo assim, na maioria dos casos você deve especificar ao menos o RootDN e um filtro de objeto, como se vê a seguir:

```
csvde -f newusers.csv -d "OU=Service,DC=cpandl,DC=com" -r  
"(objectClass=user)"
```

Exclusão de contas de usuário e de grupo

A exclusão de uma conta remove-a permanentemente. Após excluir uma conta, é possível criar uma outra com o mesmo nome mas não obter as mesmas permissões. Isso acontece porque o SID da conta nova não será igual ao SID da conta antiga.

Já que a exclusão de contas internas pode ter efeitos vastos no domínio, o Windows Server 2012 não permite que você exclua contas internas de usuário e de grupo. Para remover outros tipos de contas, selecione a conta indesejada e pressione a tecla Delete ou então pressione e mantenha pressionada ou clique com o botão direito do mouse e selecione Delete. Quando for solicitado, toque ou clique em Yes.

Algumas formas de trabalhar com várias contas com o Active Directory Users And Computers são:

- Selecionar vários nomes de usuários para edição. Pressione e segure a tecla Ctrl e toque ou clique em cada conta que deseja selecionar.
- Selecionar um intervalo de nomes de usuário. Pressione e segure a tecla Shift, selecione o primeiro nome de conta e toque ou clique na última conta do intervalo.

OBSERVAÇÃO Quando você exclui uma conta de usuário, o Windows Server 2012 não exclui o perfil do usuário, os seus arquivos pessoais ou a pasta base. Se você deseja excluir esses arquivos e pastas, faça-o manualmente. Se essa for uma tarefa que você realiza rotineiramente, crie um script que cumpra os procedimentos necessários por você. Não se esqueça de fazer backup dos arquivos ou dados de que possa precisar antes de fazer isso.

Alteração e redefinição de senhas

No papel de administrador, muitas vezes você precisa alterar ou redefinir senhas de usuário. Isso acontece quando os usuários esquecem as senhas ou quando as senhas expiram.

Para alterar ou redefinir uma senha, siga estas etapas:

1. Abra o Active Directory Users And Computers, o Active Directory Administrative Center ou o Local Users And Groups (o que for apropriado).
2. Pressione e mantenha pressionada ou clique com o botão direito do mouse no nome da conta. Em seguida, toque ou clique em Reset Password (Redefinir Senha) ou em Set Password (Definir Senha).
3. Insira uma nova senha para o usuário e confirme. A senha deve satisfazer a política necessária de complexidade da senha definida para o computador ou para o domínio.
4. A opção User Must Change Password At Next Logon força o usuário a alterar a senha no seu próximo logon. Se não quer que o usuário tenha que alterar a senha, desmarque essa caixa de seleção.
5. A propriedade Account Lockout Status On This Domain Controller mostra se a conta está bloqueada ou desbloqueada. Se a conta estiver bloqueada, selecione Unlock The User's Account para desbloqueá-la. Toque ou clique em OK.

Como habilitar contas de usuário

As contas de usuário podem ser desabilitadas por diversos motivos. Se um usuário esquecer a sua senha e tentar adivinhá-la, ele pode exceder a política de conta para tentativas de logon erradas. Pode ser que outro administrador desabilite uma conta durante as férias de um usuário ou que a conta expire. As seções seguintes descrevem como proceder quando uma conta estiver desabilitada, bloqueada ou expirada.

Conta desabilitada

O Active Directory Users And Computers e o Active Directory Administrative Center sinalizam as contas desabilitadas com uma seta para baixo ao lado do ícone do usuário no modo de exibição principal. Quando uma conta estiver desabilitada, siga estas etapas para habilitá-la:

1. Abra o Active Directory Users And Computers, o Active Directory Administrative Center ou o Local Users And Groups (o que for apropriado).
2. Pressione e mantenha pressionado ou clique com o botão direito do mouse no nome da conta do usuário. Selecione a opção relativa à ferramenta que você está utilizando, Enable ou Enable Account.

DICA Para fazer uma pesquisa rápida por contas desabilitadas no domínio atual, insira `dsquery user -disabled` em um prompt de comando.

Pode-se selecionar várias contas de uma só vez e depois usar as opções no menu de atalhos para habilitá-las ou desabilitá-las. No Active Directory Users And Computers, use a opção Enable Account para habilitar todas as contas selecionadas ou use a opção Disable Account para desabilitá-las. No Active Directory Administrative Center, use a opção Enable All para habilitar as contas ou a opção Disable All para desabilitá-las.

Conta bloqueada

Quando uma conta estiver bloqueada, siga estas etapas para desbloqueá-la:

1. Abra o Active Directory Users And Computers, o Active Directory Administrative Center ou o Local Users And Groups (o que for apropriado).
2. Dê um toque duplo ou clique duas vezes no nome da conta e depois marque a caixa de seleção `Unlock Account`. No Active Directory Users And Computers essa caixa de seleção fica na guia `Account`.

No Active Directory Administrative Center é possível desbloquear várias contas de uma só vez. Basta selecionar as contas e depois usar a opção `Unlock All` no menu de atalho para desbloquear todas as contas.

OBSERVAÇÃO Se os usuários têm suas contas bloqueadas com frequência, pense em ajustar a política de conta para o domínio. Você pode aumentar o número de tentativas de logon erradas e reduzir a duração do contador associado. Para mais informações sobre a configuração de políticas de conta, consulte “Configuração das políticas de conta” no Capítulo 8.

Conta expirada

Apenas as contas de domínio possuem uma data de validade. (As contas de usuário locais não possuem datas de validade.) Quando uma conta de domínio expirar, siga estas etapas para modificar a data de validade:

1. Abra o Active Directory Users And Computers ou o Active Directory Administrative Center.
2. Dê um toque duplo ou clique duas vezes no nome da conta do usuário. Abra a guia ou o painel Account.
3. Sob Account Expires, selecione End Of e toque ou clique na seta para baixo na caixa de listagem referente. Se você estiver trabalhando com o Active Directory Users And Computers, será exibido um calendário usado para definir uma nova data de validade. Com o Active Directory Administrative Center, insira a data no formato que é apresentado.

Gerenciamento de várias contas de usuário

O Active Directory Users And Computers pode ser usado para modificar as propriedades de várias contas simultaneamente. Qualquer alteração feita nas configurações de propriedade será aplicada a todas as contas selecionadas. Se você pressionar e manter pressionadas ou clicar com o botão direito do mouse nas contas selecionadas, as seguintes opções estarão disponíveis:

- **Add To A Group** Exibe a caixa de diálogo Select Group, usada para designar os grupos dos quais os usuários selecionados devem ser membros
- **Disable Account** Desabilita todas as contas selecionadas
- **Enable Account** Habilita todas as contas selecionadas
- **Move** Move as contas selecionadas para um novo contêiner ou OU
- **Cut** Move as contas selecionadas para um novo contêiner ou OU quando você selecionar Paste posteriormente
- **Delete** Exclui as contas selecionadas
- **Properties** Permite que você configure um conjunto limitado de propriedades para várias contas

No Active Directory Administrative Center as opções são parecidas. Você verá: Add To Group, Disable All, Enable All, Unlock All, Move, Delete e Properties.

Na seção seguinte, analisaremos a opção Properties. Como mostra a Figura 9-13, a caixa de diálogo Properties For Multiple Items possui uma interface diferente da caixa de diálogo Properties padrão para usuários.



FIGURA 9-13 A caixa de diálogo Properties possui uma interface diferente quando se está trabalhando com várias contas.

OBSERVAÇÃO Os exemplos mostrados aqui e nas seções seguintes são para o Active Directory Users And Computers. As técnicas de gerenciamento são semelhantes para o Active Directory Administrative Center.

Você deve observar as seguintes diferenças:

- As caixas de nome da conta e de senha não estão disponíveis. Mesmo assim, é possível definir o nome de domínio Domain Name System (DNS) (sufixo para o user principal name [UPN]), horário de logon, restrições de computador, opções da conta, data de validade da conta e perfis.
- É preciso determinar com quais propriedades você deseja trabalhar e marcar as caixas de seleção dessas propriedades. Depois disso, o valor que você inserir na caixa de texto será aplicado a todas as contas selecionadas.

Configuração de perfis para várias contas

Para definir as informações de perfil para várias contas, utiliza-se as opções na guia Profile. Um dos melhores motivos para trabalhar com várias contas no Active Directory Users And Computers é poder definir todos os perfis do ambiente usando uma só interface. Para isso, você precisa da variável de ambiente %UserName%, que permite a atribuição de caminhos e nomes de arquivos baseados em nomes de usuário individuais. Por exemplo: se você atribuir o nome do script de logon como sendo %UserName%.cmd, o Windows substitui esse valor pelo nome do usuário. Isso é feito para cada um dos usuários que estão sendo gerenciados. Assim, seriam atribuídos aos usuários chamados bobs, janew e ericl os seguintes scripts de logon exclusivos: Bobs.cmd, Janew.cmd e Ericl.cmd.

A Figura 9-14 mostra um exemplo de configuração das informações de perfil do ambiente para várias contas. Repare que a variável %UserName% é usada para atribuir o caminho do perfil do usuário, o nome do script de logon do usuário e a pasta base.

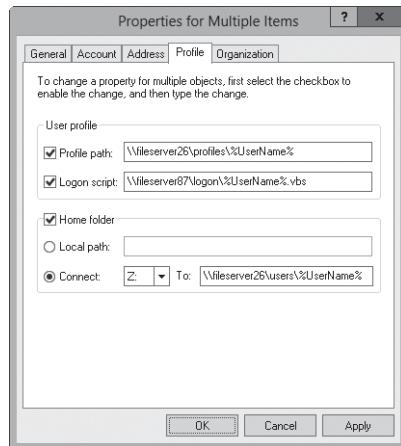


FIGURA 9-14 Use a variável de ambiente %UserName% para atribuir caminhos e nomes de arquivo baseados em nomes de usuário individuais.

Embora às vezes você possa querer que todos os usuários tenham nomes de arquivo e caminhos exclusivos, também há momentos em que você quer que os usuários compartilhem essas informações. Se você estiver utilizando perfis obrigatórios para usuários, por exemplo, pode atribuir um caminho de perfil de usuário específico em vez de um caminho criado dinamicamente.

Definição do horário de logon para várias contas

Se você selecionar várias contas de usuário no Active Directory Users And Computers, pode gerenciar o horário de logon coletivamente. Para fazê-lo, siga estas etapas:

1. Selecione as contas com as quais você deseja trabalhar no Active Directory Users And Computers.
2. Pressione e mantenha pressionadas ou clique com o botão direito do mouse nas contas selecionadas e depois toque ou clique em Properties. Na caixa de diálogo Properties, toque ou clique na guia Account.
3. Marque a caixa de seleção Logon Hours e toque ou clique em Logon Hours. Em seguida, defina o horário de logon, como foi discutido anteriormente neste capítulo em "Configuração do horário de logon".

OBSERVAÇÃO O Active Directory Users And Computers não informa o horário de logon anterior para as contas selecionadas e não avisa se os horários de logon para as contas forem diferentes.

Definição de estações de trabalho permitidas para logon para várias contas

As estações de trabalho permitidas para logon para várias contas são definidas na caixa de diálogo Logon Workstations. Para abrir essa caixa de diálogo, siga estas etapas:

1. Selecione as contas com as quais você deseja trabalhar no Active Directory Users And Computers.
2. Pressione e mantenha pressionadas ou clique com o botão direito do mouse nas contas selecionadas e depois toque ou clique em Properties. Na caixa de diálogo Properties, toque ou clique na guia Account.
3. Marque a caixa de seleção Computer Restrictions e toque ou clique em Log On To.
4. Se você deseja permitir que os usuários façam logon em qualquer estação de trabalho, selecione All Computers. Se você deseja especificar quais estações de trabalho os usuários têm permissão para usar, toque ou clique no botão The Following Computers e insira os nomes das estações de trabalho. Quando você tocar ou clicar em OK, as configurações serão aplicadas a todas as contas de usuário selecionadas.

Configuração de propriedades de logon, senha e data de validade para vários usuários

As contas de usuário possuem várias opções que controlam o logon, as senhas e a data de validade da conta. Isso tudo é configurado na guia Account da caixa de diálogo Properties. Ao trabalhar com várias contas, é preciso habilitar a opção com a qual deseja trabalhar. Marque a caixa de seleção correspondente na coluna mais à esquerda. Aqui, você tem duas opções:

- Habilitar a opção, marcando a sua caixa de seleção. Se você estiver trabalhando com a opção Password Never Expires, por exemplo, um sinalizador é configurado para que a senha dos usuários selecionados não expire quando você tocar ou clicar em OK.
- Não habilitar a opção, o que desmarca a opção efetivamente. Se você estiver trabalhando com a opção Account Is Disabled, por exemplo, as contas para os usuários selecionados serão habilitadas novamente quando você tocar ou clicar em OK.

Caso queira fixar uma data de validade para as contas selecionadas, primeiro selecione Account Expires e depois escolha o valor apropriado para a data de validade. A opção Never remove qualquer valor para a data de validade da conta que exista atualmente. Selecione a opção End Of para definir uma data de validade específica.

Solução de problemas de logon

A seção anterior elencou as formas como as contas podem ser desabilitadas. O Active Directory Users And Computers sinaliza as contas desabilitadas com um ícone de aviso vermelho ao lado do nome da conta. Para habilitar uma conta desabilitada, pressione e mantenha pressionada ou clique com o botão direito do mouse na conta no Active Directory Users And Computers e depois toque ou clique em Enable Account.

Você pode também pesquisar por usuários com contas desabilitadas em todo o diretório, digitando **dsquery user -disabled** em um prompt de comando. Para ha-

bilitar ou desabilitar uma conta na linha de comando, digite **dsmod user UserDN -disabled no**.

Se uma conta de usuário for bloqueada pela política Account Lockout, a conta não poderá ser usada para logon até que a duração do bloqueio tenha decorrido ou até que um administrador tenha desbloqueado a conta. Se a duração do bloqueio for indefinida, a única maneira da conta ser liberada é sendo desbloqueada pelo administrador, como foi discutido anteriormente.

O Windows Server 2012 pode registrar êxitos e falhas no logon através de auditoria. Se você habilitar a auditoria de falhas no logon da conta, essas falhas serão registradas no log de segurança no controlador de domínio de logon. As políticas de auditoria para um site, domínio ou OU são encontradas sob Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy de uma GPO.

Quando um usuário faz logon em uma rede utilizando a sua conta de usuário do domínio, as credenciais da conta são validadas por um controlador de domínio. Por padrão, os usuários podem fazer logon usando as suas contas de usuário do domínio mesmo se não houver conexão de rede ou se não houver um controlador de domínio disponível para autenticar o logon do usuário.

Para isso, o usuário deve ter realizado o logon no computador anteriormente e possuir credenciais válidas armazenadas em cache. Se o usuário não possuir credenciais armazenadas em cache no computador e se não houver conexão de rede ou controlador de domínio disponível, ele não conseguirá fazer logon. Por padrão, cada computador membro de um domínio pode armazenar em cache até 10 credenciais.

Quando um domínio está operando no modo nativo do Windows 2000 ou no modo Windows Server 2003, a autenticação também pode falhar se a hora do sistema no computador membro desviar da hora do sistema do controlador de domínio do logon em um valor maior do que aquele permitido pela política do Kerberos: Maximum Tolerance For Computer Clock Synchronization (Tolerância máxima para a sincronização do relógio do computador). A tolerância padrão é de cinco minutos para computadores membros.

Além dos motivos típicos para que uma conta esteja desabilitada, algumas configurações do sistema podem causar problemas de acesso. Para esse caso específico, procure pelos seguintes problemas:

- **O usuário recebe uma mensagem avisando que o usuário não pode efetuar logon interativamente** O direito do usuário de fazer logon localmente não está configurado para esse usuário e o usuário não é membro de um grupo que possua esse direito.

Pode ser que o usuário esteja tentando fazer logon em um servidor ou controlador de domínio. Nesse caso, lembre-se que o direito de fazer logon localmente aplica-se a todos os controladores de domínio no domínio. Senão, o direito se aplica apenas para uma única estação de trabalho.

Se o usuário deveria ter acesso ao sistema local, configure o direito de usuário Logon Locally, como foi mostrado em “Configuração das políticas de direitos do usuário” no Capítulo 8.

- **O usuário recebe uma mensagem avisando que o sistema não pode efetuar logon do usuário** Se você já verificou a senha e o nome da conta, confira o tipo de conta. Pode ser que o usuário esteja tentando acessar o domínio com uma conta local. Se o problema não for esse, o servidor de catálogo global pode estar indisponível, o que significa que apenas os usuários com privilégios de administrador podem fazer logon no domínio.

- **O usuário tem um perfil obrigatório e o computador que armazena o perfil está indisponível** Se o usuário tiver um perfil obrigatório, o computador que armazena esse perfil deve ser acessível durante o processo de logon. Caso o computador esteja desligado ou indisponível de alguma outra maneira, pode ser que os usuários com perfis obrigatórios não consigam fazer logon. Consulte “Perfis locais, móveis e obrigatórios” anteriormente neste capítulo.
- **O usuário recebe uma mensagem dizendo que a conta foi configurada para não permitir que o usuário efetue logon a partir desta estação de trabalho** O usuário está tentando acessar uma estação de trabalho que não está definida como uma estação de trabalho de logon permitido. Se o usuário deveria ter acesso a essa estação de trabalho, altere as informações da estação de trabalho de logon, como foi mostrado em “Definição de estações de trabalho permitida para logon para várias contas” anteriormente neste capítulo.

Visualização e configuração de permissões no Active Directory

Como já vimos em discussões anteriores, as contas de usuário, de grupo e de computador são representadas na forma de objetos no Active Directory. Os objetos do Active Directory possuem permissões de segurança padrão e avançada, que concedem ou negam o acesso aos objetos.

As permissões para os objetos do Active Directory não são tão simples quanto as outras. Tipos diferentes de objetos podem ter conjuntos de permissões específicas para esse determinado tipo de objeto. Podem também possuir permissões gerais que são específicas para o contêiner em que estão definidas.

Você pode visualizar e configurar as permissões de segurança padrão para objetos seguindo estas etapas:

1. Inicie o Active Directory Users And Computers e selecione Advanced Features no menu View para exibir as opções avançadas. Em seguida, pressione e mantenha pressionado ou clique com o botão direito do mouse no usuário, grupo ou conta de computador com o qual você deseja trabalhar e toque ou clique em Properties.
2. Na caixa de diálogo Properties, toque ou clique na guia Security. Como mostra a Figura 9-15, você verá uma lista de grupos e usuários aos quais foram atribuídas permissões no objeto que você selecionou anteriormente. Se as permissões estiverem esmaecidas, significa que elas foram herdadas de um objeto-pai.
3. Os usuários ou grupos com permissões de acesso estão listados na caixa Group Or User Names. Para alterar as permissões para esses usuários ou grupos, proceda da seguinte forma:
 - Selecione o usuário ou grupo que deseja alterar.
 - Conceda ou negue permissões de acesso na lista Permissions.
 - Se as permissões forem herdadas e não estiverem disponíveis para edição, selecione as permissões opostas para substituí-las.
4. Para definir permissões de acesso para usuários, computadores ou grupos adicionais, toque ou clique em Add. Na caixa de diálogo Select Users, Computers, Service Accounts, Or Groups, adicione usuários, computadores ou grupos.

- Na lista Group Or User Names selecione o usuário, computador ou grupo que deseja configurar. Toque ou clique em Check Names e depois toque ou clique em OK. Nas caixas de seleção na área Permissions, conceda ou negue permissões. Repita essa etapa para outros usuários, computadores ou grupos.

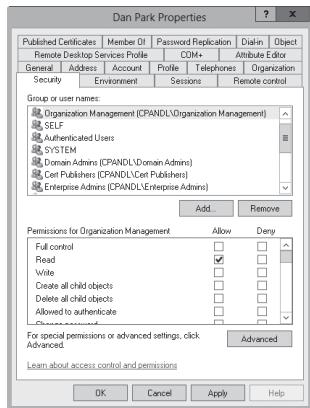


FIGURA 9-15 Visualize e configure permissões de objetos na guia Security.

- Toque ou clique em OK ao terminar.

ATENÇÃO Apenas administradores com uma compreensão sólida de Active Directory e permissões do Active Directory devem manipular permissões de objeto. A configuração incorreta de permissões de objeto pode causar problemas difíceis de rastrear.

Uma maneira de visualizar e configurar as permissões de segurança avançadas para objetos é seguindo estas etapas:

- Inicie o Active Directory Users And Computers e selecione Advanced Features no menu View para exibir as opções avançadas. Em seguida, pressione e mantenha pressionado ou clique com o botão direito do mouse no usuário, grupo ou conta de computador com o qual você deseja trabalhar e toque ou clique em Properties.
- Na caixa de diálogo Properties, toque ou clique na guia Security e depois em Advanced. Você deverá visualizar uma lista de entradas de permissão individual para o objeto selecionado anteriormente. As entradas de permissão herdadas são listadas como sendo herdadas de um determinado objeto-pai.
- Para visualizar e configurar as permissões individuais associadas a uma entrada de permissão, selecione a entrada e toque ou clique em Edit. É possível alterar permissões avançadas para o usuário ou grupo selecionado, concedendo ou negando permissões de acesso na lista Permissions. Se as permissões forem herdadas e não estiverem disponíveis para edição, selecione as permissões opostas para substituí-las.
- Toque ou clique em OK duas vezes ao terminar.

PARTE III

Administração de dados do Windows Server 2012

CAPÍTULO 10	Gerenciamento de sistemas de arquivos e unidades	383
CAPÍTULO 11	Configuração de volumes e matrizes RAID	417
CAPÍTULO 12	Compartilhamento de dados, segurança e auditoria	454
CAPÍTULO 13	Backup e recuperação de dados	516

CAPÍTULO 10

Gerenciamento de sistemas de arquivos e unidades

- Gerenciamento da função File Services **383**
- Como adicionar unidades de disco rígido **387**
- Como trabalhar com discos básicos, dinâmicos e virtuais **399**
- Utilização de discos e partições básicos **404**
- Compactação de unidades e dados **409**
- Criptografia de unidades e dados **411**

Uma unidade de disco rígido é o dispositivo de armazenamento mais comum utilizado em estações de trabalho e servidores em rede. Os usuários dependem de unidades de disco rígido para armazenar seus documentos de processamento de texto, suas planilhas e outros tipos de dados. As unidades estão organizadas em sistemas de arquivos que os usuários podem acessar local ou remotamente.

Os sistemas de arquivos locais estão instalados no computador do usuário e podem ser acessados sem conexões remotas de rede. A unidade C disponível na maioria dos servidores e estações de trabalho é um exemplo de um sistema de arquivos local. Você acessa a unidade C utilizando o caminho de arquivo C:\.

Por outro lado, se acessa os sistemas de arquivos remotos por meio de uma conexão de rede com um recurso remoto. Você pode se conectar a um sistema de arquivos remoto utilizando o recurso Map Network Drive no File Explorer (Explorador de Arquivos).

Onde quer que os recursos do disco estejam localizados, seu trabalho como administrador do sistema é gerenciá-los. As ferramentas e técnicas utilizadas para gerenciar sistemas de arquivos e unidades serão abordadas neste capítulo. O Capítulo 11, "Configuração de volumes e matrizes RAID", examina o gerenciamento de partições, os conjuntos de volumes e a tolerância a falhas.

Gerenciamento da função File Services

Um servidor de arquivos oferece uma localização central para armazenamento e compartilhamento de arquivos pela rede. Quando muitos usuários requerem acesso aos mesmos arquivos e dados de aplicativos, deve-se configurar servidores de arquivos no domínio. Em versões anteriores do sistema operacional Microsoft Windows Server, todos os servidores eram instalados com serviços de arquivos básicos.

Com o Windows Server 2012, você pode configurar especificamente um servidor para ser um servidor de arquivos adicionando a função File Services e configurando-a para utilizar os serviços de função apropriados.

A Tabela 10-1 apresenta uma visão geral dos serviços de função associados com a função File Services. Ao instalar a função File Services, talvez você também queira instalar os recursos opcionais a seguir, disponíveis por meio do Add Features Wizard:

- **Windows Server Backup** O utilitário de backup padrão incluído no Windows Server 2012.
- **Enhanced Storage** Dá suporte a funções adicionais disponibilizadas por dispositivos que suportem criptografia de hardware e armazenamento avançado. Os dispositivos de armazenamento avançado dão suporte ao Institute of Electrical and Electronic Engineers (IEEE) padrão 1667 para proporcionar segurança avançada, que pode incluir autenticação no nível de hardware do dispositivo de armazenamento.
- **Multipath I/O** Oferece suporte para o uso de vários caminhos de dados entre um servidor de arquivos e um dispositivo de armazenamento. Os servidores utilizam vários caminhos de I/O para redundância em caso de falha de um caminho e para melhorar o desempenho das transferências.

Se os binários para as ferramentas tiverem sido removidos, será preciso instalá-las especificando uma fonte, como abordado em “Princípios básicos do Server Manager e binários” no Capítulo 2, “Gerenciamento de servidores com o Windows Server 2012”.

TABELA 10-1 Serviços de função para servidores de arquivos

SERVIÇO DE FUNÇÃO	DESCRIÇÃO
BranchCache For Network Files	Habilita computadores em uma filial para armazenar em cache arquivos de pastas compartilhadas utilizados normalmente. Aproveita as técnicas de eliminação de duplicação de dados para otimizar as transferências de dados pelas wide area networks (WAN, redes de longa distância) para as filiais.
Data Deduplication	Utiliza o agrupamento e a compactação com tamanho variável de subarquivos para conseguir uma maior eficiência de armazenamento. Funciona segmentando os arquivos em partes de 32 KB a 128 KB, identificando partes duplicadas e substituindo as duplicatas por referências a uma única cópia. Os arquivos otimizados são armazenados como pontos de nova análise. Após a eliminação de duplicação, os arquivos no volume não serão mais armazenados como fluxos de dados, mas serão substituídos por stubs que apontam para blocos de dados de um repositório de partes comum.
DFS Namespaces	Permite agrupar pastas compartilhadas localizadas em diferentes servidores em um ou mais namespaces logicamente estruturados. Cada namespace aparece como uma única pasta compartilhada com uma série de subpastas. Contudo, a estrutura subjacente de um namespace pode vir de pastas compartilhadas em vários servidores em diferentes locais.

SERVIÇO DE FUNÇÃO	DESCRIÇÃO
DFS Replication	Permite sincronizar pastas em vários servidores por meio de conexões de rede locais ou de longa distância usando um mecanismo de replicação de vários mestres. O mecanismo de replicação utiliza o protocolo Remote Differential Compression (RDC) para sincronizar apenas as porções dos arquivos que tenham sido alteradas desde a última replicação. Você pode utilizar o DFS Replication em conjunto com o DFS Namespaces ou sozinho. Quando o domínio está em execução em um nível funcional de domínio Windows 2008 ou superior, os controladores de domínio utilizam o DFS Replication para proporcionar uma replicação mais robusta e granular da pasta SYSVOL.
File Server	Permite gerenciar compartilhamentos de arquivos que os usuários acessem pela rede.
File Server Resource Manager (FSRM)	Instala um pacote de ferramentas que os administradores podem utilizar para gerenciar melhor os dados armazenados em servidores. Utilizando o FSRM, os administradores podem gerar relatórios de armazenamento, configurar cotas e definir políticas de triagem de arquivos.
File Server VSS Agent Service	Permite que os utilitários de backup com reconhecimento de VSS criem cópias de sombra (instantâneos) consistentes de aplicativos que armazenem arquivos de dados no servidor de arquivos.
iSCSI Target Server	Transforma qualquer Windows Server em um dispositivo de armazenamento de blocos acessível pela rede que pode ser utilizado para testar aplicativos antes de implantar o armazenamento de storage area network (SAN, rede de área de armazenamento). Dá suporte ao armazenamento compartilhado em iniciadores iSCSI que não sejam do Windows e inicialização de rede/sem disco para servidores sem disco.
iSCSI Target Storage Provider	Dá suporte ao gerenciamento de discos virtuais e cópias de sombra (instantâneos) iSCSI a partir de um iniciador iSCSI.
Server for NFS	Oferece uma solução de compartilhamento de arquivos para empresas com um ambiente combinado de Windows e UNIX. Ao instalar o Services for Network File System (NFS), os usuários poderão transferir arquivos entre os sistemas operacionais Windows Server e UNIX utilizando o protocolo NFS.
Storage Services	Permite gerenciar o armazenamento, inclusive pools e espaços de armazenamento. Os pools de armazenamento agrupam discos a fim de que seja possível criar discos virtuais a partir da capacidade disponível. Cada disco virtual criado é um espaço de armazenamento.

Você pode adicionar a função File Services a um servidor seguindo estas etapas:

1. No Server Manager, toque ou clique em Manage e em Add Roles And Features, ou selecione Add Roles And Features no painel Quick Start. O Add Roles And Features Wizard será iniciado. Se o assistente exibir a página Before You Begin, leia o texto Welcome e toque ou clique em Next.

2. Na página Installation Type, a opção Role-Based Or Feature-Based Installation está selecionada por padrão. Toque ou clique em Next.
3. Na página Server Selection, você pode escolher instalar funções e recursos em servidores ou discos rígidos virtuais em execução. Selecione um servidor do grupo de servidores ou um do grupo de servidores no qual montar um virtual hard disk (VHD, disco rígido virtual). Se estiver adicionando funções e recursos a um VHD, toque ou clique em Browse e utilize a caixa de diálogo Browse For Virtual Hard Disks para localizá-lo. Quando estiver pronto para prosseguir, toque ou clique em Next.

OBSERVAÇÃO Somente servidores com o Windows Server 2012 e que tenham sido adicionados para gerenciamento no Server Manager serão listados.

4. Na página Server Roles, selecione File And Storage Services. Expanda o nó relacionado e selecione os serviços de função adicionais a instalar. Se recursos adicionais forem necessários para instalar uma função, você verá uma caixa de diálogo adicional. Toque ou clique em Add Features para fechar a caixa de diálogo e adicionar os recursos necessários para a instalação do servidor. Quando estiver pronto para prosseguir, toque ou clique em Next.

OBSERVAÇÃO Um resumo de cada serviço de função é fornecido na Tabela 10-1. Para permitir a interoperabilidade com o UNIX, certifique-se de adicionar Server For NFS.

5. Na página Features, selecione qualquer recurso que queira instalar. Se recursos adicionais forem necessários para instalar um recurso que selecionou, você verá uma caixa de diálogo adicional. Toque ou clique em Add Features para fechar a caixa de diálogo e adicionar os recursos necessários para a instalação do servidor. Quando estiver pronto para prosseguir, toque ou clique em Next.
6. Na página Confirm, toque ou clique no link Export Configuration Settings para gerar um relatório de instalação que possa ser exibido no Internet Explorer.
7. Se o servidor em que quer instalar os recursos e funções não tiver todos os arquivos binários de origem, o servidor os obterá via Windows Update por padrão ou de uma localização especificada na Group Policy.

MUNDO REAL Também é possível especificar um caminho alternativo para os arquivos de origem necessários. Para isso, clique no link Specify An Alternate Source Path, digite o caminho alternativo na caixa fornecida e toque ou clique em OK. Para compartilhamentos de rede, digite o caminho UNC para o compartilhamento, como \\CorpServer82\WinServer2012\. Para imagens montadas do Windows, digite o caminho do WIM prefixado com WIM: e incluindo o índice da imagem a utilizar, como WIM:\\CorpServer82\WinServer2012\install.wim:4.

8. Após examinar as opções de instalação e salvá-las conforme necessário, toque ou clique em Install para começar o processo de instalação. A página Installation Progress monitora o progresso da instalação. Se fechar o assistente, toque ou clique no ícone Notifications no Server Manager e no link fornecido para reabri-lo.
9. Quando o Setup terminar de instalar o servidor com os recursos e funções selecionados, a página Installation Progress será atualizada para refleti-lo. Revise os detalhes da instalação para garantir que todas as suas fases foram concluídas com sucesso.

Observe qualquer ação adicional que possa ser necessária para concluir a instalação, como a reinicialização do servidor ou realização de tarefas adicionais de instalação.

Se qualquer parte da instalação tiver falhado, observe a razão para essa falha. Examine as entradas do Server Manager para ver se há problemas de instalação e faça ações corretivas conforme apropriado.

Se a função File Services já estiver instalada em um servidor e você quiser instalar serviços adicionais para um servidor de arquivos, pode adicionar serviços de função no servidor utilizando um processo similar.

Como adicionar unidades de disco rígido

Antes de disponibilizar uma unidade de disco rígido para os usuários, é preciso configurá-la e considerar como será utilizada. Com o Windows Server 2012, pode-se configurar unidades de disco rígido de diversas formas. A técnica escolhida depende principalmente do tipo de dados com o qual se trabalhe e das necessidades do ambiente de rede. Para dados gerais de usuários armazenados em estações de trabalho, você talvez queira configurar unidades individuais como dispositivos de armazenamento autônomos. Nesse caso, os dados de usuários serão armazenados na unidade de disco rígido da estação de trabalho, onde poderão ser acessados e armazenados localmente.

Embora o armazenamento de dados em uma única unidade seja conveniente, não é a forma mais confiável de armazenamento. Para aprimorar a confiabilidade e o desempenho, você pode querer que um conjunto de unidades trabalhe simultaneamente. O Windows Server 2012 dá suporte a conjuntos e matrizes de unidades utilizando a tecnologia redundant array of independent disks (RAID), que é integrada ao sistema operacional.

Unidades físicas

Seja usando unidades individuais ou conjuntos de unidades, as unidades físicas são necessárias. As unidades físicas são os dispositivos de hardware reais utilizados para armazenar dados. A quantidade de dados que uma unidade pode armazenar depende de seu tamanho e de utilizar compactação. O Windows Server 2012 dá suporte às unidades de disco rígido Standard Format e Advanced Format. As unidades Standard Format têm 512 bytes por setor físico e também são chamadas de *512b drives* (unidades 512b). As unidades Advanced Format têm 4096 bytes por setor físico e também são chamadas de *512e drives* (unidades 512e). A 512e representa uma mudança significativa para o setor de unidades de disco rígido e admite unidades grandes com vários terabytes.

Os discos realizam atualizações de mídia física na granularidade do seu tamanho de setor físico. Os discos 512b trabalham com dados de 512 bytes por vez; os discos 512e trabalham com dados de 4096 bytes por vez. Em um prompt de comando elevado para administração, você pode utilizar Fsutil para determinar os bytes por setor físico digitando o seguinte:

```
Fsutil fsinfo ntfsinfo DriveDesignator
```

em que *DriveDesignator* designa a unidade a verificar, como:

```
Fsutil fsinfo sectorinfo c:
```

Ter um tamanho de setor físico maior é o que permite a capacidade da unidade saltar muito além dos limites da capacidade física anterior. Quando só há uma gravação de 512 bytes, os discos rígidos precisam realizar um trabalho adicional para completar a gravação do setor. Para terem o melhor desempenho, os aplicativos devem ser atualizados para ler e gravar dados adequadamente nesse novo nível de granularidade (4096 bytes).

O Windows Server 2012 dá suporte a muitas arquiteturas de interface de unidades, incluindo:

- Small Computer System Interface (SCSI)
- Parallel ATA (PATA), também conhecida como IDE
- Serial ATA (SATA)

Os termos SCSI, IDE e SATA designam o tipo de interface utilizado pelas unidades de disco rígido. Essa interface é utilizada para comunicação com um controlador de unidade. As unidades SCSI utilizam controladores SCSI, as unidades IDE utilizam controladores IDE e assim por diante.

A SCSI é uma das interfaces mais utilizadas normalmente e existem vários designs de barramento para SCSI e vários tipos de interface. A Parallel SCSI (também chamada de SPI), embora popular, está dando lugar à Serial Attached SCSI (SAS). A Internet SCSI (iSCSI) utiliza o modelo de arquitetura SCSI, mas usa o TCP/IP como o transporte, em vez da implementação física tradicional.

A SATA foi desenvolvida para substituir a IDE. As unidades SATA são cada vez mais populares como uma alternativa de baixo custo para a SCSI. A SATA II e a SATA III, as interfaces SATA mais comuns, foram desenvolvidas para operar a 3 gigabits por segundo e a 6 gigabits por segundo, respectivamente. A eSATA (também conhecida como SATA externa) é destinada a unidades conectadas externamente.

OBSERVAÇÃO O Windows Server 2012 apresenta melhorias para oferecer suporte aprimorado a unidades SATA. Essas melhorias reduzem as inconsistências de metadados e permitem que as unidades armazenem dados em cache com mais eficiência. O cache de disco aprimorado ajuda a proteger os dados armazenados em cache para o caso de uma perda inesperada de energia.

Ao instalar um novo servidor, deve-se dar atenção considerável à configuração das unidades. Comece escolhendo as unidades ou os sistemas de armazenamento que fornecam o nível apropriado de desempenho. Realmente, há uma diferença substancial na velocidade e no desempenho entre as várias especificações de unidade.

Não se deve apenas considerar a capacidade da unidade, mas também o seguinte:

- **Rotational speed** Uma medição de quão rápido o disco gira
- **Average seek time** Uma medição de quanto demora a busca entre faixas do disco durante operações sequenciais de input/output (I/O, entrada/saída)

Em termos gerais, ao comparar unidades de acordo com a mesma especificação, como Ultra640 SCSI ou SATA III, quanto a maior velocidade de rotação (medida em milhares de rotações por minuto) e o menor tempo de busca médio (medido em milisegundos, ou ms), melhor. Como exemplo, uma unidade com uma velocidade de rotação de 15.000 RPM dá 45-50% a mais de I/O por segundo do que a unidade média de 10.000 RPM, com todo o restante sendo igual. Uma unidade com um tempo de busca de 3,5 ms dá uma melhoria no tempo de resposta de 25-30% sobre uma unidade com um tempo de busca de 4,7 ms.

Outros fatores a considerar incluem o seguinte:

- **Maximum sustained data transfer rate** Uma medida de quantos dados a unidade pode transferir continuamente
- **Mean time to failure (MTTF)** Uma medida de quantas horas de operação se pode esperar obter da unidade antes de uma falha
- **Nonoperational temperatures** As medidas das temperaturas em que a unidade falha

A maioria das unidades de qualidade comparável tem taxas de transferência e MTTF similares. Por exemplo, se comparar unidades Ultra320 SCSI com velocidade de rotação de 15.000 RPM de diferentes fornecedores, provavelmente encontrará taxas de transferência e MTTF similares. Por exemplo, a Maxtor Atlas 15K II tem uma taxa de transferência de dados sustentada máxima de até 98 megabytes por segundo (MBps). A Seagate Cheetah 15K.4 tem uma taxa de transferência de dados sustentada máxima de até 96 MBps. Ambas têm um MTTF de 1,4 milhão de horas. As taxas de transferência também podem ser expressadas em gigabits por segundo (Gbps). Uma taxa de 1,5 Gbps é equivalente a uma taxa de dados de 187,5 MBps e 3,0 Gbps são equivalentes a 375 MBps. Algumas vezes você verá uma taxa de transferência externa máxima (por especificação com a qual a unidade é compatível) e uma taxa de transferência sustentada média. A taxa de transferência sustentada média é o fator mais importante. A unidade Seagate Barracuda 7200 SATA II tem uma velocidade de rotação de 7.200 RPM e uma taxa de transferência sustentada média de 58 MBps. Com um tempo de busca médio de 8,5 ms e um MTTF de 1 milhão de horas, a unidade tem desempenho comparável a outras unidades SATA II de 7.200 RPM. Contudo, a maioria das unidades Ultra320 SCSI tem desempenho melhor e também são melhores em operações de leitura/gravação com vários usuários.

OBSERVAÇÃO Não confunda MBps e Mbps. MBps são megabytes por segundo. Mbps são megabits por segundo. Visto que há 8 bits em um byte, uma taxa de transferência de 100 MBps é equivalente a uma taxa de transferência de 800 Mbps. Com a SATA, a taxa de transferência de dados máxima geralmente está em torno de 150 MBps ou 300 MBps. Com a PATA/IDE, a taxa de transferência de dados máxima geralmente está em torno de 100 MBps.

A temperatura é outro fator importante a considerar quando se seleciona uma unidade, porém, é um fator que poucos administradores levam em conta. Normalmente, quanto mais rápido uma unidade gira, mais quente se torna. Nem sempre esse é o caso, mas é certamente algo a ser considerado ao fazer sua escolha. Por exemplo, as unidades de 15K tendem a se tornar quentes e é preciso certificar-se de regular cuidadosamente a temperatura. A Maxtor Atlas 15K II e a Seagate Cheetah 15K.4 podem se tornar não operacionais em temperaturas de 70 graus centígrados ou mais (como a maioria das outras unidades).

O Windows Server 2012 adiciona o suporte para unidades de disco com criptografia de hardware (chamadas de unidades de disco rígido criptografadas). As unidades de disco rígido criptografadas têm processadores internos que deslocam as atividades de criptografia-descriptografia do sistema operacional para o hardware, liberando recursos do sistema operacional. O Windows Server 2012 utilizará a criptografia de hardware com o BitLocker, quando disponível. Outros recursos de segurança disponíveis no Windows Server 2012 incluem Secured Boot e Network Unlock. O recurso Secured Boot proporciona integridade de inicialização ao validar configurações

de Boot Configuration Data (BCD, Dados de Configuração da Inicialização) de acordo com as configurações de perfil de validação Trusted Platform Module (TPM). O recurso Network Unlock pode ser utilizado para desbloquear automaticamente a unidade do sistema operacional em computadores que pertençam a domínios. Para mais informações sobre TPM, BitLocker, Secured Boot, Network Unlock e unidades criptografadas, consulte “Using TPM and BitLocker Drive Encryption” no Capítulo 11 do *Windows 8 Administration Pocket Consultant* (Microsoft Press, 2012).

Preparação de uma unidade física para uso

Após instalar uma unidade, é preciso configurá-la para o uso. Configura-se a unidade particionando-a e criando sistemas de arquivos nas partições conforme necessário. Uma partição é uma seção de uma unidade física que funciona como se fosse uma unidade separada. Depois de criar uma partição, pode-se criar um sistema de arquivos nela.

Dois estilos de partição são utilizados para discos: master boot record (MBR, registro mestre de inicialização) e GUID partition table (GPT, tabela de partição GUID). O MBR contém uma tabela de partição que descreve onde as partições estão localizadas no disco. Com esse estilo de partição, o primeiro setor em um disco rígido contém o registro mestre de inicialização e um arquivo de código binário chamado de *master boot code*, que é utilizado para inicializar o sistema. Esse setor não é particionado e está oculto da visualização para proteger o sistema.

Com o estilo de particionamento MBR, os discos tradicionalmente suportam volumes de até 4 terabytes (TB) e possuem dois tipos de partições: primária e estendida. Cada unidade MBR pode ter até quatro partições primárias ou três partições primárias e uma partição estendida. As partições primárias são seções da unidade que podem ser acessadas diretamente para armazenamento de arquivos. Você torna partição primária acessível para os usuários criando um sistema de arquivos nela. Embora se possa acessar diretamente as partições primárias, não se pode acessar diretamente as partições estendidas. Ao invés disso, pode-se configurar as partições estendidas com uma ou mais unidades lógicas que serão utilizadas para armazenar arquivos. A capacidade de dividir partições estendidas em unidades lógicas permite dividir uma unidade física em mais que quatro seções.

A GPT foi originalmente desenvolvida para computadores de alto desempenho baseados em Itanium. A GPT é recomendada para discos maiores que 2 TB em sistemas x86 e x64 ou em qualquer disco utilizado em computadores baseados em Itanium. A diferença-chave entre o estilo de partição GPT e o estilo de partição MBR tem a ver com como os dados da partição são armazenados. Com a GPT, os dados cruciais da partição são armazenados em partições individuais e tabelas de partição primárias e de backup redundantes são utilizadas para uma integridade estrutural melhorada. Além disso, os discos GPT suportam volumes de até 18 exabytes e até 128 partições. Embora os estilos de particionamento GPT e MBR tenham diferenças subjacentes, a maioria das tarefas relacionadas ao disco são executadas da mesma forma.

Além de um estilo de partição, as unidades físicas têm um tipo de disco, que é básico ou dinâmico, conforme abordado posteriormente neste capítulo sob o título “Como trabalhar com discos básicos, dinâmicos e virtuais”. Após definir o estilo de partição e o tipo de disco para uma unidade física, você poderá formatar áreas livres da unidade para estabelecer partições lógicas. A formatação criará um sistema de arquivos na partição. O Windows Server 2012 dá suporte aos seguintes sistemas de arquivos:

- FAT
- FAT32
- exFAT
- NTFS
- ReFS

Com o FAT, o número de bits utilizado com a tabela de alocação de arquivos determina a variante com a qual se trabalha e o tamanho máximo do volume. O FAT16, também conhecido simplesmente como FAT, define suas tabelas de alocação de arquivos utilizando 16 bits. Os volumes que tenham 4 gigabytes (GB) ou menos de tamanho são formatados com o FAT16.

O FAT32 define suas tabelas de alocação de arquivos utilizando 32 bits e pode-se criar volumes FAT32 que tenham 32 GB ou menos utilizando as ferramentas de formatação do Windows. Embora o Windows possa montar volumes FAT32 maiores criados com ferramentas de terceiros, deve-se utilizar o NTFS para volumes maiores que 32 GB.

O extended FAT (estendido) é uma versão aprimorada do FAT. Tecnicamente, o exFAT podia ter sido chamado de FAT64 (e algumas pessoas o chamam assim). O exFAT define suas tabelas de alocação de arquivos utilizando 64 bits. Isso permite que o exFAT ultrapasse o limite de tamanho do arquivo de 4 GB e o limite de tamanho do volume de 32 GB dos sistemas de arquivos FAT32. O formato exFAT suporta tamanhos de unidade de alocação de até 128 KB para volumes de até 256 TB.

Os volumes NTFS têm uma estrutura e um conjunto de recursos muito diferentes dos volumes FAT. A primeira área do volume é o setor de inicialização, que armazena as informações sobre o layout do disco e um programa de inicialização é executado na inicialização e inicializa o sistema operacional. Em vez de uma tabela de alocação de arquivos, o NTFS utiliza um banco de dados relacional para armazenar informações sobre os arquivos. Esse banco de dados é chamado de master file table (MFT, tabela mestra de arquivos).

A MFT armazena um registro de arquivo de cada arquivo e pasta no volume, informações pertinentes ao volume e detalhes sobre a própria MFT. O NTFS oferece muitas opções avançadas, incluindo suporte para o Encrypting File System, a compactação e a opção de configurar triagens de arquivos e relatórios de armazenamento. A triagem de arquivos e os relatórios de armazenamento estão disponíveis quando se adiciona o serviço de função File Server Resource Manager em um servidor como parte da função File Services.

O Resilient File System pode ser considerado a próxima geração do NTFS. Sendo assim, o ReFS continua compatível com recursos essenciais do NTFS, ao passo que suprime recursos que não sejam fundamentais para focar inflexivelmente na confiabilidade. Isso significa que cotas de disco, Encrypting File System, compactação, triagem de arquivos e relatórios de armazenamento não estão disponíveis, mas que recursos de confiabilidade integrados foram adicionados.

Um dos maiores recursos de confiabilidade no ReFS é um scanner de integridade dos dados, também chamado de *data scrubber* (depurador de dados). O scrubber proporciona identificação, isolamento e correção de erros proativos. Se o scrubber detectar dados corrompidos, um processo de reparo será utilizado para localizar a área corrompida e realizar uma correção online automática. Por meio de um processo de salvamento online automático, as áreas corrompidas que não possam ser reparadas, como as devido a setores defeituosos no disco físico, serão removidas do volume.

dinâmico, a fim de que não possam afetar negativamente os dados sãos. Por causa dos processos de scrubber e salvamento automatizados, não há necessidade de um recurso Check Disk (verificação de disco) ao utilizar o ReFS (e não existe o utilitário Check Disk para o ReFS).

OBSERVAÇÃO Ao trabalhar com File And Storage Services, você pode agrupar discos físicos disponíveis em pools de armazenamento de modo que possa criar discos virtuais a partir da capacidade disponível. Cada disco virtual criado é um espaço de armazenamento. Visto que somente o NTFS dá suporte a espaços de armazenamento, lembre-se de que está formatando volumes em servidores de arquivos. Para mais informações sobre espaços de armazenamento, consulte “Gerenciamento de armazenamento baseado em padrões” no Capítulo 11.

Utilização do Disk Management

Utiliza-se o snap-in Disk Management do Microsoft Management Console (MMC, Console de Gerenciamento Microsoft) para configurar unidades. O Disk Management facilita o trabalho com as unidades internas e externas em um sistema local ou remoto. O Disk Management está incluído como parte do console Computer Management. Você também pode adicioná-lo a MMCs personalizados. Em Computer Management, pode-se acessar o Disk Management expandindo o nó Storage e selecionando Disk Management.

O Disk Management tem três modos de exibição: Disk List, Graphical View e Volume List. Com sistemas remotos, você está limitado às tarefas que pode realizar com o Disk Management. As tarefas de gerenciamento remoto que podem ser realizadas incluem visualizar detalhes da unidade, alterar as letras e os caminhos das unidades e converter tipos de disco. Com unidades de mídia removível, pode-se também ejetar a mídia remotamente. Para executar uma manipulação mais avançada de unidades remotas, usa-se o utilitário de linha de comando DiskPart.

OBSERVAÇÃO Antes de trabalhar com o Disk Management, você deve saber várias coisas. Se criar uma partição, mas não a formatar, ela será rotulada como Free Space. Se não tiver atribuído uma porção do disco a uma partição, essa seção do disco será rotulada como Unallocated.

Na Figura 10-1, o modo de exibição Volume List está no canto superior direito e Graphical View é utilizado no canto inferior direito. Essa é a configuração padrão. Pode-se alterar a visualização do painel superior ou inferior como se segue:

- Para alterar a visualização superior, selecione View, escolha Top e selecione o modo de exibição que quer utilizar.
- Para alterar a visualização inferior, selecione View, escolha Bottom e selecione o modo de exibição que quer utilizar.
- Para ocultar a visualização inferior, selecione View, escolha Bottom e selecione Hidden.

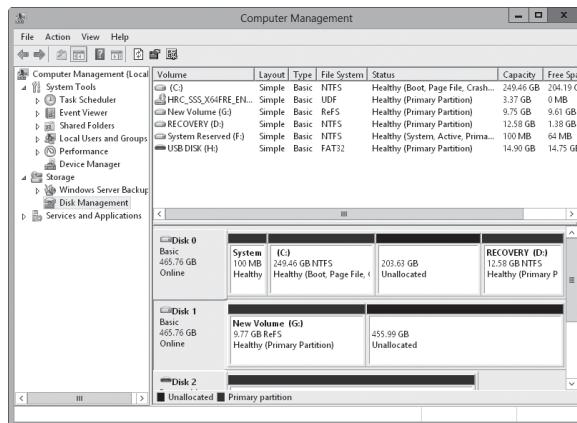


FIGURA 10-1 No Disk Management, a visualização superior apresenta um resumo detalhado de todas as unidades no computador e a visualização inferior apresenta uma visão geral das mesmas unidades, por padrão.

O Windows Server 2012 dá suporte a quatro tipos de configurações de disco:

- **Basic** O tipo de disco fixo padrão utilizado em versões anteriores do Windows. Os discos básicos são divididos em partições e são o tipo de disco original dos primeiros sistemas operacionais Windows.
- **Dynamic** Um tipo de disco fixo avançado para o Windows Server 2012 que pode ser atualizado sem reiniciar o sistema (na maioria dos casos). Os discos dinâmicos são divididos em volumes.
- **Removable** O tipo de disco padrão associado a dispositivos de armazenamento removíveis.
- **Virtual** O tipo de disco virtual hard disk (VHD) associado com a virtualização. Os computadores podem utilizar VHDS exatamente como usam discos fixos comuns e podem até mesmo ser configurados para inicializar a partir de um deles.

Na janela do Disk Management, pode-se obter informações detalhadas sobre uma seção da unidade pressionando e segurando ou clicando com o botão direito do mouse nela e selecionando Properties. Ao fazê-lo, você verá uma caixa de diálogo. A Figura 10-2 mostra as caixas de diálogo de dois discos fixos. O da esquerda utiliza NTFS. O da direita utiliza ReFS. Ambos os discos têm guias adicionais baseadas na configuração do servidor.

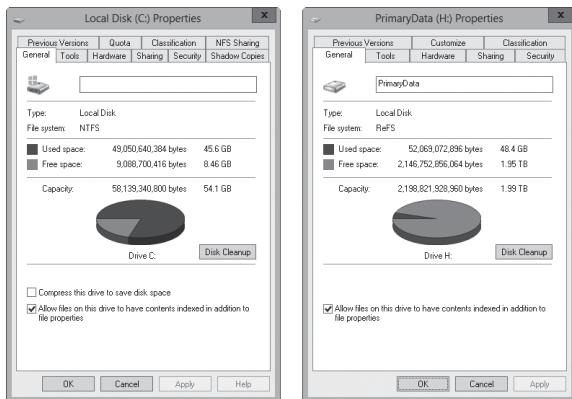


FIGURA 10-2 A guia General da caixa de diálogo Properties apresenta informações detalhadas sobre uma unidade.

Se tiver configurado o gerenciamento remoto por meio do Server Manager e de MMCs, como abordado no Capítulo 2, poderá utilizar o Disk Management para configurar os discos em computadores remotos e trabalhar com eles. Contudo, lembre-se de que suas opções são ligeiramente diferentes de quando está trabalhando com discos em um computador local. As tarefas que pode realizar incluem o seguinte:

- Visualização limitada de propriedades do disco, mas não de propriedades do volume. Quando estiver visualizando as propriedades do disco, só verá as guias General e Volumes. Não será possível ver as propriedades do volume.
- Alteração de letras das unidades e dos caminhos de montagem.
- Formatação, redução e expansão de volumes. Com volumes espelhados, estendidos e distribuídos, pode-se adicionar e configurar opções relacionadas.
- Exclusão de volumes (exceto volumes do sistema e de inicialização).
- Criação, anexação e desanexação de VHDS. Ao criar e anexar VHDS, é preciso digitar o caminho completo do arquivo e não é possível procurar o arquivo .vhd.

Algumas tarefas realizadas com discos e volumes dependem dos serviços Plug and Play e Remote Registry.

Dispositivos de armazenamento removíveis

Os dispositivos de armazenamento removíveis podem ser formatados com NTFS, FAT, FAT32 ou exFAT. Conecta-se os dispositivos de armazenamento externos ao computador, em vez de instalá-los dentro dele. Isso torna os dispositivos de armazenamento externos mais fáceis e rápidos de instalar que a maioria das unidades de disco fixo. A maioria dos dispositivos de armazenamento externos possuem conexão universal serial bus (USB, barramento serial universal) ou uma interface FireWire. Ao trabalhar com USB e FireWire, a velocidade de transferência e o desempenho geral do dispositivo a partir da perspectiva do usuário dependerá principalmente da versão suportada. Atualmente, diversas versões de USB e FireWire são utilizadas.

O USB 2.0 é o padrão da indústria atual, ao passo que está iniciando uma transição para o USB 3.0. Os dispositivos USB 2.0 podem ser classificados como velocidade total (até 12 Mbps) ou alta velocidade (até 480 Mbps). Embora o USB de alta velocidade suporte transferências de dados com uma taxa máxima de 480 Mbps, as taxas de transferência de dados normalmente são de 10-30 Mbps. A taxa de transferência sustentável real depende de muitos fatores, incluindo o tipo de dispositivo, os dados sendo transferidos e a velocidade do computador. Cada controlador USB em um computador tem uma quantidade fixa de largura de banda, que todos os dispositivos anexados a ele devem compartilhar. As taxas de transferência de dados serão significativamente mais lentas se a porta USB do computador for de uma versão mais antiga que a do dispositivo utilizado. Por exemplo, se conectar um dispositivo USB 2.0 em uma porta USB 1.0, ou vice-versa, o dispositivo irá operar na velocidade de transferência significativamente menor do USB 1.0.

Todas as portas USB 1.0, 1.1 e 2.0 têm a mesma aparência. Contudo, a maioria das portas USB 3.0 que vi tem uma cor especial para diferenciá-la. Ainda assim, a melhor maneira de determinar qual tipo de portas USB o computador tem é consultar a documentação que vem com ele. Os monitores mais recentes têm portas USB às quais também se pode conectar dispositivos. Quando tiver dispositivos USB conectados a um monitor, ele agirá como um dispositivo de hub USB. Como com qualquer dispositivo de hub USB, todos os dispositivos conectados ao hub compartilham a mesma largura de banda e a largura de banda total disponível é determinada pela velocidade da entrada USB pela qual o hub estiver conectado ao computador.

O FireWire (IEEE 1394) é um padrão de conexão de alto desempenho que utiliza uma arquitetura ponto a ponto na qual os periféricos negociam conflitos de barramento para determinar qual dispositivo pode controlar melhor a transferência de dados. Como ocorre com o USB, diversas versões do FireWires são utilizadas atualmente. O FireWire 400 (IEEE 1394a) tem taxas máximas de transferência sustentada de até 400 Mbps. O IEEE 1394b permite 400 Mbps (S400), 800 Mbps (S800) e 1600 Mbps (S1600). Como com dispositivos USB, se conectar um dispositivo IEEE 1394b a uma porta IEEE 1394a, ou vice-versa, ele irá operar na velocidade de transferência significativamente menor do FireWire 400.

Como com portas USB, a taxa de transferência sustentada para as portas IEEE 1394a e IEEE 1394b será consideravelmente menor que a taxa máxima possível. As portas e cabos IEEE 1394a e IEEE 1394b têm formas diferentes, tornando fácil ver a diferença entre eles – se souber o que está procurando. Os cabos FireWire 400 sem energia de barramento têm quatro pinos e quatro conectores. Os cabos FireWire 400 com energia de barramento têm seis pinos e seis conectores. Os cabos FireWire 800 e FireWire 1600 sempre têm energia de barramento e têm nove pinos e nove conectores.

Outra opção é a SATA externa (eSATA), que está disponível em computadores mais recentes e é uma conexão de desempenho ultra-alto para transferência de dados para e de dispositivos externos de armazenamento em massa. A eSATA opera em velocidades de até 3 Gbps. Pode-se adicionar suporte para dispositivos eSATA instalando um cartão controlador de eSATA.

Ao adquirir um dispositivo externo para um computador, também se desejará considerar que interfaces ele suporta. Em alguns casos, você pode conseguir obter um dispositivo com mais de uma interface, como um que suporte o USB 3.0 e a eSATA. Um dispositivo com várias interfaces oferece mais opções.

O trabalho com discos removíveis é similar ao com discos fixos. Você pode fazer o seguinte:

- Pressionar e segurar ou clicar com o botão direito do mouse em um disco removível e selecionar Open ou Explore para examinar o conteúdo do disco no File Explorer.
- Pressionar e segurar ou clicar com o botão direito do mouse em um disco removível e selecionar Format para formatar esse disco, conforme abordado em "Formatação de partições" mais adiante neste capítulo. Os discos removíveis geralmente são formatados com uma única partição.
- Pressionar e segurar ou clicar com o botão direito do mouse em um disco removível e selecionar Properties para visualizar ou definir propriedades. Na guia General da caixa de diálogo Properties, pode-se definir o rótulo do volume, conforme abordado em "Como alterar ou excluir o rótulo de um volume", no Capítulo 11.

Ao trabalhar com discos removíveis, pode-se personalizar os modos de exibição de disco e pasta. Para isso, pressione e segure ou clique com o botão direito do mouse no disco ou na pasta, selecione Properties e toque ou clique na guia Customize. É possível, então, especificar o tipo de pasta padrão para controlar os detalhes padrão exibidos. Por exemplo, você pode definir o tipo de pasta padrão como Documents ou Pictures And Videos. Também se pode definir as imagens e os ícones da pasta.

Os discos removíveis suportam o compartilhamento de arquivos e pastas em rede. Configura-se o compartilhamento em discos removíveis da mesma maneira que no compartilhamento de arquivos padrão. Pode-se atribuir permissões de compartilhamento, configurar opções de armazenamento em cache para uso de arquivos offline e limitar o número de usuários simultâneos. Você pode compartilhar um disco removível inteiro, bem como pastas individuais armazenadas nele. Também é possível criar várias instâncias de compartilhamento.

Os discos removíveis diferem do compartilhamento NTFS padrão por não terem necessariamente uma arquitetura de segurança subjacente. Com exFAT, FAT ou FAT32, os arquivos e as pastas armazenados em um disco removível não têm qualquer permissão ou recurso de segurança diferente dos básicos sinalizadores de atributos somente leitura ou oculto que se pode definir.

Instalação e verificação de uma nova unidade

A substituição a quente (Hot Swap, ou "troca a quente") é um recurso que permite remover dispositivos internos sem desligar o computador. Normalmente, as unidades internas com hot swap são instaladas e removidas a partir da frente do computador. Se o computador der suporte à troca a quente de unidades internas, você poderá instalar unidades sem ter de desligá-lo. Depois, abra o Disk Management e escolha Rescan Disks no menu Action. Os novos discos encontrados serão adicionados com o tipo de disco apropriado. Se um disco que tiver adicionado não for encontrado, reinicialize.

Se o computador não der suporte à troca a quente de unidades internas, é preciso desligar o computador e instalar as novas unidades. A seguir, pode-se pesquisar novos discos como descrito anteriormente. Se estiver trabalhando com novos discos que não tenham sido inicializados – ou seja, que não tenham assinaturas de disco – o Disk Management iniciará a caixa de diálogo Initialize Disk assim que for inicializado e irá detectá-los.

Você pode inicializar os discos seguindo estas etapas:

1. Cada disco instalado precisa ser inicializado. Selecione os discos que foram instalados.
2. Os discos podem utilizar o estilo de partição MBR ou GPT. Selecione o estilo de partição que quer utilizar para os discos que estiver inicializando.
3. Toque ou clique em OK. Se tiver escolhido inicializar os discos, o Windows irá gravar uma assinatura de disco neles e os inicializar com o tipo de disco básico.

Se não quiser utilizar a caixa de diálogo Initialize Disk, pode fechá-la e utilizar o Disk Management em seu lugar para visualizar o disco e trabalhar com ele. No modo de exibição Disk List, o disco está marcado com um ícone de seta apontando para baixo, o tipo do disco é listado como Unknown e o status do disco é listado como Not Initialized. Você pode pressionar e segurar ou clicar com o botão direito do mouse no ícone do disco e selecionar Online. Pressione e segure ou clique com o botão direito do mouse no ícone do disco novamente e selecione Initialize Disk. Pode-se então inicializar o disco como abordado anteriormente.

O status da unidade

Saber o status de uma unidade é útil quando se instala novas unidades ou se soluciona problemas da unidade. O Disk Management mostra o status da unidade nos modos de exibição Graphical View e Volume List. A Tabela 10-2 resume os valores de status mais comuns.

TABELA 10-2 Valores comuns de status de unidade

STATUS	DESCRIÇÃO	RESOLUÇÃO
Online	O status normal do disco. Significa que o disco está acessível e não tem problemas. Os discos dinâmicos e básicos exibem este status.	A unidade não tem qualquer problema conhecido. Não é preciso tomar uma medida corretiva.
Online (Errors)	Foram detectados erros de I/O em um disco dinâmico.	Pode-se tentar corrigir os erros temporários pressionando e segurando ou clicando com o botão direito do mouse no disco e selecionando Reactivate Disk. Se isso não funcionar, o disco pode ter um dano físico ou talvez seja preciso executar uma verificação completa nele.
Offline	O disco não está acessível e pode estar corrompido ou temporariamente indisponível. Se o nome do disco mudar para Missing, ele não pode mais ser localizado ou identificado no sistema.	Procure problemas na unidade, em seu controlador e nos cabos. Certifique-se de que a unidade tem energia e está adequadamente conectada. Utilize o comando Reactivate Disk para colocar o disco online novamente (se possível).

Continua

TABELA 10-2 Valores comuns de status de unidade (*continuação*)

STATUS	DESCRIÇÃO	RESOLUÇÃO
Foreign	O disco foi movido para seu computador, mas não foi importado para uso. Uma unidade defeituosa colocada novamente online pode algumas vezes ser listada como Foreign.	Pressione e segure ou clique com o botão direito do mouse no disco e toque ou clique em Import Foreign Disks para adicionar o disco ao sistema.
Unreadable	O disco não está acessível no momento, o que pode ocorrer quando os discos estão sendo examinados novamente. Os discos dinâmicos e básicos exibem este status.	Com leitores de cartão FireWire e USB, talvez se veja este status se o cartão não estiver formatado ou se o estiver de forma inadequada. Também se pode ver este status depois do cartão ser removido do leitor. Caso contrário, se as unidades não estiverem sendo examinadas, a unidade pode ter sido corrompida ou ter erros de I/O. Pressione e segure ou clique com o botão direito do mouse no disco e toque ou clique em Rescan Disk (no menu Action) para tentar corrigir o problema. Talvez também deseje reinicializar o sistema.
Unrecognized	O disco é de um tipo desconhecido e não pode ser utilizado no sistema. Uma unidade de um sistema diferente do Windows pode exibir este status.	Se o disco for de outro sistema operacional, não faça nada. Não é possível utilizar a unidade no computador, portanto, experimente uma unidade diferente.
Not Initialized	O disco não tem uma assinatura válida. Uma unidade de um sistema diferente do Windows pode exibir este status.	Se o disco for de outro sistema operacional, não faça nada. Não é possível utilizar a unidade no computador, portanto, experimente uma unidade diferente. Para preparar o disco para uso no Windows Server 2012, pressione e segure ou clique com o botão direito do mouse nele e toque ou clique em Initialize Disk.
No Media	Nenhuma mídia foi inserida no DVD ou na unidade de disco removível, ou a mídia foi removida. Somente os tipos DVD e disco removível exibem este status.	Insira um DVD ou um disco removível para colocar o disco online. Com leitores de cartão FireWire e USB, este status normalmente (mas nem sempre) é exibido quando o cartão é removido.

Como trabalhar com discos básicos, dinâmicos e virtuais

O Windows Server 2012 dá suporte às configurações de discos básicos, dinâmicos e virtuais. Esta seção aborda as técnicas para trabalhar com cada tipo de configuração de disco.

OBSERVAÇÃO Não se pode utilizar discos dinâmicos em computadores portáteis ou com mídia removível.

Utilização dos discos básicos e dinâmicos

Normalmente, as partições de disco do Windows Server 2012 são inicializadas como discos básicos. Não se pode criar novos conjuntos de unidades tolerantes a falhas utilizando o tipo de disco básico. É preciso convertê-los em discos dinâmicos e criar volumes que utilizem faixa de disco, espelhamento ou faixa de disco com paridade (chamados de RAID 0, 1 e 5, respectivamente). Os recursos tolerantes a falhas e a capacidade de modificar discos sem ter de reiniciar o computador são as funcionalidades-chave que distinguem os discos dinâmicos dos discos básicos. Os outros recursos disponíveis em um disco dependem da sua formatação.

Você pode utilizar discos básicos e dinâmicos no mesmo computador. Contudo, os conjuntos de volumes devem utilizar o mesmo tipo de disco e estilo de particionamento. Por exemplo, se quiser espelhar as unidades C e D, ambas devem ter o tipo de disco dinâmico e utilizar o mesmo estilo de particionamento, que pode ser MBR ou GPT. Observe que o Disk Management permite iniciar muitas tarefas de configuração do disco independentemente dos discos com que esteja trabalhando utilizarem o tipo de disco dinâmico. O senão é que, durante o processo de configuração, o Disk Management irá converter os discos para o tipo de disco dinâmico. Para aprender como converter um disco de básico para dinâmico, consulte “Alteração dos tipos de unidade” na próxima página.

Pode-se realizar diferentes tarefas de configuração de disco com discos básicos e dinâmicos. Com discos básicos, pode-se fazer o seguinte:

- Formatar partições e marcá-las como ativas
- Criar e excluir partições primárias e estendidas
- Criar e excluir unidades lógicas dentro de partições estendidas
- Converter um disco básico em um disco dinâmico

Com discos dinâmicos, pode-se fazer o seguinte:

- Criar e excluir volumes simples, distribuídos, estendidos, espelhados e RAID-5
- Remover um espelho de um volume espelhado
- Expandir volumes simples ou estendidos
- Dividir um volume em dois
- Reparar volumes espelhados ou RAID-5
- Reativar um disco não encontrado ou offline
- Reverter para um disco básico a partir de um disco dinâmico (requer a exclusão de volumes e a restauração a partir do backup)

Com os dois tipos de disco, pode-se fazer o seguinte:

- Visualizar propriedades de discos, partições e volumes
- Fazer atribuições de letra da unidade
- Configurar a segurança e o compartilhamento da unidade

Considerações especiais para discos básicos e dinâmicos

Esteja trabalhando com discos básicos ou dinâmicos, é preciso lembrar-se de cinco tipos especiais de seções da unidade:

- **Active** A partição ou o volume ativo é a seção da unidade para o armazenamento em cache e a inicialização do sistema. Alguns dispositivos com armazenamento removível podem ser listados como possuindo uma partição ativa.
- **Boot** A partição ou o volume de inicialização contém o sistema operacional e seus arquivos de suporte. O sistema e a partição ou o volume de inicialização podem ser o mesmo.
- **Crash dump** A partição na qual o computador tenta gravar arquivos de despejo caso o sistema falhe. Por padrão, os arquivos de despejo são gravados na pasta %SystemRoot%, mas podem estar localizados em qualquer partição ou volume.
- **Page file** Uma partição contendo um arquivo de paginação utilizado pelo sistema operacional. Como um computador pode paginar memória em vários discos, de acordo com a forma como a memória virtual estiver configurada, ele pode ter vários volumes ou partições com arquivo de paginação.
- **System** A partição ou o volume do sistema contém os arquivos específicos de hardware necessários para carregar o sistema operacional. A partição ou o volume do sistema não pode fazer parte de um volume distribuído ou estendido.

OBSERVAÇÃO Você pode marcar uma partição como ativa utilizando o Disk Management. No Disk Management, pressione e segure ou clique com o botão direito do mouse na partição primária que queira marcar como ativa e toque ou clique em **Mark Partition As Active**. Não é possível marcar volumes de disco dinâmico como ativos. Ao converter um disco básico contendo a partição ativa em um disco dinâmico, essa partição se torna um volume simples que está automaticamente ativo.

Alteração dos tipos de unidade

Os discos básicos foram desenvolvidos para serem utilizados com versões anteriores do Windows. Os discos dinâmicos foram desenvolvidos para que você usufrua os recursos mais recentes do Windows. Somente computadores com o Windows 2000 ou versões mais recentes do Windows podem utilizar discos dinâmicos. No entanto, pode-se utilizar discos dinâmicos com outros sistemas operacionais, como o UNIX. Para isso, é preciso criar um volume separado para o sistema operacional diferente do Windows. Não se pode utilizar discos dinâmicos em computadores portáteis.

O Windows Server 2012 fornece as ferramentas necessárias para converter um disco básico em um disco dinâmico e para transformar um disco dinâmico em um disco básico novamente. Com a conversão para um disco dinâmico, as partições são automaticamente transformadas em volumes do tipo apropriado. Não é possível transformar esses volumes novamente em partições. Em vez disso, é preciso excluir os volumes no disco dinâmico para transformá-lo novamente em um disco básico. A exclusão dos volumes destrói todas as informações no disco.

Conversão de um disco básico em um disco dinâmico

Antes de converter um disco básico em um disco dinâmico, certifique-se de que não precisa inicializar o computador em outras versões do Windows. Somente computadores com o Windows 2000 ou versões mais recentes do Windows podem utilizar discos dinâmicos.

Com discos MBR, você deve certificar-se de que o disco tenha 1 MB de espaço livre no seu final. Embora o Disk Management reserve esse espaço livre ao criar partições e volumes, as ferramentas de gerenciamento de disco em outros sistemas operacionais talvez não o façam. Sem o espaço livre no final do disco, a conversão falhará.

Com discos GPT, você deve ter partições de dados contíguas e reconhecidas. Se o disco GPT contiver partições que o Windows não reconheça, como as criadas por outro sistema operacional, não será possível convertê-lo em um disco dinâmico.

Com qualquer tipo de disco, o seguinte é válido:

- É preciso haver ao menos 1 MB de espaço livre no final do disco. O Disk Management reserva esse espaço livre automaticamente, mas outras ferramentas de gerenciamento de disco talvez não o façam.
- Não se pode utilizar discos dinâmicos em computadores portáteis ou com mídia removível. Você pode configurar essas unidades apenas como unidades básicas com partições primárias.
- Não se deve converter um disco se contiver várias instalações de sistema operacional Windows. Se o fizer, talvez consiga só inicializar o computador utilizando o Windows Server 2012.

Para converter um disco básico em um disco dinâmico, siga estas etapas:

1. No Disk Management, pressione e segure ou clique com o botão direito do mouse em um disco básico que queira converter, seja no modo de exibição Disk List ou no painel esquerdo de Graphical View. Toque ou clique em Convert To Dynamic Disk.
2. Na caixa de diálogo Convert To Dynamic Disk, marque as caixas de seleção para os discos que quer converter. Se estiver convertendo um volume estendido, distribuído, espelhado ou RAID-5, certifique-se de selecionar todos os discos básicos desse conjunto. É preciso converter o conjunto todo ao mesmo tempo. Toque ou clique em OK para prosseguir. A caixa de diálogo Disks To Convert será exibida.

Essa caixa de diálogo mostra os discos sendo convertidos. Os botões e as colunas nela contêm as seguintes informações:

- **Name** Mostra o número do disco.
- **Disk Contents** Mostra o tipo e o status das partições, como boot, active ou in use.
- **Will Convert** Especifica se a unidade será convertida. Se a unidade não satisfizer aos critérios, não será convertida e talvez seja preciso agir de forma corretiva, conforme descrito anteriormente.
- **Details** Mostra os volumes na unidade selecionada.
- **Convert** Inicia a conversão.

3. Para começar a conversão, toque ou clique em Convert. O Disk Management alertará que, após a conversão ser concluída, não será possível inicializar versões

anteriores do Windows a partir de volumes nos discos selecionados. Toque ou clique em Yes para prosseguir.

4. O Disk Management reinicia o computador se uma unidade selecionada contiver a partição de inicialização, a partição do sistema ou uma partição em uso.

Transformação de um disco dinâmico novamente em um disco básico

Antes de transformar um disco dinâmico novamente em um disco básico, é preciso excluir todos os volumes dinâmicos no disco. Após, pressione e segure ou clique com o botão direito do mouse no disco e selecione Convert To Basic Disk. Assim, o disco dinâmico será transformado em um disco básico. Você poderá então criar novas partições e unidades lógicas nele.

Reativação de discos dinâmicos

Se o status de um disco dinâmico for Online (Errors) ou Offline, muitas vezes é possível reativá-lo para corrigir o problema. Você reativa um disco seguindo estas etapas:

1. No Disk Management, pressione e segure ou clique com o botão direito do mouse no disco dinâmico que quer reativar e toque ou clique em Reactivate Disk. Confirme a ação quando for solicitado.
2. Se o status da unidade não mudar, talvez seja preciso reinicializar o computador. Se isso ainda não resolver o problema, verifique se há problemas na unidade, em seu controlador e nos cabos. Também certifique-se de que a unidade tem energia e está adequadamente conectada.

Como reexaminar os discos

O reexame de todas as unidades em um sistema atualiza as informações da configuração da unidade no computador. Algumas vezes o novo exame pode resolver um problema com unidades que mostram o status de Unreadable. Você examina novamente os discos de um computador escolhendo Rescan Disks no menu Action do Disk Management.

Como mover um disco dinâmico para um novo sistema

Uma importante vantagem dos discos dinâmicos sobre os discos básicos é que se pode facilmente movê-los de um computador para outro. Por exemplo, se após configurar um computador, você decidir que não precisa realmente de um disco rígido adicional, poderá movê-lo para outro computador em que possa ser mais bem utilizado.

O Windows Server 2012 simplifica enormemente a tarefa de mover unidades para um novo sistema. Antes de mover os discos, deve-se seguir estas etapas:

1. Abra o Disk Management no sistema em que as unidades dinâmicas estão instaladas atualmente. Verifique o status das unidades e certifique-se de que estão marcadas como Healthy. Se o status não for Healthy, você deve reparar as partições e os volumes antes de mover as unidades de disco.

OBSERVAÇÃO As unidades com BitLocker Drive Encryption (Criptografia de Unidade de Disco BitLocker) não podem ser movidas utilizando esta técnica. A BitLocker Drive Encryption encapsula as unidades em um selo protegido a fim de que qualquer adulteração offline seja detectada e os resultados no disco não estejam disponíveis até que um administrador os desbloqueie.

2. Verifique os subsistemas de disco rígido no computador original e no computador para o qual quer transferir o disco. Ambos devem ter subsistemas de disco rígido idênticos. Se não tiverem, a Plug and Play ID no disco do sistema do computador original não corresponderá ao que o computador de destino está esperando. Como resultado, o computador de destino não poderá carregar as unidades corretas e a tentativa de inicialização pode falhar.
3. Verifique se qualquer disco dinâmico que queira mover faz parte de um conjunto estendido ou distribuído. Se for o caso, você deverá observar quais discos fazem parte de qual conjunto e planejar mover todos os discos em um conjunto simultaneamente. Se estiver movendo apenas parte de um conjunto de discos, deve estar ciente das consequências. Para volumes estendidos ou distribuídos, mover apenas parte do conjunto tornará os volumes relacionados inutilizáveis no computador atual e no computador para o qual se planeja mover os discos.

Quando estiver pronto para mover os discos, siga estas etapas:

1. No computador original, inicie o Computer Management. No painel esquerdo, selecione Device Manager. Na lista Device, expanda Disk Drives. Uma lista das unidades de disco físico no computador será mostrada. Pressione e segure ou clique com o botão direito do mouse em cada disco que queira mover e toque ou clique em Uninstall. Se não tiver certeza de quais discos desinstalar, pressione e segure ou clique com o botão direito do mouse em cada disco e toque ou clique em Properties. Na caixa de diálogo Properties, toque ou clique na guia Volumes e selecione Populate. Os volumes no disco selecionado serão exibidos.
2. A seguir, no computador original, selecione o nó Disk Management em Computer Management. Se os discos que quiser mover ainda forem listados, pressione e segure ou clique com o botão direito do mouse no disco e toque ou clique em Remove Disk.
3. Depois de realizar esses procedimentos, poderá mover os discos dinâmicos. Se os discos forem passíveis de troca a quente (hot swap) e esse recurso tiver suporte em ambos os computadores, remova-os do computador original e instale-os no computador de destino. Caso contrário, desligue os dois computadores, remova as unidades do computador original e instale-as no computador de destino. Quando tiver terminado, reinicie os computadores.
4. No computador de destino, acesse o Disk Management e escolha Rescan Disks no menu Action. Quando o Disk Management terminar de examinar os discos, pressione e segure ou clique com o botão direito do mouse em qualquer disco marcado como Foreign e toque ou clique em Import. Agora deve ser possível acessar os discos e seus volumes no computador de destino.

OBSERVAÇÃO Na maioria dos casos, os volumes nos discos dinâmicos devem manter as letras de unidade que tinham no computador original. No entanto, se uma letra de unidade já for utilizada no computador de destino, o volume receberá a próxima disponível. Se um volume dinâmico não tinha uma letra de unidade anteriormente, não receberá uma ao ser movido para o computador de destino. Além disso, se a montagem automática estiver desabilitada, os volumes não serão montados automaticamente e será preciso fazê-lo manualmente e atribuir letras de unidade.

Gerenciamento de discos rígidos virtuais

Utilizando o Disk Management, pode-se criar, anexar e desanexar discos rígidos virtuais. Você pode criar um disco rígido virtual escolhendo Create VHD no menu Action. Na caixa de diálogo Create And Attach Virtual Hard Disk, toque ou clique em Browse. Utilize a caixa de diálogo Browse Virtual Disk Files para selecionar a localização em que quer criar o arquivo .vhd para o disco rígido virtual e toque ou clique em Save.

Na lista Virtual Hard Disk Size, digite o tamanho do disco em MB, GB ou TB. Especifique se o tamanho do VHD se expande dinamicamente para seu tamanho máximo fixo enquanto os dados são salvos nele ou utiliza uma quantidade fixa de espaço, independentemente da quantidade de dados que armazene. Ao tocar ou clicar em OK, o Disk Management criará o disco rígido virtual.

O VHD será automaticamente anexado e adicionado como um novo disco. Para inicializar o disco para o uso, pressione e segure ou clique com o botão direito do mouse na entrada do disco em Graphical View e toque ou clique em Initialize Disk. Na caixa de diálogo Initialize Disk, o disco está selecionado para inicialização. Especifique o tipo do disco como MBR ou GPT e toque ou clique em OK.

Depois de inicializá-lo, pressione e segure ou clique com o botão direito do mouse no espaço não particionado do disco e crie um volume do tipo apropriado. Após criar o volume, o VHD estará disponível para o uso.

Uma vez que tenha criado, anexado, inicializado e formatado um VHD, poderá trabalhar com o disco virtual praticamente da mesma forma que com outros discos. Pode-se gravar dados em um VHD e lê-los a partir dele. É possível inicializar o computador a partir do VHD. Você pode colocá-lo offline ou online pressionando e segurando ou clicando com o botão direito do mouse na entrada do disco em Graphical View e selecionando Offline ou Online, respectivamente. Se não quiser mais utilizar um VHD, pode desanexá-lo pressionando e segurando ou clicando com o botão direito do mouse na entrada do disco em Graphical View, selecionando Detach VHD e tocando ou clicando em OK na caixa de diálogo Detach Virtual Hard Disk.

Você também pode utilizar os VHDs criados com outros programas. Se tiver criado um VHD utilizando outro programa ou tiver um VHD desanexado que queira anexar, pode trabalhar com ele executando as seguintes etapas:

1. No Disk Management, toque ou clique na opção Attach VHD no menu Action.
2. Na caixa de diálogo Attach Virtual Hard Disk, toque ou clique em Browse. Utilize a caixa de diálogo Browse Virtual Disk Files para selecionar o arquivo .vhd para o disco rígido virtual e toque ou clique em Open.
3. Se quiser anexar o VHD no modo somente leitura, selecione Read-Only. Toque ou clique em OK para anexar o VHD.

Utilização de discos e partições básicos

Quando se instala um novo computador ou se atualiza um existente, muitas vezes é preciso particionar as unidades nele. Particiona-se as unidades utilizando o Disk Management.

Conceitos básicos de particionamento

No Windows Server 2012, uma unidade física utilizando o estilo de partição MBR pode ter até quatro partições primárias e apenas uma partição estendida. Isso permite con-

figurar unidades MBR de duas formas: utilizando de uma a quatro partições primárias, ou utilizando de uma a três partições primárias e uma partição estendida. Uma partição primária pode preencher um disco inteiro, ou você pode dimensioná-la conforme apropriado para a estação de trabalho ou o servidor que esteja configurando. Dentro de uma partição estendida, pode-se criar uma ou mais unidades lógicas. Uma unidade lógica é simplesmente uma parte de uma partição com seu próprio sistema de arquivos. Geralmente, se utiliza as unidades lógicas para dividir uma unidade grande em unidades menores, melhor gerenciáveis. Pensando nisso, você talvez queira dividir uma partição estendida de 600 GB em três unidades lógicas de 200 GB cada. Os discos físicos com o estilo de partição GPT podem ter até 128 partições.

Após partitionar uma unidade, formata-se as partições para atribuir as letras de unidade. Essa é uma formatação de alto nível que cria a estrutura do sistema de arquivos, em vez da formatação de baixo nível, que configura a unidade para o uso inicial. Você provavelmente conhece bem a unidade C utilizada pelo Windows Server 2012. Bem, a unidade C é simplesmente o designador de uma partição de disco. Se partitionar um disco em várias seções, cada uma pode ter sua própria letra de unidade. Utiliza-se as letras de unidade para acessar os sistemas de arquivos em várias partições de uma unidade física. Diferentemente do MS-DOS, que atribui letras de unidade automaticamente começando com a letra C, o Windows Server 2012 permite que se especifique as letras de unidade. Geralmente, as letras de unidade de C a Z estão disponíveis para uso.

OBSERVAÇÃO A letra de unidade A costumava ser atribuída à unidade de disquete do sistema. Se o sistema tivesse uma segunda unidade de disquete, a letra B era atribuída a ela, desse modo, só se podia utilizar as letras de C a Z. Não se esqueça de que as unidades de DVD e outros tipos de unidades de mídia também precisam de letras de unidade. O número total de letras de unidade que se pode utilizar de uma vez é 24. Se precisar de volumes adicionais, pode criá-los utilizando caminhos de unidade.

Utilizando letras de unidade, pode-se ter apenas 24 volumes ativos. Para contornar essa limitação, você pode montar discos para caminhos de unidade. Um caminho de unidade é configurado como a localização da pasta apontando para outra unidade. Por exemplo, você poderia montar unidades adicionais como E:\Data1, E:\Data2 e E:\Data3. Pode-se utilizar caminhos de unidade com discos básicos e dinâmicos. A única restrição para caminhos de unidade é que sejam montados em pastas vazias que estejam em unidades NTFS.

Para ajudá-lo a distinguir entre partições primárias e estendidas com unidades lógicas, o Disk Management codifica as partições por cores. Por exemplo, as partições primárias podem estar codificadas por cores com uma faixa azul-escura e as unidades lógicas em partições estendidas podem estar com uma faixa azul-clara. A legenda para o esquema de cores é mostrada na parte inferior da janela do Disk Management. Você pode alterar as cores na caixa de diálogo Settings escolhendo Settings no menu View.

Criação de partições e volumes simples

O Windows Server 2012 simplifica a interface de usuário do Disk Management utilizando um mesmo conjunto de caixas de diálogo e assistentes para as partições e os volumes. Os primeiros três volumes em uma unidade básica são criados automaticamente como partições primárias. Se tentar criar um quarto volume em uma unidade básica, o espaço livre restante na unidade será automaticamente convertido em uma partição estendida com uma unidade lógica do tamanho designado por você usando

o novo recurso de volume na partição estendida. Qualquer volume subsequente será criado automaticamente na partição estendida como unidade lógica.

No Disk Management, você cria partições, unidades lógicas e volumes simples seguindo estas etapas:

1. Em Graphical View do Disk Management, pressione e segure ou clique com o botão direito do mouse em uma área não alocada ou livre e toque ou clique em New Simple Volume. O New Simple Volume Wizard será iniciado. Leia a página Welcome e toque ou clique em Next.
2. A página Specify Volume Size, mostrada na Figura 10-3, especifica o tamanho mínimo e máximo para o volume em megabytes e permite dimensioná-lo dentro desses limites. Dimensione a partição em megabytes na caixa Simple Volume Size In MB e toque ou clique em Next.

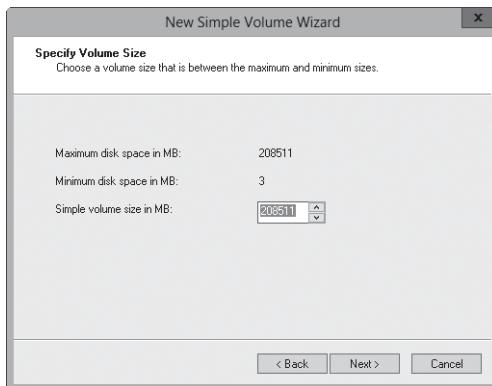


FIGURA 10-3 Defina o tamanho do volume na página Specify Volume Size.

3. Na página Assign Drive Letter Or Path, mostrada na Figura 10-4, especifique se quer atribuir uma letra ou um caminho de unidade e toque ou clique em Next. As opções a seguir estão disponíveis:
 - **Assign The Following Drive Letter** Escolha esta opção para atribuir uma letra de unidade. Selecione uma letra de unidade disponível na lista fornecida. Por padrão, o Windows Server 2012 selecionará a letra de unidade mais baixa disponível e excluirá as letras de unidade reservadas, bem como aquelas atribuídas a discos locais ou unidades de rede.
 - **Mount In The Following Empty NTFS Folder** Escolha esta opção para montar a partição em uma pasta NTFS vazia. Você deve digitar o caminho para uma pasta existente, ou tocar ou clicar em Browse para procurar ou criar uma pasta para utilização.
 - **Do Not Assign A Drive Letter Or Drive Path** Escolha esta opção se quiser criar a partição sem atribuir uma letra ou um caminho de unidade. Se quiser que a partição esteja disponível para armazenamento posteriormente, poderá atribuir uma letra ou um caminho de unidade a qualquer momento.

OBSERVAÇÃO Não é preciso atribuir uma letra ou um caminho de unidade a volumes. Um volume sem apontamentos será considerado desmontado e estará em grande parte inutilizável. Um volume desmontado pode ser montado com a atribuição de uma letra ou um caminho de unidade em um momento posterior. Consulte “Como atribuir letras e caminhos de unidade” no Capítulo 11.

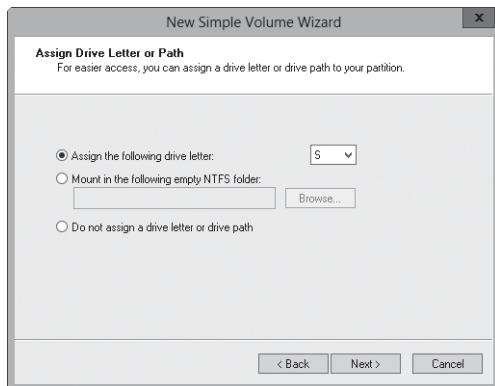


FIGURA 10-4 Na página Assign Drive Letter Or Path, atribua o apontamento da unidade ou escolha esperar para mais tarde.

4. Na página Format Partition, mostrada na Figura 10-5, determine se e como o volume deve ser formatado. Se quiser formatá-lo, selecione Format This Volume With The Following Settings e configure as seguintes opções:
 - **File System** Define o tipo do sistema de arquivos, como FAT, FAT32, exFAT, NTFS ou ReFS. Os tipos de sistema de arquivos disponíveis dependerão do tamanho do volume sendo formatado. Se utilizar FAT32, poderá converter posteriormente para NTFS com o utilitário Convert. Não é possível, no entanto, converter partições NTFS em FAT32.
 - **Allocation Unit Size** Define o tamanho do cluster para o sistema de arquivos. Esta é a unidade básica em que o espaço em disco é alocado. O tamanho da unidade de alocação padrão é baseado no tamanho do volume e definido dinamicamente antes da formatação por padrão. Para substituir esse recurso, pode-se definir o tamanho da unidade de alocação com um valor específico. Se utilizar muitos arquivos pequenos, talvez queira usar um tamanho de cluster menor, como 512 ou 1024 bytes. Com essas configurações, os arquivos pequenos utilizarão menos espaço em disco. Observe que os volumes ReFS têm um tamanho de unidade de alocação fixo.
 - **Volume Label** Define um rótulo de texto para a partição. Esse rótulo é o nome de volume da partição e está definido para New Volume por padrão. Pode-se alterar o rótulo do volume a qualquer momento pressionando e segurando ou clicando com o botão direito do mouse no volume no File Explorer, tocando ou clicando em Properties e digitando um novo valor na caixa Label fornecida na guia General.

- **Perform A Quick Format** Faz com que o Windows Server 2012 formate sem verificar erros na partição. Com partições grandes, esta opção pode poupar alguns minutos. Contudo, geralmente é melhor verificar os erros, permitindo que o Disk Management marque setores defeituosos no disco e os bloqueeie.
- **Enable File And Folder Compression** Ativa a compactação para o disco. A compactação interna está disponível apenas para o NTFS (e não tem suporte para FAT, FAT32, exFAT ou ReFS). No NTFS, a compactação é transparente para os usuários e os arquivos compactados podem ser acessados como arquivos comuns. Se selecionar esta opção, os arquivos e diretórios nessa unidade serão automaticamente compactados. Para mais informações sobre a compactação de unidades, arquivos e diretórios, consulte “Compactação de unidades e dados” mais adiante neste capítulo.

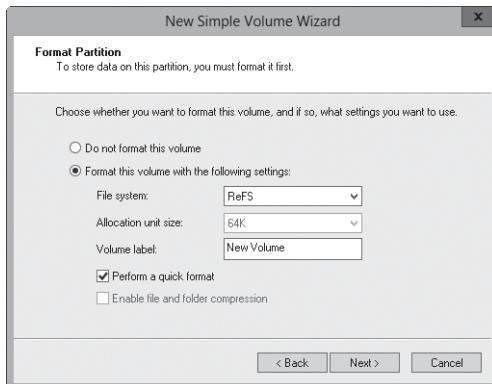


FIGURA 10-5 Defina as opções de formatação para a partição na página Format Partition.

5. Toque ou clique em Next, confirme suas opções e toque ou clique em Finish.

Formatação de partições

A formatação cria um sistema de arquivos em uma partição e exclui permanentemente todos os dados existentes. Essa é uma formatação de alto nível que cria a estrutura do sistema de arquivos, em vez da formatação de baixo nível, que inicializa a unidade para o uso. Para formatar uma partição, pressione e segure ou clique com o botão direito do mouse nela e toque ou clique em Format. A caixa de diálogo Format, mostrada na Figura 10-6, será aberta.

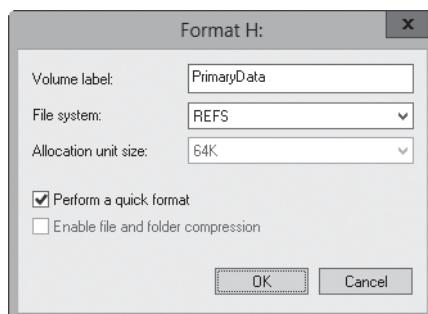


FIGURA 10-6 Formate uma partição usando a caixa de diálogo Format, especificando seu tipo de sistema de arquivos e rótulo de volume.

Pode-se utilizar as opções de formatação como se segue:

- **Volume Label** Especifica um rótulo de texto para a partição. Esse rótulo é o nome de volume da partição.
- **File System** Especifica o tipo do sistema de arquivos, como FAT, FAT32, exFAT, NTFS ou ReFS. Os tipos de sistema de arquivos disponíveis dependerão do tamanho do volume sendo formatado.
- **Allocation Unit Size** Especifica o tamanho do cluster para o sistema de arquivos. Esta é a unidade básica em que o espaço em disco é alocado. O tamanho da unidade de alocação padrão é baseado no tamanho do volume e definido dinamicamente antes da formatação. Para substituir esse recurso, pode-se definir o tamanho da unidade de alocação com um valor específico. Se utilizar muitos arquivos pequenos, talvez queira usar um tamanho de cluster menor, como 512 ou 1024 bytes. Com essas configurações, os arquivos pequenos utilizarão menos espaço em disco.
- **Perform A Quick Format** Faz com que o Windows Server 2012 formate sem verificar erros na partição. Com partições grandes, esta opção pode poupar alguns minutos. Contudo, é mais prudente verificar os erros, permitindo que o Disk Management marque setores defeituosos no disco e os bloqueeie.

Quando estiver pronto para prosseguir, toque ou clique em OK. Como a formatação de uma partição destrói todos os dados existentes, o Disk Management oferece uma última oportunidade de cancelar o procedimento. Toque ou clique em OK para começar a formatá-la. O Disk Management altera o status da unidade para refletir a formatação e a porcentagem de conclusão. Quando a formatação for concluída, o status da unidade será alterado para refleti-lo.

Compactação de unidades e dados

Quando se formata uma unidade para o NTFS, o Windows Server 2012 permite ativar o recurso interno de compactação. Com a compactação, todos os arquivos e pastas armazenados em uma unidade são automaticamente compactados ao serem criados.

Por causa da compactação ser transparente para os usuários, os arquivos compactados podem ser acessados como arquivos comuns. A diferença é que se pode armazenar mais informações em uma unidade compactada do que em uma não compactada. Observe que o File Explorer mostra os nomes de recursos compactados em azul.

MUNDO REAL Embora a compactação seja certamente um recurso útil quando se quer poupar espaço em disco, não se pode criptografar dados compactados. A compactação e a criptografia são alternativas mutuamente exclusivas para volumes NTFS, ou seja, existe a opção de utilizar a compactação ou a criptografia. Não é possível utilizar ambas as técnicas. Para mais informações sobre criptografia, consulte “Criptografia de unidades e dados” mais adiante neste capítulo. Se tentar compactar dados criptografados, o Windows Server 2012 irá automaticamente descriptografá-los e, então, compactá-los. Da mesma forma, se tentar criptografar dados compactados, o Windows Server 2012 irá automaticamente descompactá-los e, então, criptografá-los.

Compactação de unidades

Para compactar uma unidade e todo o seu conteúdo, siga estas etapas:

1. No File Explorer ou Disk Management, pressione e segure ou clique com o botão direito do mouse na unidade que queira compactar e toque ou clique em Properties.
2. Na guia General, selecione Compress Drive To Save Disk Space e toque ou clique em OK.
3. Na caixa de diálogo Confirm Attribute Changes, selecione se as alterações devem ser aplicadas a subpastas e arquivos e toque ou clique em OK.

Compactação de diretórios e arquivos

Se decidir não compactar uma unidade, o Windows Server 2012 permitirá que compacte pastas e arquivos de forma seletiva. Para compactar um arquivo ou pasta, siga estas etapas:

1. No File Explorer, pressione e segure ou clique com o botão direito do mouse no arquivo ou pasta que queira compactar e toque ou clique em Properties.
2. Na guia General da caixa de diálogo Properties, toque ou clique em Advanced. Na caixa de diálogo Advanced Attributes, marque a caixa de seleção Compress Contents To Save Disk Space. Toque ou clique em OK duas vezes.

Para um arquivo individual, o Windows Server irá marcar o arquivo como compactado e depois o compactar. Para uma pasta, o Windows Server irá marcar a pasta como compactada e depois compactar todos os arquivos nela. Se a pasta contiver subpastas, o Windows Server exibirá uma caixa de diálogo que permite compactar todas as subpastas associadas à pasta. Simplesmente selecione Apply Changes To This Folder, Subfolders, And Files e toque ou clique em OK. Uma vez que tenha compactado a pasta, qualquer arquivo novo adicionado ou copiado para ela será automaticamente compactado.

OBSERVAÇÃO Se mover um arquivo não compactado de uma unidade diferente, ele será compactado. Contudo, se mover um arquivo não compactado para uma pasta compactada na mesma unidade NTFS, ele não será compactado. Observe também que não se pode criptografar arquivos compactados.

Como expandir unidades compactadas

O File Explorer mostra os nomes de arquivos e pastas compactados em azul. Pode-se remover a compactação de uma unidade seguindo estas etapas:

1. No File Explorer ou Disk Management, pressione e segure ou clique com o botão direito do mouse na unidade que contém os dados que queira expandir e toque ou clique em Properties.
2. Desmarque a caixa de seleção Compress Drive To Save Disk Space e toque ou clique em OK.
3. Na caixa de diálogo Confirm Attribute Changes, selecione se as alterações devem ser aplicadas a subpastas e arquivos e toque ou clique em OK.

DICA O Windows sempre verifica o espaço disponível em disco antes de expandir dados compactados. Você também deve fazê-lo. Se houver menos espaço livre disponível que espaço utilizado, talvez não seja possível concluir a expansão. Por exemplo, se uma unidade compactada utilizar 150 GB de espaço e houver 70 GB de espaço livre disponível, não haverá espaço livre suficiente para expandir os dados. Geralmente, é preciso cerca de 1,5 a 2 vezes tanto espaço livre quanto se tem de dados compactados.

Como expandir pastas e arquivos compactados

Se decidir que quer expandir um arquivo ou pasta compactado, siga estas etapas:

1. Pressione e segure ou clique com o botão direito do mouse no arquivo ou pasta no File Explorer e toque ou clique em Properties.
2. Na guia General da caixa de diálogo Properties, toque ou clique em Advanced. Desmarque a caixa de seleção Compress Contents To Save Disk Space. Toque ou clique em OK duas vezes.

Com arquivos, o Windows Server irá remover a compactação e expandir o arquivo. Com pastas, o Windows Server irá expandir todos os arquivos dentro da pasta. Se a pasta contiver subpastas, também será possível remover a compactação delas. Para isso, selecione Apply Changes To This Folder, Subfolders, And Files quando for solicitado e toque ou clique em OK.

DICA O Windows Server também oferece utilitários de linha de comando para compactar e descompactar dados. O utilitário de compactação chama-se Compact (Compact.exe). O utilitário de descompactação chama-se Expand (Expand.exe).

Criptografia de unidades e dados

O NTFS tem muitas vantagens sobre outros sistemas de arquivos que se pode utilizar com o Windows Server. Uma das maiores é a capacidade de criptografar e descriptografar dados automaticamente utilizando o Encrypting File System (EFS). Quando você criptografa dados, adiciona uma camada extra de proteção a dados confidenciais e essa camada age como uma cobertura de segurança, bloqueando todos os outros usuários para leitura do conteúdo dos arquivos criptografados. De fato, um dos grandes benefícios da criptografia é que somente o usuário designado pode acessar os dados. Esse benefício também é uma desvantagem, no sentido do usuário ter que remover a criptografia antes que usuários autorizados possam acessar os dados.

OBSERVAÇÃO Conforme abordado anteriormente, não se pode compactar arquivos criptografados. Os recursos de criptografia e compactação do NTFS são mutuamente exclusivos. Você pode utilizar um recurso ou o outro, mas não ambos.

Criptografia e o Encrypting File System

A criptografia de arquivos tem suporte com base em pasta e em arquivo. Qualquer arquivo colocado em uma pasta marcada para criptografia será automaticamente criptografado. Os arquivos em formato criptografado podem ser lidos somente pela pessoa que os criptografou. Antes de outros usuários poderem ler um arquivo criptografado, o usuário deve descriptografá-lo ou conceder acesso especial ao arquivo adicionando a chave de criptografia de um usuário a ele.

Todo arquivo criptografado tem uma chave de criptografia única do usuário que o criou ou que o possui no momento. Um arquivo criptografado pode ser copiado, movido ou renomeado como qualquer outro arquivo e, na maioria dos casos, essas ações não afetam a criptografia dos dados. (Para detalhes, consulte “Como trabalhar com arquivos e pastas criptografados” mais adiante neste capítulo.) O usuário que criptografa o arquivo sempre tem acesso a ele, desde que o certificado de chave pública do usuário esteja disponível no computador que esteja utilizando. Para esse usuário, o processo de criptografia e descriptografia funciona automaticamente e é transparente.

O EFS é o processo que controla a criptografia e a descriptografia. A configuração padrão do EFS permite que os usuários criptografem os arquivos sem necessidade de uma preparação especial. Os arquivos são criptografados utilizando uma chave pública/privada que o EFS gera automaticamente com base na credencial do usuário.

Os certificados de criptografia são armazenados como parte dos dados nos perfis de usuário. Se um usuário trabalhar com vários computadores e quiser utilizar a criptografia, um administrador precisa configurar um perfil móvel para ele. Um perfil móvel garante que os dados do perfil e os certificados de chave pública do usuário estejam acessíveis em outros computadores. Sem isso, os usuários não poderão acessar seus arquivos criptografados em outro computador.

ALERTA DE SEGURANÇA Uma alternativa para um perfil móvel é copiar o certificado de criptografia do usuário para os computadores que ele utilizar. Para isso, pode-se utilizar o processo de backup e restauração abordado em “Backup e restauração do estado do sistema” no Capítulo 13, “Backup e recuperação de dados”. Simplesmente faça backup do certificado no computador original do usuário e o restaure em cada um dos computadores a que ele se conecta.

O EFS tem um sistema de recuperação de dados interno para proteção contra perdas de dados. Esse sistema de recuperação garante que os dados criptografados possam ser recuperados se o certificado da chave pública do usuário for perdido ou excluído. O cenário mais comum para isso é quando um usuário sai da empresa e a conta de usuário associada é excluída. Um gerente talvez pudesse fazer logon na conta do usuário, verificar os arquivos e salvar aqueles importantes em outras pastas, mas se a conta de usuário tiver sido excluída, os arquivos criptografados só estarão acessíveis se a criptografia for removida ou se os arquivos forem movidos para um volume exFAT, FAT ou FAT32 (nos quais a criptografia não tem suporte).

Para acessar os arquivos criptografados depois da conta de usuário ser excluída, é preciso utilizar um agente de recuperação. Os agentes de recuperação têm acesso à chave de criptografia de arquivo necessária para desbloquear os dados em arquivos criptografados. Para proteger dados confidenciais, no entanto, os agentes de recuperação não têm acesso à chave privada ou a qualquer informação de chave privada do usuário.

O Windows Server não criptografará os arquivos sem agentes de recuperação do EFS designados. Por isso, os agentes de recuperação são designados automaticamente e os certificados de recuperação necessários também são gerados automaticamente. Isso assegura que os arquivos criptografados sempre possam ser recuperados.

Os agentes de recuperação do EFS estão configurados em dois níveis:

- **Domain** O agente de recuperação de um domínio é automaticamente configurado quando o primeiro controlador de domínio do Windows Server é instalado. Por padrão, o agente de recuperação é o administrador do domínio. Por meio da Group Policy, os administradores de domínio podem designar agentes de recuperação adicionais. Os administradores de domínio também podem delegar privilégios de agente de recuperação para administradores de segurança designados.
- **Local computer** Quando um computador faz parte de um grupo de trabalho ou em uma configuração autônoma, o agente de recuperação é o administrador do computador local por padrão. Agentes de recuperação adicionais podem ser designados. Além disso, se quiser ter agentes de recuperação locais em um ambiente de domínio, em lugar de agentes de recuperação no nível de domínio, você deve excluir a política de recuperação da Group Policy para o domínio.

Pode-se excluir os agentes de recuperação se não quiser que sejam utilizados. Contudo, se excluir todos os agentes de recuperação, o EFS não irá mais criptografar arquivos. Um ou mais agentes de recuperação devem estar configurados para o EFS funcionar.

Criptografia de pastas e arquivos

Com volumes NTFS, o Windows Server permite selecionar arquivos e pastas para criptografia. Quando um arquivo é criptografado, os dados dele são convertidos em um formato criptografado que somente pode ser lido pela pessoa que o criptografou. Os usuários podem criptografar arquivos somente se tiverem as permissões de acesso apropriadas. Quando se criptografa pastas, a pasta é marcada como criptografada, mas apenas os arquivos dentro dela que estão realmente criptografados. Todos os arquivos que forem criados em uma pasta marcada como criptografada ou forem adicionados a ela serão criptografados automaticamente. Observe que o File Explorer mostra os nomes de recursos criptografados em verde.

Para criptografar um arquivo ou pasta, siga estas etapas:

1. No File Explorer, pressione e segure ou clique com o botão direito do mouse no arquivo ou diretório que queira criptografar e toque ou clique em Properties.
2. Na guia General da caixa de diálogo Properties, toque ou clique em Advanced e marque a caixa de seleção Encrypt Contents To Secure Data. Toque ou clique em OK duas vezes.

OBSERVAÇÃO Não é possível criptografar arquivos compactados, arquivos do sistema ou arquivos somente leitura. Se tentar criptografar arquivos compactados, eles serão automaticamente descompactados e, depois, criptografados. Se tentar criptografar arquivos do sistema, você obterá um erro.

Para um arquivo individual, o Windows Server irá marcar o arquivo como criptografado e depois o criptografar. Para uma pasta, o Windows Server irá marcar a pasta como criptografada e depois criptografar todos os arquivos nela. Se a pasta contiver subpastas, o Windows Server exibirá uma caixa de diálogo que permite criptografar

todas as subpastas associadas à pasta. Simplesmente selecione Apply Changes To This Folder, Subfolders, And Files e toque ou clique em OK.

OBSERVAÇÃO Em volumes NTFS, os arquivos permanecerão criptografados mesmo quando forem movidos, copiados ou renomeados. Se copiar ou mover um arquivo criptografado para um volume exFAT, FAT ou FAT32, ele será automaticamente descriptografado antes de ser copiado ou movido. Portanto, é preciso ter permissões adequadas para copiar ou mover o arquivo.

Você pode conceder acesso especial a uma pasta ou um arquivo criptografado pressionando e segurando ou clicando com o botão direito do mouse no arquivo ou na pasta no File Explorer e selecionando Properties. Na guia General da caixa de diálogo Properties, toque ou clique em Advanced. Na caixa de diálogo Advanced Attributes, toque ou clique em Details. Na caixa de diálogo Encryption Details For, os usuários que tiverem acesso ao arquivo criptografado serão listados por nome. Para permitir que outro usuário accesse o arquivo, toque ou clique em Add. Se um certificado de usuário estiver disponível para o usuário, selecione o nome dele na lista fornecida e toque ou clique em OK. Caso contrário, toque ou clique em Find User para localizar o certificado para ele.

Como trabalhar com arquivos e pastas criptografados

Anteriormente, afirmei que você pode copiar, mover e renomear arquivos e pastas criptografados como qualquer outro arquivo. Isso é verdade, mas o qualifiquei dizendo "na maioria dos casos". Quando se trabalha com arquivos criptografados, você terá menos problemas, desde que trabalhe com volumes NTFS no mesmo computador. Quando se trabalha com outros sistemas de arquivos ou outros computadores, pode-se encontrar problemas. Dois dos cenários mais comuns são os seguintes:

- **Cópia entre volumes no mesmo computador** Quando se copia ou move uma pasta ou um arquivo criptografado de um volume NTFS para outro volume NTFS no mesmo computador, os arquivos permanecem criptografados. No entanto, se copiar ou mover arquivos criptografados para um volume FAT, eles serão descriptografados antes da transferência e, então, transferidos como arquivos padrão e, portanto, acabam como arquivos não criptografados em seu destino. O FAT não dá suporte à criptografia.
- **Cópia entre volumes de um computador diferente** Quando se copia ou move uma pasta ou um arquivo criptografado de um volume NTFS para outro volume NTFS em um computador diferente, os arquivos permanecem criptografados desde que o computador de destino permita que se criptografe arquivos e o computador remoto seja confiável para delegação. Caso contrário, os arquivos serão descriptografados e transferidos como arquivos padrão. O mesmo é verdadeiro quando se copia ou move arquivos criptografados para um volume FAT em outro computador. O FAT não dá suporte à criptografia.

Após transferir um arquivo confidencial que tenha sido criptografado, talvez se queira confirmar se a criptografia ainda está aplicada. Pressione e segure ou clique com o botão direito do mouse no arquivo e selecione Properties. Na guia General da caixa de diálogo Properties, toque ou clique em Advanced. A opção Encrypt Contents To Secure Data deve estar selecionada.

Configuração da política de recuperação

As políticas de recuperação são configuradas automaticamente para controladores de domínio e estações de trabalho. Por padrão, os administradores de domínio são os agentes de recuperação designados para domínios e o administrador local é o agente de recuperação designado para uma estação de trabalho autônoma.

Por meio do console da Group Policy, pode-se visualizar, atribuir e excluir os agentes de recuperação. Para isso, siga estas etapas:

1. Abra o console da Group Policy para o computador local, site, domínio ou a unidade organizacional com que queira trabalhar. Para detalhes sobre como trabalhar com a Group Policy, consulte "Group Policies" no Capítulo 4, "Automatização de tarefas administrativas, políticas e procedimentos".
2. Abra o nó Encrypted Data Recovery Agents em Group Policy. Para isso, expanda Computer Configuration, Windows Settings, Security Settings e Public Key Policies e selecione Encrypting File System.
3. O painel à direita lista os certificados de recuperação atribuídos atualmente. Os certificados de recuperação estão listados de acordo com quem os emitiu, a quem foram emitidos, data de validade, finalidade e mais.
4. Para designar um agente de recuperação adicional, pressione e segure ou clique com o botão direito do mouse em Encrypting File System e toque ou clique em Add Data Recovery Agent. O Add Data Recovery Agent Wizard será iniciado, podendo ser utilizado para selecionar um certificado gerado anteriormente que tenha sido atribuído a um usuário e marcá-lo como um certificado de recuperação designado. Toque ou clique em Next.
5. Na página Select Recovery Agents, pode-se selecionar certificados publicados no Active Directory ou utilizar arquivos de certificado. Se quiser utilizar um certificado publicado, toque ou clique em Browse Directory e – na caixa de diálogo Find Users, Contacts, And Groups – selecione o usuário com o qual quer trabalhar. Assim poderá utilizar o certificado publicado desse usuário. Se quiser utilizar um arquivo de certificado, toque ou clique em Browse Folders. Na caixa de diálogo Open, utilize as opções fornecidas para selecionar e abrir o arquivo de certificado que queira utilizar.

ALERTA DE SEGURANÇA Antes de designar agentes de recuperação adicionais, você deve considerar a configuração de uma root certificate authority (CA, autoridade de certificação raiz) no domínio. Então poderá utilizar o snap-in Certificates para gerar um certificado pessoal que utilize o modelo Recovery Agent do EFS. A CA raiz deve aprovar a solicitação do certificado a fim de que ele possa ser utilizado.

6. Para excluir um agente de recuperação, selecione o certificado dele no painel direito e pressione Delete. Quando for solicitado que confirme a ação, toque ou clique em Yes para o excluir permanente e irrevogavelmente. Se a política de recuperação estiver vazia (ou seja, não tiver qualquer outro agente de recuperação designado), o EFS será desativado, a fim de que os arquivos não possam mais ser criptografados; os recursos criptografados do EFS existentes não terão um agente de recuperação.

Descriptografia de arquivos e diretórios

O File Explorer mostra os nomes de recursos criptografados em verde. Se quiser descriptografar um arquivo ou pasta, siga estas etapas:

1. No File Explorer, pressione e segure ou clique com o botão direito do mouse no arquivo ou diretório e toque ou clique em Properties.
2. Na guia General da caixa de diálogo Properties, toque ou clique em Advanced. Desmarque a caixa de seleção Encrypt Contents To Secure Data. Toque ou clique em OK duas vezes.

Com arquivos, o Windows Server irá descriptografar o arquivo e restaurá-lo ao seu formato original. Com pastas, o Windows Server irá descriptografar todos os arquivos dentro da pasta. Se a pasta contiver subpastas, também será possível remover a criptografia delas. Para isso, selecione Apply Changes To This Folder, Subfolders, And Files quando for solicitado e toque ou clique em OK.

DICA O Windows Server também oferece um utilitário de linha de comando chamado Cipher (Cipher.exe) para criptografar e descriptografar seus dados. Digitando cipher em um prompt de comando sem parâmetros adicionais, o status de criptografia de todas as pastas no diretório atual será exibido.

CAPÍTULO 11

Configuração de volumes e matrizes RAID

- Como utilizar volumes e conjuntos de volumes **418**
- Como melhorar o desempenho e a tolerância a falhas com RAID **424**
- Implementação de RAID no Windows Server 2012 **425**
- Gerenciamento de RAID e recuperação após falhas **430**
- Gerenciamento de armazenamento baseado em padrões **433**
- Gerenciamento de partições e unidades existentes **441**

O gerenciamento de armazenamento mudou consideravelmente nos últimos anos, assim como mudaram as formas como o Microsoft Windows Server trabalha com discos. Embora as técnicas tradicionais de gerenciamento de armazenamento lidem com unidades físicas localizadas dentro do servidor, muitos servidores utilizam armazenamento anexado e discos virtuais nos dias de hoje.

Em geral, quando você trabalha com unidades internas fixas, costuma ser necessário realizar procedimentos avançados de configuração de disco, como criar um conjunto de volumes ou um RAID (Redundant Array of Independent Disks, Matriz Redundante de Discos Independentes). Nestes, são criados volumes ou arrays que podem expandir-se por diversas unidades e você sabe o layout físico exato dessas unidades.

Normalmente, quando você trabalha com armazenamento anexado, pode não saber em qual disco físico (ou discos) se encontra o volume com o qual está trabalhando. Nesse caso, ao contrário do anterior, você verá um disco virtual, também chamado de *número de unidade lógica* (LUN), que é uma referência lógica a uma parte do subsistema de armazenamento. Embora o disco virtual possa estar localizado em um ou mais discos físicos (eixos), o layout dos discos físicos é controlado separadamente do sistema operacional (pelo subsistema de armazenamento).

Quando preciso diferenciar entre as duas abordagens de gerenciamento de armazenamento, refiro-me à primeira técnica como *tradicional* (*traditional*) e à outra como *baseada em padrões* (*standards-based*). Neste capítulo, começo abordando as técnicas tradicionais para a criação de conjuntos de volumes e matrizes e passo para as técnicas baseadas em padrões para a criação de volumes. Independentemente de um volume ser criado utilizando a abordagem tradicional ou a abordagem baseada em padrões, seu gerenciamento se dá por meio de técnicas similares. Por esse motivo, na seção final deste capítulo, discuto as técnicas para trabalhar com volumes e unidades existentes.

MUNDO REAL Abordagens baseadas em padrões para gerenciamento de armazenamento também podem ser utilizadas com os discos internos de um servidor. No entanto, quando discos internos são utilizados dessa forma, os discos internos (como discos virtuais em armazenamento anexado, por exemplo) são recursos a serem alocados utilizando abordagens baseadas em padrões. Isso significa que você pode criar volumes de discos virtuais nos discos físicos, adicionar os discos físicos ao pool de armazenamento e criar discos virtuais de Internet SCSI (iSCSI) que podem ser direcionados. Também é possível habilitar a eliminação de duplicação de dados em discos virtuais. Entretanto, não é possível utilizar os recursos de conjunto de volumes ou de arrays RAID do sistema operacional. Isso se deve ao fato de que as abordagens de gerenciamento de armazenamento baseadas em padrões dependem do subsistema de armazenamento para gerenciar a arquitetura de disco físico.

Como utilizar volumes e conjuntos de volumes

Com um conjunto de volumes, é possível criar um único volume que expanda-se por diversas unidades. Os usuários podem acessar esse volume como se fosse uma unidade única, independentemente de por quantas unidades o volume está estendido. Um volume que se encontre em uma única unidade é chamado de *volume simples*. Um volume que se encontre em várias unidades é chamado de *volume estendido*.

Com uma array RAID, é possível proteger dados importantes de negócios e às vezes melhorar o desempenho das unidades. O RAID pode ser implementado utilizando os recursos internos do sistema operacional (uma abordagem de software) ou utilizando um hardware. O Windows Server dá suporte a três níveis de software RAID: 0, 1 e 5. Matrizes RAID são implementadas como volumes espelhados, distribuídos e distribuídos com paridade.

Conjuntos de volumes e matrizes RAID são criados em unidades dinâmicas, que são acessíveis somente por meio do Microsoft Windows 2000 e versões mais recentes. Entretanto, computadores com versões anteriores do Windows podem acessar as unidades por meio da rede, assim como podem acessar qualquer outra unidade da rede.

A criação e o gerenciamento de volumes ocorrem de forma muito parecida à criação e ao gerenciamento de partições. Um *volume* é uma parte de uma unidade e pode ser utilizado para armazenar dados diretamente.

OBSERVAÇÃO Em relação a volumes estendidos e distribuídos em discos básicos, é possível excluir um volume, mas não é possível criar ou estender volumes. Com volumes espelhados em discos básicos, é possível excluir, reparar e resincronizar o espelho. Você também pode quebrar o espelho. Para volumes distribuídos com paridade (RAID-5) em discos básicos, é possível excluir ou reparar o volume, mas não é possível criar novos volumes.

Noções básicas sobre volumes

O Disk Management codifica por cores os tipos de volumes, similar à maneira como codifica partições. Como mostra a Figura 11-1, os volumes também têm as seguintes propriedades:

- **Layout** Layouts de volumes incluem simples, estendido, distribuído e distribuído com paridade.
- **Tipo** Os volumes podem ser do tipo *dinâmico* e *básico*.
- **Sistema de arquivos** Assim como as partições, cada volume pode ter um tipo de sistema de arquivos diferente, como o sistema de arquivos NTFS ou o FAT.

Perceba que o FAT16 só torna-se disponível quando a partição ou volume tiver tamanho menor ou igual a 2GB.

- **Status** O estado da unidade. Em Graphical View, o estado é indicado como Healthy, Failed Redundancy e assim por diante. A próxima seção, "Sobre conjuntos de volumes", discute conjuntos de volumes e os vários estados possíveis.
- **Capacidade** O tamanho total de armazenamento da unidade.
- **Espaço livre** O espaço disponível total no volume.
- **% disponível** A porcentagem de espaço livre em relação ao tamanho total de armazenamento do volume.

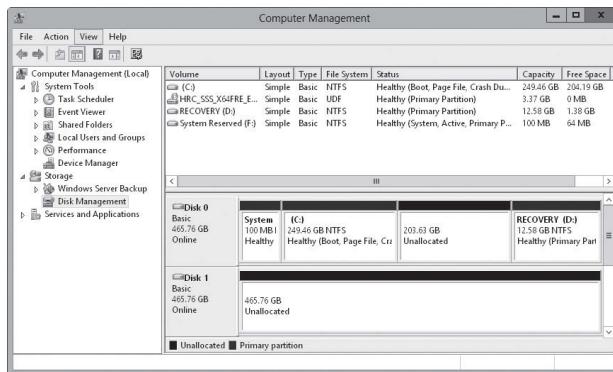


FIGURA 11-1 O Disk Management exibe volumes de maneira parecida com a qual exibe partições.

Uma vantagem importante dos volumes dinâmicos em relação aos volumes básicos é que eles possibilitam realizar alterações nos volumes e unidades sem ser necessário reiniciar o sistema (na maioria dos casos). Volumes também permitem que você aproveite as melhorias na tolerância a falhas do Windows Server 2012. Você pode instalar outros sistemas operacionais e realizar uma inicialização dupla do sistema Windows Server 2012. Para isso, é preciso criar um volume em separado para o outro sistema operacional. Por exemplo, você poderia instalar o Windows Server 2012 no volume C e o Windows 8 no volume D.

Com volumes, é possível:

- Atribuir letras de unidade e caminhos de unidade como discutido em "Como atribuir letras e caminhos de unidade", adiante neste capítulo
- Criar qualquer quantia de volumes em um disco contanto que haja espaço livre
- Criar volumes que estendem-se por dois ou mais discos e, se necessário, configurar a tolerância a falhas
- Estender volumes para aumentar a capacidade desses volumes
- Designar volumes ativo, de inicialização e de sistema, como descrito em "Considerações especiais para discos básicos e dinâmicos", no Capítulo 10, "Gerenciamento de sistemas de arquivos e unidades"

Sobre conjuntos de volumes

Com conjuntos de volumes, você pode criar volumes que estendem-se por diversas unidades. Para isso, você utiliza espaço livre em diferentes unidades para criar o que os usuários verão como um único volume. Os arquivos são armazenados no conjunto de volumes segmento por segmento, com o primeiro segmento de espaço livre sendo utilizado para armazenar arquivos antes dos outros segmentos. Quando o primeiro segmento estiver preenchido, o segundo segmento será utilizado, e assim por diante.

É possível criar um conjunto de volumes utilizando o espaço livre de até 32 unidades de disco rígido. A principal vantagem dos conjuntos de volumes é que eles permitem que você toque em um espaço livre disponível e crie um sistema de arquivos utilizável. A principal desvantagem é que se uma das unidades de disco rígido no conjunto de volumes falhar, o conjunto de volumes não poderá mais ser utilizado; ou seja, todos os dados do conjunto de volumes serão perdidos.

Compreender o estado do volume é útil durante a instalação de novos volumes ou quando se está tentando solucionar problemas. O Disk Management indica o estado da unidade no Graphical View e no Volume List View. A Tabela 11-1 resume as características dos possíveis estados dos volumes dinâmicos.

TABELA 11-1 Sobre problemas de estados de volumes e como resolvê-los

STATUS	DESCRIÇÃO	RESOLUÇÃO
Data Incomplete	Volumes estendidos em um disco externo estão incompletos. Você deve ter esquecido de adicionar os outros discos do conjunto de volumes estendidos.	Adicione os discos que contêm o resto do volume estendido e então importe todos os discos de uma só vez.
Data Not Redundant	Volumes tolerantes a falhas em um disco externo estão incompletos. Você deve ter esquecido de adicionar os outros discos de um conjunto de espelhos ou de RAID-5.	Adicione os discos que faltam e então importe todos os discos de uma só vez.
Failed	Erro de disco. O disco está inacessível ou danificado.	Certifique-se de que o disco dinâmico relacionado está online. Se necessário, pressione e mantenha pressionado ou clique com o botão direito do mouse no volume e então toque ou clique em Reactivate Volume. Para um disco básico, talvez seja necessário checar se há falha na conexão.
Failed Redundancy	Erro de disco. Um dos discos em um conjunto de espelhos ou de RAID-5 está offline.	Certifique-se de que o disco dinâmico relacionado está online. Se necessário, reactive o volume. Em seguida, talvez seja necessário substituir um espelho com falha ou reparar um volume RAID-5 com falha.

STATUS	DESCRIÇÃO	RESOLUÇÃO
Formatting	Estado temporário que indica que o volume está sendo formatado.	O progresso da formatação é indicado pela porcentagem concluída, a menos que você escolha a opção Perform A Quick Format.
Healthy	Estado normal de volume.	O volume não possui problema conhecido. Não é preciso tomar uma medida corretiva.
Healthy (At Risk)	O Windows encontrou problemas na leitura ou gravação do disco físico no qual o volume dinâmico está alocado. Esse estado aparece quando o Windows encontra erros.	Pressione e mantenha pressionado ou clique com o botão direito do mouse no volume e então toque ou clique em Reactivate Volume. Se o disco continuar com esse estado ou adquirir esse estado periodicamente, o disco pode estar falhando e você deve fazer o backup de todos os dados contidos nele.
Healthy (Unknown Partition)	O Windows não reconhece a partição. Isso pode ocorrer porque a partição pertence a um sistema operacional diferente ou porque é uma partição criada pelo fabricante e utilizada para armazenar arquivos do sistema.	Não é necessário realizar ação corretiva.
Initializing	Estado temporário que indica que o disco está sendo inicializado.	O estado da unidade deve mudar depois de alguns segundos.
Regenerating	Estado temporário que indica que os dados e a paridade do volume RAID-5 estão sendo regenerados.	O progresso é indicado por meio da porcentagem concluída. O volume deve retornar ao estado Healthy.
Resynching	Estado temporário que indica que um conjunto de espelhos está sendo ressincronizado.	O progresso é indicado por meio da porcentagem concluída. O volume deve retornar ao estado Healthy.
Stale Data	Dados em discos externos que são tolerantes a falhas estão dessincronizados.	Examine novamente os discos ou reinicie o computador e verifique o estado. Um novo estado deve ser exibido, como Failed Redundancy.
Unknown	O volume não pode ser acessado. Ele pode ter o setor de inicialização corrompido.	O volume pode ter um vírus em um setor de inicialização. Verifique isso com um programa antivírus atualizado. Examine novamente os discos ou reinicie o computador e verifique o estado.

Como criar volumes e conjuntos de volumes

Você pode formatar volumes simples como exFAT, FAT, FAT32 ou NTFS. Para facilitar o gerenciamento, recomenda-se formatar com NTFS os volumes para que eles possam ser estendidos por vários discos. A formatação NTFS permite que você expanda o conjunto de volumes caso necessário. Se achar que precisa de mais espaço em um volume, você pode expandir volumes simples e estendidos. Basta selecionar uma área do espaço livre e adicioná-la ao volume. Você pode expandir um volume simples dentro do mesmo disco. Também pode expandir um volume simples para outros discos. Ao fazer isso, você cria um volume estendido, e deve formatá-lo como NTFS.

Para criar volumes e conjuntos de volumes, siga estas etapas:

1. Em Graphical View, no Disk Management, pressione e mantenha pressionado ou clique com o botão direito em uma área não alocada; toque ou clique em New Spanned Volume ou New Striped Volume, conforme apropriado. Leia a página Welcome e toque ou clique em Next.
2. Deve aparecer a página Select Disks, como mostra a Figura 11-2. Selecione os discos desejados para que façam parte do volume e dimensione os segmentos do volume nesses discos.

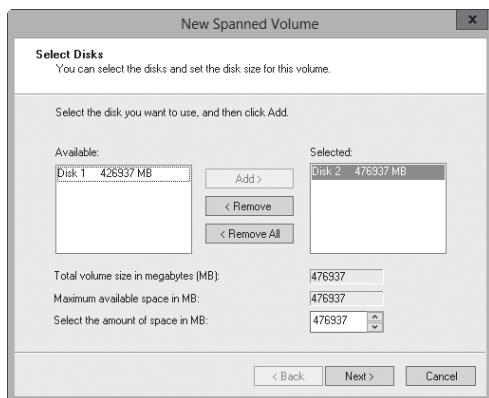


FIGURA 11-2 Na página Select Disks, selecione os discos que farão parte do volume; dimensione o volume em cada disco.

3. Os discos disponíveis são mostrados na lista Available. Se necessário, selecione um disco da lista e toque ou clique em Add para adicionar o disco à lista Selected. Se cometer um erro, pode remover os discos da lista Selected selecionando o disco e tocando ou clicando em Remove.

ATENÇÃO Os assistentes de disco no Windows Server 2012 mostram tanto os discos básicos quanto os discos dinâmicos com espaço em disco disponível. Se você adicionar espaço de um disco básico, o assistente transformará o disco em disco dinâmico antes de criar o conjunto de volumes. Antes de tocar ou clicar em Yes para continuar, certifique-se de que realmente deseja realizar essa ação, pois ela pode afetar a forma como o disco é utilizado pelo sistema operacional.

4. Selecione um disco da lista Selected e especifique o tamanho do volume em disco na caixa Select The Amount Of Space In MB. A caixa Maximum Available Space In MB mostra a maior área de espaço livre disponível no disco. A caixa Total Volume Size In Megabytes mostra o espaço total do disco selecionado para uso com o volume. Toque ou clique em Next.

DICA Embora você possa dimensionar o conjunto de volumes da forma que achar melhor, considere como irá utilizar conjuntos de volumes no sistema. Volumes simples e estendidos não têm tolerância a falhas; em vez de criar um volume gigantesco com todo o espaço livre disponível, recomenda-se criar diversos volumes menores para ajudar a garantir que perder um volume não signifique perder todos os dados.

5. Especifique se deseja atribuir uma letra ou caminho de unidade ao volume, então toque ou clique em Next. Existem as seguintes opções:

- **Assign The Following Drive Letter** Para atribuir uma letra de unidade, escolha esta opção e selecione uma letra de unidade disponível na lista fornecida.
- **Mount In The Following Empty NTFS Folder** Para atribuir um caminho de unidade, escolha esta opção e digite o caminho para uma pasta existente na unidade NTFS, ou toque ou clique em Browse para buscar ou criar uma pasta.
- **Do Not Assign A Drive Letter Or Drive Path** Para criar o volume sem atribuir uma letra ou caminho de unidade, escolha esta opção. É possível atribuir uma letra ou caminho de unidade mais tarde, se necessário.

6. Especifique se o volume deve ser formatado. Se escolher formatar um volume, configure as seguintes opções de formatação:

- **File System** Especifica o tipo de sistema de arquivos. O sistema de arquivos NTFS é a única opção dentro do Disk Management.
- **Allocation Unit Size** Especifica o tamanho do cluster para o sistema de arquivos. Esta é a unidade básica na qual o espaço em disco é alocado. O tamanho padrão da unidade de alocação é baseado no tamanho do volume e é definido dinamicamente antes da formatação. Para substituir esse recurso, pode-se definir o tamanho da unidade de alocação com um valor específico. Se utilizar diversos arquivos pequenos, recomenda-se usar um tamanho de cluster menor, como de 512 ou 1024 bytes. Com essa configuração, os arquivos pequenos utilizam menos espaço em disco.
- **Volume Label** Especifica um rótulo para a partição. Esse rótulo é o nome do volume.
- **Perform A Quick Format** Deixa que o Windows realize uma formatação rápida sem verificar erros na partição. Com partições grandes, esta opção pode economizar alguns minutos do seu trabalho. Entretanto, é mais prudente verificar erros, o que possibilita que o Disk Management marque setores defeituosos no disco e bloqueeie-os.
- **Enable File And Folder Compression** Ativa a compactação do disco. A compactação é transparente para os usuários, e os arquivos compactados podem ser acessados da mesma forma que os arquivos normais. Caso selecione esta opção, os arquivos e diretórios nesta unidade serão compactados automaticamente. Para mais informações sobre a compactação de unidades, arquivos e diretórios, consulte "Compactação de unidades e dados" no Capítulo 10.

7. Toque ou clique em Next e em Finish.

Como excluir volumes e conjuntos de volumes

Usa-se a mesma técnica para excluir todos os tipos de volumes, ou seja, para volumes estendidos, espelhados, distribuídos ou RAID-5 (distribuídos com paridade). Ao excluir um conjunto de volumes, o sistema de arquivos associado também é excluído e todos os dados são perdidos. Antes de excluir um conjunto de volumes, deve-se fazer o backup de todos os arquivos e diretórios contidos no conjunto de volumes.

Não é possível excluir um volume que contenha arquivos de paginação, de sistema, de inicialização ou de ativação do Windows Server 2012.

Para excluir volumes, siga estas etapas:

1. No Disk Management, pressione e mantenha pressionado ou clique com o botão direito em qualquer volume do conjunto, então toque ou clique em Delete Volume. Não há como excluir uma parte de um volume estendido sem excluir o volume inteiro.
2. Toque ou clique em Yes para confirmar que deseja excluir o volume.

Gerenciamento de volumes

O gerenciamento de volumes se dá de forma muito similar ao gerenciamento de partições. Siga as técnicas descritas em “Gerenciamento de partições e unidades existentes”, adiante neste capítulo.

Como melhorar o desempenho e a tolerância a falhas com RAID

Muitas vezes, você desejará dar atenção especial à proteção de dados importantes para que não sejam vítimas de falhas em uma unidade. Para isso, pode utilizar a tecnologia RAID e com ela adicionar tolerância a falhas aos seus sistemas de arquivos. Com a tecnologia RAID, a integridade e disponibilidade dos dados são aumentadas, pois são criadas cópias redundantes dos dados. A tecnologia RAID também pode ser utilizada para aumentar o desempenho de discos.

Há diferentes implementações disponíveis da tecnologia RAID. Essas implementações são descritas em termos de níveis. Atualmente, são definidos os níveis 0 a 5 de RAID. Cada nível de RAID apresenta recursos diferentes. O Windows Server 2012 dá suporte aos níveis 0, 1 e 5 de RAID. O RAID-0 pode ser utilizado para melhorar o desempenho das unidades. O RAID-1 e o RAID-5 são utilizados para fornecer tolerância a falhas aos dados.

A Tabela 11-2 fornece uma breve visão geral dos níveis de RAID suportados. Esse suporte é completamente baseado em software.

Os níveis mais comuns de RAID em uso em servidores com Windows Server 2012 são o nível 1 (espelhamento de disco) e o nível 5 (faixa de disco com paridade). Em relação a custos iniciais, o espelhamento de disco é a forma mais econômica de aumentar a proteção de dados com redundância. Nesse caso, dois volumes de tamanhos idênticos são utilizados em duas unidades diferentes para criar um conjunto de dados redundante. Caso uma das unidades falhe, ainda há como obter os dados usando a outra unidade.

Por outro lado, a faixa de disco com paridade requer mais discos (um mínimo de três), mas oferece tolerância a falhas com menos sobrecarga que o espelhamento de disco. Caso uma das unidades falhe, é possível recuperar os dados combinando blocos de dados nos discos restantes com um registro de paridade. A paridade é um método

de verificação de erros que utiliza uma operação OR exclusiva para criar uma soma de verificação para cada bloco de dados gravado em um disco. Essa soma de verificação é utilizada para recuperar dados em caso de falha.

TABELA 11-2 Suporte do Windows Server 2012 para RAID

NÍVEL DE RAID	TIPO DE RAID	DESCRIÇÃO	PRINCIPAIS VANTAGENS
0	Faixa de disco	Dois ou mais volumes, cada um em uma unidade diferente, são configurados como um conjunto distribuído. Os dados são divididos em blocos, chamados de <i>faixas</i> , e então gravados sequencialmente em todas as unidades do conjunto distribuído.	Velocidade e desempenho.
1	Espelhamento de disco	Duas ou mais unidades são configuradas de forma idêntica. Os dados são gravados nas duas unidades. Se uma unidade falhar, não ocorre perda de dados porque a outra unidade contém os dados. (Esse nível não inclui faixa de disco.)	Redundância. Melhor desempenho de gravação do que a faixa de disco com paridade.
5	Faixa de disco com paridade	Utiliza três ou mais volumes, cada um em uma unidade separada, para criar um conjunto distribuído com verificação de erros por meio de paridade. No caso de falha, os dados podem ser recuperados.	Tolerância a falhas com menos sobrecarga que o espelhamento. Melhor desempenho de leitura do que o espelhamento de disco.

MUNDO REAL Embora seja verdade que os custos iniciais do espelhamento sejam menores do que os custos iniciais da faixa de disco com paridade, o custo real por gigabyte pode ser maior com o espelhamento de disco. Com o espelhamento de disco, há uma sobrecarga de 50%. Por exemplo, se você espelhar duas unidades de 750 GB (um total de espaço de armazenamento de 1500 GB), o espaço para uso é de apenas 750 GB. Com a faixa de disco com paridade, por outro lado, há uma sobrecarga de aproximadamente 33%. Por exemplo, se você criar um conjunto de RAID-5 utilizando três unidades de 500 GB (um total de espaço de armazenamento de 1500 GB), o espaço para uso (com um terço perdido em sobrecarga) é de 1000 GB.

Implementação de RAID no Windows Server 2012

O Windows Server 2012 dá suporte ao espelhamento de disco, à faixa de disco e à faixa de disco com paridade. A implementação dessas técnicas de RAID é discutida nas seções a seguir.

ATENÇÃO Alguns sistemas operacionais, como o MS-DOS, não dão suporte à tecnologia RAID. Se você configurar uma inicialização dupla para seu sistema utilizando um desses sistemas operacionais incompatíveis, suas unidades configuradas como RAID ficarão indisponíveis.

Implementação do RAID-0: Faixa de disco

O nível 0 de RAID equivale à faixa de disco. Na faixa de disco, dois ou mais volumes (cada um em uma unidade diferente) são configurados como um conjunto distribuído. Os dados gravados no conjunto distribuído são divididos em blocos chamados de *faixas*. Essas faixas são gravadas sequencialmente em todas as unidades do conjunto distribuído. É possível colocar volumes de um conjunto distribuído em até 32 unidades, mas na maioria das vezes, conjuntos de dois a cinco volumes apresentam o melhor desempenho. Com um número de volumes maior que esse, a melhoria de desempenho diminui significativamente.

A maior vantagem da faixa de disco é a velocidade. Os dados podem ser acessados em diversos discos utilizando diversas cabeças de unidades, o que melhora o desempenho consideravelmente. Entretanto, essa melhoria no desempenho tem um preço. Como ocorre com conjuntos de volumes, se uma das unidades de disco rígido no conjunto distribuído falhar, o conjunto distribuído não poderá mais ser utilizado, ou seja, todos os dados do conjunto de volumes serão perdidos. Você precisará recriar o conjunto distribuído e restaurar os dados a partir de backups. A restauração e a recuperação de dados são discutidas no Capítulo 13, "Backup e recuperação de dados".

ATENÇÃO Os volumes de inicialização e de sistema não devem fazer parte de um conjunto distribuído. Não utilize faixa de disco com esses volumes.

Ao criar conjuntos distribuídos, utilize volumes que tenham tamanhos iguais. O Disk Management estima o tamanho total de um conjunto distribuído baseando-se no volume de menor tamanho. Especificamente, o tamanho máximo de um conjunto distribuído é um múltiplo do volume de menor tamanho. Por exemplo, se o menor volume tiver 20 GB e você quiser criar um conjunto distribuído com três volumes, o tamanho máximo do conjunto distribuído será 60 GB.

Para melhorar o desempenho do conjunto distribuído, você pode:

- Utilizar discos que estejam em controladores de disco diferentes. Isso permite que o sistema acesse as unidades simultaneamente.
- Não utilizar os discos com o conjunto distribuído para outros fins. Isso permite que o disco dedique seu tempo ao conjunto distribuído.

Para criar um conjunto distribuído, siga estas etapas:

1. No Graphical View do Disk Management, pressione e segure ou clique com o botão direito do mouse em uma área não alocada de um disco dinâmico, então toque ou clique em New Striped Volume. Isso iniciará o assistente New Striped Volume. Leia a página Welcome e toque ou clique em Next.
2. Crie um volume como descrito em "Como criar volumes e conjuntos de volumes" anteriormente neste capítulo. A principal diferença é que você precisa de pelo menos dois discos dinâmicos para criar um conjunto distribuído.

Após criar um volume distribuído, você pode utilizar o volume como utilizaria qualquer outro tipo de volume. Não é possível estender um conjunto distribuído após criá-lo. Portanto, considere cuidadosamente a configuração antes de implementá-lo.

Implementação do RAID-1: Espelhamento de disco

O nível 1 de RAID equivale ao espelhamento de disco. Nesse caso, volumes com tamanhos idênticos são utilizados em duas unidades diferentes para criar um conjunto de dados redundantes. As unidades são gravadas com conjuntos de informações idênticos, e se uma das unidades falhar, os dados ainda podem ser obtidos a partir da outra unidade.

O espelhamento de disco oferece aproximadamente a mesma tolerância a falhas que a faixa de disco com paridade. Como discos espelhados não precisam gravar informações de paridade, podem apresentar um melhor desempenho de gravação na maioria dos casos. Entretanto, a faixa de disco com paridade geralmente oferece um melhor desempenho de leitura porque as operações de leitura estão espalhadas em diversas unidades.

A principal desvantagem do espelhamento de disco é que ele reduz pela metade o espaço de armazenamento. Por exemplo, para espelhar uma unidade de 500 GB, você precisa de outra unidade de 500 GB. Isso significa que você utiliza um espaço de 1000 GB para armazenar 500 GB de informações.

DICA Se possível, recomenda-se espelhar os volumes de inicialização e de sistema. O espelhamento desses volumes garante que você consiga inicializar o servidor em caso de falha de uma única unidade.

Como ocorre com a faixa de disco, é recomendável que os discos espelhados encontrem-se em controladores de disco diferentes. Isso fornece proteção extra contra falhas do controlador de disco. Se um dos controladores de disco falhar, o disco no outro controlador ainda estará disponível. Tecnicamente, ao utilizar dois controladores de disco diferentes para duplicar dados, você está utilizando uma técnica conhecida como *duplicação de disco*. A Figura 11-3 mostra a diferença entre as duas técnicas. Enquanto o espelhamento de disco usa, normalmente, um único controlador de unidade, a duplicação de disco utiliza dois controladores de unidade. Exceto isso, as duas técnicas são essencialmente iguais.

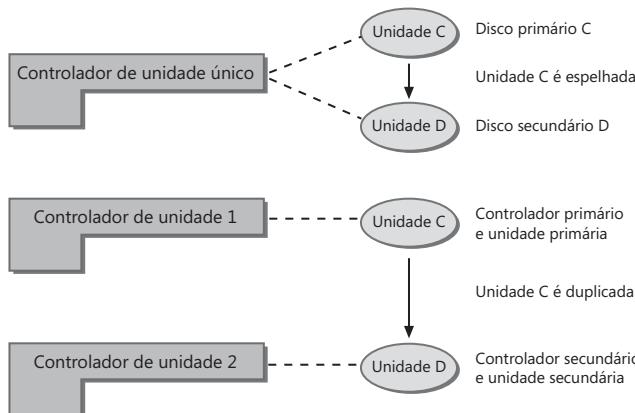


FIGURA 11-3 Embora o espelhamento de disco costume utilizar um único controlador de unidade para criar um conjunto de dados redundantes, a duplicação de disco utiliza dois controladores de unidade.

Se uma das unidades espelhadas de um conjunto falhar, as operações de disco podem continuar. Aqui, quando usuários leem e gravam dados, os dados são gravados no disco remanescente. É preciso quebrar o espelho antes de corrigi-lo. Para aprender como, consulte "Gerenciamento de RAID e recuperação após falhas" adiante neste capítulo.

Como criar um conjunto de espelhos no Disk Management

Para criar um conjunto de espelhos, siga estas etapas:

1. No Graphical View do Disk Management, pressione e segure ou clique com o botão direito do mouse em uma área não alocada de um disco dinâmico, então toque ou clique em New Mirrored Volume. Isso iniciará o New Mirrored Volume Wizard. Leia a página Welcome e toque ou clique em Next.
2. Crie um volume como descrito em "Como criar volumes e conjuntos de volumes" anteriormente neste capítulo. A principal diferença é que você precisa criar dois volumes de tamanhos idênticos, sendo que esses volumes devem estar em unidades dinâmicas diferentes. Não será possível continuar o processo após a janela Select Disks até que selecione os dois discos com os quais deseja trabalhar.

Como outras técnicas de RAID, o espelhamento é transparente aos usuários. Os usuários veem o conjunto espelhado como uma unidade única que podem acessar e utilizar como o fazem com qualquer outra unidade.

OBSERVAÇÃO O estado normal de um espelho é Healthy. Durante o processo de criação de um espelho, aparecerá o estado Resynching para informar que o Disk Management está criando o espelho.

Como espelhar um volume existente

Em vez de criar um novo volume espelhado, é possível utilizar um volume existente para criar um conjunto espelhado. Para isso, o volume que deseja espelhar deve ser um volume simples e deve existir uma área de espaço não alocado em uma segunda unidade dinâmica de tamanho igual ou maior ao tamanho do volume existente.

Siga estas etapas para espelhar um volume existente utilizando o Disk Management:

1. Pressione e mantenha pressionado ou clique com o botão direito do mouse no volume simples que deseja espelhar, então toque ou clique em Add Mirror. A caixa de diálogo Add Mirror será exibida.
2. Na lista Disks, mostrada na Figura 11-4, selecione um local para o espelho e toque ou clique em Add Mirror. O Windows Server 2012 começará o processo de criação do espelho. Em Disk Management, aparecerá o estado Resynching em ambos os volumes. O disco no qual o volume espelhado estiver sendo criado terá um ícone de aviso.

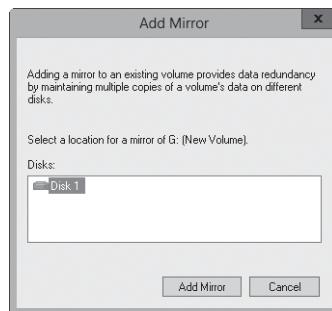


FIGURA 11-4 Selecione o local para o espelho.

Implementação do RAID-5: Faixa de disco com paridade

O nível 5 de RAID equivale à faixa de disco com paridade. Para essa técnica, você precisa de no mínimo três unidades de disco rígido para estabelecer tolerância a falhas. O Disk Management distribui os volumes igualmente nessas unidades.

O RAID-5 é essencialmente uma versão aprimorada do RAID-0, com a vantagem adicional da tolerância a falhas. A tolerância a falhas garante que a falha de uma única unidade não irá parar o conjunto inteiro de unidades. Em vez disso, o conjunto continua a funcionar com as operações de disco dirigidas aos volumes remanescentes do conjunto.

Para possibilitar a tolerância a falhas, o RAID-5 grava somas de verificação de paridade com os blocos de dados. Se uma das unidades do conjunto distribuído falhar, você pode utilizar as informações de paridade para recuperar os dados. (Esse processo, chamado de *regeneração do conjunto distribuído*, é abordado em “Gerenciamento de RAID e recuperação após falhas” adiante neste capítulo.) Entretanto, se dois discos falharem, as informações de paridade não são o suficiente para recuperar os dados, e é necessário recuperar o conjunto distribuído por meio de backup.

Como criar um conjunto distribuído com paridade no Disk Management

Para criar um conjunto distribuído com paridade por meio do Disk Management, siga estas etapas:

1. No Graphical View do Disk Management, pressione e segure ou clique com o botão direito do mouse em uma área não alocada de um disco dinâmico, então toque ou clique em New RAID-5 Volume. O New RAID 5 Volume Wizard será iniciado. Leia a página Welcome e toque ou clique em Next.
2. Crie o volume como descrito em “Como criar volumes e conjuntos de volumes”. A principal diferença é que você precisa selecionar espaço livre nas três unidades dinâmicas.

Após criado um conjunto distribuído com paridade (RAID-5), os usuários poderão utilizar o conjunto como utilizam uma unidade normal. Lembre-se de que não é possível expandir um conjunto distribuído com paridade após criá-lo. Portanto, considere cuidadosamente a configuração antes de implementá-lo.

Gerenciamento de RAID e recuperação após falhas

O gerenciamento de unidades espelhadas e de conjuntos distribuídos é um pouco diferente do gerenciamento de outros volumes de unidade, especialmente quando se trata de recuperação após falhas. As técnicas utilizadas para gerenciar matrizes RAID e para recuperação após falhas são discutidas nesta seção.

Como quebrar um conjunto espelhado

Pode ser desejável quebrar um espelho em duas situações:

- Se uma das unidades espelhadas de um conjunto falhar, as operações de disco podem continuar. Quando os usuários leem e gravam dados, essas operações utilizam o disco remanescente. Entretanto, em algum momento, você precisa corrigir o espelho, e para isso precisa primeiramente quebrar o espelho e substituir a unidade defeituosa para então restabelecer o espelho.
- Se você não quiser mais espelhar suas unidades, talvez também seja recomendável quebrar um espelho. Isso permitirá que você utilize o espaço em disco para outros fins.

PRÁTICAS RECOMENDADAS Embora quebrar um espelho não exclua os dados de um conjunto, deve-se sempre fazer backup dos dados antes de realizar esse procedimento. Isso garante que se houver problemas, os dados podem ser recuperados.

Para quebrar um conjunto espelhado por meio do Disk Management, siga estas etapas:

1. Pressione e mantenha pressionado ou clique com o botão direito do mouse em um dos volumes do conjunto espelhado; toque ou clique em Break Mirrored Volume.
2. Confirme que você deseja quebrar o espelho tocando ou clicando em Yes. Se o volume estiver em uso, surgirá uma outra caixa de diálogo de aviso. Confirme para continuar tocando ou clicando em Yes.

O Windows Server 2012 quebrará o espelho, criando dois volumes independentes.

Como ressincronizar e reparar um conjunto espelhado

O Windows Server 2012 sincroniza automaticamente os volumes espelhados em unidades dinâmicas. Entretanto, os dados nas unidades espelhadas podem ficar fora de sincronia. Por exemplo, se uma das unidades ficar offline, os dados são gravados somente na unidade que estiver online.

Você pode ressincronizar e reparar conjuntos espelhados, mas precisa recompor o conjunto utilizando discos com o mesmo estilo de partição: registro mestre de inicialização (MBR) ou tabela de partição GUID (GPT). É preciso fazer com que as duas unidades do conjunto espelhado fiquem online. O estado do conjunto espelhado provavelmente será Failed Redundancy. A ação corretiva escolhida dependerá do estado do volume defeituoso:

- Se o estado for Missing ou Offline, certifique-se de que a unidade tem energia e está conectada apropriadamente. Inicie o Disk Management, pressione e mantenha pressionado ou clique com o botão direito do mouse no volume defeituoso e toque ou clique em Reactivate Volume. O estado da unidade deverá mudar para

Regenerating e depois para Healthy. Se o volume não voltar para o estado Healthy, pressione e mantenha pressionado ou clique com o botão direito do mouse no volume, então toque ou clique em Resynchronize Mirror.

- Se o estado atual for Online (Errors), pressione e mantenha pressionado ou clique com o botão direito do mouse no volume defeituoso, então toque ou clique em Reactivate Volume. O estado da unidade deverá mudar para Regenerating e depois para Healthy. Se o volume não voltar para o estado Healthy, pressione e mantenha pressionado ou clique com o botão direito do mouse no volume, então toque ou clique em Resynchronize Mirror.
- Se o estado atual de uma das unidades for Unreadable, talvez seja necessário examinar novamente as unidades do sistema escolhendo a opção Rescan Disks no menu Action do Disk Management. Se o status da unidade não mudar, talvez seja preciso reinicializar o computador.
- Se uma das unidades ainda não voltar para o estado online, pressione e mantenha pressionado ou clique com o botão direito do mouse no volume defeituoso, então toque ou clique em Remove Mirror. A seguir, pressione e mantenha pressionado ou clique com o botão direito do mouse no volume remanescente no espelho original, então toque ou clique em Add Mirror. Agora é preciso espelhar o volume em uma área de espaço livre não alocado. Se não houver espaço livre, é preciso criar espaço por meio da exclusão de outros volumes ou por substituição da unidade defeituosa.

Como reparar um volume de sistema espelhado para habilitar inicialização

A falha de uma unidade espelhada pode impedir a inicialização do sistema. Normalmente, isso ocorre quando você está espelhando o volume de sistema ou de inicialização, ou ambos, e a unidade espelhada principal falha. Em versões anteriores do sistema operacional Windows, muitas vezes era preciso realizar diversos procedimentos para colocar o sistema em funcionamento novamente. Com o Windows Server 2012, a falha de um espelho principal costuma ser muito mais fácil de resolver.

Quando você espelha um volume de sistema, o sistema operacional deve adicionar uma entrada para o gerenciador de inicialização do sistema que permite a você inicializar a partir do segundo membro do espelho. Resolver uma falha no espelho principal é muito mais fácil com essa entrada no arquivo gerenciador de inicialização do que sem ela, pois tudo o que precisa fazer é selecionar a entrada para inicializar a partir do segundo espelho. Se você espelhar o volume de inicialização e uma segunda entrada espelhada não for criada, você pode modificar as entradas de inicialização no gerenciador de inicialização para criar uma entrada por meio do BCD Editor (Bcdedit.exe).

Se o sistema falhar em inicializar a partir do volume de sistema principal, reinicie o sistema e selecione a opção Windows Server 2012 – Secondary Plex para o sistema operacional que deseja iniciar. O sistema deve iniciar normalmente. Após inicializar o sistema com sucesso a partir da segunda unidade, é possível agendar a manutenção necessária para recompilar o espelho. Para isso, siga estas etapas:

1. Desligue o sistema e substitua o volume defeituoso ou adicione uma unidade de disco rígido. Reinicie o sistema.
2. Quebre o conjunto de espelhos e recrie o espelho na unidade substituída, que geralmente corresponde à unidade 0. Pressione e mantenha pressionado ou cli-

que com o botão direito do mouse no volume remanescente do espelho original, então toque ou clique em Add Mirror. A seguir, siga a técnica de "Como espelhar um volume existente" anteriormente neste capítulo.

3. Se quiser que o espelho principal esteja na unidade adicionada ou substituída, utilize o Disk Management para quebrar o espelho novamente. Certifique-se de que a unidade principal no conjunto de espelhos original tem a letra de unidade que foi anteriormente atribuída ao espelho completo. Se não tiver, atribua a letra de unidade apropriada.
4. Pressione e mantenha pressionado ou clique com o botão direito do mouse no volume de sistema original, então toque ou clique em Add Mirror. Agora, recrie o espelho.
5. Verifique as entradas de inicialização no gerenciador de inicialização e utilize o BCD Editor para garantir que o volume de sistema original seja utilizado durante a inicialização.

Como remover um conjunto espelhado

Por meio do Disk Management, é possível remover um dos volumes de um conjunto espelhado. Ao fazer isso, todos os dados desse espelho removido são excluídos e o espaço que era utilizado é marcado como não alocado.

Para remover um espelho, siga estas etapas:

1. No Disk Management, pressione e mantenha pressionado ou clique com o botão direito do mouse em um dos volumes do conjunto espelhado; toque ou clique em Remove Mirror. A caixa de diálogo Remove Mirror será exibida.
2. Na caixa de diálogo Remove Mirror, selecione o disco do qual deseja remover o espelho.
3. Confirme a ação quando for solicitado. Todos os dados do espelho removido são excluídos.

Como reparar um conjunto distribuído sem paridade

Conjuntos distribuídos sem paridade não têm tolerância a falhas. Se uma unidade que faz parte de um conjunto distribuído falhar, o conjunto distribuído inteiro torna-se inutilizável. Antes de tentar restaurar um conjunto distribuído, é preciso reparar ou substituir a unidade defeituosa. Então, é preciso recriar o conjunto distribuído e recuperar os dados contidos no conjunto distribuído utilizando o backup.

Como regenerar um conjunto distribuído com paridade

Com o RAID-5, é possível recuperar o conjunto distribuído com paridade se uma única unidade falhar. Você saberá que uma unidade de um conjunto distribuído com paridade falhou quando o estado do conjunto for alterado para Failed Redundancy e o estado de um volume individual for alterado para Missing, Offline ou Online (Errors).

Você pode reparar os discos do RAID-5, mas precisa recompilar o conjunto utilizando discos com o mesmo estilo de partição: MBR ou GPT. É preciso fazer com que todas as unidades do conjunto RAID-5 fiquem online. O estado do conjunto deverá aparecer como Failed Redundancy. A ação corretiva escolhida dependerá do estado do volume defeituoso:

- Se o estado for Missing ou Offline, certifique-se de que a unidade tem energia e está conectada apropriadamente. Inicie o Disk Management, pressione e mantenha pressionado ou clique com o botão direito do mouse no volume defeituoso e toque ou clique em Reactivate Volume. O estado da unidade deverá mudar para Regenerating e depois para Healthy. Se o estado da unidade não retornar para Healthy, pressione e mantenha pressionado ou clique com o botão direito do mouse no volume e selecione Regenerate Parity.
- Se o estado atual for Online (Errors), pressione e mantenha pressionado ou clique com o botão direito do mouse no volume defeituoso, então toque ou clique em Reactivate Volume. O estado da unidade deverá mudar para Regenerating e depois para Healthy. Se o estado da unidade não retornar para Healthy, pressione e mantenha pressionado ou clique com o botão direito do mouse no volume e selecione Regenerate Parity.
- Se o estado atual de uma das unidades for Unreadable, talvez seja necessário examinar novamente as unidades do sistema escolhendo a opção Rescan Disks no menu Action do Disk Management. Se o status da unidade não mudar, talvez seja preciso reinicializar o computador.
- Se uma das unidades ainda não retornar ao estado online, é preciso reparar a região defeituosa do conjunto RAID-5. Pressione e mantenha pressionado ou clique com o botão direito do mouse no volume defeituoso e toque ou clique em Remove Volume. Agora, é preciso selecionar um espaço não alocado em um disco dinâmico diferente para o conjunto RAID-5. Esse espaço deve ser pelo menos tão grande quanto a região a ser reparada e não pode encontrar-se em uma unidade que o conjunto RAID-5 já esteja utilizando. Se não houver espaço livre suficiente, o comando Repair Volume estará indisponível, e é preciso criar espaço livre por meio da exclusão de outros volumes ou por substituição da unidade defeituosa.

PRÁTICAS RECOMENDADAS Se possível, recomenda-se fazer backup dos dados antes de realizar esse procedimento. Isso garante que se houver problemas, os dados possam ser recuperados.

Gerenciamento de armazenamento baseado em padrões

O gerenciamento de armazenamento baseado em padrões foca nos próprios volumes de armazenamento em vez de focar no layout físico subjacente; conta que o hardware lide com as particularidades de arquitetura em relação à redundância de dados e às porções de discos que apresentam-se como discos utilizáveis. Isso significa que o layout dos discos físicos é controlado pelo subsistema de armazenamento e não pelo sistema operacional.

Introdução ao armazenamento baseado em padrões

No gerenciamento baseado em padrões do Windows, o layout físico dos discos (eixos) é abstruído. Aqui, um "disco" pode ser uma referência lógica a uma parte de um subsistema de armazenamento (um disco virtual) ou um disco físico real. Isso significa que um disco simplesmente torna-se uma unidade de armazenamento e que volumes podem ser criados para alojar espaço dentro dos discos para sistemas de arquivos.

Levando esse conceito adiante, você pode agrupar espaços disponíveis em discos para que unidades de armazenamento (discos virtuais) possam ser alocadas nesse pool conforme o necessário. Essas unidades de armazenamento, por sua vez, recebem os volumes onde alocarão espaço e criarão sistemas de arquivos utilizáveis.

Tecnicamente, esse armazenamento é chamado de *pool de armazenamento*, e os discos virtuais criados dentro do pool são chamados de *espaços de armazenamento*. Dado um conjunto de “discos”, você pode criar um único pool de armazenamento alocando todos os discos no pool ou pode criar diversos pools de armazenamento alocando os discos separadamente em cada pool.

MUNDO REAL Acredite quando digo que tudo isso parece mais complicado do que realmente é. Quando você adiciona subsistemas de armazenamento nesse caso, torna-se simplesmente uma arquitetura de três camadas. Na camada 1, o layout dos discos físicos é controlado pelo subsistema de armazenamento. O sistema de armazenamento provavelmente irá utilizar algum tipo de RAID para garantir a redundância dos dados e sua recuperação em caso de falha. Na camada 2, os discos virtuais criados pelas matrizes são disponibilizados aos servidores. Os servidores simplesmente veem os discos como armazenamento que pode ser alocado. O Windows Server pode aplicar um RAID a nível de software ou outras abordagens de redundância para ajudar na proteção contra falhas. Na camada 3, o servidor cria volumes nos discos virtuais e esses volumes fornecem os sistemas de arquivos utilizáveis para o armazenamento de arquivos e de dados.

Como trabalhar com o armazenamento baseado em padrões

Para utilizar o armazenamento baseado em padrões, é recomendável adicionar o recurso Windows Standards-Based Storage Management aos seus servidores de arquivos. Quando um servidor é configurado com a função File Services And Storage, o recurso Windows Standards-Based Storage Management adiciona componentes e atualiza o Server Manager com as opções para trabalhar com volumes baseados em padrões. Talvez também deseje fazer o seguinte:

- Adicionar o serviço de função Data Deduplication se quiser habilitar a eliminação de duplicação de dados.
- Adicionar os serviços de função iSCSI Target Server e iSCSI Target Storage Provider se quiser que o servidor hospede discos virtuais iSCSI.

Após configurar seus servidores de maneira apropriada para seu ambiente, pode selecionar o nó File And Storage Services no Server Manager para trabalhar com seus volumes de armazenamento; não haverá opções adicionais. O subnó Volumes lista servidores de arquivo que foram configurados para gerenciamento baseado em padrões.

Como mostra a Figura 11-5, o subnó Volumes lista o armazenamento alocado em cada servidor de acordo com a forma como os volumes são provisionados e quanto espaço livre cada volume tem. Os volumes são listados independentemente de os discos subjacentes serem físicos ou virtuais. Pressione e mantenha pressionado ou clique com o botão direito do mouse em um volume para exibir as opções de gerenciamento, incluindo estas:

- **Configure Data Deduplication** Permite que você habilite e configure a eliminação de duplicação de dados para volumes NTFS. Se esse recurso estiver habilitado, também é possível utilizar essa opção para desabilitar a eliminação de duplicação de dados.
- **Delete Volume** Permite que você exclua o volume. O espaço que estava sendo utilizado por ele é marcado como não alocado no disco relacionado.

- **Extend Volume** Permite que você expanda o volume para um espaço não alocado do disco relacionado.
- **Format** Permite que você crie um novo sistema de arquivos no volume que irá substituir o atual.
- **Manage Drive Letter And Access Paths** Permite que você altere a letra de unidade ou o caminho de acesso associado ao volume.
- **New iSCSI Virtual Disk** Permite que você crie um novo disco virtual iSCSI que será armazenado no volume.
- **New Share** Permite que você crie um novo compartilhamento Server Message Block (SMB) ou Network File System (NFS) no volume.
- **Properties** Exibe informações sobre o tipo, o sistema de arquivos, o estado, a capacidade, o espaço utilizado e o espaço livre do volume. Essa opção também pode ser utilizada para definir o rótulo do volume.
- **Repair File System Errors** Permite que você repare os erros detectados durante uma verificação online do sistema de arquivos.
- **Scan File System For Errors** Permite que você realize uma verificação online do sistema de arquivos. Embora o Windows tente reparar qualquer erro encontrado, alguns erros só podem ser corrigidos por meio de um procedimento de reparo.

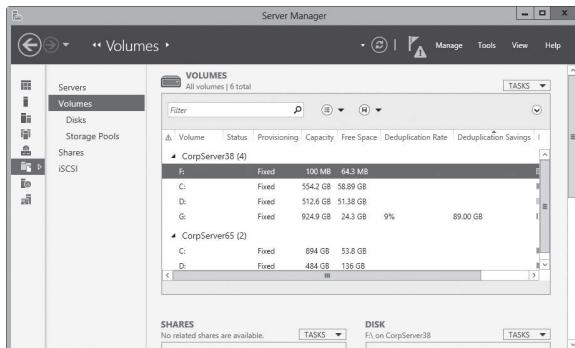


FIGURA 11-5 Observe como os volumes são provisionados.

Como mostra a Figura 11-6, o subnó Disks lista os discos disponíveis para cada servidor de acordo com sua capacidade total, espaço não alocado, estilo de partição, subsistema e tipo de barramento. O Server Manager diferencia entre discos físicos e discos virtuais mostrando o rótulo do disco virtual (se foi fornecido) e o subsistema de armazenamento de origem. Pressione e mantenha pressionado ou clique com o botão direito do mouse em um disco para exibir as opções de gerenciamento, incluindo estas:

- **Bring Online** Permite que você faça com que um disco offline fique disponível para uso.
- **Take Offline** Permite que você coloque um disco em offline de forma que não fique mais disponível para uso.

- **Reset Disk** Permite que você reinicie (reset) o disco completamente; isso exclui todos os volumes no disco e remove todos os dados disponíveis no disco.
- **New Volume** Permite que você crie um novo volume no disco.

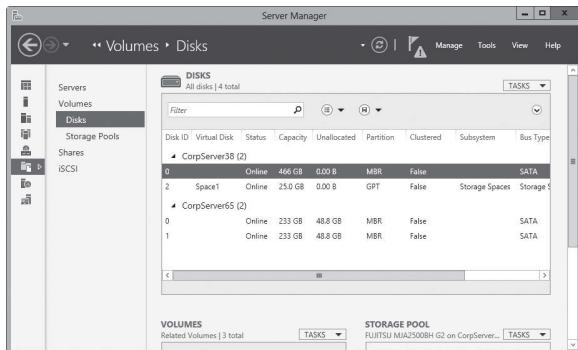


FIGURA 11-6 Observe os discos disponíveis e quanto espaço não alocado encontra-se disponível.

Como criar pools de armazenamento e alocar espaço

Em Services Manager, você pode trabalhar com pools de armazenamento e alocar espaço selecionando o nó File And Storage Services e então o subnó Storage Pools. Como mostra a Figura 11-7, o subnó Storage Pools lista os pools de armazenamento disponíveis, os discos virtuais criados dentro dos pools de armazenamento e os discos físicos disponíveis. Lembre-se de que o que está apresentado como disco físico pode ser, na verdade, uma LUN (disco virtual) de um subsistema de armazenamento.

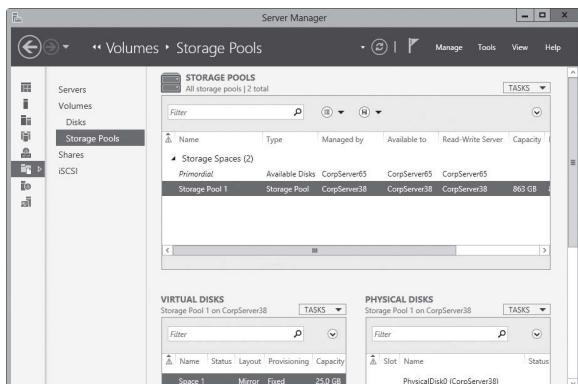


FIGURA 11-7 Crie e gerencie pools de armazenamento.

Trabalhar com pools de armazenamento é um processo que envolve várias etapas:

1. Você cria pools de armazenamento para reunir espaços disponíveis em um ou mais discos.
2. Você aloca os espaços desse pool para criar um ou mais discos virtuais.
3. Você cria um ou mais volumes em cada disco virtual para alocar armazenamento para sistemas de arquivos.

As seções a seguir analisam os procedimentos relacionados a cada uma dessas etapas.

Como criar espaços de armazenamento

Pools de armazenamento permitem que você reúna espaços disponíveis em discos para que as unidades de armazenamento (discos virtuais) possam ser alocadas nesses pools. Para criar um pool de armazenamento, é preciso ter pelo menos um disco não utilizado e um subsistema de armazenamento para gerenciá-lo. Esse subsistema de armazenamento pode ser aquele incluso no recurso Storage Spaces ou pode ser um subsistema associado ao armazenamento anexado.

Cada disco físico alocado no pool pode ser tratado destas três formas:

- Como um armazenamento de dados disponível para uso
- Como um armazenamento de dados que pode ser alocado manualmente para uso
- Como um hot spare em caso de um disco do pool falhar ou ser removido do subsistema

Para criar um pool de armazenamento, siga estas etapas:

1. Em Server Manager, selecione o nó File And Storage Services e o subnó Shares relacionado.
2. Toque ou clique em Tasks no painel Storage Pools e então em New Storage Pool. O New Storage Pool Wizard será iniciado. Se o assistente exibir a página Before You Begin, leia o texto Welcome e toque ou clique em Next.
3. Na página Specify A Storage Pool Name And Subsystem, digite um nome e uma descrição para o pool de armazenamento. Selecione o pool primordial com o qual deseja trabalhar. Um pool primordial é, simplesmente, um grupo de discos gerenciado por e disponível para um servidor específico por meio de um subsistema de armazenamento. Toque ou clique em Next.

DICA Seleccione o pool primordial para o servidor ao qual deseja associar o pool e para o qual deseja alocar armazenamento. Por exemplo, se estiver configurando armazenamento para CorpServer38, selecione o pool primordial disponível para o CorpServer 38.

4. Na página Select Physical Disks For The Storage Pool, selecione os discos físicos não utilizados que farão parte do pool de armazenamento e especifique o tipo de alocação para cada disco. Um pool de armazenamento deve ter mais de um disco para poder utilizar os recursos de espelhamento e paridade disponíveis para proteger os dados em caso de erro ou falha. Ao definir o valor de Alocação, lembre-se do seguinte:
 - Escolha Data Store para alocar o disco no pool e disponibilizá-lo para uso.

- Escolha Manual para alocar o disco no pool mas impedir que seja utilizado até que seja alocado manualmente.
 - Escolhe Hot Spare para alocar o disco no pool como um disco sobressalente que só será disponibilizado para uso se outro disco do pool falhar ou for removido do subsistema.
5. Quando estiver pronto para continuar, toque ou clique em Next. Após confirmar suas seleções, toque ou clique em Create. O assistente acompanhará o progresso de criação do pool. Quando o assistente terminar de criar o pool, a página View Results será atualizada para refletir isso. Revise os detalhes para garantir que todas as fases foram completadas com sucesso, então toque ou clique em Close.
- Se qualquer parte da configuração falhar, verifique a razão da falha e realize as ações corretivas conforme apropriado antes de repetir o procedimento.

Como criar um disco virtual em um espaço de armazenamento

Após criar um pool de armazenamento, você pode alocar espaço do pool para discos virtuais que estão disponíveis aos seus servidores. Cada disco físico alocado no pool pode ser tratado destas três formas:

- Como um armazenamento de dados disponível para uso
- Como um armazenamento de dados que pode ser alocado manualmente para uso
- Como um hot spare em caso de um disco do pool falhar ou ser removido do subsistema

Quando um pool de armazenamento possui um único disco, a única opção para alocar espaço nesse disco é criando discos virtuais com um layout simples. Um layout simples não fornece proteção contra falha de disco. Se um pool de armazenamento possui múltiplos discos, há estas opções de layout adicionais:

- **Mirror** Com o layout de espelho, os dados são duplicados nos discos utilizando uma técnica de espelhamento parecida com a discutida anteriormente neste capítulo. Entretanto, a técnica de espelhamento é mais sofisticada no que diz respeito aos dados serem espelhados em dois ou três discos por vez. Como no espelhamento padrão, essa abordagem tem suas vantagens e desvantagens. Aqui, se um espaço de armazenamento tiver dois ou três discos, você estará completamente protegido contra as falhas de disco único e, se um espaço de armazenamento tiver cinco ou mais discos, você estará completamente protegido contra as falhas de dois discos simultâneos. A desvantagem é que o espelhamento reduz a capacidade em até 50%. Por exemplo, se você espelhar dois discos de 1 TB, o espaço utilizável será de 1 TB.
- **Parity** Com o layout de paridade, os dados e as informações de paridade são distribuídos nos discos físicos utilizando uma técnica de faixa de disco com paridade parecida com a discutida anteriormente neste capítulo. Como na faixa de disco com paridade padrão, essa abordagem tem suas vantagens e desvantagens. Você precisa de pelo menos três discos para estar protegido completamente contra falha de disco único. Um pouco da capacidade é perdida devido à faixa, mas não tanta quanto no espelhamento.

Para criar um disco virtual em um pool de armazenamento, siga estas etapas:

1. Em Server Manager, selecione o nó File And Storage Services e o subnó Shares relacionado.
2. Toque ou clique em Tasks no painel Virtual Disks e então em New Virtual Disk. O New Virtual Disk Wizard será iniciado.
3. Na página Storage Pool, toque ou clique no pool de armazenamento no qual deseja criar o disco virtual e toque ou clique em Next. Cada pool de armazenamento disponível é listado de acordo com o servidor pelo qual é gerenciado e para o qual é disponibilizado. Certifique-se de que o pool possui espaço livre suficiente para criar o disco virtual.

DICA Selecione o pool de armazenamento para o servidor ao qual deseja associar o disco virtual e para o qual deseja alocar armazenamento. Por exemplo, se estiver configurando armazenamento para CorpServer38, selecione um pool de armazenamento disponível para o CorpServer 38.

4. Na página Specify The Virtual Disk Name, digite um nome e uma descrição para o disco virtual. Toque ou clique em Next.
5. Na página Select The Storage Layout, selecione o layout de armazenamento apropriado para seus requisitos de confiabilidade e redundância. O layout simples é a única opção para pools de armazenamento que contenham um único disco. Se o pool de armazenamento em questão possuir múltiplos discos, você pode escolher o layout simples, espelhado ou com paridade. Toque ou clique em Next.
6. Na página Specify The Provisioning Type, selecione o tipo de provisionamento. Um armazenamento pode ser provisionado em um disco thin ou em um disco fixo. Com o provisionamento de disco thin, o volume utiliza espaço do pool de armazenamento conforme necessário, até o tamanho total do volume. Com o provisionamento fixo, o volume possui um tamanho fixo e utiliza o espaço do pool de armazenamento equivalente ao tamanho do volume. Toque ou clique em Next.
7. Na página Specify The Size Of The Virtual Disk, utilize as opções fornecidas para definir o tamanho do disco virtual. Ao marcar a caixa de seleção Create The Largest Virtual Disk Possible, você está garantindo que o disco seja criado e dimensionado dentro do espaço disponível. Se estiver tentando criar um disco fixo de 2 TB com layout simples e houver apenas 1,5 TB de espaço disponível, um disco fixo de 1,5 TB será criado. Lembre-se de que se um disco for espelhado ou distribuído, ele usará mais espaço livre do que você especificar.
8. Quando estiver pronto para continuar, toque ou clique em Next. Após confirmar suas seleções, toque ou clique em Create. O assistente acompanhará o progresso de criação do disco. Quando o assistente terminar de criar o disco, a página View Results será atualizada para refletir isso. Examine os detalhes para se assegurar de que todas as fases foram concluídas com sucesso. Se qualquer parte da configuração falhar, verifique a razão da falha e realize as ações corretivas conforme apropriado antes de repetir o procedimento.
9. Quando você tocar ou clicar em Close, o New Volume Wizard deverá iniciar automaticamente. Utilize o assistente para criar um volume no disco conforme discutido em “Como criar um volume padrão”.

Como criar um volume padrão

Volumes padrão podem ser criados em qualquer disco físico ou virtual disponível. A técnica utilizada é a mesma independentemente de como o disco for apresentado ao servidor. Isso permite que você crie volumes nos discos internos de um servidor, em discos virtuais em um subsistema de armazenamento disponível para um servidor e em discos virtuais iSCSI disponíveis para um servidor. Se adicionar o recurso de eliminação de duplicação de dados a um servidor, pode habilitar a eliminação de duplicação de dados para volumes padrão criados para aquele servidor.

Para criar um volume padrão, siga estas etapas:

1. Inicie o New Volume Wizard. Se acabou de criar um espaço de armazenamento, talvez o New Volume Wizard inicie automaticamente. Caso contrário, realize umas destas ações:
 - No subnó Disks, todos os discos disponíveis estão listados no painel Disks. Selecione o disco com o qual deseja trabalhar e, sob Tasks, selecione New Volume.
 - No subnó Storage Pools, todos os discos virtuais disponíveis estão listados no painel Virtual Disks. Selecione o disco com o qual deseja trabalhar e, sob Tasks, selecione New Volume.
2. Na página Select The Server And Disk, selecione o servidor para o qual está provisionando armazenamento, selecione o disco onde o volume deve ser criado e toque ou clique em Next. Se acabou de criar um espaço de armazenamento e o New Volume Wizard iniciou automaticamente, o servidor e disco relacionados serão selecionados automaticamente e só é necessário tocar ou clicar em Next.
3. Na página Specify The Size Of The Volume, utilize as opções fornecidas para definir o tamanho do volume. Por padrão, o tamanho do volume está configurado para o máximo disponível no disco relacionado. Toque ou clique em Next.
4. Na página Assign To A Drive Letter Or Folder, especifique se deseja atribuir uma letra ou caminho de unidade ao volume e toque ou clique em Next. Existem as seguintes opções:
 - **Drive Letter** Para atribuir uma letra de unidade, escolha esta opção e selecione uma letra de unidade disponível na lista fornecida.
 - **The Following Folder** Para atribuir um caminho de unidade, escolha esta opção e digite o caminho para uma pasta existente em uma unidade NTFS, ou toque ou clique em Browse para procurar ou criar uma pasta.
 - **Don't Assign A Drive Letter Or Drive Path** Para criar o volume sem atribuir uma letra ou caminho de unidade, escolha esta opção. É possível atribuir uma letra ou caminho de unidade mais tarde, se necessário.
5. Na página Select File System Settings, especifique como o volume deve ser formatado utilizando estas opções:
 - **File System** Define o tipo do sistema de arquivos, como NTFS ou ReFS.
 - **Allocation Unit Size** Define o tamanho do cluster para o sistema de arquivos. Esta é a unidade básica na qual o espaço em disco é alocado. O tamanho padrão da unidade de alocação é baseado no tamanho do volume e é definido

dinamicamente antes da formatação. Para substituir essa configuração, pode-se definir o tamanho da unidade de alocação com um valor específico.

- **Volume Label** Define um rótulo para a partição. Esse rótulo é o nome do volume.
6. Se escolheu criar um volume NTFS e adicionou eliminação de duplicação de dados ao servidor, pode habilitar e configurar a eliminação de duplicação de dados. Quando estiver pronto para continuar, toque ou clique em Next.
 7. Após confirmar suas seleções, toque ou clique em Create. O assistente acompanhará o progresso de criação do volume. Quando o assistente terminar de criar o volume, a página View Results será atualizada para refletir isso. Examine os detalhes para se assegurar de que todas as fases foram concluídas com sucesso. Se qualquer parte da configuração falhar, verifique a razão da falha e realize as ações corretivas conforme apropriado antes de repetir o procedimento.
 8. Toque ou clique em Close.

Gerenciamento de partições e unidades existentes

O Disk Management fornece muitas formas de gerenciar partições e unidades existentes. Utilize esses recursos para atribuir letras de unidades, excluir partições, configurar a partição ativa e mais. Além disso, o Windows Server 2012 fornece outros utilitários para realizar tarefas comuns como converter um volume para NTFS, verificar erros em uma unidade e limpar espaço em disco não utilizado.

OBSERVAÇÃO O Windows Vista, assim como versões mais recentes do Windows, dá suporte a mídias que podem ser conectadas com a máquina ligada e que utilizam volumes NTFS. Esse novo recurso permite que você formate dispositivos flash USB, e outras mídias semelhantes, com NTFS. Também há melhorias na prevenção da perda de dados ao ejectar uma mídia removível formatada com NTFS.

Como atribuir letras e caminhos de unidade

É possível atribuir às unidades uma letra de unidade e um ou mais caminhos de unidade, contanto que os caminhos de unidade estejam montados em unidades NTFS. Não é necessário atribuir uma letra ou um caminho de unidade a unidades. Uma unidade sem designadores será considerada desmontada, e você poderá montá-la atribuindo uma letra ou caminho de unidade em um outro momento. É preciso desmontar uma unidade antes de movê-la para outro computador.

O Windows não pode modificar a letra de unidade de volumes de sistema, inicialização ou de arquivo de paginação. Para alterar a letra de unidade de um volume de sistema ou inicialização, é preciso editar o registro como descrito no artigo 223188 do Microsoft Knowledge Base (support.microsoft.com/kb/223188/). Antes de poder alterar a letra de unidade de um volume que contém um arquivo de paginação, talvez seja preciso mover o arquivo de paginação para um volume diferente.

Para gerenciar letras e caminhos de unidade, pressione e mantenha pressionado ou clique com o botão direito do mouse na unidade que deseja configurar no Disk Management, então toque ou clique em Change Drive Letter And Paths. A caixa de diálogo mostrada na Figura 11-8 será aberta. As ações disponíveis são:

- **Adicionar um caminho de unidade** Toque ou clique em Add, selecione Mount In The Following Empty NTFS Folder, então digite o caminho para uma pasta existente ou toque ou clique em Browse para procurar ou criar uma pasta.
- **Remover um caminho de unidade** Selecione o caminho de unidade a remover, toque ou clique em Remove e então em Yes.
- **Atribuir uma letra de unidade** Toque ou clique em Add, selecione Assign The Following Drive Letter e escolha uma letra disponível para atribuir à unidade.
- **Alterar a letra de unidade** Selecione a letra da unidade atual e toque ou clique em Change. Selecione Assign The Following Drive Letter e escolha uma letra diferente para atribuir à unidade.
- **Remover uma letra de unidade** Selecione a letra de unidade atual, toque ou clique em Remove e então em Yes.

OBSERVAÇÃO Se você tentar alterar a letra de uma unidade em uso, o Windows Server 2012 exibirá um aviso. É necessário fechar os programas que estejam utilizando a unidade e tentar novamente ou permitir que o Disk Management force a alteração tocando ou clicando em Yes quando solicitado.

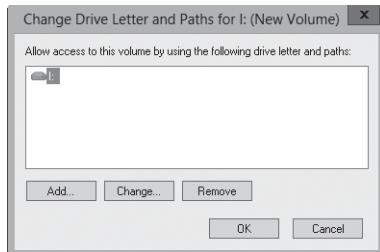


FIGURA 11-8 Você pode alterar a letra e o caminho de uma unidade na caixa de diálogo

Como alterar ou excluir o rótulo de um volume

O rótulo de um volume é um descritor textual de uma unidade. Com o FAT, o rótulo do volume pode ter até 11 caracteres e pode incluir espaços. Com o NTFS, o rótulo do volume pode ter até 32 caracteres. Além disso, o FAT não permite a utilização de alguns caracteres especiais (incluindo * / \ [] : ; | = , . + ? < >), mas o NTFS permite.

Como o rótulo do volume é exibido quando a unidade é acessada em vários utilitários do Windows Server 2012, incluindo o File Explorer, ele pode fornecer informações sobre o conteúdo de uma unidade. Você pode alterar ou excluir o rótulo de um volume utilizando o Disk Management ou o File Explorer.

Para alterar ou excluir um rótulo utilizando o Disk Management, siga estas etapas:

1. Pressione e mantenha pressionado ou clique com o botão direito do mouse na partição e toque ou clique em Properties.
2. Na guia General da caixa de diálogo Properties, digite um novo rótulo para o volume na caixa de texto Label, ou exclua o rótulo existente. Toque ou clique em OK.

Para alterar ou excluir um rótulo utilizando o File Explorer, siga estas etapas:

1. Pressione e mantenha pressionado ou clique com o botão direito do mouse no ícone da unidade e toque ou clique em Properties.
2. Na guia General da caixa de diálogo Properties, digite um novo rótulo para o volume na caixa de texto Label, ou exclua o rótulo existente. Toque ou clique em OK.

Como excluir partições e unidades

Para alterar a configuração de uma unidade totalmente alocada, talvez seja necessário excluir partições e unidades lógicas existentes. Excluir uma partição ou uma unidade resulta na remoção do sistema de arquivos associado e todos os dados do sistema de arquivos são perdidos. Antes de excluir uma partição ou uma unidade, deve-se fazer o backup de todos os arquivos e diretórios contidos na partição ou na unidade.

OBSERVAÇÃO Para proteger a integridade do sistema, não é possível excluir a partição do sistema ou de inicialização. Entretanto, o Windows Server 2012 permite a exclusão da partição ou volume ativos se não forem designados como inicialização ou sistema. Sempre certifique-se de que a partição ou volume que está excluindo não contém dados ou arquivos importantes.

Para excluir um volume, unidade lógica ou partição primária, siga estas etapas:

1. No Disk Management, pressione e mantenha pressionado ou clique com o botão direito do mouse na partição, volume ou unidade que deseja excluir e toque ou clique em Explore. Utilizando o File Explorer, mova todos os dados para outro volume ou verifique um backup existente para assegurar-se de que os dados estão salvos apropriadamente.
2. No Disk Management, pressione e mantenha pressionado ou clique com o botão direito do mouse na partição, volume ou unidade novamente, toque ou clique em Delete Partition, Delete Volume ou Delete Logical Drive conforme apropriado.
3. Confirme que você deseja selecionar o item tocando ou clicando em Yes.

As etapas para excluir um partição estendida diferem um pouco das etapas para excluir uma partição primária ou uma unidade lógica. Para excluir uma partição estendida, siga estas etapas:

1. Exclua todas as unidades lógicas na partição seguindo as etapas listadas no procedimento anterior.
2. Selecione a área da partição estendida em si e exclua-a.

Como converter volumes FAT em NTFS

O Windows Server 2012 fornece um utilitário para converter volumes FAT em NTFS. Esse utilitário, Convert(Convert.exe), está localizado na pasta %SystemRoot%. Quando um volume é convertido por meio dessa ferramenta, a estrutura do arquivo e do diretório é preservada e os dados não são perdidos. Entretanto, lembre-se de que o Windows Server 2012 não fornece um utilitário para converter NTFS em FAT. A única forma de converter um volume NTFS em FAT é excluindo a partição por meio das etapas listadas na seção anterior e recriando a partição como volume FAT.

A sintaxe do utilitário Convert

O Convert é executado no prompt de comando. Para converter uma unidade, utilize a seguinte sintaxe:

```
convert volume /FS:NTFS
```

Aqui, *volume* é a letra da unidade seguida por dois-pontos, caminho da unidade ou nome do volume. Por exemplo, se quiser converter a unidade D em NTFS, utilize o seguinte comando:

```
convert D: /FS:NTFS
```

Se o volume tiver um rótulo, será solicitado que você insira o rótulo do volume para a unidade. Isso não será solicitado caso o disco não possua um rótulo.

A sintaxe completa para o Convert é a seguinte:

```
convert volume /FS:NTFS [/V] [/X] [/CvtArea:filename] [/NoSecurity]
```

As opções do Convert são utilizadas das seguintes formas:

volume	Define o volume com o qual você irá trabalhar
/FS:NTFS	Converte em NTFS
/V	Estabelece o modo detalhado
/X	Força o volume a desmontar antes da conversão (se necessário)
/CvtArea:filename	Estabelece o nome de um arquivo contíguo no diretório-raiz para que ele seja um espaço reservado para arquivos de sistema do NTFS
/NoSecurity	Remove todos os atributos de segurança e faz com que todos os arquivos e diretórios fiquem acessíveis ao grupo Everyone

A seguir, um exemplo de uso do Convert:

```
convert C: /FS:NTFS /V
```

Como utilizar o utilitário Convert

Antes de utilizar o utilitário Convert, determine se a partição está sendo utilizada como partição do sistema ou de inicialização ativa contendo o sistema operacional. Você pode converter a partição de inicialização ativa em NTFS. Isso requer que o sistema adquira acesso exclusivo a essa partição, o que pode ser obtido somente durante a inicialização. Portanto, se tentar converter a partição de inicialização ativa para NTFS, o Windows Server 2012 irá exibir um prompt perguntando se você deseja fazer um agendamento para que a unidade seja convertida na próxima vez em que o sistema iniciar. Se tocar ou clicar em Yes, deverá reiniciar o sistema para iniciar o processo de conversão.

DICA Muitas vezes você precisará reiniciar o sistema diversas vezes para converter a partição de inicialização ativa completamente. Não se preocupe. Deixe que o sistema prossiga com a conversão.

Antes que o utilitário Convert realmente converta a unidade para NTFS, o utilitário verifica se a unidade possui espaço livre suficiente para realizar a conversão. Geralmente, o Convert precisa um bloco de espaço livre que equivale a aproximadamente 25% do espaço total utilizado na unidade. Por exemplo, se a unidade armazenar 200 GB de

dados, o Convert precisa de aproximadamente 50 GB de espaço livre. Se a unidade não tiver espaço livre suficiente, o Convert aborta e informa que é preciso liberar espaço. Se a unidade tiver espaço livre suficiente, o Convert inicia a conversão. Seja paciente. O processo de conversão leva alguns minutos (é mais longo para unidades maiores). Não accesse arquivos ou aplicativos da unidade enquanto a conversão está em andamento.

Você pode utilizar a opção `/CvtArea` para melhorar o desempenho no volume de forma a deixar espaço reservado para a master file table (MFT, tabela mestra de arquivos). Essa opção ajuda a impedir a fragmentação da MFT. Como? No decorrer do tempo, a MFT pode ultrapassar o espaço alocado para ela. Então, o sistema operacional deve expandir a MFT para outras áreas do disco. Embora o uso do utilitário Optimize Drives possa desfragmentar a MFT, ele não pode mover a primeira seção da MFT, e é muito improvável que haja espaço após a MFT porque ele estará preenchido por dados de arquivo.

Para ajudar a impedir a fragmentação em alguns casos, é recomendável reservar mais espaço do que o padrão (12,5% do tamanho da partição ou volume). Por exemplo, é recomendável aumentar o tamanho da MFT se você planeja que o volume tenha muitos arquivos pequenos ou médios em vez de uns poucos arquivos grandes. Para especificar a quantidade de espaço a ser reservado, você pode utilizar o FSUtil para criar um arquivo de espaço reservado de tamanho igual ao da MFT que deseja criar. Então pode converter o volume em NTFS e especificar o nome do arquivo de espaço reservado a utilizar com a opção `/CvtArea`.

No exemplo a seguir, o FSUtil é utilizado para criar um arquivo de espaço reservado de 1,5 GB (1.500.000.000 bytes) com o nome de Temp.txt:

```
fsutil file createnew c:\temp.txt 15000000000
```

Para utilizar esse arquivo de espaço reservado para a MFT enquanto converte a unidade C em NTFS, seria preciso digitar o seguinte comando:

```
convert c: /fs:ntfs /cvtarea:temp.txt
```

Observe que o arquivo de espaço reservado é criado na partição ou volume que está sendo convertido. Durante o processo de conversão, o arquivo é substituído por metadados de NTFS e qualquer espaço não utilizado no arquivo é reservado para uso futuro pela MFT.

Como redimensionar partições e volumes

O Windows Server 2012 não utiliza o Ntldr nem o Boot.ini para carregar o sistema operacional. Em vez disso, o Windows Server possui um ambiente de pré-inicialização no qual o Windows Boot Manager (Gerenciador de Inicialização do Windows) é utilizado para controlar a inicialização e para carregar o aplicativo de inicialização selecionado. Finalmente, o Windows Boot Manager também libera o sistema operacional Windows da relação de dependência com o MS-DOS, de forma a permitir que você utilize unidades de novas maneiras. Com o Windows Server 2012, é possível expandir e reduzir tanto discos básicos como discos dinâmicos. Você pode utilizar o Disk Management ou o DiskPart para expandir e reduzir volumes. Não é possível reduzir ou expandir volumes distribuídos, espelhados ou distribuídos com paridade.

Ao expandir um volume, você converte áreas de espaço não alocado e adiciona-as ao volume existente. Para volumes estendidos em discos dinâmicos, o espaço pode originar de qualquer disco dinâmico disponível, não apenas daqueles nos quais o vo-

lume foi originalmente criado. Portanto, é possível combinar áreas de espaço livre em múltiplos discos dinâmicos e utilizar essas áreas para aumentar o tamanho de um volume existente.

ATENÇÃO Antes de tentar expandir um volume, conheça as diversas limitações. Primeiramente, você pode expandir volumes simples e estendidos somente se eles forem formatados e o sistema de arquivos for NTFS. Não é possível expandir volumes distribuídos. Não é possível expandir volumes que não sejam formatados ou que tenham sido formatados com FAT. Além disso, você não pode expandir um volume de sistema ou de inicialização, independentemente de sua configuração.

Para reduzir um volume simples ou estendido siga estas etapas:

1. No Disk Management, pressione e segure ou clique com o botão direito do mouse no volume que deseja reduzir e toque ou clique em Shrink Volume. Essa opção só estará disponível caso o volume preencha os critérios discutidos anteriormente.
2. Na caixa fornecida na caixa de diálogo Shrink, mostrada na Figura 11-9, insira a quantidade de espaço a reduzir.

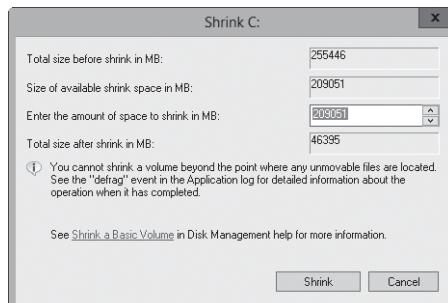


FIGURA 11-9 Especifique a quantidade de espaço a reduzir do volume.

A caixa de diálogo Shrink fornece as seguintes informações:

- **Total Size Before Shrink In MB** Lista a capacidade total do volume em megabytes. Esse é o tamanho formatado do volume.
- **Size Of Available Shrink Space In MB** Lista a quantidade máxima que o volume pode ser reduzido. Essa quantidade não representa a quantidade total de espaço livre no volume; mas sim, a quantidade de espaço que pode ser removido, sem incluir dados reservados à MFT, instantâneo de volume, arquivos de paginação e arquivos temporários.
- **Enter The Amount Of Space To Shrink In MB** Lista a quantidade de espaço total que será removido do volume. O valor inicial padrão equivale à quantidade máxima de espaço que pode ser removida do volume. Para desempenho ótimo da unidade, recomenda-se que a unidade possua pelo menos 10% de espaço livre após a operação de redução.
- **Total Size After Shrink In MB** Lista a capacidade total que o volume terá (em megabytes) após a redução. Esse será o novo tamanho formatado do volume.

3. Toque ou clique em Yes para confirmar a ação.

Para expandir um volume simples ou estendido siga estas etapas:

1. No Disk Management, pressione e segure ou clique com o botão direito do mouse no volume que deseja expandir e toque ou clique em Extend Volume. Essa opção só estará disponível caso o volume preencha os critérios discutidos anteriormente e caso haja espaço livre disponível em um ou mais discos dinâmicos do sistema.
2. No Extend Volume Wizard, leia a mensagem introdutória e toque ou clique em Next.
3. Na página Select Disks, selecione o disco ou discos dos quais deseja alocar espaço livre. Qualquer disco que estiver sendo utilizado pelo volume nesse momento será automaticamente selecionado. Por padrão, todo o espaço livre remanescente nesses discos será selecionado para uso.
4. Com discos dinâmicos, você pode especificar espaço adicional que queira utilizar em outros discos; para isso, siga estas etapas:
 - Toque ou clique no disco e em Add para adicionar o disco à lista Selected.
 - Selecione cada disco da lista Selected e, na lista Select The Amount Of Space In MB, especifique a quantia de espaço não alocado a ser utilizado no disco selecionado.
5. Toque ou clique em Next, confirme suas opções e toque ou clique em Finish.

Como reparar erros e inconsistências de disco automaticamente

O Windows Server 2012 inclui melhorias de recursos que reduzem a quantidade de manutenção manual que necessita ser realizada em unidades de disco. As seguintes melhorias são as que têm maior impacto na forma como se trabalha com discos:

- NTFS Transacional
- Autorrecuperação do NTFS

O NTFS transacional permite que as operações de arquivos em um volume NTFS sejam realizadas transacionalmente. Isso significa que os programas podem utilizar uma transação para agrupar conjuntos de arquivos e operações do registro de operações de forma que todas (ou nenhuma) tenham êxito. Enquanto uma transação estiver ativa, as alterações não estarão visíveis fora da transação. As alterações só são confirmadas e gravadas completamente no disco quando uma transação for realizada com êxito. Se uma transação falhar ou estiver incompleta, o programa reverte a transação para restaurar o sistema de arquivos para o estado no qual estava antes da transação.

MUNDO REAL O Resilient File System (ReFS, Sistema de Arquivos Resiliente) leva os recursos de transação e autorrecuperação do NTFS mais longe. Com o ReFS, diversos processos em segundo plano são utilizados para manter a integridade do disco automaticamente. O processo scrubber verifica se há inconsistências e erros no disco. Se houver, um processo de reparação localiza os problemas e realiza uma correção online automática. No caso raro de um problema estar sendo causado por setores defeituosos de uma unidade física, o ReFS utiliza um processo de salvamento para marcar esses setores defeituosos e removê-los do sistema de arquivos; tudo isso é realizado com o volume online.

Transações que estendem-se por vários volumes são coordenadas pelo Kernel Transaction Manager (KTM, Gerenciador de Transações do Kernel). O KTM dá suporte à recuperação individual de volumes se uma transação falhar. O gerenciador de recursos locais de um volume mantém um log de transação separado e é responsável por manter threads de transações separados de threads que realizam o trabalho de arquivo.

Tradicionalmente, era preciso utilizar a ferramenta Check Disk para corrigir erros e inconsistências nos volumes NTFS em um disco. Como esse processo pode interromper a disponibilidade de sistemas Windows, o Windows Server 2012 utiliza a autorrecuperação do NTFS para proteger sistemas de arquivos sem que você precise utilizar ferramentas de manutenção para corrigir os problemas. Como grande parte do processo de autocorreção é habilitada e realizada automaticamente, talvez seja necessário realizar a manutenção do volume manualmente somente quando o sistema operacional informar que um problema não pode ser corrigido automaticamente. Se isso ocorrer, o Windows Server 2012 informará sobre o problema e fornecerá as soluções possíveis.

A autocorreção do NTFS possui muitas vantagens em relação ao Check Disk, incluindo as seguintes:

- O Check Disk precisa de acesso exclusivo aos volumes, ou seja, volumes de sistema e de inicialização só podem ser verificados quando o sistema operacional iniciar. Por outro lado, com a autocorreção do NTFS, o sistema de arquivos está sempre disponível e não precisa ser corrigido offline (na maioria dos casos).
- A autocorreção do NTFS busca preservar a maior quantidade de dados possível no caso de haver corrompimento, também reduz montagens falhas de sistemas de arquivos que podiam ocorrer caso um volume tivesse erros e inconsistências. Durante a reinicialização, a autocorreção do NTFS repara o volume imediatamente para que ele possa ser montado.
- A autocorreção do NTFS reporta alterações feitas no volume durante o reparo por meio de mecanismos Chkdsk.exe, notificações de diretório e de registros de journal do update sequence number (USN, números de sequência de atualização). Esse recurso também possibilita que administradores e usuários autorizados monitem operações de reparo através das mensagens Verification, Waiting For Repair Completion e Progress Status.
- A autocorreção do NTFS pode recuperar um volume caso o setor de inicialização esteja legível mas não consiga identificar um volume NTFS. Nesse caso, é preciso executar uma ferramenta offline que repara o setor de inicialização e permite que a autocorreção do NTFS inicie a recuperação.

Embora a autocorreção do NTFS seja uma melhoria incrível, às vezes é desejável (ou necessário) verificar manualmente a integridade de um disco. Nesses casos, o Check Disk (Chkdsk.exe) pode ser utilizado para procurar e (opcionalmente) reparar problemas encontrados em volumes FAT, FAT32, exFAT e NTFS. Embora o Check Disk consiga procurar e corrigir muitos tipos de erros, o principal uso do utilitário é procurar inconsistências no sistema de arquivos e em metadados relacionados. Uma das maneiras utilizadas pelo Check Disk para encontrar erros é comparando o bitmap do volume aos setores de disco atribuídos aos arquivos no sistema de arquivos. Para além disso, a utilidade do Check Disk é limitada. Por exemplo, o Check Disk não repara dados corrompidos em arquivos que pareçam estar estruturalmente intactos.

Como parte da manutenção automatizada, o Windows Server 2012 realiza uma verificação proativa em volumes NTFS. Como ocorre com outras tarefas de manutenção

automáticas, o Windows varre os discos às 03:00 utilizando o Check Disk se o computador estiver conectado à rede elétrica e o sistema operacional estiver ocioso. Caso contrário, o Windows varre os discos na próxima ocasião em que o computador estiver ligado à rede elétrica e o sistema operacional estiver ocioso. Embora a manutenção automatizada acione a verificação, o processo de ativação e gerenciamento do Check Disk é controlado por uma tarefa diferente. Em Task Scheduler, você encontrará a tarefa ProactiveScan na biblioteca do agendador sob Microsoft\Windows\Chkdsk, e pode obter detalhes de execução analisando as informações fornecidas na guia History da tarefa.

MUNDO REAL A Manutenção Automatizada provém da estrutura do Windows Diagnostics. Por padrão, o Windows periodicamente realiza uma manutenção de rotina às 03:00 se o computador estiver ligado à rede elétrica e o sistema operacional estiver ocioso. Caso contrário, a manutenção iniciará na próxima ocasião em que o computador estiver ligado à rede elétrica e o sistema operacional estiver ocioso. Como a manutenção é executada apenas quando o sistema operacional está ocioso, a manutenção pode ser executada em segundo plano por até três dias. Isso permite que o Windows complete tarefas de manutenção complexas automaticamente. Tarefas de manutenção incluem atualizações de software, verificação de segurança, diagnósticos de sistema, verificação de discos e otimização de disco.

Como verificar discos manualmente

Com o Windows Server 2012, o Check Disk realiza verificações e reparos automaticamente, em vez de utilizar modos de verificação e reparo herdados das versões anteriores do Windows. Aqui, ao utilizar o Check Disk com volumes NTFS, o Check Disk realiza uma verificação online e uma análise do disco para detectar erros. O Check Disk grava informações sobre qualquer corrompimento detectado no arquivo de sistema \$corrupt. Se o volume estiver em uso, corrompimentos detectados podem ser reparados colocando o volume em offline temporariamente. Entretanto, desmontar o volume para reparo invalida todos os identificadores de arquivos abertos. Com o volume de inicialização/sistema, os reparos são realizados na próxima ocasião em que o computador é iniciado.

Armazenar as informações de corrompimentos e então reparar o volume enquanto ele é desmontado permite que o Windows repare volumes rapidamente. Também permite que você continue utilizando o disco enquanto uma verificação é realizada. Normalmente, o reparo offline leva apenas alguns segundos, comparado ao que levaria horas no caso de reparar volumes grandes por meio da técnica de verificação e reparo herdados.

OBSERVAÇÃO O FAT, FAT32 e exFAT não dão suporte aos recursos melhorados. Quando o Check Disk é utilizado com o FAT, FAT32 ou exFAT, o Windows Server 2012 utiliza o processo de verificação e reparo herdados. Isso significa que o processo de verificação e reparo normalmente exige que o volume seja colocado em offline para impedir que seja utilizado.

É possível executar o Check Disk por meio do prompt de comando ou dentro de outros utilitários. Em um prompt de comando, é possível testar a integridade da unidade E digitando o seguinte comando:

```
chkdsk /scan E:
```

O Check Disk realizará uma análise do disco e retornará uma mensagem de status a respeito de qualquer problema encontrado. Porém, a menos que você especifique opções adicionais, o Check Disk não irá reparar os problemas. Para reparar erros na unidade E, utilize este comando:

```
chkdsk /spotfix E:
```

Corrigir o volume requer acesso exclusivo ao volume. A forma como isso funciona depende do tipo de volume:

- Para volumes que não sejam do sistema, aparecerá um prompt perguntando se você deseja forçar um desmonte do volume para reparo. Nesse caso, pode digitar **Y** para prosseguir ou **N** para cancelar o desmonte. Se cancelar o desmonte, receberá um prompt perguntando se deseja agendar o reparo do volume para a próxima ocasião em que o computador for inicializado. Nesse caso, pode digitar **Y** para agendar o reparo ou **N** para cancelar o reparo.
- Para volumes do sistema, aparecerá um prompt perguntando se você deseja agendar o reparo do volume para a próxima ocasião em que o computador for inicializado. Nesse caso, pode digitar **Y** para agendar o reparo ou **N** para cancelar o reparo.

Não é possível executar o Check Disk com as opções */scan* e */spotfix*. Isso ocorre porque agora as tarefas de verificação e reparo são independentes uma da outra.

A sintaxe completa para o Check Disk é a seguinte:

```
CHKDSK [volume[[path]filename]] [/F] [/V] [/R] [/X] [/I] [/C] [/B]
[ /L[:size] ] [/scan] [/forceofflinefix] [/perf] [/spotfix]
[ /sdcleanup ] [/offlineScanAndFix]
```

As opções do Check Disk são utilizadas das seguintes formas:

volume	Define o volume com o qual você irá trabalhar.
[path]filename	Somente FAT. Especifica os arquivos que serão verificados em relação à fragmentação.
/B	Reavalia clusters inválidos nos volumes (apenas NTFS; torna /R necessário).
/C	Somente NTFS. Pula a verificação de ciclos dentro da estrutura de pastas.
/F	Corrige erros no disco por meio da verificação offline (herdada) e comportamento de reparo.
/I	Somente NTFS. Realiza uma verificação mínima nas entradas de índice.
/L:size	Somente NTFS. Altera o tamanho do arquivo de log.
/R	Encontra setores defeituosos e recupera informações legíveis (torna /F necessário).
/V	Em FAT, exibe o caminho completo e nome de cada arquivo no disco. Em NTFS, exibe mensagens de limpeza, se houver alguma.
/X	Força o volume a desmontar, se necessário (torna /F necessário).

Para volumes NTFS, o Check Disk dá suporte a estas opções melhoradas:

/forceofflinefix	Deve ser utilizado com <i>/scan</i> . Ignora todos os reparos online e enumera os erros para reparo offline.
/offlineScanAndFix	Realiza uma verificação offline e corrige o volume.
/perf	Realiza a verificação o mais rápido possível utilizando recursos do sistema.
/scan	Realiza uma verificação online do volume (o padrão). Erros detectados durante a verificação são adicionados ao arquivo de sistema \$corrupt.

<code>/sdcleanup</code>	Limpa dados do descriptor de segurança desnecessários. Torna /F necessário (com verificação e reparo herdados).
<code>/spotfix</code>	Permite que certos tipos de erros sejam reparados online (o padrão).

Como executar o Check Disk de forma interativa

É possível executar o Check Disk de forma interativa por meio do File Explorer ou do Disk Management. Siga estas etapas:

1. Pressione e mantenha pressionado ou clique com o botão direito do mouse na unidade e toque ou clique em Properties.
2. Na guia Tools da caixa de diálogo Properties, clique em Check. A caixa de diálogo Error Checking mostrada na Figura 11-10 será aberta.

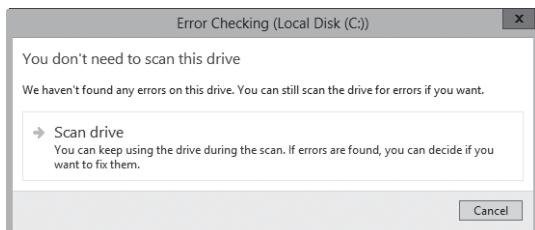


FIGURA 11-10 Use o Check Disk para verificar se há erros em um disco e reparar qualquer erro encontrado.

3. Clique em Scan Drive para iniciar a verificação. Se não houver erro, o Windows confirmará isso. Se erros forem encontrados, opções adicionais serão apresentadas. Em relação à verificação de discos por meio de um prompt, a forma como isso ocorre depende de você estar trabalhando com um volume que seja do sistema ou com um volume que não seja do sistema.

OBSERVAÇÃO Para volumes FAT, FAT32 e exFAT, o Windows utiliza o Check Disk herdado. Para iniciar a verificação, toque ou clique em Scan And Repair Drive. Se a verificação encontrar erros, talvez seja preciso reiniciar o computador para repará-los.

Como analisar e otimizar discos

Toda vez que você adicionar ou remover arquivos de uma unidade, os dados da unidade podem tornar-se fragmentados. Quando uma unidade é fragmentada, arquivos grandes não conseguem ser gravados em uma única área contínua do disco. Como resultado, o sistema operacional precisa gravar o arquivo em diversas áreas menores no disco, ou seja, mais tempo é gasto na leitura do arquivo no disco. Para reduzir a fragmentação, o Windows Server 2012 pode analisar discos manualmente ou automaticamente e otimizá-los por meio do utilitário Optimize Drives.

Com a otimização manual, o Optimize Drives realiza uma análise online dos volumes e reporta a porcentagem de fragmentação. Se a desfragmentação for necessária, é possível escolher realizar desfragmentação online. Volumes de sistema e de inicialização também podem ser desfragmentados online, e o Optimize Drives pode ser utilizado com volumes FAT, FAT32, exFAT, NTFS e ReFS.

Você pode analisar manualmente e otimizar um disco seguindo estas etapas:

1. Em Computer Management, selecione o nó Storage e então o nó Disk Management. Pressione e mantenha pressionado ou clique com o botão direito do mouse em uma unidade e toque ou clique em Properties.
2. Na guia Tools, toque ou clique em Optimize. Na caixa de diálogo Optimize Drives, selecione uma unidade e toque ou clique em Analyze. O Optimize Drives analisará o disco, como mostra a Figura 11-11, para definir se ele precisa ser desfragmentado. Caso precise, o Optimize Drive recomendará a desfragmentação nesse momento.
3. Se um disco precisar ser desfragmentado, selecione o disco e toque ou clique em Optimize.

OBSERVAÇÃO Dependendo do tamanho do disco, a desfragmentação pode levar horas. Você pode tocar ou clicar em Stop Operation a qualquer momento para parar a desfragmentação.

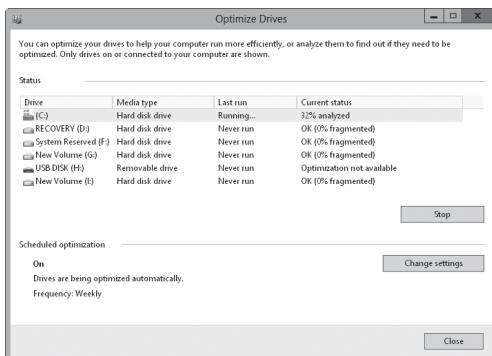


FIGURA 11-11 O Optimize Drives analisa e desfragmenta os discos com eficiência.

A análise e otimização automáticas de discos podem ocorrer enquanto os discos estiverem online, contanto que o computador esteja ligado à rede elétrica e o sistema operacional esteja ocioso. Por padrão, a otimização de disco é uma tarefa semanal, não diária, e há uma boa razão para isso. Normalmente, só é preciso otimizar os discos de um servidor periodicamente, sendo uma vez por semana o suficiente na maioria dos casos. Observe, no entanto, que embora discos que não sejam do sistema possam ser analisados e otimizados rapidamente, otimizar discos online que sejam do sistema pode ser mais demorado.

É possível controlar o horário aproximado do início da análise e otimização de discos alterando o horário de início da manutenção automática. O Windows Server também informa se três execuções consecutivas forem perdidas. Todas as unidades internas e certas unidades externas são otimizadas automaticamente como parte da agenda regular, assim como ocorre com novas unidades que você conectar ao servidor.

OBSERVAÇÃO O Windows Server 2012 realiza automaticamente uma desfragmentação cíclica. Com esse recurso, quando a passagem de uma desfragmentação agendada é pausada e reiniciada, o computador prossegue de onde parou ou começa com o próximo volume não finalizado da lista a desfragmentar.

Para configurar e gerenciar a desfragmentação automática, siga estas etapas:

1. Em Computer Management, selecione o nó Storage e então o nó Disk Management. Pressione e mantenha pressionado ou clique com o botão direito do mouse em uma unidade e toque ou clique em Properties.
2. Na guia Tools, toque ou clique em Optimize. A caixa de diálogo Optimize Drives será exibida.
3. Se quiser alterar como a otimização funciona, toque ou clique em Change Settings. A caixa de diálogo mostrada na Figura 11-12 será exibida. Para cancelar a desfragmentação automática, desmarque a caixa de seleção Run On A Schedule. Para habilitar a desfragmentação automática, selecione Run On A Schedule.

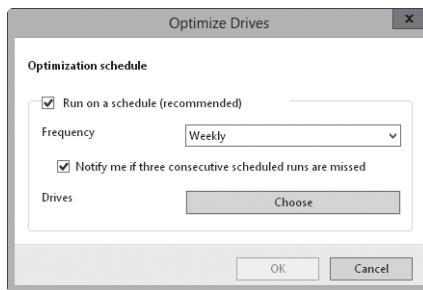


FIGURA 11-12 Defina a agenda de execução para a desfragmentação automática.

4. A frequência de execução padrão é definida conforme mostrado. Na lista Frequency, você pode escolher entre Daily (Diariamente), Weekly (Semanalmente) ou Monthly (Mensalmente) para a execução. Se não quiser ser notificado quanto a execuções perdidas, desmarque a caixa de seleção Notify Me.
5. Se quiser gerenciar os discos a serem desfragmentados, toque ou clique em Choose e selecione os volumes desejados. Por padrão, todos os discos instalados no ou conectados ao computador são desfragmentados, e qualquer disco novo também é desfragmentado automaticamente. Marque as caixas de seleção dos discos que devem ser desfragmentados automaticamente e desmarque as caixas de seleção dos discos que não devem ser desfragmentados automaticamente. Toque ou clique em OK para salvar suas configurações.
6. Toque ou clique em OK e em Close.

CAPÍTULO 12

Compartilhamento de dados, segurança e auditoria

- Como utilizar e habilitar o compartilhamento de arquivos **455**
- Configuração de compartilhamento de arquivos padrão **458**
- Gerenciamento de permissões de compartilhamento **466**
- Gerenciamento de compartilhamentos existentes **471**
- Configuração do compartilhamento NFS **476**
- Utilização de cópias de sombra **478**
- Conexão com unidades de rede **481**
- Gerenciamento, posse e herança de objetos **482**
- Permissões de arquivos e pastas **485**
- Auditoria de recursos do sistema **495**
- Utilização, configuração e gerenciamento de cotas de disco do NTFS **500**
- Utilização, configuração e gerenciamento de cotas de disco do Resource Manager **511**

O protocolo Server Message Block (SMB) é o principal protocolo de compartilhamento de arquivos utilizado por computadores com o Microsoft Windows. Quando pastas são compartilhadas por uma rede, um cliente SMB lê e grava arquivos e solicita serviços de computadores hospedando pastas compartilhadas via SMB. O Windows 8 e o Windows Server 2012 dão suporte à versão 3.0 do SMB e incluem um cliente compatível com ele.

O SMB 3.0 traz muitas melhorias para o desempenho, especialmente quando se utiliza servidores de arquivos em cluster. Uma melhoria importante que não depende de uma configuração especial é a criptografia de um extremo a outro de dados SMB, que elimina a necessidade de utilizar o Internet Protocol security (protocolo IPsec), hardware especializado ou aceleradores de wide area network (WAN, rede de longa distância) para proteger os dados de escutas. A criptografia SMB pode ser habilitada por compartilhamento.

Com o SMB, o Windows Server 2012 dá suporte a dois modelos de compartilhamento de arquivos: *standard file sharing* (*compartilhamento de arquivos padrão*) e *public folder sharing* (*compartilhamento de pasta pública*). O compartilhamento de arquivos padrão permite que os usuários remotos acessem os recursos de rede, como arquivos, pastas e unidades. Quando se compartilha uma pasta ou unidade, todos os seus arquivos e subpastas são disponibilizados para um conjunto especificado de usuários. Como não é necessário mover os arquivos de sua localização atual, o compartilhamento de arquivos padrão também é chamado de *in-place file sharing* (*compartilhamento de arquivos no local*).

Pode-se habilitar o compartilhamento de arquivos padrão em discos formatados com FAT, FAT32, exFAT, NTFS ou Resilient File System (ReFS). Um conjunto de permissões é aplicado aos discos formatados com exFAT, FAT ou FAT32. Essas permissões são chamadas de *share permissions* (permissões de compartilhamento). Dois conjuntos de permissões são aplicados aos discos formatados com NTFS ou ReFS: As *permissões NTFS* (também chamadas de *access permissions* [permissões de acesso]) e as *permissões de compartilhamento*. Ter dois conjuntos de permissões permite determinar exatamente quem tem acesso aos arquivos compartilhados e o nível de acesso atribuído. Com as permissões do NTFS ou as permissões de compartilhamento, não é preciso mover os arquivos que se compartilha.

Com o compartilhamento de pasta pública, se compartilha arquivos simplesmente copiando ou movendo-os para a pasta Public do computador. Os arquivos públicos estão disponíveis para qualquer pessoa que se conecte ao computador localmente, não importando se tem uma conta de usuário padrão ou de administrador nele. Também se pode conceder acesso via rede para a pasta Public. Se o fizer, no entanto, não haverá restrições de acesso. A pasta Public e seu conteúdo estarão abertos para qualquer pessoa que possa acessar o computador pela rede local.

Como utilizar e habilitar o compartilhamento de arquivos

As configurações de compartilhamento do computador determinam a maneira como os arquivos podem ser compartilhados. Os dois modelos de compartilhamento de arquivos a que o Windows Server 2012 dá suporte têm as seguintes diferenças:

- **Standard (in-place) file sharing** Permite que os usuários remotos acessem arquivos, pastas e unidades por meio da rede. Quando se compartilha uma pasta ou unidade, todos os seus arquivos e subpastas são disponibilizados para um conjunto especificado de usuários. As permissões de compartilhamento e as permissões de acesso juntas permitem controlar quem tem acesso aos arquivos compartilhados e o nível de acesso atribuído. Não é preciso mover os arquivos que estão sendo compartilhados.
- **Public folder sharing** Permite que os usuários locais e (opcionalmente) os usuários remotos acessem qualquer arquivo colocado na pasta %SystemDrive%\Users\Public do computador. As permissões de acesso na pasta Public determinam quais usuários e grupos têm acesso aos arquivos compartilhados publicamente, bem como o seu nível de acesso. Quando se copia ou move arquivos para a pasta Public, as permissões de acesso são alteradas para corresponderem à dessa pasta. Outras permissões também são adicionadas. Quando um computador faz parte de um grupo de trabalho, pode-se adicionar à pasta Public a proteção por senha. A proteção por senha separada não é necessária em um domínio. Em um domínio, somente os usuários do domínio podem acessar os dados da pasta Public.

Com o compartilhamento de arquivos padrão, os usuários locais não têm acesso automático a qualquer dado armazenado no computador. Controla-se o acesso local a arquivos e pastas utilizando as configurações de segurança no disco local. Com o compartilhamento de pasta pública, por outro lado, os arquivos copiados ou movidos para a pasta Public ficam disponíveis para qualquer pessoa que se conecte localmente.

Também se pode conceder acesso via rede para a pasta Public. Fazê-lo, no entanto, deixa a pasta Public e seu conteúdo abertos para qualquer pessoa que possa acessar o computador pela rede.

O Windows Server 2012 adiciona novas camadas de segurança por meio de identidades compostas, controles de acesso com base em declarações (claims) e políticas de acesso central. Com o Windows 8 e o Windows Server 2012, pode-se atribuir controles de acesso com base em declarações para recursos de arquivos e pastas em volumes NTFS e ReFS. Com o Windows Server 2012, os usuários recebem acesso aos recursos de arquivos e pastas, seja diretamente, com permissões de acesso e permissões de compartilhamento, ou indiretamente, com controles de acesso baseados em declarações e políticas de acesso central.

O SMB 3.0 torna possível criptografar dados sendo transferidos pela rede. Pode-se habilitar a criptografia SMB para compartilhamentos configurados em volumes NTFS e ReFS. A criptografia SMB funciona somente quando o computador solicitando os dados de um compartilhamento baseado no SMB (seja um compartilhamento de arquivo padrão ou um compartilhamento do DFS) e o servidor fornecendo os dados suportam o SMB 3.0. O Windows 8 e o Windows Server 2012 dão suporte ao SMB 3.0. (Eles têm um cliente SMB 3.0.)

MUNDO REAL Embora o ReFS ofereça um sistema de arquivos altamente confiável, lembre-se de que ele não suporta cópias de sombra. Portanto, se criar compartilhamentos em volumes ReFS, os usuários não poderão voltar a versões anteriores de arquivos e pastas armazenados em compartilhamentos.

O compartilhamento de pasta pública foi desenvolvido para permitir que os usuários compartilhem arquivos e pastas a partir de um único local. Com o compartilhamento de pasta pública, basta copiar ou mover os arquivos que se quer compartilhar para a pasta %SystemDrive%\Users\Public do computador. É possível acessar as pastas públicas no File Explorer. No File Explorer, toque ou clique duas vezes na unidade do sistema e acesse a pasta Users\Public.

A pasta Public tem diversas subpastas que podem ser utilizadas para ajudar a organizar os arquivos públicos:

- **Public Desktop** Utilizada para itens compartilhados da área de trabalho. Qualquer arquivo ou atalho de programa colocado na pasta Public Desktop aparecerá na área de trabalho de todos os usuários que se conectem ao computador (e ficam disponíveis para todos os usuários da rede que tenham recebido acesso à pasta Public).
- **Public Documents, Public Music, Public Pictures, Public Videos** Utilizada para documentos e arquivos de mídia compartilhados. Todos os arquivos colocados em uma destas subpastas estarão disponíveis para todos os usuários que se conectem ao computador (e para todos os usuários da rede se o acesso à rede tiver sido concedido para a pasta Public).
- **Public Downloads** Utilizada para downloads compartilhados. Todos os arquivos colocados na subpastas Public Downloads estarão disponíveis para todos os usuários que se conectem ao computador (e para todos os usuários da rede se o acesso a ela tiver sido concedido para a pasta Public).

Por padrão, qualquer pessoa com uma conta de usuário e senha em um computador pode acessar a pasta Public dele. Quando se copia ou move arquivos para a pasta Public, as permissões de acesso são alteradas para corresponder às dessa pasta e outras permissões também são adicionadas.

Pode-se alterar a configuração de compartilhamento da pasta Public de duas maneiras principais:

- Permitir que os usuários conectados ao computador visualizem e gerenciem arquivos públicos, mas restringir o acesso de usuários da rede a eles. Quando se configura essa opção, os grupos implícitos Interactive, Batch e Service recebem permissões especiais para arquivos e pastas públicos.
- Permitir que os usuários com acesso à rede visualizem e gerenciem arquivos públicos. Permite aos usuários da rede abrir, alterar, criar e excluir arquivos públicos. Quando se configura essa opção, o grupo implícito Everyone recebe a permissão Full Control para arquivos e pastas públicos.

O Windows Server 2012 pode utilizar qualqure um dos modelos de compartilhamento ou ambos a qualquer momento. No entanto, o compartilhamento de arquivos padrão oferece mais segurança e melhor proteção que o compartilhamento de pasta pública, e o aumento da segurança é essencial para proteger os dados de sua empresa. Com o compartilhamento de arquivos padrão, as permissões de compartilhamento são utilizadas somente quando um usuário tenta acessar um arquivo ou uma pasta de um computador diferente na rede. As permissões de acesso são sempre utilizadas, esteja o usuário conectado ao console ou utilizando um sistema remoto para acessar um arquivo ou uma pasta pela rede. Quando os dados são acessados remotamente, primeiro, as permissões de compartilhamento são aplicadas e, depois, as permissões de acesso.

Como mostrado na Figura 12-1, pode-se fazer as configurações básicas de compartilhamento de arquivos para um servidor utilizando Advanced Sharing Settings em Network And Sharing Center. Opções separadas são oferecidas para descoberta de rede, compartilhamento de arquivos e impressora, e compartilhamento de pasta pública.

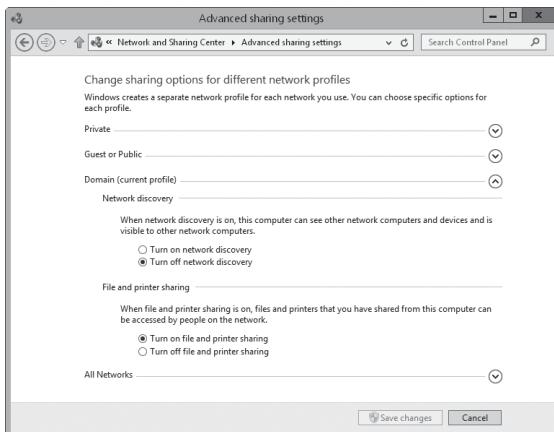


FIGURA 12-1 O Network And Sharing Center mostra a configuração atual de compartilhamento.

Pode-se gerenciar a configuração de compartilhamento do computador seguindo estas etapas:

1. No Control Panel, toque ou clique em View Network Status And Tasks sob o título Network And Internet. O Network And Sharing Center será aberto.
2. No Network And Sharing Center, toque ou clique em Change Advanced Sharing Settings no painel esquerdo. Selecione o perfil de rede para a rede na qual quer habilitar o compartilhamento de arquivos e impressora. Normalmente, esse será o perfil Domain.
3. O compartilhamento de arquivos e impressoras padrão controla o acesso à rede para recursos compartilhados. Para configurar o compartilhamento de arquivos padrão, faça uma das opções a seguir:
 - Selecione Turn On File And Printer Sharing para habilitar o compartilhamento de arquivos.
 - Selecione Turn Off File And Printer Sharing para desabilitar o compartilhamento de arquivos.
4. O compartilhamento de pasta pública controla o acesso à pasta Public do computador. Para configurar o compartilhamento de pasta pública, expanda o painel All Networks Public Folder Sharing tocando ou clicando no botão de expansão relacionado. Escolha uma das seguintes opções:
 - **Turn On Sharing So Anyone With Network Access Can Read And Write Files In The Public Folders** Permite o compartilhamento de pasta pública concedendo acesso à pasta Public e a todos os dados públicos a todos que possam acessar o computador pela rede. As configurações do Firewall do Windows talvez impeçam o acesso externo.
 - **Turn Off Public Folder Sharing** Desabilita o compartilhamento de pasta pública, impedindo o acesso via rede local à pasta Public. Todos que se conectarem localmente ao computador ainda poderão acessar a pasta Public e seus arquivos.
5. Toque ou clique em Save Changes.

Configuração de compartilhamento de arquivos padrão

Utiliza-se compartilhamentos para controlar o acesso de usuários remotos. As permissões em pastas compartilhadas não têm qualquer efeito para usuários que se conectem localmente a um servidor ou a uma estação de trabalho que tenha pastas compartilhadas.

Visualização de compartilhamentos existentes

Pode-se utilizar o Computer Management e o Server Manager para trabalhar com compartilhamentos. Também é possível visualizar os compartilhamentos atuais do computador digitando **net share** em um prompt de comando ou digitando **get-smbshare** em um prompt do PowerShell.

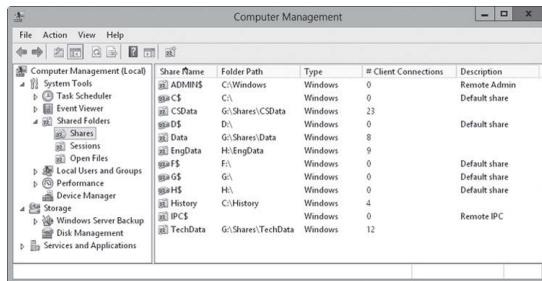
DICA O cmdlet **get-smbshare** é apenas um dos muitos cmdlets associados com o módulo **smbshare**. Para obter uma lista de outros cmdlets disponíveis para trabalhar com compartilhamentos SMB, digite **get-command –module smbshare** em um prompt do PowerShell.

OBSERVAÇÃO Computer Management, **net share** e **get-smbshare** exibem informações sobre os compartilhamentos com base no SMB, incluindo compartilhamentos de pastas SMB padrão, compartilhamentos de pastas SMB ocultos (aqueles que terminam com o sufixo \$) e as pas-

tas SMB compartilhadas utilizando o Distributed File System (DFS). O Server Manager exibe informações sobre os compartilhamentos de pastas SMB padrão, pastas SMB compartilhadas utilizando o DFS e pastas compartilhadas utilizando o NFS. O Server Manager não exibe informações sobre compartilhamentos de pastas SMB ocultos.

No Computer Management, pode-se visualizar as pastas compartilhadas em um computador local ou remoto seguindo estas etapas:

1. Você está conectado ao computador local por padrão. Se quiser se conectar a um computador remoto, pressione e segure ou clique com o botão direito do mouse no nó Computer Management e toque ou clique em Connect To Another Computer. Escolha Another Computer, digite o nome ou endereço IP do computador ao qual quer se conectar e toque ou clique em OK.
2. Na árvore de console, expanda System Tools, Shared Folders e selecione Shares. Os compartilhamentos atuais no sistema serão exibidos, como mostrado na Figura 12-2.



The screenshot shows the Windows Server 2012 Computer Management interface. The left navigation pane is collapsed. The main window title is "Computer Management". Under the "Shares" node in the tree view, a table lists various shared folders. The columns are: Share Name, Folder Path, Type, # Client Connections, and Description. The data is as follows:

Share Name	Folder Path	Type	# Client Connections	Description
ADMIN\$	C:\Windows	Windows	0	Remote Admin
C\$	C:\	Windows	0	Default share
C\$Data	G:\Shares\CSData	Windows	23	
D\$	D:\	Windows	0	Default share
Data	G:\Shares\Data	Windows	8	
EngData	H:\EngData	Windows	9	
F\$	F:\	Windows	0	Default share
G\$	G:\	Windows	0	Default share
H\$	H:\	Windows	0	Default share
History	C:\History	Windows	4	
IPC\$		Windows	0	Remote IPC
TechData	G:\Shares\TechData	Windows	12	

FIGURA 12-2 Os compartilhamentos disponíveis são listados no nó Shared Folders.

3. As colunas do nó Shares fornecem as seguintes informações:
 - **Share Name** O nome da pasta compartilhada.
 - **Folder Path** O caminho completo para a pasta no sistema local.
 - **Type** Quais tipos de computadores podem utilizar o compartilhamento. Normalmente, mostrará o Windows, pois os compartilhamentos SMB são para computadores baseados no Windows.
 - **# Client Connections** O número de clientes acessando o compartilhamento no momento.
 - **Description** A descrição do compartilhamento.

No Server Manager, pode-se visualizar as pastas compartilhadas em um computador local ou remoto seguindo estas etapas:

1. Selecione o nó File And Storage Services e o subnó Shares relacionado.
2. Como a Figura 12-3 mostra, o subnó Shares fornece informações sobre os compartilhamentos em cada servidor de arquivos que tenha sido adicionado para gerenciamento. As colunas do subnó Shares fornecem as seguintes informações:
 - **Share** O nome da pasta compartilhada.
 - **Local Path** O caminho completo para a pasta no sistema local.

- **Protocol** Qual protocolo o compartilhamento utiliza, SMB ou NFS.
- **Cluster Role** Se o servidor compartilhando a pasta fizer parte do cluster, a função de cluster será mostrada aqui. Caso contrário, a função cluster será listada como None.

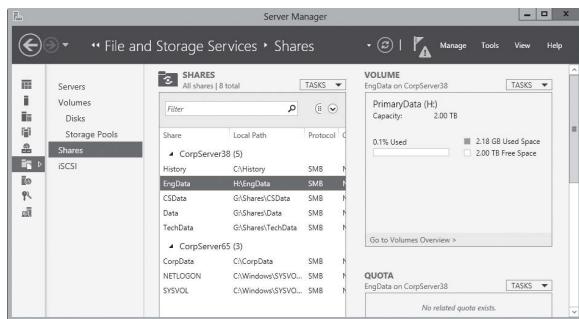


FIGURA 12-3 Toque ou clique em Shares no painel principal (à esquerda) para visualizar os compartilhamentos disponíveis.

3. Ao tocar ou clicar em um compartilhamento no painel Shares, as informações sobre o volume relacionado serão exibidas no painel Volume.

MUNDO REAL O Network File System (NFS) é o protocolo de compartilhamento de arquivos utilizado pelos sistemas baseados em UNIX, o que inclui computadores com o Apple OS X. Conforme abordado em “Configuração do compartilhamento NFS” mais adiante neste capítulo, pode-se habilitar o suporte para o NFS instalando o serviço de função Server For NFS como parte da configuração do servidor de arquivos.

Criação de pastas compartilhadas no Computer Management

O Windows Server 2012 oferece diversas formas de compartilhar pastas. Pode-se compartilhar pastas locais utilizando o File Explorer e as pastas locais e remotas usando o Computer Management ou o Server Manager.

Quando você cria um compartilhamento com o Computer Management, configura suas permissões de compartilhamento e faz suas configurações offline. Quando cria um compartilhamento com o Server Manager, pode provisionar todos os aspectos do compartilhamento, incluindo as permissões do NTFS, o acesso a dados criptografados, as configurações offline para armazenamento em cache e as permissões de compartilhamento. Normalmente, cria-se compartilhamentos em volumes NTFS, pois o NTFS oferece a solução mais robusta.

No Computer Management, compartilha-se uma pasta seguindo estas etapas:

1. Se necessário, conecte-se a um computador remoto. Na árvore de console, expanda System Tools, Shared Folders e selecione Shares. Os compartilhamentos atuais no sistema serão exibidos.
2. Pressione e segure ou clique com o botão direito do mouse em Shares e toque ou clique em New Share. O Provision A Shared Folder Wizard será iniciado. Toque ou clique em Next.

3. Na caixa de texto Folder Path, digite o caminho do arquivo local para a pasta que quer compartilhar. O caminho do arquivo deve ser exato, como **C:\EntData\Documents**. Se não souber o caminho completo, toque ou clique em Browse, utilize a caixa de diálogo Browse For Folder para localizar a pasta que quer compartilhar e toque ou clique em OK. Toque ou clique em Next.
- DICA** Se o caminho de arquivo especificado não existir, o assistente poderá criá-lo para você. Toque ou clique em Yes quando for solicitado, se deseja criar as pastas necessárias.
4. Na caixa de texto Share Name, digite um nome para o compartilhamento, como mostrado na Figura 12-4. Esse é o nome da pasta com a qual os usuários irão se conectar. Os nomes de compartilhamento devem ser exclusivos para cada sistema.

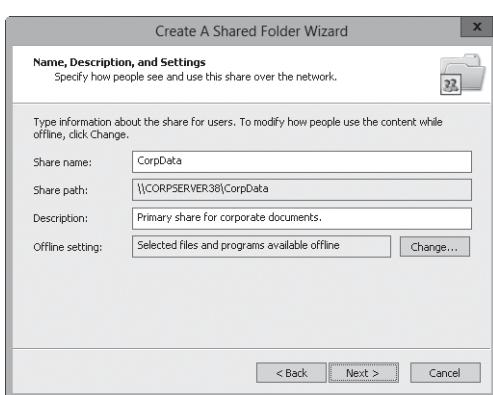


FIGURA 12-4 Utilize o Create A Shared Folder Wizard para configurar as propriedades essenciais de compartilhamento, incluindo o nome, a descrição e o uso de recursos offline.

DICA Se quiser ocultar dos usuários um compartilhamento (isso significa que não poderão ver o recurso compartilhado quando tentarem procurá-lo no File Explorer ou em uma linha de comando), digite um cifrão (\$) como o último caractere do nome do recurso compartilhado. Por exemplo, você poderia criar um compartilhamento chamado PrivEngData\$, que estaria oculto no File Explorer, Net View e outros utilitários similares. Os usuários continuarão podendo se conectar ao compartilhamento e acessar seus dados se tiverem recebido a permissão de acesso e souberem o nome do compartilhamento. Observe que o \$ deve ser digitado como parte do nome de compartilhamento ao mapear para o recurso compartilhado.

5. Se quiser, digite uma descrição do compartilhamento na caixa de texto Description. Ao visualizar compartilhamentos em um determinado computador, a descrição será exibida no Computer Management.
6. Por padrão, o compartilhamento é configurado de modo que somente arquivos e programas que os usuários especifiquem estejam disponíveis para uso offline. Normalmente, essa é a opção que se quer utilizar, pois ela também permite que os usuários aproveitem o novo recurso Always Offline. Se quiser utilizar configurações de arquivos offline diferentes, toque ou clique em Change, selecione as opções apropriadas na caixa de diálogo Offline Settings e toque ou clique em OK. As configurações de disponibilidade offline incluem o seguinte:

- **Only The Files And Programs That Users Specify Are Available Offline** Seleione esta opção se quiser que os computadores clientes armazenem em cache somente os arquivos e programas que os usuários especificarem para uso offline. Opcionalmente, se o serviço de função BranchCache For Network Files estiver instalado no servidor de arquivos, selecione Enable BranchCache para habilitar computadores em uma filial para armazenar em cache os arquivos que sejam baixados da pasta compartilhada e compartilhar os arquivos com outros computadores na filial de modo seguro.
- **No Files Or Programs From The Shared Folder Are Available Offline** Seleione esta opção se não quiser que cópias possam ser armazenadas em cache dos arquivos e programas do compartilhamento para que estejam disponíveis em computadores clientes para uso offline.
- **All Files And Programs That Users Open From The Share Are Automatically Available Offline** Seleione esta opção se quiser que os computadores clientes armazenem em cache todos os arquivos e programas que os usuários abram do compartilhamento. Opcionalmente, selecione Optimize For Performance para executar arquivos de programas armazenados em cache a partir do cache local, em vez da pasta compartilhada no servidor.

7. Toque ou clique em Next e defina as permissões básicas para o compartilhamento. Você encontrará informações úteis em "Gerenciamento de permissões de compartilhamento" mais adiante neste capítulo. As opções disponíveis são as seguintes:

- **All Users Have Read-Only Access** Oferece aos usuários acesso para visualizar arquivos e ler dados. Eles não podem criar, modificar ou excluir arquivos e pastas.
- **Administrators Have Full Access; Other Users Have Read-Only Access** Oferece aos administradores controle total sobre o compartilhamento. O acesso completo permite que os administradores criem, modifiquem e excluam arquivos e pastas. Em um volume ou uma partição NTFS, também dá aos administradores o direito de alterar permissões e apropriar-se de arquivos e pastas. Os outros usuários só podem visualizar os arquivos e ler os dados. Eles não podem criar, modificar ou excluir arquivos e pastas.
- **Administrators Have Full Access; Other Users Have No Access** Oferece aos administradores o controle total sobre o compartilhamento, mas impede que os outros usuários o accessem.
- **Customize Permissions** Permite configurar o acesso para usuários e grupos específicos, que, normalmente, é a melhor técnica a utilizar. A configuração de permissões de compartilhamento é abordada em "Gerenciamento de permissões de compartilhamento".

8. Ao tocar ou clicar em Finish, o assistente irá criar e exibir um relatório de status, que deve declarar "Sharing Was Successful". Se um erro for exibido, observe-o e tome uma medida corretiva conforme apropriado antes de repetir esse procedimento para criar o compartilhamento. Toque ou clique em Finish.

As pastas individuais podem ter vários compartilhamentos. Cada compartilhamento pode ter um nome diferente e um conjunto diferente de permissões de acesso. Para criar compartilhamentos adicionais em um compartilhamento existente, simplesmente siga as etapas anteriores para criar um compartilhamento com as modificações:

- Na etapa 4, ao nomear o compartilhamento, certifique-se de utilizar um nome diferente.
- Na etapa 5, ao adicionar uma descrição ao compartilhamento, utilize uma que explique para que o compartilhamento é utilizado e como é diferente dos outros compartilhamentos da mesma pasta.

Criação de pastas compartilhadas no Server Manager

No Server Manager, compartilha-se uma pasta seguindo estas etapas:

1. O subnó Shares do nó File And Storage Services mostra os compartilhamentos existentes para os servidores de arquivos que tenham sido adicionados para gerenciamento.
2. No painel Shares, toque ou clique em Tasks e em New Share. O New Share Wizard será iniciado. Escolha um dos perfis de compartilhamento de arquivos disponíveis e toque ou clique em Next. O New Share Wizard tem diversos perfis de compartilhamento de arquivos:
 - **SMB Share—Quick** Um perfil básico para a criação de compartilhamentos de arquivos SMB que permite definir suas configurações e permissões.
 - **SMB Share—Advanced** Um perfil avançado para a criação de compartilhamentos de arquivos SMB que permite definir suas configurações, permissões, propriedades de gerenciamento e perfil de cota do NTFS (conforme aplicável).
 - **SMB Share—Applications** Um perfil personalizado para a criação de compartilhamentos de arquivos SMB com configurações apropriadas para Hyper-V, certos bancos de dados e outros aplicativos de servidor. Essencialmente, é o mesmo que o perfil quick (rápido), mas não permite habilitar a enumeração baseada em acesso ou o armazenamento em cache offline.

OBSERVAÇÃO Se estiver utilizando o serviço de função Server For NFS, também estarão disponíveis as opções para criar compartilhamentos NFS.

MUNDO REAL O SMB 3.0 inclui melhorias para aplicativos baseados em servidor. Elas melhoraram o desempenho de pequenas leituras e gravações aleatórias, que são comuns com aplicativos baseados em servidor, como o Microsoft SQL Server OLTP. Com o SMB 3.0, os pacotes também utilizam grandes Maximum Transmission Units (MTUs), o que melhora o desempenho de grandes transferências de dados sequenciais, como aquelas utilizadas para implantar e copiar virtual hard disks (VHDs, discos rígidos virtuais) pela rede, fazer backup de banco de dados e restaurá-lo pela rede, e fazer transações de repositório de dados (data-warehouse) do SQL Server pela rede.

3. Na página Select The Server And Path For This Share, selecione o servidor e o volume em que quer que o compartilhamento seja criado. Somente os servidores de arquivos que tenham sido adicionados para gerenciamento estarão disponíveis. Quando estiver pronto para continuar, toque ou clique em Next.

Por padrão, o Server Manager criará o compartilhamento de arquivos como uma nova pasta no caminho \Shares do volume selecionado. Para substituí-lo, escolha a opção Type A Custom Path e digite o caminho de compartilhamento desejado, como C:\Data, ou clique em Browse para utilizar a caixa de diálogo Select Folder para selecionar o caminho do compartilhamento.

4. Na página Specify Share Name, digite um nome para o compartilhamento, como mostrado na Figura 12-5. Esse é o nome da pasta com a qual os usuários irão se conectar. Os nomes de compartilhamento devem ser exclusivos para cada sistema.

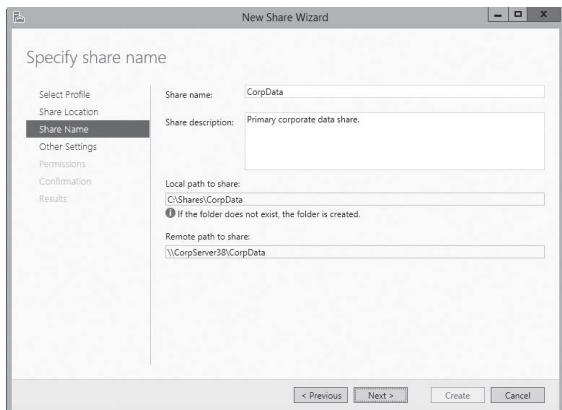


FIGURA 12-5 Defina o nome e a descrição para cada compartilhamento.

5. Se quiser, digite uma descrição do compartilhamento na caixa de texto Description. Ao visualizar compartilhamentos em um determinado computador, a descrição será exibida no Computer Management.
6. Observe os caminhos local e remoto para o compartilhamento. Esses caminhos são definidos com base na localização e no nome do compartilhamento especificados. Quando estiver pronto para continuar, toque ou clique em Next.
7. Na página Configure Share Settings, utilize as opções a seguir para configurar a forma como o compartilhamento será utilizado:
- **Enable Access-Based Enumeration** Configura as permissões de modo que, quando os usuários procurarem a pasta, somente os arquivos e as pastas a que tenham recebido ao menos o acesso Read (leitura) sejam exibidos. Se o usuário não tiver ao menos a permissão Read (ou equivalente) para um arquivo ou uma pasta da pasta compartilhada, esse arquivo ou pasta estará oculto na visualização. (Esta opção estará esmaecida se estiver criando um compartilhamento SMB otimizado para aplicativos.)
 - **Allow Caching Of Share** Configura o compartilhamento para armazenar em cache somente os arquivos e programas que os usuários especificarem para o uso offline. Embora se possa editar posteriormente as propriedades de compartilhamento e alterar as configurações de disponibilidade dos arquivos offline, normalmente se quer selecionar esta opção, porque permite que os usuários aproveitem o novo recurso Always Offline. Opcionalmente, se o serviço de função BranchCache For Network Files estiver instalado no servidor de arquivos, selecione Enable BranchCache para habilitar os computadores em uma filial a armazenar em cache os arquivos que sejam baixados da pasta compartilhada e compartilhar os arquivos com outros computadores na filial de modo

seguro. (Esta opção estará esmaecida se estiver criando um compartilhamento SMB otimizado para aplicativos.)

- **Encrypt Data Access** Configura o compartilhamento para utilizar a criptografia SMB, que protege os dados dos arquivos de escutas (eavesdropping) enquanto são transferidos pela rede. Esta opção será útil em redes não confiáveis.
8. Na página Specify Permissions To Control Access, as permissões padrão atribuídas ao compartilhamento serão listadas. Por padrão, o grupo especial Everyone recebe a permissão de compartilhamento Full Control e as permissões de pastas subjacentes são listadas. Para alterar as permissões de compartilhamento, pasta, ou ambas, toque ou clique em Customize Permissions e utilize a caixa de diálogo Advanced Security Settings para configurar as permissões desejadas. A configuração de permissões de compartilhamento é abordada em "Gerenciamento de permissões de compartilhamento". A configuração de permissões de pastas é abordada em "Permissões de arquivos e pastas" mais adiante neste capítulo.
- OBSERVAÇÃO** Se o compartilhamento for utilizado para Hyper-V, pode ser necessário habilitar a delegação restrita para o gerenciamento remoto do host Hyper-V.
9. Se estiver utilizando o perfil avançado, como opção, defina as propriedades de gerenciamento da pasta e toque ou clique em Next. Essas propriedades especificam a finalidade da pasta e o tipo de dados armazenados nela, a fim de que políticas de gerenciamento de dados, como as regras de classificação, possam utilizar essas propriedades.
10. Se estiver utilizando o perfil avançado, opcionalmente, aplique à pasta uma cota baseada em um modelo e toque ou clique em Next. Você pode selecionar sómente modelos de cota que já tenham sido criados. Para mais informações, consulte "Gerenciamento de modelos de cotas de disco" mais adiante neste capítulo.
11. Na página Confirm Selections, revise suas seleções. Ao tocar ou clicar em Create, o assistente irá criar o compartilhamento, configurá-lo e definir as permissões. O status deve declarar: "The share was successfully created". Se um erro for exibido, observe-o e tome uma medida corretiva conforme apropriado antes de repetir esse procedimento para criar o compartilhamento. Toque ou clique em Close.

Alteração das configurações de pasta compartilhada

Ao criar um compartilhamento, pode-se fazer muitas configurações básicas e avançadas, incluindo aquelas para enumeração baseada em acesso, acesso a dados criptografados, configurações offline para armazenamento em cache e propriedades de gerenciamento. No Server Manager, pode-se modificar essas configurações seguindo estas etapas:

1. O subnó Shares do nó File And Storage Services mostra os compartilhamentos existentes para os servidores de arquivos que tenham sido adicionados para gerenciamento.
2. Pressione e segure ou clique com o botão direito do mouse no compartilhamento com o qual quer trabalhar e toque ou clique em Properties.
3. Na caixa de diálogo Properties, mostrada na Figura 12-6, você tem diversos painéis de opções que podem ser acessados usando os controles no painel esquerdo. Pode-se expandir os painéis um a um ou tocar ou clicar em Show All para expandir todos ao mesmo tempo.

4. Utilize as opções fornecidas para modificar as configurações conforme necessário e toque ou clique em OK. As opções disponíveis serão as mesmas quer utilize o perfil básico, avançado ou de aplicativos para criar a pasta compartilhada.

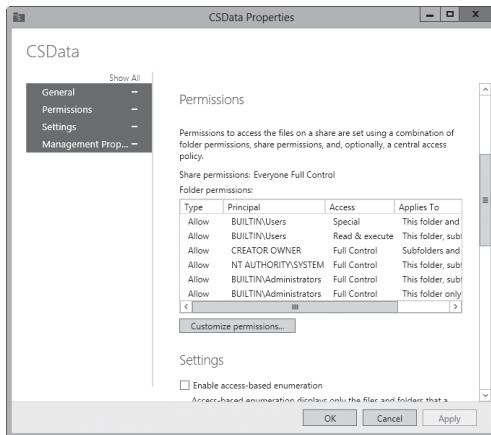


FIGURA 12-6 Modifique as configurações de compartilhamento utilizando as opções fornecidas.

DICA Se estiver criando um compartilhamento para uso e acesso geral, poderá publicar o recurso compartilhado no Active Directory. A publicação do recurso no Active Directory torna a localização do compartilhamento mais fácil para os usuários. Contudo, essa opção não está disponível no Server Manager. Para publicar um compartilhamento no Active Directory, pressione e segure ou clique com o botão direito do mouse no compartilhamento no Computer Management e toque ou clique em Properties. Na guia Publish, marque a caixa de seleção Publish This Share In Active Directory, adicione uma descrição opcional e informações do proprietário e toque ou clique em OK.

Gerenciamento de permissões de compartilhamento

As permissões de compartilhamento determinam as ações permitidas máximas disponíveis dentro de uma pasta compartilhada. Por padrão, quando se cria um compartilhamento, todos que têm acesso à rede têm acesso Read ao conteúdo do compartilhamento. Essa é uma importante alteração de segurança – em versões anteriores do Windows Server, a permissão padrão era Full Control.

Com volumes NTFS e ReFS, pode-se utilizar permissões de arquivo e pasta e posse, bem como permissões de compartilhamento, para restringir ainda mais as ações dentro do compartilhamento. Com volumes FAT, somente as permissões de compartilhamento controlam o acesso.

Permissões de compartilhamento variadas

Das mais às menos restritivas, as permissões de compartilhamento disponíveis são as seguintes:

- **No Access** Nenhuma permissão é concedida no compartilhamento.
- **Read** Com esta permissão, os usuários podem fazer o seguinte:
 - Visualizar os nomes dos arquivos e subpastas
 - Acessar as subpastas no compartilhamento
 - Ler dados e atributos de arquivos
 - Executar arquivos de programas
- **Change** Os usuários têm a permissão Read e a capacidade de fazer o seguinte:
 - Criar arquivos e subpastas
 - Modificar arquivos
 - Alterar atributos nos arquivos e subpastas
 - Excluir arquivos e subpastas
- **Full Control** Os usuários têm as permissões Read e Change, bem como as seguintes capacidades adicionais em volumes NTFS:
 - Alterar permissões de arquivo e pasta
 - Apropriar-se de arquivos e pastas

É possível atribuir as permissões de compartilhamento a usuários e grupos. Pode-se até mesmo atribuir permissões a grupos implícitos. Para detalhes sobre grupos implícitos, consulte “Grupos implícitos e identidades especiais” no Capítulo 8, “Como criar contas de usuário e de grupo”.

Visualização e configuração de permissões de compartilhamento

Você pode visualizar e configurar as permissões de compartilhamento no Computer Management ou no Server Manager. Para visualizar e configurar as permissões de compartilhamento no Computer Management, siga estas etapas:

1. No Computer Management, conecte-se ao computador em que o compartilhamento foi criado. Na árvore de console, expanda System Tools, Shared Folders e selecione Shares.
2. Pressione e segure ou clique com o botão direito do mouse no compartilhamento com o qual quer trabalhar e toque ou clique em Properties.
3. Na caixa de diálogo Properties, toque ou clique na guia Share Permissions, mostrada na Figura 12-7. Você visualizará os usuários e grupos que têm acesso ao compartilhamento e o tipo de acesso que possuem.
4. Os usuários ou grupos que já têm acesso ao compartilhamento são listados na lista Group Or User Names. Pode-se remover as permissões para esses usuários e grupos selecionando o usuário ou o grupo que quer remover e tocando ou clicando em Remove. Você pode alterar as permissões para esses usuários e grupos fazendo o seguinte:
 - a. Selecione o usuário ou grupo que quer alterar.
 - b. Conceda ou negue as permissões de acesso na caixa da lista Permissions.

5. Para adicionar permissões para outro usuário ou grupo, toque ou clique em Add. A caixa de diálogo Select Users, Computers, Service Accounts, Or Groups, mostrada na Figura 12-8, será aberta.

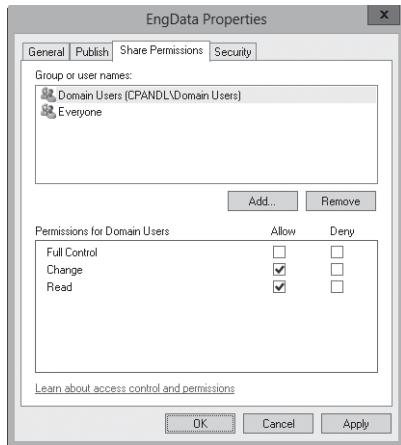


FIGURA 12-7 A guia Share Permissions mostra quais usuários e grupos têm acesso ao compartilhamento e qual tipo de acesso possuem.

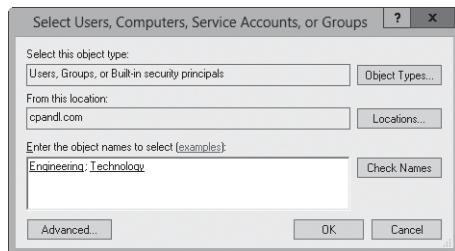


FIGURA 12-8 Adicione usuários e grupos ao compartilhamento.

6. Digite o nome de um usuário, computador ou grupo no domínio atual e toque ou clique em Check Names. Um dos seguintes resultados será produzido:
- Se uma única correspondência for encontrada, a caixa de diálogo será automaticamente atualizada e a entrada estará sublinhada.
 - Se nenhuma correspondência for encontrada, ou uma parte do nome digitado está incorreta, ou você está trabalhando com uma localização incorreta. Modifique o nome e tente de novo, ou toque ou clique em Locations para selecionar uma nova localização.
 - Se várias correspondências forem encontradas, selecione os nomes que quer utilizar e toque ou clique em OK. Para atribuir permissões a outros usuários, computadores ou grupos, digite um ponto e vírgula (;) e repita esta etapa.

OBSERVAÇÃO O botão Locations permite acessar nomes de contas em outros domínios. Toque ou clique em Locations para ver uma lista com o domínio atual, os domínios confiáveis e outros recursos que você pode acessar. Por causa das relações de confiança transitivas no Windows Server, normalmente se pode acessar todos os domínios na árvore ou floresta do Active Directory.

7. Toque ou clique em OK. Os usuários e grupos serão adicionados à lista Group Or User Names do compartilhamento.
8. Configure as permissões de acesso para cada usuário, computador e grupo selecionando um nome de conta e concedendo ou negando as permissões de acesso. Lembre-se de que está determinando as permissões admissíveis (permitidas) máximas para uma determinada conta.
9. Toque ou clique em OK. Para atribuir permissões de segurança adicionais para o NTFS, consulte “Permissões de arquivos e pastas” mais adiante neste capítulo.

Para visualizar e configurar as permissões de compartilhamento no Server Manager, siga estas etapas:

1. O subnó Shares do nó File And Storage Services mostra os compartilhamentos existentes para os servidores de arquivos que tenham sido adicionados para gerenciamento.
2. Pressione e segure ou clique com o botão direito do mouse no compartilhamento com o qual quer trabalhar e toque ou clique em Properties.
3. Na caixa de diálogo Properties, toque ou clique em Permissions no painel esquerdo. Você visualizará os usuários e grupos que têm acesso ao compartilhamento e o tipo de acesso que possuem.
4. Para alterar as permissões de compartilhamento, pasta ou ambas, toque ou clique em Customize Permissions. A seguir, selecione a guia Share na caixa de diálogo Advanced Security Settings, como mostrado na Figura 12-9.

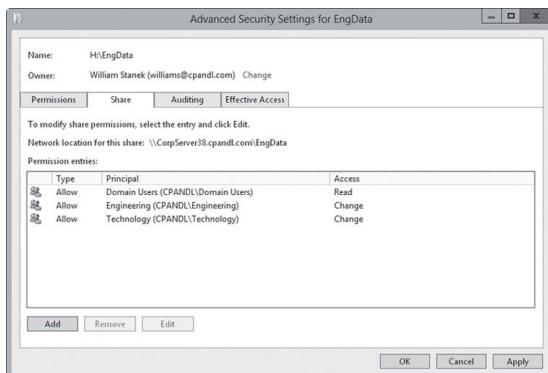


FIGURA 12-9 A guia Share mostra quais usuários e grupos têm acesso ao compartilhamento e qual tipo de acesso possuem.

5. Os usuários ou grupos que já têm acesso ao compartilhamento são listados na lista Permission Entries. Pode-se remover as permissões para esses usuários e grupos sele-

cionando o usuário ou o grupo que quer remover e tocando ou clicando em Remove. Você pode alterar as permissões para esses usuários e grupos fazendo o seguinte:

- a. Selecione o usuário ou grupo que quer alterar e selecione Edit.
- b. Conceda ou negue as permissões de acesso na lista Permissions Entries e toque ou clique em OK.
6. Para adicionar permissões para outro usuário ou grupo, toque ou clique em Add. A caixa de diálogo Permission Entry, mostrada na Figura 12-10, será aberta.

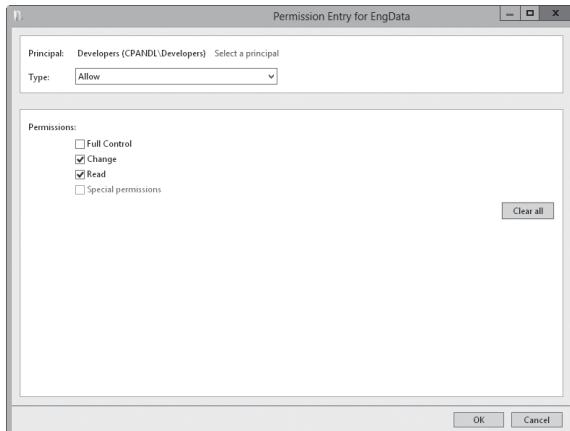


FIGURA 12-10 Adicione entradas de permissão para um usuário ou grupo específico.

7. Toque ou clique em Select A Principal para exibir a caixa de diálogo Select User, Computer, Service Account Or Group. Digite o nome de um usuário ou de uma conta de grupo. Certifique-se de fazer referência ao nome da conta de usuário, em vez do nome completo do usuário. Apenas um nome por vez pode ser digitado.
8. Toque ou clique em Check Names. Se uma única correspondência for encontrada para a entrada, a caixa de diálogo será automaticamente atualizada e a entrada estará sublinhada. Caso contrário, você verá uma caixa de diálogo adicional. Se nenhuma correspondência for encontrada, ou o nome foi digitado incorretamente, ou você está trabalhando com uma localização incorreta. Modifique o nome na caixa de diálogo Name Not Found e tente de novo, ou toque ou clique em Locations para selecionar uma nova localização. Se várias correspondências forem encontradas, na caixa de diálogo Multiple Names Found, selecione o nome que quer utilizar e toque ou clique em OK.
9. Toque ou clique em OK. O usuário ou o grupo é adicionado como Principal e a caixa de diálogo Permission Entry será atualizada para mostrá-lo.
10. Utilize a lista Type para especificar se está configurando permissões concedidas ou negadas e selecione as permissões que quer conceder ou negar.
11. Toque ou clique em OK para retornar à caixa de diálogo Advanced Security Settings. Para atribuir permissões de segurança adicionais para NTFS, consulte "Permissões de arquivos e pastas" mais adiante neste capítulo.

Gerenciamento de compartilhamentos existentes

Como administrador, você muitas vezes tem de gerenciar pastas compartilhadas. Esta seção aborda as tarefas administrativas comuns do gerenciamento de compartilhamentos.

Os compartilhamentos especiais

Quando se instala o Windows Server, o sistema operacional cria compartilhamentos especiais automaticamente. Esses compartilhamentos são conhecidos como *administrative shares* (compartilhamentos administrativos) e *hidden shares* (compartilhamentos ocultos). Eles foram desenvolvidos para ajudar a tornar a administração de sistemas mais fácil. Não se pode definir permissões de acesso em compartilhamentos especiais criados automaticamente; o Windows Server atribui as permissões de acesso. (Você pode criar seus próprios compartilhamentos ocultos adicionando o símbolo \$ como último caractere do nome do compartilhamento.)

Pode-se excluir compartilhamentos especiais temporariamente se tiver certeza de que não são necessários. Contudo, os compartilhamentos serão automaticamente recriados na próxima vez que o sistema operacional for inicializado. Para desabilitar permanentemente os compartilhamentos administrativos, altere os seguintes valores de registro para 0 (zero):

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\AutoShareServer
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\AutoShareWks

Quais compartilhamentos especiais estarão disponíveis dependerá de sua configuração do sistema. A Tabela 12-1 lista os compartilhamentos especiais que você pode ver e como são utilizados.

TABELA 12-1 Os compartilhamentos especiais utilizados pelo Windows Server 2012

NOME DO COMPARTILHAMENTO	DESCRIÇÃO	USO
ADMIN\$	Um compartilhamento utilizado durante a administração remota de um sistema. Fornece acesso à %SystemRoot% do sistema operacional.	Em estações de trabalho e servidores, os administradores e operadores de backup podem acessar esses compartilhamentos. Em controladores de domínio, os operadores de servidor também têm acesso.
FAX\$	Dá suporte aos fax de rede.	É utilizado por clientes de fax ao enviar fax.
IPC\$	Dá suporte aos pipes nomeados durante o acesso de interprocess communications (IPC, comunicações entre processos) remotas.	É utilizado por programas ao realizar a administração remota e visualizar recursos compartilhados.

Continua

TABELA 12-1 Os compartilhamentos especiais utilizados pelo Windows Server 2012
(continuação)

NOME DO COMPARTILHAMENTO	DESCRIÇÃO	USO
NETLOGON	Dá suporte ao serviço Net Logon.	É utilizado pelo serviço Net Logon ao processar solicitações de logon no domínio. Todos têm acesso Read.
PRINT\$	Dá suporte aos recursos de impressora compartilhada fornecendo acesso aos drivers de impressora.	É utilizado por impressoras compartilhadas. Todos têm acesso Read. Os administradores, operadores de servidor e operadores de impressão têm Full Control.
SYSVOL	Dá suporte ao Active Directory.	É utilizado para armazenar dados e objetos do Active Directory.
Driveletter\$	Um compartilhamento que permite aos administradores se conectar à pasta raiz de uma unidade. Esses compartilhamentos são mostrados como C\$, D\$, E\$, e assim por diante.	Em estações de trabalho e servidores, os administradores e operadores de backup podem acessar esses compartilhamentos. Em controladores de domínio, os operadores de servidor também têm acesso.

Conexão com compartilhamentos especiais

Os compartilhamentos especiais terminam com o símbolo \$. Embora esses compartilhamentos não sejam exibidos no File Explorer, os administradores e certos operadores podem se conectar a eles. Para se conectar a um compartilhamento especial, siga estas etapas:

1. Abra o File Explorer, toque ou clique no botão da opção mais à esquerda na lista de endereços e em Computer.
2. A seguir, toque ou clique no botão Map Network Drive no painel Computer e em Map Network Drive. A caixa de diálogo Map Network Drive, mostrada na Figura 12-11, será exibida.

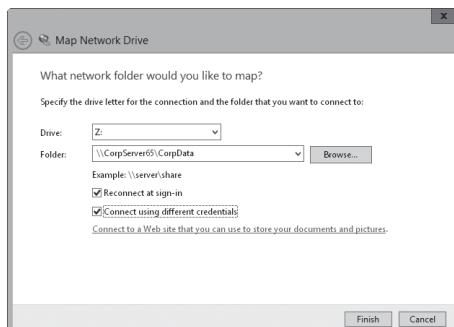


FIGURA 12-11 Conecte-se a compartilhamentos especiais mapeando-os com a caixa de diálogo Map Network

3. Na lista Drive, selecione uma letra de unidade livre. Essa letra de unidade será utilizada para acessar o compartilhamento especial.
4. Na caixa de texto Folder, digite o caminho Universal Naming Convention (UNC) para o compartilhamento. Por exemplo, para acessar o compartilhamento C\$ em um servidor chamado Twiddle, você utilizaria o caminho \\TWIDDLE\C\$.
5. A caixa de seleção Reconnect At Sign-In está marcada automaticamente para garantir que a unidade de rede esteja conectada sempre que fizer logon. Se precisar acessar o compartilhamento somente durante a sessão de logon atual, desmarque essa caixa de seleção.
6. Se precisar se conectar ao compartilhamento utilizando credenciais de usuário diferente, marque a caixa de seleção Connect Using Different Credentials.
7. Toque ou clique em Finish. Se estiver se conectando utilizando credenciais diferentes, digite o nome do usuário e a senha quando for solicitado. Digite o nome do usuário no formato Domain\Username, como **Cpandl\Williams**. Antes de tocar ou clicar em OK, selecione Remember My Credentials se quiser que as credenciais sejam salvas. Caso contrário, será necessário fornecer as credenciais no futuro.

Depois de se conectar a um compartilhamento especial, poderá acessá-lo como faria com qualquer outra unidade. Como os compartilhamentos especiais são protegidos, não é preciso se preocupar com usuários comuns acessando-os. Na primeira vez que se conectar ao compartilhamento, talvez seja pedido um nome de usuário e uma senha. Se for solicitado, forneça essas informações.

Visualização de sessões de usuário e computador

Você pode utilizar o Computer Management para monitorar todas as conexões com recursos compartilhados em um sistema Windows Server 2012. Toda vez que um usuário ou computador se conectar a um recurso compartilhado, o Windows Server 2012 listará uma conexão no nó Sessions.

Para visualizar as conexões com recursos compartilhados, digite **net session** em um prompt de comando ou siga estas etapas:

1. No Computer Management, conecte-se ao computador em que o recurso compartilhado foi criado.
2. Na árvore de console, expanda System Tools, Shared Folders e selecione Sessions. Você visualizará as conexões de usuários e computadores com compartilhamentos.

As colunas do nó Sessions fornecem as seguintes informações importantes sobre as conexões de usuário e computador:

- **User** Os nomes dos usuários ou computadores conectados aos recursos compartilhados. Os nomes dos computadores são mostrados com um sufixo \$ para diferenciá-los dos usuários.
- **Computer** O nome do computador sendo utilizado.
- **Type** O tipo de conexão de rede sendo utilizado.
- **# Open Files** O número de arquivos com o qual o usuário está trabalhandoativamente. Para obter informações mais detalhadas, acesse o nó Open Files.
- **Connected Time** O tempo decorrido desde que a conexão foi estabelecida.

- **Idle Time** O tempo decorrido desde que a conexão foi utilizada pela última vez.
- **Guest** Se o usuário que está conectado é um convidado.

Gerenciamento de sessões e compartilhamentos

O gerenciamento de sessões e compartilhamentos é uma tarefa administrativa comum. Antes de desligar um servidor ou um aplicativo em execução em um servidor, talvez queira desconectar os usuários dos recursos compartilhados. Talvez também seja preciso desconectar os usuários quando se planeja alterar as permissões de acesso ou excluir totalmente um compartilhamento. Outra razão para desconectar os usuários é a quebra de bloqueios em arquivos. Você desconecta os usuários dos recursos compartilhados encerrando as sessões de usuários relacionadas.

ENCERRAMENTO DE SESSÕES INDIVIDUAIS

Para desconectar os usuários individuais dos recursos compartilhados, digite **net session \\computername /delete** em um prompt de comando ou siga estas etapas:

1. No Computer Management, conecte-se ao computador em que o compartilhamento foi criado.
2. Na árvore de console, expanda System Tools, Shared Folders e selecione Sessions.
3. Pressione e segure ou clique com o botão direito do mouse nas sessões de usuários que quer encerrar e toque ou clique em Close Session.
4. Toque ou clique em Yes para confirmar a ação.

ENCERRAMENTO DE TODAS AS SESSÕES

Para desconectar todos os usuários dos recursos compartilhados, siga estas etapas:

1. No Computer Management, conecte-se ao computador em que o compartilhamento foi criado.
2. Na árvore de console, expanda System Tools, Shared Folders e pressione e segure ou clique com o botão direito do mouse em Sessions.
3. Toque ou clique em Disconnect All Sessions e em Yes para confirmar a ação.

OBSERVAÇÃO Lembre-se de que está desconectando os usuários dos recursos compartilhados, não do domínio. Você pode utilizar somente horários de logon e a Group Policy para forçar a desconexão de usuários uma vez que eles tenham feito logon no domínio. Portanto, desconectar os usuários não os desconecta da rede. Simplesmente os desconecta do recurso compartilhado.

Gerenciamento de recursos abertos

Toda vez que os usuários se conectarem aos compartilhamentos, os recursos individuais de arquivo e objeto com os quais estiverem trabalhando serão exibidos no nó Open Files. O nó Open Files pode mostrar os arquivos que o usuário tiver aberto mas não esteja editando no momento.

Pode-se acessar o nó Open Files seguindo estas etapas:

1. No Computer Management, conecte-se ao computador em que o compartilhamento foi criado.

2. Na árvore de console, expanda System Tools, Shared Folders e selecione Open Files. O nó Open Files será exibido, fornecendo as seguintes informações sobre o uso de recursos:
 - **Open File** O caminho do arquivo ou pasta para o arquivo aberto no sistema local. O caminho também pode ser um pipe nomeado, como \PIPE\spools, que é utilizado para o spool de impressoras.
 - **Accessed By** O nome do usuário acessando o arquivo.
 - **Type** O tipo de conexão de rede sendo utilizado.
 - **# Locks** O número de bloqueios no recurso.
 - **Open Mode** O modo de acesso utilizado quando o recurso foi aberto, como read (leitura), write (gravação) ou write+read (leitura+gravação).

FECHAMENTO DE UM ARQUIVO ABERTO

Para fechar um arquivo aberto em compartilhamentos do computador, siga estas etapas:

1. No Computer Management, conecte-se ao computador com o qual quer trabalhar.
2. Na árvore de console, expanda System Tools, Shared Folders e selecione Open Files.
3. Pressione e segure ou clique com o botão direito do mouse no arquivo aberto que quer fechar e toque ou clique em Close Open File.
4. Toque ou clique em Yes para confirmar a ação.

FECHAMENTO DE TODOS OS ARQUIVOS ABERTOS

Para fechar todos os arquivos abertos em compartilhamentos do computador, siga estas etapas:

1. No Computer Management, conecte-se ao computador em que o compartilhamento foi criado.
2. Na árvore de console, expanda System Tools, Shared Folders e pressione e segure ou clique com o botão direito do mouse em Open Files.
3. Toque ou clique em Disconnect All Open Files e em Yes para confirmar a ação.

Interrupção do compartilhamento de arquivos e pastas

Para parar de compartilhar uma pasta, siga estas etapas:

1. Faça uma das opções a seguir:
 - No Server Manager, selecione o compartilhamento que quer gerenciar no sub-nó Shares do nó File And Storage Services.
 - No Computer Management, conecte-se ao computador em que o compartilhamento foi criado e acesse o nó Shares.
2. Pressione e segure ou clique com o botão direito do mouse no compartilhamento que quer remover, toque ou clique em Stop Sharing e em Yes para confirmar a ação.

ATENÇÃO Nunca se deve excluir uma pasta contendo compartilhamentos sem antes interrompê-los. Se não conseguir interrompê-los, o Windows Server 2012 tentará restabelecê-los na próxima vez que o computador for inicializado e o erro resultante será registrado no log de eventos do sistema.

Configuração do compartilhamento NFS

Como discutido no Capítulo 10, “Gerenciamento de sistemas de arquivos e unidades”, você pode instalar o Server For NFS como um serviço de função em um servidor de arquivos. O Server For NFS fornece uma solução para compartilhamento de arquivos para empresas com ambientes combinados de Windows, OS X e UNIX, permitindo que os usuários transfiram arquivos entre os sistemas operacionais Windows Server 2012, OS X e UNIX utilizando o protocolo Network File System (NFS).

Pode-se configurar o compartilhamento NFS para pastas locais em volumes NTFS utilizando o File Explorer. Você também pode configurar o compartilhamento NFS de pastas locais e remotas em volumes NTFS utilizando o Server Manager. No File Explorer, siga estas etapas para habilitar e configurar o compartilhamento NFS:

1. Pressione e segure ou clique com o botão direito do mouse no compartilhamento que quer gerenciar e toque ou clique em Properties. A caixa de diálogo Properties do compartilhamento será exibida.
2. Na guia NFS Sharing, toque ou clique em Manage NFS Sharing.
3. Na caixa de diálogo NFS Advanced Sharing, marque a caixa de seleção Share This Folder, como mostrado na Figura 12-12.

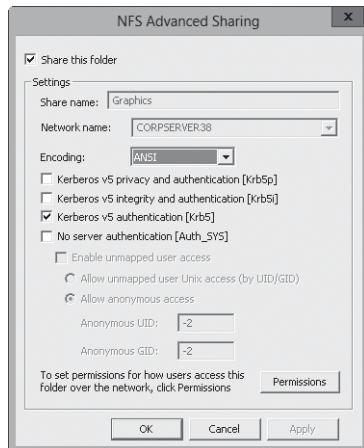


FIGURA 12-12 Você pode utilizar o compartilhamento NFS para compartilhar recursos entre computadores com o Windows e o UNIX.

4. Na caixa de texto Share Name, digite um nome para o compartilhamento. Esse será o nome da pasta à qual os usuários do UNIX irão se conectar. Os nomes de

compartilhamento NFS devem ser exclusivos para cada sistema e podem ser os mesmos que os utilizados para o compartilhamento de arquivos padrão.

5. ANSI é a codificação padrão para o texto associado com as listagens de diretório e os nomes de arquivos. Se os computadores UNIX utilizarem uma codificação padrão diferente, pode-se escolhê-la na lista Encoding.
6. Os computadores UNIX utilizam a autenticação Kerberos v5 por padrão. Normalmente, você desejará permitir a integridade e a autenticação Kerberos, bem como a autenticação Kerberos padrão. Marque as caixas de seleção dos mecanismos de autenticação que quer utilizar. Desmarque as caixas de seleção dos que não quer utilizar.
7. O compartilhamento pode ser configurado de modo que nenhuma autenticação do servidor seja exigida. Se quiser exigir a autenticação do servidor, marque a caixa de seleção No Server Authentication e escolha as opções adicionais conforme apropriado. O acesso de usuário não mapeado pode ser permitido e habilitado. Se quiser permitir o acesso anônimo para o compartilhamento NFS, selecione a opção Allow Anonymous Access e digite o UID de usuário anônimo e o GID de grupo anônimo.
8. Para computadores UNIX, configura-se o acesso baseado principalmente nos nomes de computador (também chamados de *host names* [nomes de host]). Por padrão, nenhum computador UNIX tem acesso ao compartilhamento NFS. Se quiser conceder permissões somente leitura ou de leitura/gravação, toque ou clique em Permissions, defina as permissões que quer utilizar na caixa de diálogo NFS Share Permissions e toque ou clique em OK. Pode-se configurar nenhum acesso, acesso somente leitura ou acesso de leitura/gravação por nome de computador cliente e grupos de computadores clientes.
9. Toque ou clique em OK duas vezes para fechar as caixas de diálogo abertas e salvar as configurações.

No File Explorer, pode-se desabilitar o compartilhamento NFS seguindo estas etapas:

1. Pressione e segure ou clique com o botão direito do mouse no compartilhamento que quer gerenciar e toque ou clique em Properties. A caixa de diálogo Properties do compartilhamento será exibida.
2. Na guia NFS Sharing, toque ou clique em Manage NFS Sharing.
3. Na caixa de diálogo NFS Advanced Sharing, desmarque a caixa de seleção Share This Folder e toque ou clique em OK duas vezes.

Com o Server Manager, você pode configurar as permissões NFS como parte da configuração inicial de compartilhamento quando estiver provisionando um compartilhamento. No subnó Shares do nó File And Storage Services, pode-se criar um compartilhamento NFS seguindo estas etapas:

1. No painel Shares, toque ou clique em Tasks e em New Share. O New Share Wizard será iniciado. Escolha NFS Share–Quick ou NFS Share– Advanced como o perfil de compartilhamento e toque ou clique em Next.
2. Especifique o nome do compartilhamento e a localização, como faria para um compartilhamento SMB.

3. Na página Specify Authentication Methods, configure Kerberos v5 Authentication e No Server Authentication. As opções fornecidas são similares àquelas abordadas anteriormente nesta seção.
4. Na página Specify Share Permissions, configure o acesso para os hosts do UNIX. Os hosts podem ser configurados para no access (nenhum acesso), read-only access (acesso somente leitura) ou read/write access (acesso de leitura/gravação) para o compartilhamento.
5. Em Specify Permissions To Control Access, opcionalmente, defina as permissões NTFS para o compartilhamento.
6. Na página Confirm Selections, revise suas seleções. Ao tocar ou clicar em Create, o assistente irá criar o compartilhamento, configura-lo e definir as permissões. O status deve declarar: "The share was successfully created". Se em vez disso um erro for exibido, observe-o e tome uma medida corretiva. No entanto, como os erros típicos se relacionam à configuração de acesso do host, provavelmente não será necessário repetir esse procedimento para criar o compartilhamento. Em vez disso, talvez seja preciso modificar apenas as permissões de compartilhamento. Toque ou clique em Close.

Utilização de cópias de sombra

Toda vez que sua empresa utilizar pastas compartilhadas, considere criar cópias de sombra (shadow copy) delas também. As cópias de sombra são backups pontuais ("pontos no tempo") de arquivo de dados que os usuários podem acessar diretamente em pastas compartilhadas. Esses backups pontuais podem poupar muito trabalho para você e outros administradores da empresa, especialmente se tiver de recuperar rotineiramente os arquivos de dados perdidos, substituídos ou corrompidos a partir de backups. O procedimento normal para recuperar cópias de sombra é utilizar o cliente Previous Versions ou Shadow Copy. O Windows Server 2012 inclui uma melhoria de recurso que permite reverter um volume inteiro (que não seja do sistema) para o estado de uma cópia de sombra anterior.

As cópias de sombra

Só se pode criar cópias de sombra em volumes NTFS. Utiliza-se o recurso Shadow Copy para criar backups automáticos dos arquivos em pastas compartilhadas por volume. Por exemplo, em um servidor de arquivos que tenha três volumes NTFS, cada um contendo pastas compartilhadas, é preciso configurar esse recurso para cada volume separadamente.

Se habilitar esse recurso em sua configuração padrão, as cópias de sombra serão criadas duas vezes por dia útil (de segunda a sexta-feira) às 7h e ao meio-dia. Você precisa de ao menos 100 MB de espaço livre para criar a primeira cópia de sombra em um volume. O espaço total em disco utilizado além disso dependerá da quantidade de dados nas pastas compartilhadas do volume. Pode-se restringir a quantidade total de espaço em disco utilizada pelo Shadow Copy configurando o tamanho máximo para esses backups pontuais.

Você configura e visualiza as configurações atuais de Shadow Copy na guia Shadow Copies da caixa de diálogo Properties do disco. No File Explorer ou no Computer

Management, pressione e segure ou clique com o botão direito do mouse no ícone do disco com o qual quer trabalhar, toque ou clique em Properties e na guia Shadow Copies. O painel Select A Volume exibirá o seguinte:

- **Volume** O rótulo de volume dos volumes NTFS na unidade de disco selecionada
- **Next Run Time** O status de Shadow Copy como Disabled, ou a próxima vez que uma cópia de sombra do volume será criada
- **Shares** O número de pastas compartilhadas no volume
- **Used** A quantidade de espaço em disco utilizada por Shadow Copy

As cópias de sombra individuais do volume atualmente selecionado serão listadas no painel Shadow Copies Of Selected Volume por data e hora.

Criação de cópias de sombra

Para criar uma cópia de sombra em um volume NTFS com pastas compartilhadas, siga estas etapas:

1. Abra o Computer Management. Se necessário, conecte-se a um computador remoto.
2. Na árvore de console, expanda Storage e selecione Disk Management. Os volumes configurados no computador selecionado serão exibidos no painel de detalhes.
3. Pressione e segure ou clique com o botão direito do mouse em Disk Management, aponte para All Tasks e toque ou clique em Configure Shadow Copies.
4. Na guia Shadow Copies, selecione o volume com o qual quer trabalhar em Select A Volume list.
5. Toque ou clique em Settings para configurar o tamanho máximo de todas as cópias de sombra para este volume e para alterar o cronograma padrão. Toque ou clique em OK.
6. Depois de configurar o volume para as cópias de sombra, toque ou clique em Enable, se necessário. Quando for solicitado que confirme essa ação, toque ou clique em Yes. A habilitação de cópias de sombra irá criar a primeira cópia de sombra e definir o cronograma para as cópias de sombra posteriores.

OBSERVAÇÃO Se criar um cronograma de execução ao fazer as configurações de cópia de sombra, a cópia de sombra será habilitada automaticamente para o volume quando tocar ou clicar em OK para fechar a caixa de diálogo Settings. No entanto, a primeira cópia de sombra não será criada até a próxima execução agendada. Se quiser criar uma cópia de sombra de um volume neste momento, selecione-o e toque ou clique em Create Now.

Restauração de uma cópia de sombra

Os usuários trabalhando em computadores clientes acessam as cópias de sombra de pastas compartilhadas individuais utilizando o cliente Previous Versions ou Shadow Copy. A melhor maneira de acessar cópias de sombra em um computador cliente é seguir estas etapas:

1. No File Explorer, pressione e segure ou clique com o botão direito do mouse no compartilhamento do qual quer acessar versões anteriores de arquivos, toque ou clique em Properties e na guia Previous Versions.

2. Na guia Previous Versions, selecione a versão da pasta com a qual quer trabalhar. Cada pasta tem um carimbo de data/hora. Toque ou clique no botão correspondente à ação que quer realizar:
 - Toque ou clique em Open para abrir a cópia de sombra no File Explorer.
 - Toque ou clique em Copy para exibir a caixa de diálogo Copy Items, que permite copiar a imagem instantânea (snapshot) da pasta para a localização que for especificada.
 - Toque ou clique em Restore para reverter a pasta compartilhada ao seu estado no momento da imagem instantânea selecionada.

Reversão de um volume inteiro para uma cópia de sombra anterior

O Windows Server 2012 apresenta uma melhoria de cópia de sombra que permite reverter um volume inteiro para o estado que tinha quando uma determinada cópia de sombra foi criada. Como os volumes contendo arquivos do sistema operacional não podem ser revertidos, o volume que queira reverter não deve ser um volume do sistema. O mesmo vale para volumes em um disco compartilhado de um cluster.

Para reverter um volume inteiro para um estado anterior, siga estas etapas:

1. Abra o Computer Management. Se necessário, conecte-se a um computador remoto.
2. Na árvore de console, expanda Storage. Pressione e segure ou clique com o botão direito do mouse em Disk Management, aponte para All Tasks e toque ou clique em Configure Shadow Copies.
3. Na guia Shadow Copies, selecione o volume com o qual quer trabalhar em Select A Volume list.
4. As cópias de sombra individuais do volume selecionado no momento serão listadas por data e hora no painel Shadow Copies Of Selected Volume. Selecione a cópia de sombra com o carimbo de data/hora para o qual quer fazer a reversão e toque ou clique em Revert.
5. Para confirmar essa ação, marque a caixa de seleção Check Here If You Want To Revert This Volume e toque ou clique em Revert Now. Toque ou clique em OK para fechar a caixa de diálogo Shadow Copies.

Exclusão de cópias de sombra

Cada backup pontual é mantido separadamente. Você pode excluir cópias de sombra individuais de um volume conforme necessário. Assim, o espaço em disco utilizado pelas cópias de sombra é recuperado.

Para excluir uma cópia de sombra, siga estas etapas:

1. Abra o Computer Management. Se necessário, conecte-se a um computador remoto.
2. Na árvore de console, expanda Storage. Pressione e segure ou clique com o botão direito do mouse em Disk Management, aponte para All Tasks e toque ou clique em Configure Shadow Copies.
3. Na guia Shadow Copies, selecione o volume com o qual quer trabalhar em Select A Volume list.

4. As cópias de sombra individuais do volume selecionado no momento serão listadas por data e hora no painel Shadow Copies Of Selected Volume. Selecione a cópia de sombra que quer excluir e toque ou clique em Delete Now. Toque ou clique em Yes para confirmar a ação.

Como desabilitar cópias de sombra

Se não quiser mais manter cópias de sombra de um volume, pode desabilitar o recurso Shadow Copy. Desabilitar esse recurso desativa o cronograma de backups pontuais automatizados e remove qualquer cópia de sombra existente.

Para desabilitar as cópias de sombra de um volume, siga estas etapas:

1. Abra o Computer Management. Se necessário, conecte-se a um computador remoto.
2. Na árvore de console, expanda Storage. Pressione e segure ou clique com o botão direito do mouse em Disk Management, aponte para All Tasks e toque ou clique em Configure Shadow Copies.
3. Na guia Shadow Copies, selecione o volume com o qual quer trabalhar em Select A Volume list e toque ou clique em Disable.
4. Quando for solicitado, confirme a ação tocando ou clicando em Yes. Toque ou clique em OK para fechar a caixa de diálogo Shadow Copies.

Coneção com unidades de rede

Os usuários podem se conectar a uma unidade de rede e a recursos compartilhados disponíveis na rede. Essa conexão é mostrada como uma unidade de rede que os usuários podem acessar como qualquer outra unidade em seus sistemas.

OBSERVAÇÃO Quando os usuários se conectam a unidades de rede, estão sujeitos não apenas às permissões definidas para os recursos compartilhados, mas também às permissões de arquivos e pastas do Windows Server 2012. As diferenças entre esses conjuntos de permissões geralmente são a razão por que os usuários talvez não possam acessar um determinado arquivo ou subpasta dentro da unidade de rede.

Mapeamento de uma unidade de rede

No Windows Server 2012, você se conecta a uma unidade de rede através de mapeamento usando o comando NET USE com a seguinte sintaxe:

```
net use DeviceName \\ComputerName\ShareName
```

DeviceName especifica a letra da unidade ou um asterisco (*) para utilizar a próxima letra de unidade disponível e *\\ComputerName\ShareName* é o caminho UNC para o compartilhamento, como nos exemplos seguintes:

```
net use g: \\ROMEO\DOCS
```

ou

```
net use * \\ROMEO\DOCS
```

OBSERVAÇÃO Para assegurar que a unidade mapeada esteja disponível toda vez que o usuário se conectar, torne o mapeamento persistente adicionando a opção /Persistent:Yes.

Se o computador cliente tiver o Windows 8, você pode mapear as unidades de rede concluindo as etapas a seguir:

1. No File Explorer, toque ou clique no botão de opção mais à esquerda na lista de endereços e em Computer.
2. A seguir, toque ou clique no botão Map Network Drive no painel Computer e em Map Network Drive.
3. Utilize a lista Drive para selecionar uma letra de unidade livre para utilizar e toque ou clique no botão Browse à direita da lista Folder. Na caixa de diálogo Browse For Folder, expanda as pastas de rede até que possa selecionar o nome do grupo de trabalho ou domínio com o qual quer trabalhar.
4. Ao expandir o nome de um computador em um grupo de trabalho ou um domínio, você verá uma lista de pastas compartilhadas. Selecione a pasta compartilhada com a qual quer trabalhar e toque ou clique em OK.
5. Selecione Reconnect At Logon se quiser que o Windows se conecte à pasta compartilhada automaticamente no início de cada sessão.
6. Toque ou clique em Finish. Se o usuário conectado no momento não tiver as permissões de acesso apropriadas para o compartilhamento, selecione Connect Using Different Credentials e toque ou clique em Finish. Depois de tocar ou clicar em Finish, poderá digitar o nome de usuário e a senha da conta com a qual quer se conectar à pasta compartilhada. Digite o nome do usuário no formato Domain\ Username, como **Cpandi\Williams**. Antes de tocar ou clicar em OK, selecione Remember My Credentials se quiser que as credenciais sejam salvas. Caso contrário, será necessário fornecer as credenciais no futuro.

Desconexão de uma unidade de rede

Para desconectar uma unidade de rede, siga estas etapas:

1. No File Explorer, toque ou clique no botão de opção mais à esquerda na lista de endereços e em Computer.
2. Sob Network Location, pressione e segure ou clique com o botão direito do mouse no ícone da unidade de rede e toque ou clique em Disconnect.

Gerenciamento, posse e herança de objetos

O Windows Server 2012 faz uma abordagem baseada em objeto para descrever recursos e gerenciar permissões. Os objetos que descrevem recursos estão definidos em volumes NTFS e no Active Directory. Com volumes NTFS, pode-se definir permissões para arquivos e pastas. Com o Active Directory, pode-se definir permissões para outros tipos de objetos, como usuários, computadores e grupos. Você pode utilizar essas permissões para controlar o acesso com precisão.

Objetos e gerenciadores de objetos

Estão definidos em um volume NTFS ou no Active Directory, cada tipo de objeto tem um gerenciador de objeto e ferramentas de gerenciamento primárias. O gerenciador de objeto controla as configurações e permissões do objeto. As ferramentas de gerenciamento primárias são aquelas preferencialmente escolhidas para trabalhar

com o objeto. Os objetos, seus gerenciadores e ferramentas de gerenciamento estão resumidos na Tabela 12-2.

TABELA 12-2 Objetos do Windows Server 2012

TIPO DE OBJETO	GERENCIADOR DO OBJETO	FERRAMENTAS DE GERENCIAMENTO
Arquivos e pastas	NTFS	File Explorer
Impressoras	Print spooler (Spooler de impressão)	Printers no Control Panel
Chaves do registro	Windows registry (Registro do Windows)	Registry Editor
Serviços	Service controllers (Controladores de Serviços)	Security Configuration Tool Set
Compartilhamentos	Server service (Serviço Servidor)	File Explorer, Computer Management, Share And Storage Management

Posse e transferência de objetos

É importante entender o conceito de posse de objeto. No Windows Server 2012, o proprietário do objeto não necessariamente é o seu criador. Em vez disso, o proprietário do objeto é a pessoa que tem controle direto sobre o objeto. Os proprietários de objetos podem conceder permissões de acesso e dar permissão a outros usuários para se apropriarem do objeto.

Como administrador, você pode se apropriar de objetos da rede. Isso assegura que administradores autorizados não possam ser bloqueados em arquivos, pastas, impressoras e outros recursos. Depois de se apropriar de arquivos, no entanto, não poderá retornar a posse ao proprietário original (na maioria dos casos). Isso evita que os administradores accessem arquivos e tentem ocultar o fato.

A maneira como a posse é atribuída inicialmente depende da localização do recurso sendo criado. Na maioria dos casos, o grupo Administrators será listado como o proprietário atual e o criador real do objeto será listado como uma pessoa que pode assumir a posse.

A posse pode ser transferida de diversas formas:

- Se o grupo Administrators estiver inicialmente atribuído como o proprietário, o criador do objeto pode assumir a posse, desde que o faça antes de outra pessoa.
- O proprietário atual pode conceder a permissão Take Ownership a outros usuários, permitindo que eles se apropriem do objeto.
- Um administrador pode se apropriar de um objeto, desde que o objeto esteja sob seu controle administrativo.

Para se apropriar de um objeto, siga estas etapas:

1. Abra a ferramenta de gerenciamento para o objeto. Por exemplo, se quiser trabalhar com arquivos e pastas, inicie o File Explorer.
2. Pressione e segure ou clique com o botão direito do mouse no objeto do qual quer se apropriar e toque ou clique em Properties. Na caixa de diálogo Properties, clique ou toque na guia Security.

3. Na guia Security, toque ou clique em Advanced para exibir a caixa de diálogo Advanced Security Settings, na qual o proprietário atual estará listado sob o nome do arquivo ou da pasta.
4. Toque ou clique em Change. Utilize as opções na caixa de diálogo Select User, Computer, Service Account, Or Group para selecionar o novo proprietário.
5. Toque ou clique em OK duas vezes quando tiver terminado.

DICA Se estiver se apropriando de uma pasta, poderá assumir a posse de todos os arquivos e as subpastas dentro da pasta marcando a caixa de seleção Replace Owner On Subcontainers And Objects. Essa opção também funciona com objetos que contenham outros objetos. Assim, você se apropriaria de todos os objetos filhos.

Herança de objeto

Os objetos são definidos usando uma estrutura pai-filho. Um objeto pai é um objeto de nível superior. Um objeto filho é um objeto definido abaixo de um objeto pai na hierarquia. Por exemplo, a pasta C:\ é o objeto pai das pastas C:\Data e C:\Backups. Qualquer subpasta criada em C:\Data e C:\Backups será filha dessas pastas e neta de C:\.

Os objetos filhos podem herdar as permissões dos objetos pais. De fato, todos os objetos do Windows Server 2012 são criados com a herança habilitada por padrão. Isso significa que os objetos filhos automaticamente herdaram as permissões do pai. Por causa disso, as permissões do objeto pai controlam o acesso para o objeto filho. Se quiser alterar as permissões em um objeto filho, deverá executar um dos procedimentos a seguir:

1. Edite as permissões do objeto pai.
2. Interrompa a herança de permissões do objeto pai e atribua as permissões ao objeto filho.
3. Selecione a permissão oposta para substituir a permissão herdada. Por exemplo, se o pai der a permissão, você poderia negá-la para o objeto filho.

Para interromper a herança de permissões de um objeto pai, siga estas etapas:

1. Abra a ferramenta de gerenciamento do objeto. Por exemplo, se quiser trabalhar com arquivos e pastas, inicie o File Explorer.
2. Pressione e segure ou clique com o botão direito do mouse no objeto com o qual quer trabalhar e toque ou clique em Properties. Na caixa de diálogo Properties, clique ou toque na guia Security.
3. Toque ou clique em Advanced para exibir a caixa de diálogo Advanced Security Settings.
4. Na guia Permissions, toque ou clique em Change Permissions para exibir uma versão editável desta guia.
5. Na guia Permissions, você verá um botão Disable Inheritance se a herança estiver habilitada no momento. Toque ou clique em Disable Inheritance.
6. Agora você poderá converter as permissões herdadas em permissões explícitas ou remover todas permissões herdadas e aplicar somente as permissões que deseja definir explicitamente na pasta ou no arquivo.

Lembre-se de que se remover as permissões herdadas e nenhuma outra permissão for atribuída, todos, menos o proprietário do recurso, terão o acesso negado. Assim, todos

são efetivamente bloqueados, exceto o proprietário de uma pasta ou um arquivo. Contudo, os administradores ainda terão o direito de se apropriar do recurso, independentemente das permissões. Portanto, se um administrador for bloqueado em um arquivo ou uma pasta e realmente precisar de acesso, poderá assumir a posse e ter acesso irrestrito.

Para iniciar a herança de permissões de um objeto pai, siga estas etapas:

1. Abra a ferramenta de gerenciamento do objeto. Por exemplo, se quiser trabalhar com arquivos e pastas, inicie o File Explorer.
2. Pressione e segure ou clique com o botão direito do mouse no objeto com o qual quer trabalhar e toque ou clique em Properties. Na caixa de diálogo Properties, clique ou toque na guia Security.
3. Toque ou clique em Advanced para exibir a caixa de diálogo Advanced Security Settings.
4. Na guia Permissions, toque ou clique em Enable Inheritance e em OK. Observe que o botão Enable Inheritance estará disponível somente se a herança de permissão estiver desabilitada no momento.

Permissões de arquivos e pastas

As permissões NTFS são sempre avaliadas quando um arquivo é acessado. Com volumes NTFS e ReFS, pode-se definir permissões de segurança em arquivos e pastas. Essas permissões concedem ou negam acesso aos arquivos e pastas. Como o Windows Server 2012 adiciona novas camadas de segurança, as permissões NTFS agora abrangem o seguinte:

- Permissões básicas
- Permissões baseadas em declarações (*claims-based*)
- Permissões especiais

Pode-se visualizar as permissões NTFS para arquivos e pastas seguindo estas etapas:

1. No File Explorer, pressione e segure ou clique com o botão direito do mouse no arquivo ou na pasta com que quer trabalhar e toque ou clique em Properties. Na caixa de diálogo Properties, clique ou toque na guia Security.
2. Na lista Group Or User Names, selecione o usuário, computador ou grupo cujas permissões quer visualizar. Se as permissões não estiverem disponíveis para edição (esmaecidas), elas são herdadas de um objeto pai.

Conforme abordado anteriormente no capítulo, as pastas compartilhadas possuem as permissões de compartilhamento e as permissões NTFS. Pode-se visualizar as permissões NTFS aplicadas a uma das pastas compartilhadas seguindo estas etapas:

1. No Server Manager, o subnó Shares do nó File And Storage Services mostra os compartilhamentos existentes para os servidores de arquivos que tenham sido adicionados para gerenciamento.
2. Pressione e segure ou clique com o botão direito do mouse na pasta com a qual quer trabalhar e toque ou clique em Properties. A caixa de diálogo Properties será exibida.
3. Ao tocar ou clicar em Permissions no painel esquerdo, as permissões de compartilhamento atuais e as permissões NTFS serão mostradas no painel principal.

4. Para obter mais informações, toque ou clique em Costumize Permissions para abrir a caixa de diálogo Advanced Security Settings.

Em servidores de arquivos com o Windows Server 2012, também se pode utilizar as políticas de acesso central para definir precisamente os atributos específicos que os usuários e os dispositivos devem ter para acessar os recursos.

As permissões de arquivos e pastas

As permissões básicas que se pode atribuir a arquivos e pastas são resumidas na Tabela 12-3. As permissões de arquivo incluem Full Control (Controle Total), Modify (Modificar), Read & Execute (Ler e Executar), Read (Ler) e Write (Escrever). As permissões de pasta incluem Full Control, Modify, Read & Execute, List Folder Contents (Listar Conteúdos da pasta), Read e Write.

TABELA 12-3 As permissões de arquivos e pastas utilizadas pelo Windows Server 2012

PERMISSÃO	SIGNIFICADO PARA PASTAS	SIGNIFICADO PARA ARQUIVOS
Read	Permite visualizar e listar arquivos e subpastas	Permite visualizar ou acessar o conteúdo de um arquivo
Write	Permite adicionar arquivos e subpastas	Permite gravar em um arquivo
Read & Execute	Permite visualizar e listar arquivos e subpastas, bem como executar arquivos; herdada por arquivos e pastas	Permite visualizar e acessar o conteúdo do arquivo, bem como executar arquivos;
List Folder Contents	Permite visualizar e listar o conteúdo de uma pasta e de sub-pastas, bem como executar arquivos; herdada somente por pastas	N/A
Modify	Permite a leitura e gravação de arquivos e subpastas; permite a exclusão da pasta	Permite a leitura e gravação de um arquivo; permite a exclusão de um arquivo
Full Control	Permite ler, gravar, alterar e excluir arquivos e subpastas	Permite ler, gravar, alterar e excluir um arquivo

Sempre que trabalhar com permissões de arquivos e pastas, deve lembrar-se do seguinte:

- Read (Ler) é a única permissão necessária para executar scripts. A permissão para execução não importa.
- O acesso de leitura é necessário para acessar um atalho e seu destino.
- Dar a permissão a um usuário para gravação em um arquivo, mas não para excluí-lo, não impedirá o usuário de excluir o conteúdo do arquivo. Ele ainda poderá excluir o conteúdo.
- Se um usuário tiver controle total sobre uma pasta, poderá excluir os arquivos nela, independentemente da permissão nos arquivos.

As permissões básicas foram criadas combinando permissões especiais em grupos lógicos. A Tabela 12-4 mostra as permissões especiais utilizadas para criar as permis-

sões básicas para arquivos. Utilizando configurações de permissões avançadas, pode-se atribuir essas permissões individualmente, se necessário. Conforme for estudando as permissões especiais, lembre-se do seguinte:

- Por padrão, se nenhum acesso for especificamente concedido ou negado, o usuário terá o acesso negado.
- As ações que os usuários podem executar se baseiam na soma de todas as permissões atribuídas ao usuário e a todos os grupos dos quais ele seja membro. Por exemplo, se o usuário GeorgeJ tiver o acesso Read e for membro do grupo Techies, que tem o acesso Change, GeorgeJ terá o acesso Change. Se Techies for membro de Administrators, que tem Full Control, GeorgeJ terá controle total sobre o arquivo.

TABELA 12-4 As permissões especiais para arquivos

PERMISSÕES ESPECIAIS	PERMISSÕES BÁSICAS				
	FULL CONTROL	MODIFY	READ & EXECUTE	READ	WRITE
Traverse Folder/Execute File (Desviar pasta/Executar arquivo)	Sim	Sim	Sim		
List Folder/Read Data (Listar pasta/Ler dados)	Sim	Sim	Sim	Sim	
Read Attributes (Atributos de leitura)	Sim	Sim	Sim	Sim	
Read Extended Attributes (Atributos extendidos de leitura)	Sim	Sim	Sim	Sim	
Create Files/Write Data (Criar arquivos/Gravar dados)	Sim	Sim			Sim
Create Folders/Append Data (Criar pastas/Acrecentar dados)	Sim	Sim			Sim
Write Attributes (Gravar atributos)	Sim	Sim			Sim
Write Extended Attributes (Gravar atributos extendidos)	Sim	Sim			Sim
Delete Subfolders And Files (Excluir subpastas e arquivos)	Sim				
Delete (Excluir)	Sim	Sim			
Read Permissions (Ler permissões)	Sim	Sim	Sim	Sim	Sim
Change Permissions (Alterar permissões)	Sim				
Take Ownership (Apropriar-se)	Sim				

A Tabela 12-5 mostra as permissões especiais utilizadas para criar as permissões básicas para pastas. Conforme for estudando as permissões especiais, lembre-se de que, ao criar arquivos e pastas, eles herdarão certas configurações de permissões dos objetos pais. Essas configurações de permissões são mostradas como permissões padrão.

TABELA 12-5 As permissões especiais para pastas

PERMISSÕES ESPECIAIS	PERMISSÕES BÁSICAS					
	FULL CONTROL	MODIFY	READ & EXECUTE	LIST FOLDER CONTENTS	READ	WRITE
Traverse Folder/Execute File (Desviar pasta/Executar arquivo)	Sim	Sim	Sim	Sim		
List Folder/Read Data (Listar pasta/Ler dados)	Sim	Sim	Sim	Sim	Sim	
Read Attributes (Atributos de leitura)	Sim	Sim	Sim	Sim	Sim	
Read Extended Attributes (Atributos extendidos de leitura)	Sim	Sim	Sim	Sim	Sim	
Create Files/Write Data (Criar arquivos/Gravar dados)	Sim	Sim				Sim
Create Folders/Append Data (Criar pastas/Acrecentar dados)	Sim	Sim				Sim
Write Attributes (Gravar atributos)	Sim	Sim				Sim
Write Extended Attributes (Gravar atributos extendidos)	Sim	Sim				Sim
Delete Subfolders And Files (Excluir subpastas e arquivos)	Sim					
Delete (Excluir)	Sim	Sim				
Read Permissions (Ler permissões)	Sim	Sim	Sim	Sim	Sim	Sim
Change Permissions (Alterar permissões)	Sim					
Take Ownership (Apropriar-se)	Sim					

Configuração de permissões básicas de arquivos e pastas

Para definir as permissões NTFS básicas para arquivos e pastas, siga estas etapas:

1. No File Explorer, pressione e segure ou clique com o botão direito do mouse no arquivo ou na pasta com que quer trabalhar e toque ou clique em Properties. Na caixa de diálogo Properties, clique ou toque na guia Security.
2. Toque ou clique em Edit para exibir uma versão editável da guia Security, como mostrado na Figura 12-13.

3. Os usuários ou grupos que já têm acesso ao arquivo ou pasta serão listados na lista Group Or User Names. Você pode alterar as permissões para esses usuários e grupos fazendo o seguinte:
 - a. Selecione o usuário ou grupo que quer alterar.
 - b. Conceda ou negue as permissões de acesso na caixa da lista Permissions.

DICA As permissões herdadas estarão sombreadas (esmaecidas). Se quiser substituir uma permissão herdada, selecione a permissão oposta.

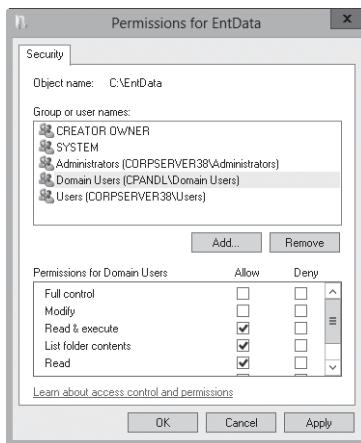


FIGURA 12-13 Configure as permissões básicas de arquivos ou pastas na guia Security.

4. Para definir as permissões de acesso para usuários, computadores ou grupos adicionais, toque ou clique em Add. A caixa de diálogo Select Users, Computers, Service Accounts, Or Groups será exibida.
5. Digite o nome de um usuário, computador ou grupo no domínio atual e toque ou clique em Check Names. Uma das seguintes ações ocorrerá:
 - Se uma única correspondência for encontrada, a caixa de diálogo será atualizada e a entrada estará sublinhada.
 - Se nenhuma correspondência for encontrada, ou uma parte do nome digitado está incorreta, ou você está trabalhando com uma localização incorreta. Modifique o nome e tente de novo, ou toque ou clique em Locations para selecionar uma nova localização.
 - Se várias correspondências forem encontradas, selecione os nomes que quer utilizar e toque ou clique em OK. Para adicionar mais usuários, computadores ou grupos, digite um ponto e vírgula (;) e repita esta etapa.

OBSERVAÇÃO O botão Locations permite acessar nomes de contas em outros domínios. Toque ou clique em Locations para ver uma lista com o domínio atual, os domínios confiáveis e outros recursos que pode acessar. Por causa das relações de confiança transitivas no Windows Server 2012, normalmente se pode acessar todos os domínios na árvore ou floresta.

6. Na lista Group Or User Names, selecione o usuário, computador ou grupo que quer configurar e, nas caixas de seleção da lista Permissions, conceda ou negue as permissões. Repita para outros usuários, computadores ou grupos.

7. Toque ou clique em OK.

Como as pastas compartilhadas também têm permissões NTFS, talvez queira definir permissões NTFS básicas utilizando o Server Manager. Para fazê-lo, siga estas etapas:

1. No Server Manager, pressione e segure ou clique com o botão direito do mouse na pasta com a qual quer trabalhar e toque ou clique em Properties. A caixa de diálogo Properties será exibida.
2. Ao tocar ou clicar em Permissions no painel esquerdo, as permissões de compartilhamento atuais e as permissões NTFS serão mostradas no painel principal.
3. Toque ou clique em Customize Permissions para abrir a caixa de diálogo Advanced Security Settings com a guia Permissions selecionada.
4. Os usuários ou grupos que já têm acesso ao arquivo ou pasta são listados na lista sob Permission Entries. Utilize as opções fornecidas para visualizar, editar, adicionar ou remover as permissões para usuários e grupos.

Configuração de permissões especiais em arquivos e pastas

Para definir as permissões NTFS especiais para arquivos e pastas, siga estas etapas:

1. No File Explorer, pressione e segure ou clique com o botão direito do mouse no arquivo ou na pasta com que quer trabalhar e toque ou clique em Properties.
2. Na caixa de diálogo Properties, selecione a guia Security e toque ou clique em Advanced para exibir a caixa de diálogo Advanced Security Settings. Antes de poder modificar as permissões, deve-se clicar em Change Permissions. Como mostrado na Figura 12-14, as permissões são apresentadas praticamente como na guia Security. As principais diferenças são que você verá conjuntos de permissões concedidas ou negadas individuais, não importando se são herdadas e de onde vêm, e os recursos aos quais se apliquem.

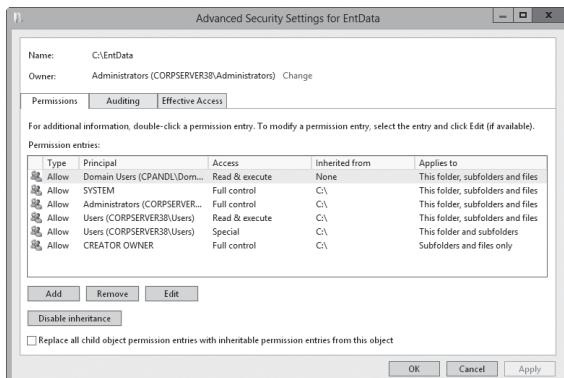


FIGURA 12-14 Configure permissões especiais em arquivos e pastas.

3. Se um usuário ou grupo já tiver permissões definidas para o arquivo ou a pasta (e essas permissões não estiverem sendo herdadas), você pode modificar as permissões especiais selecionando o usuário ou grupo e clicando em Edit. Depois, pule as etapas de 4 a 7 e siga as etapas restantes deste procedimento.
4. Para adicionar permissões especiais para um usuário ou grupo, toque ou clique em Add para exibir a caixa de diálogo Permission Entry. Toque ou clique em Select A Principal para exibir a caixa de diálogo Select User, Computer, Service Account Or Group.
5. Digite o nome de um usuário ou de uma conta de grupo. Certifique-se de fazer referência ao nome da conta de usuário, em vez do nome completo do usuário. Apenas um nome por vez pode ser digitado.
6. Toque ou clique em Check Names. Se uma única correspondência for encontrada para cada entrada, a caixa de diálogo será automaticamente atualizada e a entrada estará sublinhada. Caso contrário, você verá uma caixa de diálogo adicional. Se nenhuma correspondência for encontrada, ou o nome foi digitado incorretamente, ou você está trabalhando com uma localização incorreta. Modifique o nome na caixa de diálogo Name Not Found e tente de novo, ou toque ou clique em Locations para selecionar uma nova localização. Se várias correspondências forem encontradas, na caixa de diálogo Multiple Names Found, selecione o nome que quer utilizar e toque ou clique em OK.
7. Toque ou clique em OK. O usuário ou o grupo será adicionado como Principal e a caixa de diálogo Permission Entry será atualizada para mostrá-lo.
8. Quando estiver editando as permissões, somente as permissões básicas serão listadas por padrão. Toque ou clique em Show Advanced Permissions para exibir as permissões especiais, como mostrado na Figura 12-15.

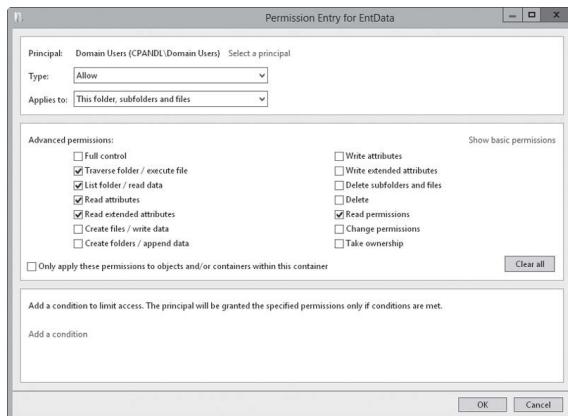


FIGURA 12-15 Configure as permissões especiais que devem ser concedidas ou negadas.

9. Utilize a lista Type para especificar se está configurando permissões especiais concedidas ou negadas e selecione as permissões especiais que quer conceder ou

negar. Se qualquer permissão estiver esmaecida (não disponível para edição), ela foi herdada de uma pasta pai.

OBSERVAÇÃO As permissões especiais são concedidas ou negadas separadamente. Portanto, se quiser conceder e negar permissões especiais, é preciso configurar as permissões concedidas e repetir esse procedimento começando pela etapa 1 para configurar as permissões negadas.

10. Se as opções na lista Applies To estiverem disponíveis, escolha apropriada para garantir que as permissões sejam herdadas adequadamente. As opções incluem o seguinte:

- **This Folder Only** As permissões serão aplicadas apenas à pasta selecionada atualmente.
- **This Folder, Subfolders And Files** As permissões serão aplicadas a esta pasta, a qualquer subpasta desta pasta e a qualquer arquivo em qualquer dessas pastas.
- **This Folder And Files** As permissões serão aplicadas a esta pasta e a qualquer subpasta desta pasta. Elas não se aplicam a qualquer arquivo em qualquer dessas pastas.
- **This Folder And Files** As permissões serão aplicadas a esta pasta e a qualquer arquivo nesta pasta. Elas não se aplicam a qualquer subpasta desta pasta.
- **Subfolders And Files** As permissões serão aplicadas a qualquer subpasta desta pasta e a qualquer arquivo em qualquer dessas pastas. Elas não se aplicam a esta pasta.
- **Subfolder Only** As permissões serão aplicadas a qualquer subpasta desta pasta, mas não a esta pasta ou a qualquer arquivo em qualquer dessas pastas.
- **Files Only** As permissões serão aplicadas a qualquer arquivo nesta pasta e a qualquer arquivo em subpastas desta pasta. Elas não se aplicam a esta pasta ou às subpastas.

11. Quando tiver terminado de configurar as permissões, toque ou clique em OK.

Como as pastas compartilhadas também têm permissões NTFS, talvez queira definir permissões NTFS especiais utilizando o Server Manager. Para fazê-lo, siga estas etapas:

1. No Server Manager, selecione File And Storage Services e então selecione Shares. A seguir, pressione e segure ou clique com o botão direito do mouse na pasta com a qual quer trabalhar e toque ou clique em Properties. A caixa de diálogo Properties será exibida.
2. Ao tocar ou clicar em Permissions no painel esquerdo, as permissões de compartilhamento atuais e as permissões NTFS serão mostradas no painel principal.
3. Toque ou clique em Customize Permissions para abrir a caixa de diálogo Advanced Security Settings com a guia Permissions selecionada.
4. Os usuários ou grupos que já têm acesso ao arquivo ou pasta são listados na lista sob Permission Entries. Utilize as opções fornecidas para visualizar, editar, adicionar ou remover as permissões para usuários e grupos. Quando estiver editando ou adicionando permissões na caixa de diálogo Permission Entry, siga as etapas de 8 a 11 do procedimento anterior para exibir as permissões especiais e trabalhar com elas.

Configuração de permissões baseadas em declarações

Os controles de acesso baseados em declarações (claims-based) utilizam identidades compostas que incorporam não apenas os grupos dos quais o usuário faz parte e os grupos dos quais o computador do usuário faz parte, mas também tipos de declaração, que são asserções sobre objetos baseados em atributos do Active Directory, e propriedades de recursos, que classificam os objetos e descrevem seus atributos. Quando os recursos são acessados remotamente, os controles de acesso baseados em declarações e as políticas de acesso central dependem do Kerberos with Armoring (Kerberos com blindagem) para a autenticação de declarações acerca do computador. O Kerberos with Armoring aumenta a segurança do domínio permitindo aos clientes que ingressaram no domínio e os controladores de domínio se comunicarem por canais seguros e criptografados.

Utiliza-se as permissões baseadas em declarações para ajustar o acesso. Isso é feito definindo as condições que limitam o acesso como parte das permissões de segurança avançadas de um recurso. Normalmente, essas condições adicionam declarações de dispositivos e usuários aos controles de acesso. As declarações de usuários identificam os usuários e as declarações de dispositivos identificam os dispositivos. Por exemplo, você poderia definir os tipos de declaração baseados na categoria comercial e no código do país. Os atributos do Active Directory são businessCategory e countryCode, respectivamente. Utilizando esses tipos de declaração, pode-se então ajustar o acesso para garantir que somente usuários, dispositivos, ou ambos que pertençam a categorias comerciais específicas e tenham certos códigos de país recebam acesso a um recurso. Também se poderia definir uma propriedade de recurso chamada Project para ajudar a ajustar ainda mais o acesso.

MAIS INFORMAÇÕES Com políticas de acesso central, define-se as regras de acesso central no Active Directory e essas regras são aplicadas dinamicamente pela empresa. As regras de acesso central usam expressões condicionais que requerem que se determine as propriedades do recurso, os tipos de declaração e/ou os grupos de segurança exigidos pela política, bem como os servidores em que ela deva ser aplicada.

Antes de poder definir e aplicar as condições das declarações aos arquivos e pastas de um computador, uma política baseada em declarações deve ser habilitada. Para computadores que não tenham ingressado no domínio, pode-se fazê-lo habilitando e configurando a política KDC Support For Claims, Compound Authentication And Kerberos Armoring nas políticas Administrative Templates para Computer Configuration sob System\KDC. A política deve ser configurada para utilizar um dos seguintes modos:

- **Supported** Os controladores de domínio suportam declarações, identidades compostas e blindagem Kerberos. Os computadores clientes que não suportam Kerberos with Armoring podem ser autenticados.
- **Always Provide Claims** Este é o mesmo que o modo Supported, mas os controladores de domínio sempre retornam declarações para contas.
- **Fail Unarmored Authentication Requests** O Kerberos with Armoring é obrigatório. Os computadores clientes que não suportam Kerberos with Armoring não podem ser autenticados.

A política Kerberos Client Support For Claims, Compound Authentication And Kerberos Armoring controla se o cliente Kerberos com Windows 8 e Windows Server

2012 solicita declarações e autenticação composta. A política deve estar habilitada para clientes Kerberos compatíveis para solicitar declarações e autenticação composta para Dynamic Access Control e blindagem Kerberos. Você encontrará essa política nas políticas Administrative Templates para Computer Configuration sob System\Kerberos.

Para aplicação por um domínio, uma política baseada em declarações deve estar habilitada para todos os controladores de domínio no domínio para garantir uma aplicação consistente. Por causa disso, normalmente se habilita e configura essa política por meio da Default Domain Controllers Group Policy Object (GPO) ou da GPO mais alta vinculada à unidade organizacional (OU, organizational unit) dos controladores de domínio.

Uma vez que tenha habilitado e configurado a política baseada em declarações, poderá definir as condições de declaração concluindo estas etapas:

1. No File Explorer, pressione e segure ou clique com o botão direito do mouse no arquivo ou na pasta com que quer trabalhar e toque ou clique em Properties. Na caixa de diálogo Properties, selecione a guia Security e toque ou clique em Advanced para exibir a caixa de diálogo Advanced Security Settings.
2. Se o usuário ou grupo já tiver permissões definidas para o arquivo ou a pasta, você poderá editar suas permissões existentes. Então, toque ou clique no usuário com o qual quer trabalhar, em Edit e pule as etapas de 3 a 6.
3. Toque ou clique em Add para exibir a caixa de diálogo Permission Entry. Toque ou clique em Select A Principal para exibir a caixa de diálogo Select User, Computer, Service Account Or Group.
4. Digite o nome de um usuário ou de uma conta de grupo. Certifique-se de fazer referência ao nome da conta de usuário, em vez do nome completo do usuário. Apenas um nome por vez pode ser digitado.
5. Toque ou clique em Check Names. Se uma única correspondência for encontrada para cada entrada, a caixa de diálogo será automaticamente atualizada e a entrada estará sublinhada. Caso contrário, você verá uma caixa de diálogo adicional. Se nenhuma correspondência for encontrada, ou o nome foi digitado incorretamente, ou você está trabalhando com uma localização incorreta. Modifique o nome na caixa de diálogo Name Not Found e tente de novo, ou toque ou clique em Locations para selecionar uma nova localização. Se várias correspondências forem encontradas, na caixa de diálogo Multiple Names Found, selecione o nome que quer utilizar e toque ou clique em OK.
6. Toque ou clique em OK. O usuário ou grupo será adicionado como o Principal. Toque ou clique em Add A Condition.
7. Utilize as opções fornecidas para definir as condições que devem ser atendidas para conceder acesso. Com usuários e grupos, defina declarações básicas baseadas em associações de grupo, tipos de declaração definidos anteriormente, ou ambos. Com propriedades de recursos, defina as condições para os valores de propriedade.
8. Quando tiver terminado de configurar as condições, toque ou clique em OK.

Como as pastas compartilhadas também têm permissões NTFS, talvez queira definir permissões baseadas em declarações utilizando o Server Manager. Para fazê-lo, siga estas etapas:

1. No Server Manager, pressione e segure ou clique com o botão direito do mouse na pasta com a qual quer trabalhar e toque ou clique em Properties. A caixa de diálogo Properties será exibida.
2. Ao tocar ou clicar em Permissions no painel esquerdo, as permissões de compartilhamento atuais e as permissões NTFS serão mostradas no painel principal.
3. Toque ou clique em Customize Permissions para abrir a caixa de diálogo Advanced Security Settings com a guia Permissions selecionada.
4. Os usuários ou grupos que já têm acesso ao arquivo ou pasta são listados na lista sob Permission Entries. Utilize as opções fornecidas para visualizar, editar, adicionar ou remover as permissões para usuários e grupos. Quando estiver editando ou adicionando as permissões na caixa de diálogo Permission Entry, poderá adicionar condições conforme descrito nas etapas de 6 a 8 do procedimento anterior.

Auditoria de recursos do sistema

A auditoria é a melhor forma de monitorar o que está acontecendo em seus sistemas com o Windows Server 2012. Você pode utilizar a auditoria para coletar informações relacionadas ao uso de recursos, como acesso aos arquivos, logons no sistema e alterações na configuração do sistema. Sempre que uma ação que tenha configurado para auditoria ocorrer, ela será gravada no log de segurança do sistema, onde será armazenada para que você a examine. O log de segurança está acessível no Event Viewer.

OBSERVAÇÃO Para a maioria das alterações em auditoria, é preciso estar conectado utilizando uma conta que faça parte do grupo Administrators ou é preciso receber o direito Manage Auditing And Security Log via Group Policy.

Configuração de políticas de auditoria

As políticas de auditoria são essenciais para garantir a segurança e a integridade de seus sistemas. Basicamente, todo sistema de computador na rede deve ser configurado com algum tipo de log de segurança. Configura-se políticas de auditoria para computadores individuais com a Local Group Policy (Política Local) e para todos os computadores nos domínios com a Group Policy baseada no Active Directory. Por meio da Group Policy, pode-se definir as políticas de auditoria para um site, um domínio ou uma unidade organizacional inteiros. Também se pode definir as políticas para uma estação de trabalho ou um servidor individuais.

Depois de acessar a GPO com a qual quer trabalhar, poderá definir as políticas de auditoria seguindo estas etapas:

1. No Group Policy Management Editor, mostrado na Figura 12-16, acesse o nó Audit Policy percorrendo a árvore de console. Expanda Computer Configuration, Policies, Windows Settings, Security Settings e Local Policies, e selecione Audit Policy.



FIGURA 12-16 Defina as políticas de auditoria utilizando o nó Audit Policy na Group Policy.

2. As opções de auditoria são as seguintes:
 - **Audit Account Logon Events** Monitora os eventos relacionados ao logon e logoff do usuário.
 - **Audit Account Management** Monitora o gerenciamento de contas por meio do Active Directory Users And Computers. Os eventos serão gerados sempre que contas de usuário, computador ou grupo forem criadas, modificadas ou excluídas.
 - **Audit Directory Service Access** Monitora o acesso ao Active Directory. Os eventos serão gerados sempre que os usuários ou computadores acessarem o diretório.
 - **Audit Logon Events** Monitora os eventos relacionados ao logon, logoff e conexões remotas do usuário a sistemas de rede.
 - **Audit Object Access** Monitora o uso de recursos do sistema para arquivos, pastas, compartilhamentos, impressoras e objetos do Active Directory.
 - **Audit Policy Change** Monitora as alterações em direitos do usuário, auditoria e relações de confiança.
 - **Audit Privilege Use** Monitora o uso de direitos e privilégios do usuário, como o direito de fazer backup de arquivos e pastas.

OBSERVAÇÃO A política Audit Privilege Use não monitora eventos relacionados ao acesso ao sistema, como o uso do direito de fazer logon interativamente ou do direito de acessar o computador a partir da rede. Esses eventos são monitorados com a auditoria de logon e logoff.

- **Audit Process Tracking** Monitora os processos do sistema e os recursos que eles utilizam.
- **Audit System Events** Monitora a inicialização, o desligamento e a reinicialização do sistema, bem como as ações que afetem a segurança do sistema ou o log de segurança.

3. Para configurar uma política de auditoria, toque ou clique duas vezes em sua entrada, ou pressione e segure ou clique com o botão direito do mouse na entrada e toque ou clique em Properties.
4. Na caixa de diálogo que será exibida, marque a caixa de seleção Define These Policy Settings e a caixa de seleção Success, Failure, ou ambas. A opção Success registra em log os eventos bem-sucedidos, como as tentativas de logon bem-sucedidas. A opção Failure registra em log os eventos com falha, como as tentativas de logon que falharam.
5. Toque ou clique em OK.

Quando a auditoria está habilitada, o log de eventos de segurança refletirá o seguinte:

- IDs de evento de 560 e 562 detalhando auditorias de usuários
- IDs de evento de 592 e 593 detalhando auditorias de processos

Auditoria de arquivos e pastas

Se configurar uma GPO para habilitar a opção Audit Object Access, poderá definir o nível de auditoria para pastas e arquivos individuais. Isso permitirá controlar precisamente como o uso de pastas e arquivos é monitorado. Esse tipo de auditoria está disponível apenas em volumes NTFS.

A auditoria de arquivos e pastas pode ser configurada seguindo estas etapas:

1. No File Explorer, pressione e segure ou clique com o botão direito do mouse no arquivo ou na pasta a auditar e toque ou clique em Properties.
2. Toque ou clique na guia Security e em Advanced. A caixa de diálogo Advanced Security Settings será exibida.
3. Na guia Auditing, toque ou clique em Continue. Você poderá visualizar e gerenciar as configurações de auditoria utilizando as opções mostradas na Figura 12-17.

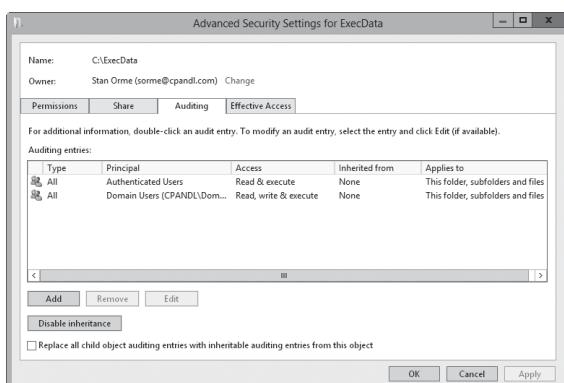


FIGURA 12-17 Depois de auditar o acesso a objetos, você poderá definir as políticas de auditoria em arquivos e pastas individuais na guia Auditing.

4. A lista Auditing Entries mostra os usuários, grupos ou computadores cujas ações se quer auditar. Para remover uma conta, selecione-a na lista Auditing Entries e toque ou clique em Remove.
5. Para configurar a auditoria para usuários, computadores ou grupos adicionais, toque ou clique em Add. A caixa de diálogo Select Users, Computers, Service Accounts, Or Groups será exibida.
6. Digite o nome de um usuário, computador ou grupo no domínio atual e toque ou clique em Check Names. Se uma única correspondência for encontrada, a caixa de diálogo será automaticamente atualizada e a entrada estará sublinhada. Caso contrário, você verá uma caixa de diálogo adicional. Se nenhuma correspondência for encontrada, ou o nome foi digitado incorretamente, ou você está trabalhando com uma localização incorreta. Modifique o nome na caixa de diálogo Name Not Found e tente de novo, ou toque ou clique em Locations para selecionar uma nova localização. Se várias correspondências forem encontradas, na caixa de diálogo Multiple Names Found, selecione o nome que quer utilizar e toque ou clique em OK.
7. Toque ou clique em OK. O usuário ou o grupo será adicionado e as caixas de diálogo Principal e Auditing Entry serão atualizadas para mostrá-lo. Somente as permissões básicas são listadas por padrão. Se quiser trabalhar com permissões avançadas, toque ou clique em Show Advanced Permissions para exibir as permissões especiais.
8. Conforme necessário, utilize a lista Applies To para especificar onde os objetos são auditados. Se estiver trabalhando com uma pasta e quiser substituir as entradas de auditoria em todos os objetos filhos dela (e não na pasta em si), selecione Only Apply These Settings To Objects And/Or Containers Within This Container.

Lembre-se de que a lista Applies To permite especificar as localizações *onde* se quer que as configurações de auditoria sejam aplicadas. A caixa de seleção Only Apply These Settings To Objects And/Or Containers Within This Container controla *como* as configurações de auditoria são aplicadas. Quando essa caixa de seleção está marcada, as configurações de auditoria no objeto pai substituem as configurações nos objetos filhos. Quando está desmarcada, as configurações de auditoria no pai são mescladas com as configurações existentes nos objetos filhos.

9. Utilize a lista Type para especificar se está configurando a auditoria para sucesso, falha, ou ambos, e especifique quais ações devem ser auditadas. A opção Success registra em log os eventos bem-sucedidos, como as leituras de arquivos bem-sucedidas. A opção Failure registra em log os eventos com falha, como as exclusões de arquivos que falharam. Os eventos que podem ser auditados são os mesmos que as permissões especiais listadas nas Tabelas 12-4 e 12-5, exceto que não se pode auditar a sincronização de arquivos e pastas offline. Para arquivos e pastas essenciais, normalmente se desejará monitorar o seguinte:

- Write Attributes–Successful
- Write Extended Attributes–Successful
- Delete Subfolders And Files–Successful
- Delete–Successful
- Change Permissions–Successful

DICA Se quiser auditar ações de todos os usuários, utilize o grupo especial Everyone. Caso contrário, selecione os grupos de usuários ou usuários específicos, ou ambos, que quer auditar.

10. Se estiver utilizando políticas baseadas em declarações e quiser limitar o escopo da entrada de auditoria, poderá adicionar condições baseadas em declarações à entrada de auditoria. Por exemplo, se todos os computadores da empresa forem membros do grupo Domain Computers, talvez queira auditar minuciosamente o acesso por dispositivos que não façam parte desse grupo.
11. Quando tiver terminado de configurar a auditoria, toque ou clique em OK. Repita esse processo para auditar outros usuários, grupos ou computadores.

Auditoria de registro

Se configurar uma GPO para habilitar a opção Audit Object Access, poderá definir o nível de auditoria para chaves dentro do registro. Isso permitirá monitorar quando os valores da chave são definidos, as subchaves são criadas e as chaves são excluídas.

A auditoria do registro pode ser configurada seguindo estas etapas:

1. Abra o Registry Editor. Em um prompt de comando, digite **regedit**, ou digite **regedit** na caixa Apps Search e pressione Enter.
2. Procure a chave que quer auditar. No menu Edit, selecione Permissions.
3. Na caixa de diálogo Permissions, toque ou clique em Advanced. Na caixa de diálogo Advanced Security Settings, clique ou toque na guia Auditing.
4. Toque ou clique em Add para exibir a caixa de diálogo Auditing Entry. Toque ou clique em Select A Principal para exibir a caixa de diálogo Select User, Computer, Service Account Or Group.
5. Na caixa de diálogo Select User, Computer, Service Account, Or Group, digite **Everyone**, toque ou clique em Check Names e em OK.
6. Na caixa de diálogo Auditing Entry, apenas as permissões básicas são listadas por padrão. Toque ou clique em Show Advanced Permissions para exibir as permissões especiais.
7. Utilize a lista Applies To para especificar como a entrada de auditoria deve ser aplicada.
8. Utilize a lista Type para especificar se está configurando a auditoria para sucesso, falha, ou ambos, e especifique quais ações devem ser auditadas. Normalmente, você desejará monitorar as seguintes permissões avançadas:
 - Set Value—Successful e Failed
 - Create Subkey—Successful e Failed
 - Delete—Successful e Failed
9. Clique em OK três vezes para fechar todas as caixas de diálogo abertas e aplicar as configurações de auditoria.

Auditoria de objetos do Active Directory

Se configurar uma GPO para habilitar a opção Audit Directory Service Access, poderá definir o nível de auditoria para objetos do Active Directory. Isso permitirá controlar precisamente como o uso de objetos é monitorado.

Para configurar a auditoria de objetos, siga estas etapas:

1. Em Active Directory Users And Computers, certifique-se de que Advanced Features esteja selecionado no menu View e acesse o contêiner do objeto.
2. Toque ou clique duas vezes no objeto a ser auditado. A caixa de diálogo Properties relacionada será aberta.
3. Toque ou clique na guia Security e em Advanced.
4. Na caixa de diálogo Advanced Settings, toque ou clique na guia Auditing. A lista Auditing Entries mostra os usuários, grupos ou computadores cujas ações estão sendo auditadas (se alguma). Para remover uma conta, selecione-a na lista Auditing Entries e toque ou clique em Remove.
5. Para adicionar contas específicas, toque ou clique em Add para exibir a caixa de diálogo Auditing Entry. Toque ou clique em Select A Principal para exibir a caixa de diálogo Select User, Computer, Service Account Or Group.
6. Digite o nome de um usuário, computador ou grupo no domínio atual e toque ou clique em Check Names. Se uma única correspondência for encontrada, a caixa de diálogo será automaticamente atualizada e a entrada estará sublinhada. Caso contrário, você verá uma caixa de diálogo adicional. Se nenhuma correspondência for encontrada, ou o nome foi digitado incorretamente, ou você está trabalhando com uma localização incorreta. Modifique o nome na caixa de diálogo Name Not Found e tente de novo, ou toque ou clique em Locations para selecionar uma nova localização. Se várias correspondências forem encontradas, na caixa de diálogo Multiple Names Found, selecione o nome que quer utilizar e toque ou clique em OK.
7. Toque ou clique em OK para retornar à caixa de diálogo Auditing Entry. Utilize a lista Applies To para especificar como a entrada de auditoria deve ser aplicada.
8. Utilize a lista Type para especificar se está configurando a auditoria para sucesso, falha, ou ambos, e especifique quais ações devem ser auditadas. A opção Success registra em log os eventos bem-sucedidos, como uma tentativa bem-sucedida de modificar as permissões de um objeto. A opção Failed registra em log os eventos com falhas, como uma tentativa de modificar a posse de um objeto que tenha falhado.
9. Toque ou clique em OK. Repita esse processo para auditar outros usuários, grupos ou computadores.

Utilização, configuração e gerenciamento de cotas de disco do NTFS

O Windows Server 2012 dá suporte a dois tipos mutuamente exclusivos de cotas de disco:

- **Cotas de disco do NTFS** As cotas de disco do NTFS têm suporte em todas as edições do Windows Server 2012 e permitem gerenciar o uso do espaço em disco pelos usuários. Configura-se as cotas por volume. Embora os usuários que excedam os limites vejam avisos, os administradores são notificados principalmente por meio dos logs de eventos.
- **Cotas de disco do Resource Manager** As cotas de disco do Resource Manager têm suporte em todas as edições do Windows Server 2012 e permitem gerenciar

o uso do espaço em disco por pasta e por volume. Os usuários que estejam se aproximando de um limite ou o tenham excedido podem ser notificados automaticamente por email. O sistema de notificações também permite notificar os administradores por email, disparar relatórios de incidentes, executar comandos e registrar em log os eventos relacionados.

As seções a seguir abordam as cotas de disco NTFS.

OBSERVAÇÃO Independentemente do sistema de cotas que está sendo utilizado, pode-se configurá-las apenas para volumes NTFS. Não é possível criar cotas para volumes FAT, FAT32 ou ReFS.

MUNDO REAL Quando você aplica cotas de disco, é preciso ser muito cuidadoso com a maneira como as impõe, especialmente no que diz respeito às contas do sistema, contas de serviço ou outras contas com finalidades especiais. A aplicação inadequada de cotas de disco a esses tipos de contas pode causar sérios problemas que são difíceis de diagnosticar e resolver. A imposição de cotas em contas System, NetworkService e LocalService poderia impedir o computador de concluir importantes tarefas do sistema operacional. Como exemplo, se essas contas alcançarem seu limite de cota imposto, você não poderia aplicar alterações à Group Policy, pois o cliente de Group Policy é executado dentro de um contexto LocalSystem por padrão e não poderia gravar no disco do sistema. Se um serviço não puder gravar no disco do sistema, as alterações da Group Policy não podem ser feitas e não poder alterar a Group Policy poderia ter todos os tipos de consequências inesperadas, pois você estaria preso às configurações feitas anteriormente. Não seria possível desabilitar ou modificar as configurações de cotas por meio da Group Policy, por exemplo.

Nesse cenário, em que os contextos de serviço alcançaram um limite de cota imposto, qualquer outra configuração que utilize esses contextos e exija fazer alterações em arquivos no disco provavelmente também iria falhar. Por exemplo, você não poderia concluir a instalação ou remoção de funções, serviços de função e recursos. Isso deixaria o servidor em um estado em que o Server Manager sempre incluiria um aviso de que é preciso reiniciar o computador para concluir as tarefas de configuração, mas a reinicialização do computador não resolveria esses problemas.

Para tratar desse problema, é preciso editar as entradas de cotas de disco para o disco do sistema, aumentar os limites impostos nas contas de serviço e reiniciar o computador. A reinicialização do computador dispara as tarefas de finalização e permite que ele conclua qualquer tarefa de configuração parada em um status pendente. Como o serviço de cliente da Group Policy poderia processar as alterações e gravá-las no disco do sistema, as alterações na Group Policy também seriam aplicadas.

O que são cotas de disco NTFS e como elas são utilizadas

Os administradores utilizam as cotas de disco NTFS para gerenciar o uso do espaço em disco de volumes críticos, como os que fornecem compartilhamentos de dados corporativos ou compartilhamentos de dados de usuário. Quando se habilita as cotas de disco NTFS, pode-se configurar dois valores:

- **Disk quota limit** Define o limite máximo para o uso de espaço, que pode ser utilizado para impedir que os usuários gravem informações adicionais em um volume, para registrar em log eventos em relação aos usuários que excederam esse limite, ou ambos.
- **Disk quota warning** Alerta os usuários e registra em log eventos de aviso quando os usuários estiverem se aproximando de seu limite de cota do disco.

DICA Você pode definir cotas de disco, mas não impô-las, e talvez esteja se perguntando por que o faria. Algumas vezes, se quer monitorar o uso do espaço em disco por usuário e saber quando os usuários excederam algum limite predefinido, mas em vez de negar o espaço em disco

adicional, registrar um evento no log de aplicativos para monitorar o excedente. Você pode então enviar mensagens de aviso ou descobrir outras maneiras de reduzir o uso do espaço.

As cotas de disco NTFS se aplicam somente aos usuários finais. Elas não se aplicam aos administradores. Não se pode negar espaço em disco aos administradores, mesmo se excederem os limites de cotas de disco impostos.

Em um ambiente típico, você restringe o uso do espaço em disco em megabytes (MB) ou gigabytes (GB). Por exemplo, em um compartilhamento de dados corporativos utilizado por vários usuários de um departamento, talvez queira limitar o uso do espaço em disco para 20 a 100 GB. Para um compartilhamento de dados de usuário, talvez queira definir o nível mais abaixo, como de 5 a 20 GB, para restringir a criação de grandes quantidades de dados pessoais pelo usuário. Muitas vezes, você definirá o limite de aviso da cota de disco como uma porcentagem do limite da cota do disco. Por exemplo, pode definir o aviso para 90% a 95% do limite da cota de disco.

Como as cotas de disco NTFS são monitoradas por volume e por usuário, o espaço em disco utilizado por um usuário não afeta as cotas de disco dos outros. Portanto, se um usuário exceder seu limite, qualquer restrição aplicada a ele não será aplicada a outros usuários. Por exemplo, se um usuário exceder um limite de cota de disco de 5 GB e o volume estiver configurado para impedir a gravação além do limite, o usuário não poderá mais gravar dados no volume. Os usuários podem, no entanto, remover arquivos e pastas do volume para liberar espaço em disco. Também podem mover arquivos e pastas para uma área compactada no volume, o que poderia liberar espaço, ou podem escolher compactar os próprios arquivos. A restrição de cota não é afetada ao mover os arquivos para uma localização diferente no mesmo volume. A quantidade de espaço para os arquivos é a mesma, a menos que o usuário mova arquivos e pastas não compactados para uma pasta com compactação. De qualquer forma, a restrição para um único usuário não afetará a capacidade dos demais de gravação no volume (desde que haja espaço livre total nele).

Pode-se habilitar cotas de disco NTFS em:

- **Volumes locais** Para gerenciar cotas de disco em volumes locais, trabalha-se com o próprio disco local. A cota de disco habilitada em um volume local terá os arquivos de sistema do Windows incluídos no uso do volume para o usuário que os tenha instalado. Algumas vezes, isso pode fazer com que o usuário ultrapasse o limite de cota de disco. Para evitá-lo, talvez queira definir um limite maior em um volume local da estação de trabalho.
- **Volumes remotos** Para gerenciar cotas de disco em volumes remotos, deve-se compartilhar o diretório raiz do volume e definir a cota de disco nele. Lembre-se, as cotas são definidas por volume, portanto, se um servidor de arquivos remoto tiver volumes separados para diferentes tipos de dados – isto é, um volume de dados corporativos e um volume de dados de usuário –, esses volumes deverão ter cotas diferentes.

Somente os membros do grupo Domain Admins ou do grupo Administrators do sistema local podem configurar as cotas de disco. A primeira etapa ao utilizar cotas é habilitá-las na Group Policy. Você pode fazê-lo em dois níveis:

- **Local** Por meio da Group Policy local, você pode habilitar cotas de disco para um computador individual.
- **Enterprise** Por meio da Group Policy que é aplicada a um site, um domínio ou uma unidade organizacional, você pode habilitar cotas de disco para grupos de usuários e computadores.

Ter de monitorar as cotas de disco pode causar alguma sobrecarga em computadores. Essa sobrecarga é em função do número de cotas de disco sendo impostas, do tamanho total dos volumes e seus dados e do número de usuários aos quais as cotas de disco são aplicadas.

Embora na superfície as cotas de disco sejam monitoradas por usuário, nos bastidores, o Windows Server 2012 gerencia as cotas de disco de acordo com os security identifiers (SIDs, identificadores de segurança). Como as cotas de disco monitoram os SIDs, pode-se modificar os nomes de usuários com segurança sem afetar a configuração de cotas de disco. O monitoramento através de SIDs provoca alguma sobrecarga adicional ao visualizar estatísticas de cotas de disco para os usuários. Isso se deve ao fato de que o Windows Server 2012 precisa correlacionar os SIDs aos nomes das contas de usuário a fim de que os nomes das contas possam ser exibidos nas caixas de diálogo. Isso significa contatar o gerenciador de usuários local e o controlador de domínio do Active Directory conforme necessário.

Depois do Windows Server 2012 procurar os nomes, ele os armazena em cache em um arquivo local, de modo que possam estar disponíveis imediatamente da próxima vez que forem necessários. O cache de consulta não é atualizado com frequência – se perceber uma discrepância entre o que é exibido e o que está configurado, é preciso atualizar as informações. Normalmente, isso significa escolher Refresh no menu View ou pressionar F5 na janela atual.

Configuração de políticas de cotas de disco NTFS

A melhor maneira de configurar as cotas de disco NTFS é por meio da Group Policy. Quando se configura as cotas de disco por meio da política local ou da política de OU (unidade organizacional), domínio e site, se definem as políticas gerais que são configuradas automaticamente quando se habilita o gerenciamento de cotas em volumes individuais. Portanto, em vez de ter de configurar cada volume separadamente, pode-se utilizar o mesmo conjunto de regras e aplicá-las, por sua vez, a cada volume que queira gerenciar.

As políticas que controlam as cotas de disco NTFS são aplicadas no nível do sistema. Você acessa essas políticas por Computer Configuration\Administrative Templates\System\Disk Quotas. A Tabela 12-6 resume as políticas disponíveis.

TABELA 12-6 Políticas para a configuração de cotas de disco NTFS

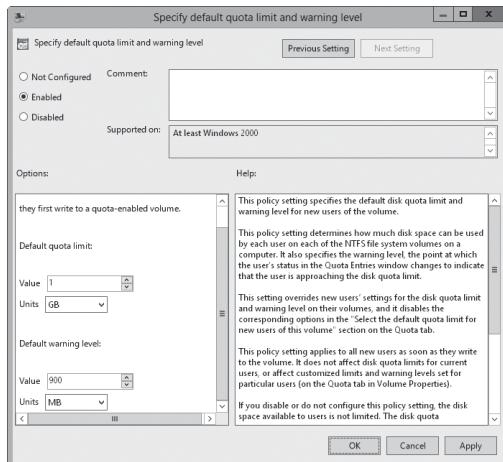
NOME DA POLÍTICA	DESCRIÇÃO
Apply Policy To Removable Media	Determina se as políticas de cotas se aplicam a volumes NTFS em mídia removível. Se não habilitar esta política, os limites de cota serão aplicados apenas a unidades de mídia fixa.
Enable Disk Quotas	Ativa ou desativa as cotas de disco para todos os volumes NTFS do computador e impede que os usuários alterem esta configuração.
Enforce Disk Quota Limit	Especifica se os limites de cotas são impostos. Se as cotas forem impostas, o espaço em disco será negado aos usuários que excederem a cota. Isso substitui as configurações na guia Quota do volume NTFS.
Log Event When Quota Limit Exceeded	Determina se um evento é registrado em log quando os usuários atingem seu limite e impede que os usuários alterem suas opções de registro em log.

TABELA 12-6 Políticas para a configuração de cotas de disco NTFS (*continuação*)

NOME DA POLÍTICA	DESCRIÇÃO
Log Event When Quota Warning Level Exceeded	Determina se um evento é registrado em log quando os usuários atingem o nível de aviso.
Specify Default Quota Limit And Warning Level	Define um limite de cota padrão e nível de aviso para todos os usuários. Esta configuração substitui outras configurações e só afeta os novos usuários.

Sempre que trabalhar com limites de cota, deverá utilizar um conjunto padrão de políticas em todos os sistemas. Normalmente, você não desejará habilitar todas as políticas. Em vez disso, irá habilitar as políticas seletivamente e utilizar os recursos NTFS padrão para controlar as cotas em vários volumes. Se quiser habilitar os limites de cota, siga estas etapas:

1. Acesse a Group Policy do sistema (por exemplo, um servidor de arquivos) com o qual quer trabalhar. Acesse o nó Disk Quotas expandindo Computer Configuration, Administrative Templates, System e selecionando Disk Quotas.
2. Toque ou clique duas vezes em Enable Disk Quotas. Selecione Enabled e toque ou clique em OK.
3. Toque ou clique duas vezes em Enforce Disk Quota Limit. Se quiser impor cotas de disco em todos os volumes NTFS localizados neste computador, toque ou clique em Enabled. Caso contrário, toque ou clique em Disabled e configure os limites específicos por volume. Toque ou clique em OK.
4. Toque ou clique duas vezes em Specify Default Quota Limit And Warning Level. Na caixa de diálogo mostrada na Figura 12-18, selecione Enabled.

**FIGURA 12-18** Imponha cotas de disco na caixa de diálogo Specify Default Quota Limit And Warning Level.

5. Sob Default Quota Limit, defina um limite padrão que será aplicado aos usuários quando fizerem a primeira gravação no volume habilitado para controle de cotas. O limite não será aplicado aos usuários atuais ou afetará os limites em funcionamento. Em um compartilhamento corporativo, como um utilizado por membros de uma equipe de projetos, um bom limite está entre 5 e 10 GB. Claro, isso depende do tamanho dos arquivos de dados com que os usuários trabalhem rotineiramente, do número de usuários e do tamanho do volume de disco. Os designers gráficos e engenheiros de dados talvez precisem de muito mais espaço em disco.
6. Para definir um limite de aviso, role para baixo a janela Options. Um bom limite de aviso é cerca de 90% do limite de cota padrão, ou seja, se definir o limite de cota padrão para 10 GB, deve configurar o limite de aviso para 9 GB. Toque ou clique em OK.
7. Toque ou clique duas vezes em Log Event When Quota Limit Exceeded. Selecione Enabled a fim de que os eventos sobre o limite sejam gravados no log de aplicativo e toque ou clique em OK.
8. Toque ou clique duas vezes em Log Event When Quota Warning Level Exceeded. Selecione Enabled a fim de que os eventos sobre avisos sejam gravados no log de aplicativo e toque ou clique em OK.
9. Toque ou clique duas vezes em Apply Policy To Removable Media. Selecione Disabled a fim de que os limites de cota sejam aplicados apenas a volumes de mídia fixa no computador e toque ou clique em OK.

DICA Para garantir que as políticas sejam imediatamente impostas, acesse o nó Computer Configuration\Administrative Templates\System\Group Policy e toque ou clique duas vezes em Configure Disk Quota Policy Processing. Selecione Enabled e marque a caixa de seleção Process Even If The Group Policy Objects Have Not Changed. Toque ou clique em OK.

Habilitação de cotas de disco NTFS em volumes NTFS

Pode-se habilitar cotas de disco NTFS por volume. Somente os volumes NTFS podem ter cotas de disco. Depois de configurar as políticas de grupo apropriadas, poderá utilizar o Computer Management para definir as cotas de disco para volumes locais e remotos.

OBSERVAÇÃO Se utilizar a configuração de política Enforce Disk Quota Limit para impor as cotas, o espaço em disco será negado aos usuários que excederem a cota. Isso substitui as configurações na guia Quota do volume NTFS.

Para habilitar as cotas de disco NTFS em um volume NTFS, siga estas etapas:

1. Abra o Computer Management. Se necessário, conecte-se a um computador remoto.
2. Na árvore de console, expanda Storage e selecione Disk Management. Os volumes configurados no computador selecionado serão exibidos no painel de detalhes.
3. Utilizando o modo de exibição Volume List ou Graphical View, pressione e segure ou clique com o botão direito do mouse no volume com o qual quer trabalhar e toque ou clique em Properties.

- Na guia Quota, marque a caixa de seleção Enable Quota Management, mostrada na Figura 12-19. Se já tiver definido os valores de gerenciamento de cotas por meio da Group Policy, as opções não estarão disponíveis e não será possível alterá-las. Em lugar disso, deve-se modificar as opções por meio da Group Policy.

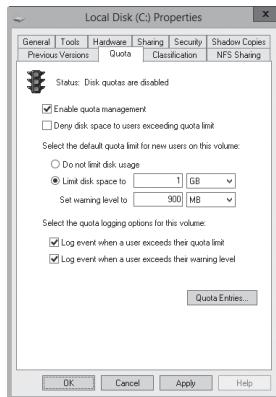


FIGURA 12-19 Depois de habilitar o gerenciamento de cotas, poderá configurar um limite de cota e um nível de aviso de cota para todos os usuários.

PRÁTICAS RECOMENDADAS Sempre que trabalhar com a guia Quota, preste atenção especial ao texto de Status e ao ícone de semáforo associado. Ambos mudam baseados no estado do gerenciamento de cotas. Se as cotas não estiverem configuradas, o ícone de semáforo mostrará uma luz vermelha e o status será inactive (inativo) ou not configured (não configurado). Se o sistema operacional estiver trabalhando com as cotas ou atualizando-as, o ícone de semáforo mostrará uma luz amarela e o status mostrará a atividade sendo realizada. Se as cotas estiverem configuradas, o ícone de semáforo mostrará uma luz verde e o texto do status declarará que o sistema de cotas está ativo.

- Para definir um limite de cota de disco padrão para todos os usuários, selecione Limit Disk Space To. Nas caixas de texto fornecidas, defina um limite em quilobytes, megabytes, gigabytes, terabytes, petabytes ou exabytes. Defina o limite de aviso padrão nas caixas de texto Set Warning Level To. Mais uma vez, normalmente você desejará que o limite de aviso de cota de disco seja 90-95% do limite de cota de disco.

DICA Embora o limite de cota padrão e o nível de aviso sejam aplicados a todos os usuários, pode-se configurar níveis diferentes para usuários individuais. Isso é feito na caixa de diálogo Quota Entries. Se criar muitas entradas de cotas exclusivas e não quiser recriá-las em um volume com características e uso similares, poderá exportar as entradas de cotas e importá-las para um volume diferente.

- Para impor o limite de cota de disco e impedir que os usuários o ultrapassem, marque a caixa de seleção Deny Disk Space To Users Exceeding Quota Limit. Lembre-se de que isso criará uma limitação física real para os usuários (mas não para os administradores).

7. Para configurar o registro em log quando os usuários excederem o limite de aviso ou de cota, marque as caixas de seleção sobre logs de eventos. Toque ou clique em OK para salvar suas alterações.
8. Se o sistema de cotas não estiver habilitado no momento, você verá um prompt solicitando que o habilite. Toque ou clique em OK para permitir que o Windows Server 2012 examine novamente o volume e atualize as estatísticas de uso de disco. Medidas podem ser tomadas contra os usuários que excederem o limite atual ou o nível de aviso. Essas medidas podem incluir impedir novas gravações no volume, a notificação na próxima vez que o volume for acessado e o registro em log de eventos aplicáveis no log de aplicativo.

Visualização de entradas de cota de disco

O uso do espaço em disco é monitorado por usuário. Quando as cotas de disco estão habilitadas, cada usuário que armazena dados em um volume tem uma entrada no arquivo de cotas de disco. Essa entrada é atualizada periodicamente para mostrar o espaço do disco atual utilizado, o limite de cota aplicável, o nível de aviso aplicável e a porcentagem de espaço permitido sendo utilizada. Como administrador, você pode modificar as entradas de cota de disco para definir limites e níveis de aviso diferentes para certos usuários. Também é possível criar entradas de cota de disco para usuários que ainda não tenham salvo dados em um volume. A principal razão para criar entradas é garantir que, quando o usuário utilizar o volume, terá um limite e um nível de aviso apropriados.

Para visualizar as entradas de cota de disco atuais de um volume, siga estas etapas:

1. Abra o Computer Management. Se necessário, conecte-se a um computador remoto.
2. Na árvore de console, expanda Storage e selecione Disk Management. Os volumes configurados no computador selecionado serão exibidos no painel de detalhes.
3. Utilizando o modo de exibição Volume List ou Graphical View, pressione e segure ou clique com o botão direito do mouse no volume com o qual quer trabalhar e toque ou clique em Properties.
4. Na guia Quota, toque ou clique em Quota Entries. A caixa de diálogo Quota Entries será exibida. Cada entrada de cota será listada de acordo com um status. O status deve descrever rapidamente se um usuário ultrapassou um limite. Um status de OK significa que o usuário está trabalhando dentro dos limites da cota. Qualquer outro status normalmente significa que o usuário atingiu o nível de aviso ou o limite de cota.

Criação de entradas de cota de disco

É possível criar entradas de cota de disco para usuários que ainda não tenham salvo dados em um volume. Isso permite definir limites personalizados e níveis de aviso para um determinado usuário. Em geral, se utiliza esse recurso quando um usuário armazena com frequência mais informações que outros e você quer permitir que ele ultrapasse o limite normal, ou quando quer definir um limite específico para administradores. Como deve se lembrar, os administradores não estão sujeitos aos limites de cota de disco, portanto, se quiser impor limites para administradores individuais, deve criar entradas de cota para cada administrador que quiser limitar.

MUNDO REAL Você não deve criar entradas de cota de disco individuais ao acaso. É preciso monitorar as entradas individuais com cuidado. Idealmente, você deveria manter um log que detalhe qualquer entrada individual a fim de que outros administradores entendam as políticas em funcionamento e como elas são aplicadas. Quando modificar as regras básicas para cotas em um volume, você deve reexaminar as entradas individuais para ver se ainda são aplicáveis ou se também precisam ser atualizadas. Descobri que certos tipos de usuários são mais frequentemente exceções do que não e que às vezes é melhor colocar diferentes classes de usuários em volumes diferentes e, então, aplicar as cotas de disco a cada volume. Dessa forma, cada classe ou categoria de usuário tem um limite de cota que seja apropriado para o uso típico de seus membros e se terá menos (talvez nenhuma) exceções. Por exemplo, você poderia utilizar volumes separados para executivos, gerentes e usuários padrão, ou ter volumes separados para gerência, designers gráficos, engenheiros e todos os outros usuários.

Para criar uma entrada de cota em um volume, siga estas etapas:

1. Abra a caixa de diálogo Quota Entries, como abordado em “Visualização de entradas de cota de disco” anteriormente neste capítulo. As entradas de cota atuais para todos os usuários serão listadas. Para atualizar a listagem, pressione F5 ou escolha Refresh no menu View.
2. Se o usuário não tiver uma entrada existente no volume, poderá criá-la escolhendo New Quota Entry no menu Quota. A caixa de diálogo Select Users será aberta.
3. Na caixa de diálogo Select Users, digite o nome de um usuário que você quer utilizar na caixa de texto Enter The Object Names To Select e toque ou clique em Check Names. Se uma correspondência for encontrada, selecione a conta que quer utilizar e toque ou clique em OK. Se nenhuma correspondência for encontrada, atualize o nome digitado e tente pesquisar de novo. Repita esta etapa conforme necessário e toque ou clique em OK.
4. Depois de selecionar um usuário, a caixa de diálogo Add New Quota Entry será exibida, como mostrado na Figura 12-20. Você tem duas opções. Pode remover todas as restrições de cota para esse usuário selecionando Do Not Limit Disk Usage, ou definir um limite específico e um nível de aviso selecionando Limit Disk Space To e digitando os valores apropriados. Toque ou clique em OK.

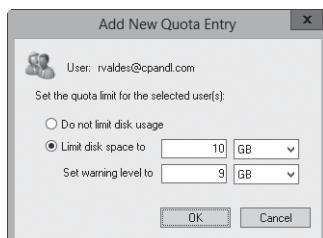


FIGURA 12-20 Na caixa de diálogo Add New Quota Entry, você pode personalizar o limite de cota e o nível de aviso de um usuário ou remover por completo as restrições de cota.

Exclusão de entradas de cota de disco

Quando tiver criado entradas de cota de disco em um volume e um usuário não precisar mais utilizá-lo, pode-se excluir a entrada de cota de disco associada. Quando se exclui uma entrada de cota de disco, todos os arquivos possuídos pelo usuário são coletados e exibidos em uma caixa de diálogo, a fim de que se possa excluí-los permanentemente, apropriar-se deles ou movê-los para uma pasta em um volume diferente.

Para excluir uma entrada de cota de disco de um usuário e gerenciar os arquivos remanescentes dele no volume, siga estas etapas:

1. Abra a caixa de diálogo Quota Entries, como abordado em "Visualização de entradas de cota de disco" anteriormente neste capítulo. As entradas de cota atuais de todos os usuários serão listadas. Para atualizar a listagem, pressione F5 ou escolha Refresh no menu View.
2. Selecione a entrada de cota de disco que quer excluir e pressione Delete, ou escolha Delete Quota Entry no menu Quota. Pode-se selecionar várias entradas utilizando as teclas Shift e Ctrl.
3. Quando for solicitado que confirme a ação, toque ou clique em Yes. A caixa de diálogo Disk Quota será exibida com uma lista dos arquivos atuais possuídos pelos usuários selecionados.
4. Na lista List Files Owned By, exiba os arquivos de um usuário cuja entrada de cota esteja excluindo. Agora é preciso especificar como se deve lidar com os arquivos do usuário. Pode-se tratar de cada arquivo separadamente, selecionando os arquivos individuais e escolhendo a opção apropriada. Você pode selecionar vários arquivos utilizando as teclas Shift e Ctrl. As opções a seguir estão disponíveis:
 - **Permanently Delete Files** Selecione os arquivos a excluir e pressione Delete. Quando for solicitado que confirme a ação, toque ou clique em Yes.
 - **Take Ownership Of Files** Selecione os arquivos de que quer se apropriar e toque ou clique em Take Ownership Of Files.
 - **Move Files To** Selecione os arquivos que quer mover e digite o caminho para uma pasta em um volume diferente. Se não souber o caminho que quer utilizar, toque ou clique em Browse para exibir a caixa de diálogo Browse For Folder. Assim que encontrar a pasta, toque ou clique em Move.
5. Toque ou clique em Close quando tiver concluído o gerenciamento dos arquivos. Se tiver lidado adequadamente com todos os arquivos dos usuários, as entradas de cota de disco serão excluídas.

Exportação e importação de configurações de cotas de disco NTFS

Em vez de recriar entradas de cota de disco personalizadas em volumes individuais, você pode exportar as configurações de um volume de origem e importá-las em outro. É preciso formatar ambos os volumes utilizando o NTFS. Para exportar e depois importar as entradas de cota de disco, siga estas etapas:

1. Abra a caixa de diálogo Quota Entries, como abordado em "Visualização de entradas de cota de disco" anteriormente neste capítulo. As entradas de cota atuais

para todos os usuários serão listadas. Para atualizar a listagem, pressione F5 ou escolha Refresh no menu View.

2. Selecione Export no menu Quota. A caixa de diálogo Export Quota Settings será exibida. Escolha a localização para salvar o arquivo contendo as configurações de cotas e digite um nome para ele na caixa de texto File Name. Toque ou clique em Save.

OBSERVAÇÃO Se salvar o arquivo de configurações em uma unidade mapeada no volume de destino, terá mais facilidade para importar as configurações. Os arquivos de cotas geralmente são pequenos, portanto, não é preciso se preocupar com o uso do espaço em disco.

3. No menu Quota, toque ou clique em Close para sair da caixa de diálogo Quota Entries.
4. Pressione e segure ou clique com o botão direito do mouse em Computer Management na árvore de console e toque ou clique em Connect To Another Computer. Na caixa de diálogo Select Computer, escolha o computador contendo o volume de destino. O volume de destino é aquele em que quer utilizar as configurações exportadas.
5. Conforme explicado anteriormente, abra a caixa de diálogo Properties do volume de destino. Toque ou clique em Quota Entries na guia Quota. A caixa de diálogo Quota Entries do volume de destino será exibida.
6. Toque ou clique em Import no menu Quota. Na caixa de diálogo Import Quota Settings, selecione o arquivo de configurações de cotas que salvou anteriormente. Toque ou clique em Open.
7. Se o volume tiver entradas de cota anteriores, você terá a opção de substituir as entradas existentes ou mantê-las. Quando for questionado a respeito de conflitos, toque ou clique em Yes para substituir a entrada existente ou em No para mantê-la. Para aplicar a opção para substituir ou manter as entradas existentes para todas as entradas do volume, marque a caixa de seleção Do This For All Quota Entries antes de tocar ou clicar em Yes ou No.

Como desabilitar cotas de disco NTFS

Pode-se desabilitar as cotas para usuários individuais ou todos os usuários em um volume. Quando se desabilita as cotas para um determinado usuário, ele não estará mais sujeito às restrições de cota, mas as cotas de disco ainda serão monitoradas para outros usuários. Ao desabilitar cotas em um volume, o monitoramento e gerenciamento de cotas será completamente removido. Para desabilitar cotas para um determinado usuário, siga a técnica descrita anteriormente no capítulo em "Visualização de entradas de cota de disco". Para desabilitar o monitoramento e gerenciamento de cotas em um volume, siga estas etapas:

1. Abra o Computer Management. Se necessário, conecte-se a um computador remoto.
2. Abra a caixa de diálogo Properties do volume em que quer desabilitar as cotas NTFS.
3. Na guia Quota, desmarque a caixa de seleção Enable Quota Management. Toque ou clique em OK. Quando solicitado para confirmar, toque ou clique em OK.

Utilização, configuração e gerenciamento de cotas de disco do Resource Manager

O Windows Server 2012 dá suporte a um sistema de gerenciamento de cotas aprimorado chamado de *Resource Manager disk quotas* (cotas de disco do Resource Manager). Utilizando as cotas de disco do Resource Manager, pode-se gerenciar o uso do espaço em disco por pasta e por volume.

DICA Como se gerencia as cotas de disco do Resource Manager separadamente das cotas de disco NTFS, você pode configurar um único volume para utilizar os dois sistemas de cotas. No entanto, é recomendável utilizar um sistema de cotas ou o outro. Como opção, se já tiver configurado as cotas de disco NTFS, talvez queira continuar utilizando-as por volume e suplementar esse gerenciamento de cotas com as cotas de disco do Resource Manager para pastas importantes.

As cotas de disco do Resource Manager

Ao trabalhar com o Windows Server 2012, as cotas de disco do Resource Manager são outra ferramenta que se pode utilizar para gerenciar o uso do disco. É possível configurar cotas de disco do Resource Manager por volume ou por pasta. Pode-se definir cotas de disco com um limite rígido específico – isto é, um limite que não possa ser excedido – ou um limite flexível, ou seja, que possa ser excedido.

Geralmente, deve-se utilizar os limites rígidos quando se quer impedir que os usuários excedam uma limitação de uso do disco específica. Utilize limites flexíveis quando quiser monitorar o uso e simplesmente avisar os usuários que excederem as diretrizes de uso ou estiverem prestes a fazê-lo. Todas as cotas têm um caminho de cota, que designa o caminho base do volume ou da pasta em que a cota foi aplicada. A cota é aplicada ao volume ou à pasta designados e a todas as suas subpastas. Os detalhes de como as cotas funcionam e como usuários são limitados ou avisados são derivados de um modelo de origem que define as propriedades das cotas.

O Windows Server 2012 inclui os modelos de cotas listados na Tabela 12-7. Utilizando o File Server Resource Manager, pode-se definir com facilidade modelos adicionais que estariam disponíveis sempre que cotas fossem definidas ou pode-se configurar propriedades de cotas personalizadas para único uso ao definir uma cota.

Os modelos de cotas ou propriedades personalizadas definem o seguinte:

- **Límite** O limite de uso do espaço em disco
- **Tipo de cota** Rígida ou flexível
- **Limites de notificação** Os tipos de notificação que ocorrem quando o uso atinge uma porcentagem específica do limite

Embora cada cota tenha um limite e tipo específico, pode-se definir vários limites de notificação como um limite de aviso ou um limiar de limite. Os limites de aviso são considerados qualquer porcentagem do limite que seja menor que 100%. O limiar de limite ocorre quando o limite alcançado é 100%. Por exemplo, você poderia definir os limites de aviso que serão disparados a 85% e a 95% do limite e um limiar de limite que será disparado quando 100% do limite for alcançado.

Os usuários que estejam se aproximando de um limite ou o tenham excedido podem ser notificados automaticamente por email. O sistema de notificações também permite notificar os administradores por email, disparar relatórios de incidentes, executar comandos e registrar em log os eventos relacionados.

TABELA 12-7 Modelos de cotas de disco

MODELO DE COTA	LIMITE	TIPO DE COTA	DESCRIÇÃO
100 MB Limit	100 MB	Rígido	Envia avisos aos usuários conforme se aproximem ou excedam o limite
200 MB Limit Reports To User	200 MB	Rígido	Envia relatórios de armazenamento aos usuários que tenham excedido o limite
200 MB Limit With 50 MB Extension	200 MB	Rígido	Utiliza o comando DIRQUOTA para conceder uma extensão de 50 MB automática uma única vez a usuários que tenham excedido o limite de cota
250 MB Extended Limit	250 MB	Rígido	Destinada a ser utilizada por aqueles cujo limite tenha sido estendido de 200 MB a 250 MB
Monitor 200 GB Volume Usage	200 GB	Flexível	Monitora o uso do volume e alerta quando o limite estiver próximo ou for excedido
Monitor 500 MB Share	500 MB	Flexível	Monitira o uso de compartilhamentos e alerta quando o limite estiver próximo ou for excedido

Gerenciamento de modelos de cotas de disco

Utiliza-se os modelos de cotas de disco para definir as propriedades de cotas, incluindo o limite, tipo de cota e limites de notificação. No File Server Resource Manager, pode-se visualizar os modelos de cotas de disco definidos atualmente expandindo o nó Quota Management e selecionando Quota Templates. A Tabela 12-7, mostrada anteriormente, fornece um resumo dos modelos de cotas de disco padrão. A Tabela 12-8 mostra as variáveis que podem ser utilizadas para mensagens e eventos gerados automaticamente.

TABELA 12-8 As principais variáveis disponíveis para mensagens de cotas de disco e registro em log de eventos

NOME DA VARIÁVEL	DESCRIÇÃO
[Admin Email]	Insere os endereços de email dos administradores definidos nas opções globais
[File Screen Path]	Insere o caminho local, como C:\Data
[File Screen Remote Path]	Insere o caminho remoto, como \\server\share
[File Screen System Path]	Insere o caminho canônico, como \\?\VolumeGUID
[Server Domain]	Insere o domínio do servidor no qual a notificação ocorreu
[Server]	Insere o servidor no qual a notificação ocorreu

NOME DA VARIÁVEL	DESCRIÇÃO
[Source File Owner]	Insere o nome de usuário do proprietário do arquivo/da pasta
[Source File Owner Email]	Insere o endereço de email do proprietário do arquivo/da pasta
[Source File Path]	Insere o caminho de origem do arquivo/da pasta

Pode-se modificar os modelos de cotas de disco existentes seguindo estas etapas:

1. No File Server Resource Manager, expanda o nó Quota Management e selecione Quota Templates.
2. Os modelos de cotas de disco definidos atualmente serão listados por nome, limite e tipo de cota.
3. Para modificar as propriedades dos modelos de cotas de disco, toque ou clique duas vezes no nome do modelo de cotas de disco. A caixa de diálogo Properties relacionada será aberta, como mostrado na Figura 12-21.

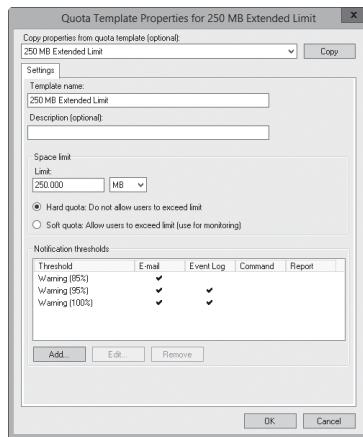


FIGURA 12-21 Utilize as propriedades de cotas de disco para configurar o limite, o tipo de cota e os limites de notificação.

3. Na guia Settings, pode-se definir o nome do modelo, o limite e o tipo de cota. Os limites de notificação atuais serão listados. Para modificar um limite existente, selecione-o e toque ou clique em Edit. Para definir um novo limite, toque ou clique em Add.
4. Quando tiver terminado de modificar o modelo de cotas, toque ou clique em OK para salvar as alterações.

Você pode criar um novo modelo de cotas de disco seguindo estas etapas:

1. No File Server Resource Manager, expanda o nó Quota Management e selecione Quota Templates.
2. No menu Action ou no painel Actions, toque ou clique em Create Quota Template. A caixa de diálogo Create Quota Template será exibida.
3. Na guia Settings, defina o nome do modelo, o limite e o tipo de cota. Você deve criar um limiar de limite primeiro e depois criar os limites de aviso adicionais conforme necessário. Na lista Limit, digite o valor limite e especifique se está configurando o limite em quilobytes, megabytes, gigabytes ou terabytes.
4. Toque ou clique em Add para adicionar os limites de aviso. Na caixa de diálogo Add Threshold, digite um valor em porcentagem sob Generate Notifications When Usage Reaches (%). Os limites de aviso são considerados qualquer porcentagem do limite que seja menos que 100%. O limiar de limite ocorre quando o limite alcançado é 100%.
5. Na guia E-Mail Message, pode-se configurar a notificação como se segue:
 - Para notificar um administrador quando o gatilho da cota de disco for disparado, marque a caixa de seleção Send E-Mail To The Following Administrators e digite os endereços de email a utilizar. Certifique-se de separar os endereços de email com um ponto e vírgula. Utilize o valor [Admin Email] para especificar o administrador padrão conforme configurado anteriormente nas opções globais.
 - Para notificar os usuários, marque a caixa de seleção Send E-Mail To The User Who Exceeded The Threshold.
 - Especifique o conteúdo da mensagem de notificação nas caixas de texto Subject e Message Body. A Tabela 12-8 lista as variáveis disponíveis e seus significados.
6. Na guia Event Log, pode-se configurar o log de eventos. Marque a caixa de seleção Send Warning To Event Log para habilitar o registro em log e especifique o texto da entrada de log na caixa de texto Log Entry. A Tabela 12-8 lista as variáveis disponíveis e seus significados.
7. Na guia Report, marque a caixa de seleção Generate Reports para habilitar a geração de relatórios de incidentes e selecione os tipos de relatórios a serem gerados. Os relatórios de incidentes são armazenados sob %SystemDrive%\StorageReports\Incident por padrão e também podem ser enviados para administradores designados. Utilize o valor [Admin Email] para especificar o administrador padrão conforme configurado anteriormente nas opções globais.
8. Repita as etapas de 5 a 7 para definir limites de notificação adicionais.
9. Toque ou clique em OK quando tiver terminado de criar o modelo.

Criação de cotas de disco do Resource Manager

Utiliza-se cotas de disco para designar caminhos de arquivos que tenham limites de uso específicos. No File Server Resource Manager, pode-se visualizar cotas de disco atuais expandindo o nó Quota Management e selecionando Quotas. Antes de definir as cotas de disco, você deve especificar grupos de triagem de arquivos e os modelos

de cotas de disco que irá utilizar, como abordado em “Gerenciamento de modelos de cotas de disco” anteriormente neste capítulo.

Depois de definir os grupos de arquivos e modelos de cotas de disco necessários, poderá criar cota de disco seguindo estas etapas:

1. No File Server Resource Manager, expanda o nó Quota Management e selecione Quotas.
2. Toque ou clique em Create Quota no menu Action ou no painel Actions.
3. Na caixa de diálogo Create Quota, defina o caminho do computador local para a cota tocando ou clicando em Browse e utilizando a caixa de diálogo Browse For Folder para selecionar o caminho, como C:\Data. Toque ou clique em OK.
4. Na lista Derive Properties From This Quota Template, escolha o modelo de cotas de disco que define as propriedades de cota que queira utilizar.
5. Toque ou clique em Create.

CAPÍTULO 13

Backup e recuperação de dados

- Como criar um plano de backup e recuperação **516**
- Backup de dados: fundamentos básicos **523**
- Realização de backups do servidor **530**
- Gerenciamento de políticas de recuperação de criptografia **548**
- Backup e restauração de dados criptografados e certificados **551**

Tendo em vista que os dados são a essência de uma empresa, a proteção deles é crucial. Para proteger os dados da sua organização, é preciso implementar um backup de dados e um plano de recuperação. O backup de arquivos protege contra a perda acidental de dados do usuário, corrupção do banco de dados, falhas de hardware e até mesmo desastres naturais. O seu trabalho como administrador é garantir que os backups sejam realizados e que sejam armazenados em um local seguro.

Como criar um plano de backup e recuperação

O backup de dados funciona como um seguro. A exclusão acidental de arquivos importantes acontece com frequência. Dados críticos da empresa podem ser corrompidos. Desastres naturais podem destruir o seu escritório. Com um plano sólido de backup e recuperação, você pode se recuperar de qualquer um desses acontecimentos. Sem um plano, você não teria como retomar o seu trabalho.

Elaboração de um plano de backup

A criação e implementação de um plano de backup e recuperação demanda bastante tempo. É preciso resolver quais dados precisam de backup e com que frequência o backup deve ser feito, entre outros aspectos. Para ajudá-lo na criação de um plano, refletiu sobre as seguintes questões:

- **O quanto importantes ou confidenciais são os dados no seu sistema?** Saber a importância dos dados é de grande valia para determinar o que deve ser incluso no backup, bem como quando e de que forma ele deve ser realizado. Para dados críticos, como é o caso de um banco de dados, deve-se ter conjuntos de backup redundantes que cubram vários períodos no backup. Para dados confidenciais, deve-se garantir que os dados de backup estejam fisicamente seguros ou criptografados. Para dados de menor importância, como arquivos de usuário diários, não é preciso um plano de backup tão elaborado. Basta fazer o backup regularmente e garantir que os dados possam ser recuperados com facilidade.
- **Os dados contêm que tipo de informações?** Alguns dados que não parecem importantes para você podem ser de grande importância para outra pessoa. O

tipo da informação contida nos dados pode ajudá-lo a determinar se o backup é necessário, bem como quando e como fazer backup desses dados.

- **Com que frequência os dados são alterados?** A frequência de alteração pode afetar a decisão sobre a frequência de backup dos dados. Dados que sejam alterados diariamente, por exemplo, devem ter backup executado diariamente.
- **Pode-se complementar os backups com cópias de sombra?** *Shadow copies* ou cópias de sombra são cópias point-in-time de documentos em pastas compartilhadas. Essas cópias point-in-time facilitam a recuperação de documentos porque você pode retornar a uma versão mais antiga caso o documento seja excluído ou substituído acidentalmente. As cópias de sombra devem ser usadas além dos backups padrão e não para substituí-los.
- **O quanto rapidamente é preciso recuperar os dados?** O tempo de recuperação é um fator importante em um plano de recuperação. Para sistemas críticos, pode ser necessário voltar a ficar online rapidamente. Para isso, o plano de backup pode precisar de alterações.
- **Você possui os equipamentos para realizar os backups?** É preciso ter hardware de backup para realizar backups. Para fazer os backups no tempo certo, podem ser necessários vários dispositivos de backup e vários conjuntos de mídia de backup. O hardware de backup inclui unidades de disco rígido, unidades de fita, unidades óticas e unidades de disco removível. Na maioria dos ambientes, as unidades de disco rígido tornaram-se as mídias de backup preferenciais.
- **Quem será o responsável pelo plano de backup e recuperação?** O ideal seria que alguém fosse o responsável principal para o plano de backup e recuperação da organização. Essa pessoa também poderia ser responsável por realizar o backup e a recuperação dos dados.
- **Qual é o melhor momento para agendar backups?** O agendamento de backups para quando o uso do sistema for o menor possível agilizará o processo de backup. Entretanto, não é sempre que se pode agendar backups fora do horário de pico, sendo preciso planejar cuidadosamente quando será feito o backup dos dados-chave do sistema.
- **É necessário armazenar backups fora do local?** O armazenamento de cópias de backup fora do local é essencial para a recuperação dos sistemas em caso de desastre natural. No seu local de armazenamento alternativo, inclua também cópias de software que precise ser instalado para reestabelecer sistemas operacionais.

MUNDO REAL O recovery time objective (RTO, objetivo de tempo de recuperação) e o recovery point objective (RPO, objetivo de ponto de recuperação) são fatores importantes a se considerar. O RTO representa o tempo de recuperação, que pode ser de duas horas para um servidor e de quatro horas para outro. O RPO representa a sua potencial perda de dados, que pode ser de um dia de trabalho para dados em um servidor e de dois dias para outro. Um ambiente de RTO alto é um ambiente em que se pode recuperar rapidamente a funcionalidade do servidor após uma interrupção. Um ambiente de RPO alto é um ambiente em que a recuperação de dados é tão atualizada quanto for possível.

A frequência do backup completo do servidor varia de acordo com a velocidade do seu sistema de backup e da quantidade de dados para o backup. A frequência com a qual se pode criar backups controla o RPO e o RTO disponíveis para você. Com backups noturnos, por exemplo, o seu RPO será de um dia de trabalho. Isso significa que qualquer interrupção no servidor

provavelmente resultará na perda dos dados de um dia inteiro de trabalho. Já o seu RTO, indicativo de quanto tempo levará a recuperação, irá variar de acordo com a quantidade de dados que precisam ser restaurados.

Os tipos básicos de backup

Existem diversas técnicas para fazer o backup de arquivos. As técnicas escolhidas dependem do tipo de dados que sofrerão backup e do quão conveniente você quer que seja o processo de recuperação, entre outros fatores.

Se você visualizar as propriedades de um arquivo ou pasta no File Explorer, verá um atributo chamado *archive*. Esse atributo é bastante usado para determinar se o backup de um arquivo ou pasta deve ser feito. Se o atributo estiver ativo, provavelmente o arquivo ou pasta precise de backup. Pode-se realizar os seguintes tipos básicos de backup:

- **Normal/full backups (Normal)** É feito o backup de todos os arquivos selecionados, independentemente da configuração do atributo *archive*. Quando é efetuado o backup de um arquivo, o atributo *archive* é desmarcado. Se o arquivo for modificado posteriormente, o atributo será configurado para indicar a necessidade de backup.
- **Copy backups (Cópia)** É feito o backup de todos os arquivos selecionados, independentemente da configuração do atributo *archive*. Ao contrário de um backup normal, o atributo *archive* não é alterado. Isso permite que você realize outros tipos de backup nos arquivos em um outro momento.
- **Differential backups (Diferencial)** Projetado para criar cópias de backup de arquivos que tenham sofrido alterações desde o último backup normal. A presença do atributo *archive* indica que o arquivo foi modificado e apenas arquivos com esse atributo configurado serão inclusos no backup. Entretanto, o atributo *archive* nos arquivos não é alterado. Isso permite que você realize outros tipos de backup nos arquivos em um outro momento.
- **Incremental backups (Incremental)** Projetado para criar backups de arquivos que foram modificados depois do backup normal ou incremental mais recente. A presença do atributo *archive* indica que o arquivo foi modificado e apenas arquivos com esse atributo configurado serão inclusos no backup. Quando é feito o backup de um arquivo, o atributo *archive* é desmarcado. Se o arquivo for modificado posteriormente, o atributo será configurado para indicar a necessidade de novo backup.
- **Daily backups (Diário)** Projetado para fazer backup de arquivos usando a data de modificação que consta no próprio arquivo. Se um arquivo foi modificado no mesmo dia que o backup, o arquivo será incluso no backup. Essa técnica não altera o atributo *archive* de arquivos.

Como parte das suas operações de backup, provavelmente você realizará backups completos semanalmente, complementando-os com backups diários, diferenciais ou incrementais. Também é desejável criar um conjunto de backup estendido para backups mensais ou trimestrais que incluem arquivos adicionais não selecionados para backup regularmente.

DICA Frequentemente acontecerá de passar semanas ou meses até que alguém perceba que está faltando um arquivo ou fonte de dados. Isso não significa que o arquivo não seja importante. Mesmo que alguns tipos de dados não sejam muito usados, ainda assim são necessários. Portanto, lembre-se de criar conjuntos de backup adicionais para períodos mensais, trimestrais ou ambos, garantindo que se possa recuperar dados antigos.

Backup diferencial e backup incremental

A diferença entre os backups diferencial e incremental é de extrema importância. Para entender essa distinção, analise a Tabela 13-1. Veja que em backups diferenciais é feito o backup de arquivos que foram modificados desde o último backup completo (isso significa que o tamanho do backup diferencial aumenta com o tempo).

Já em backups incrementais, é feito o backup apenas de arquivos que foram modificados depois do backup completo ou incremental mais recente (isso significa que o backup incremental é, normalmente, bem menor que um backup completo).

TABELA 13-1 Técnicas de backup incremental e diferencial

DIA DA SEMANA	BACKUP COMPLETO SEMANAL COM BACKUP DIFERENCIAL DIÁRIO	BACKUP COMPLETO SEMANAL COM BACKUP INCREMENTAL DIÁRIO
Domingo	É realizado um backup completo.	É realizado um backup completo.
Segunda-feira	Um backup diferencial contém todas as alterações feitas desde domingo.	Um backup incremental contém as alterações feitas desde domingo.
Terça-feira	Um backup diferencial contém todas as alterações feitas desde domingo.	Um backup incremental contém as alterações feitas desde segunda-feira.
Quarta-feira	Um backup diferencial contém todas as alterações feitas desde domingo.	Um backup incremental contém as alterações feitas desde terça-feira.
Quinta-feira	Um backup diferencial contém todas as alterações feitas desde domingo.	Um backup incremental contém as alterações feitas desde quarta-feira.
Sexta-feira	Um backup diferencial contém todas as alterações feitas desde domingo.	Um backup incremental contém as alterações feitas desde quinta-feira.
Sábado	Um backup diferencial contém todas as alterações feitas desde domingo.	Um backup incremental contém as alterações feitas desde sexta-feira.

Uma vez que você tenha determinado de quais dados será feito o backup e com que frequência, você deve selecionar os dispositivos e mídias de backup que darão suporte às suas escolhas. Isso será abordado na próxima seção.

Seleção de dispositivos e mídias de backup

Existem diversas ferramentas disponíveis para o backup de dados: algumas são rápidas e caras e outras são lentas porém muito confiáveis. A solução de backup adequada para a sua organização depende de vários fatores, como:

- **Capacidade** A quantidade de dados que precisa de backup rotineiramente. Será que o hardware de backup suporta a carga necessária, considerando-se as limitações de tempo e de recursos?
- **Confiabilidade** A confiabilidade do hardware e da mídia de backup. Será que você pode sacrificar a confiabilidade para atender às necessidades de orçamento e tempo?
- **Extensibilidade** A extensibilidade da solução de backup. Será que essa solução atenderá as necessidades da sua organização, conforme ela vá crescendo?

- **Velocidade** A velocidade com a qual se pode fazer o backup dos dados e recuperá-los. Será que você pode sacrificar a velocidade em relação ao tempo de inatividade do servidor ou do serviço para reduzir custos?
- **Custo** O custo da solução de backup. Será que cabe no seu orçamento?

Soluções comuns de backup

Capacidade, confiabilidade, extensibilidade, velocidade e custo são os aspectos que orientam o seu plano de backup. Se você compreender como cada um afeta a sua organização, estará no caminho certo pra selecionar a solução de backup adequada. Algumas das soluções de backup mais utilizadas são:

- **Unidades de fita** As unidades de fita são os dispositivos de backup mais comuns. Elas utilizam cartuchos de fita magnética para armazenar dados. As fitas magnéticas são relativamente baratas mas não são muito confiáveis, já que podem sofrer ruptura ou estiramento. Elas também podem ter perda de informações depois de um tempo. A capacidade média dos cartuchos de fita varia entre 24 gigabytes (GB) e 160 GB. Em relação a outras soluções de backup, as unidades de fita são lentas. Ainda assim, o preço baixo é um atrativo.
- **Unidades de fita de áudio digital (DAT)** As unidades DAT estão substituindo rapidamente as unidades de fita padrão como os dispositivos de backup preferenciais. Existem muitos formatos DAT disponíveis. Os formatos mais comuns são Digital Linear Tape (DLT, fita digital linear) e Super DLT (SDLT). Com SDLT 320 e 600, as fitas têm uma capacidade de 160 GB ou 300 GB não compactado (320 GB ou 600 GB compactado). Para organizações de grande porte, confira as tecnologias de fita do tipo Linear Tape Open (LTO). As fitas LTO-3, LTO-4 e LTO-5 possuem uma capacidade não compactada de 400 GB, 800 GB e 1500 GB respectivamente (a capacidade compactada é o dobro disso).
- **Sistemas de fita autoloader** Os sistemas de fita autoloader (carregador automático) utilizam magazine de fitas para criar volumes de backup estendidos capazes de atender às necessidades de alta capacidade de uma empresa. Com um sistema autoloader, as fitas em uma magazine são trocadas automaticamente durante o processo de backup ou de recuperação conforme for necessário. A maioria dos sistemas de fita autoloader utilizam fitas DAT em formato DLT, SDLT ou LTO. As unidades DLT típicas podem gravar até 45 GB por hora, sendo que essa velocidade pode ser aumentada com a aquisição de um sistema de biblioteca de fitas com várias unidades. Dessa forma, pode-se gravar em várias fitas simultaneamente. Em contrapartida, a maioria das unidades SDLT e LTO gravam mais de 100 GB por hora. Se forem utilizadas várias unidades em um sistema, pode-se gravar centenas de GB por hora. Uma solução para uma empresa hipotética utilizaria 16 unidades LTO para atingir taxas de transferência de dados de mais de 13,8 terabytes (TB) por hora e pode armazenar até 500 fitas, chegando a uma capacidade de armazenamento total de mais de 800 TB.
- **Unidades de disco** O uso de unidades de disco é uma das maneiras mais rápidas de fazer backup e restaurar arquivos. Com unidades de disco pode-se realizar em minutos algo que levaria horas com uma unidade de fita. Quando as necessidades de trabalho exigem uma recuperação rápida, nenhuma outra solução supera a unidade de disco. A desvantagem das unidades de disco é o custo relativamente alto quando comparado ao de sistemas de biblioteca de fitas.

■ **Sistemas de backup baseados em disco** Os sistemas de backup baseados em disco oferecem soluções de backup e restauração completas, usando grandes matrizes para atingir um alto desempenho. Para atingir uma alta confiabilidade, utiliza-se uma matriz redundante de discos independentes (RAID) para agregar redundância e tolerância a falhas. Os sistemas de backup baseados em discos típicos utilizam a tecnologia de biblioteca virtual para que o Microsoft Windows os veja como sistemas de biblioteca de fitas autoloader. Isso torna mais fácil trabalhar com esses sistemas. Uma solução de uma empresa hipotética possuiria 128 unidades virtuais e 16 bibliotecas virtuais por nó para um armazenamento total de até 7,5 TB por nó. Em sua dimensão total essa solução pode armazenar até 640 TB e transferir até 17,2 TB por hora.

OBSERVAÇÃO Os discos e os sistemas de backup baseados em discos podem ser usados entre os servidores dos quais está sendo feito o backup e um autoloader da empresa. Os servidores são salvos primeiro em disco (o que é muito rápido comparado às fitas) e depois em um autoloader da empresa. Os dados em fitas também facilitam o giro dos conjuntos de backup para armazenamento em outros locais. Dito isso, os backups de fita vêm sendo cada vez mais substituídos por backups de disco. Se você fizer backup para matrizes de disco, replique os dados para uma matriz secundária em um data center alternativo para manter os dados em outro local.

Antes de poder utilizar um dispositivo de backup, é preciso fazer a sua instalação. Ao instalar dispositivos de backup que não sejam fita padrão ou unidades DAT, é preciso informar o sistema operacional sobre a placa e os drivers da controladora que são utilizados pelo dispositivo de backup.

Compra e uso de mídia de backup

A seleção de um dispositivo de backup é uma etapa importante para a implementação de um plano de backup e recuperação. Também é preciso adquirir fitas, discos ou ambos para que seja possível implementar o seu plano. O número de fitas e discos necessários depende da quantidade de dados para backup, com que frequência o backup é feito e por quanto tempo é preciso guardar conjuntos de dados adicionais.

A maneira tradicional de utilizar fitas de backup é configurando um agendamento de rotação onde se faz o giro entre dois ou mais conjuntos de fitas. A ideia é aumentar a vida útil da fita através da redução do uso da fita e, ao mesmo tempo, reduzir o número de fitas necessárias para garantir que se tenham dados antigos à mão quando for preciso.

Um dos agendamentos de rotação de fitas mais comuns é a rotação de 10 fitas. Com esse agendamento, utilizam-se 10 fitas divididas em dois conjuntos de cinco (uma para cada dia útil). O primeiro conjunto de fitas é usado em uma semana e o segundo será usado na semana seguinte. Em sextas-feiras estão agendados backups completos. De segunda a quinta-feira estão agendados backups incrementais. Se você adicionar um terceiro conjunto de fitas, pode fazer o giro de um dos conjuntos de fitas para um outro local de armazenamento semanalmente.

O método de rotação de 10 fitas foi projetado pensando naqueles que trabalham em horário comercial. Se você trabalha em um ambiente 24 horas, certamente precisará de fitas adicionais para sábados e domingos. Nesse caso, utilize a rotação de 14 fitas com dois conjuntos de sete fitas. Agende backups completos aos domingos. Agende backups incrementais de segunda-feira a sábado.

Com as unidades de disco tornando-se mais acessíveis, muitas organizações têm usado backup em disco em vez de backup em fita. Para os discos, pode-se usar um

agendamento de rotação semelhante ao usado com fitas. Porém, será preciso alterar a forma de rotação dos discos para acomodar a quantidade de dados inclusos no backup. O ponto mais importante é lembrar-se de fazer o giro dos discos para armazenamento fora do local periodicamente.

Seleção de um utilitário de backup

Existem várias soluções de backup e recuperação disponíveis para uso com o Windows Server 2012. Ao selecionar um utilitário de backup, é preciso lembrar-se dos tipos de backup que deseja fazer e dos tipos de dados dos quais serão feitos backups. O Windows Server 2012 inclui quatro recursos instaláveis de backup e recuperação:

- **Windows Server Backup** Um utilitário de backup e recuperação básico e fácil de usar. Ao instalar esse recurso em um servidor, a ferramenta é aberta usando o menu Tools no Server Manager.
- **Backup Command-Line Tools** Um conjunto de comandos de backup e recuperação acessíveis com a ferramenta de linha de comando Wbadmin. Para executar e usar o Wbadmin, utilize um prompt de comando elevado com privilégio de administrador. Insira **wbadmin/?** para uma lista completa dos comandos com suporte. Também estão disponíveis cmdlets do Windows PowerShell para o gerenciamento de backups.
- **Microsoft Online Backup Service** Esse serviço é um complemento que pode ser baixado e instalado de dentro do Windows Server Backup para agendar backups de um servidor para um serviço baseado na nuvem via Internet na Microsoft. Os backups online são possíveis apenas para volumes NTFS fixos que não utilizem BitLocker Drive Encryption (Criptografia de Unidade de Disco BitLocker). Os volumes não podem ser compartilhamentos e devem estar configurados para acesso de leitura/gravação.
- **Repair Your Computer** Pode-se restaurar um servidor com as opções de reparo, caso você não consiga acessar as opções de recuperação fornecidas pelo fabricante do servidor.

OBSERVAÇÃO O Windows Server Backup e as ferramentas de linha de comando de backup estão disponíveis apenas para o gerenciamento de backups quando você adiciona o recurso Windows Server Backup a um servidor. Se você adicionar ferramentas de administração do servidor a um servidor, pode ser que consiga abrir o Windows Server Backup. Entretanto, não será possível usar o Windows Server Backup para configurar e gerenciar backups.

O Windows Server Backup é o recurso que você mais utilizará. Ele pode ser usado para realizar backups completos ou backups de cópia mas não pode ser usado para realizar backups diferenciais. O Windows Server Backup usa o Volume Shadow Copy Service (VSS, Serviço de Cópias de Sombra de Volume) para criar backups rápidos em nível de bloco do sistema operacional, de arquivos e pastas e de volumes de disco. Uma vez que você tenha criado o primeiro backup completo, o Windows Server Backup pode ser configurado para realizar automaticamente backups completos ou incrementais regularmente.

Ao usar o Windows Server Backup precisa-se de mídia separada dedicada ao armazenamento de arquivos de backups agendados. O backup pode ser feito para discos internos e externos, DVDs e pastas compartilhadas. Embora se possa recuperar volumes completos de backups em DVDs, não se pode recuperar arquivos individuais, pastas ou dados de aplicativos de backups em DVDs.

OBSERVAÇÃO Não é possível fazer backup em fitas com o Windows Server Backup. Se desejar fazer backup em fitas, você precisará de um utilitário de backup de terceiros.

O Windows Server Backup pode ser usado para recuperar pastas e arquivos individuais com facilidade. Em vez de restaurar manualmente os arquivos de vários backups se os arquivos estiverem armazenados em backups incrementais, você pode recuperar pastas e arquivos ao selecionar a data em que foi feito o backup da versão do item ou dos itens que você quer restaurar. O Windows Server Backup também trabalha com as ferramentas do Windows Recovery, facilitando a recuperação do sistema operacional. Pode-se fazer a recuperação para o mesmo servidor ou para um novo servidor que não tenha sistema operacional. Como o Windows Server Backup utiliza o VSS, é fácil fazer backup de dados de aplicativos compatíveis, como o Microsoft SQL Server e o Windows SharePoint Services.

O Windows Server Backup inclui ainda o gerenciamento de disco automático. Para executar backups de vários discos usando rotação, basta adicionar cada disco como um local de backup agendado. Após configurar um disco como um local de backup agendado, o Windows Server Backup gerencia automaticamente o armazenamento no disco e você não precisa mais se preocupar se o disco está ficando sem espaço. O Windows Server Backup reutiliza o espaço de backups antigos quando cria novos backups. Para garantir que você planeje necessidades de armazenamento adicionais, o Windows Server Backup exibe os backups disponíveis e as informações atuais de uso do disco.

Backup de dados: fundamentos básicos

O Windows Server 2012 oferece o Windows Server Backup para a criação de backups. O Windows Server Backup é usado para arquivar pastas e arquivos, restaurar arquivos e pastas arquivados, criar instantâneos (snapshots) do estado do sistema (system state) para backup e restauração e agendar backups automatizados.

Instalação dos utilitários de backup e recuperação do Windows

As ferramentas de backup e recuperação do Windows Server estão disponíveis em todas as edições do Windows Server 2012. Porém, não é possível instalar os componentes gráficos desses utilitários em instalações core do Windows Server 2012. Em servidores com instalações core é preciso usar a linha de comando ou gerenciar os backups através de uma sessão remota em outro computador.

Para instalar as ferramentas de backup e recuperação do Windows, siga estas etapas:

1. No Server Manager, selecione Add Roles And Features no menu Manage. Isso iniciará o Add Roles And Features Wizard (Assistente de Adição de Funções e Recursos). Se o Assistente exibir a página Before You Begin, leia o texto introdutório e depois toque ou clique em Next.
2. Na página Installation Type está selecionada por padrão Role-Based Or Feature-Based Installation. Toque ou clique em Next.
3. Na página Server Selection pode-se escolher instalar funções e recursos em servidores em execução ou em discos rígidos virtuais. Selecione um servidor do pool de servidores ou então selecione um servidor do pool de servidores no qual monitorar um disco rígido virtual (VHD). Se estiver adicionando funções e recursos a

um VHD, toque ou clique em Browse e depois use a caixa de diálogo Browse For Virtual Hard Disks para localizar o VHD. Quando estiver pronto para prosseguir, toque ou clique em Next duas vezes.

4. Na página Select Features, selecione Windows Server Backup. Toque ou clique em Next.
5. Toque ou clique em Install. Quando o assistente terminar a instalação dos recursos selecionados, toque ou clique em Close. De agora em diante, o Windows Server Backup e as ferramentas de linha de comando relacionadas estarão disponíveis para o gerenciamento de backups.

MUNDO REAL Ao utilizar o Windows Server Backup para o Microsoft Exchange Server 2010, só é possível usar backups completos (normal). Também não há suporte para o uso das ferramentas de linha de comando do Windows Server Backup com o Exchange Server 2010. Para mais informações sobre o backup do Exchange Server 2010, consulte o Capítulo 13 “Backing Up and Restoring Exchange Server 2010,” do livro *Microsoft Exchange Server 2010 Administrator’s Pocket Consultant* (Microsoft Press, 2009).

Como iniciar os trabalhos com o Windows Server Backup

Para iniciar o Windows Server Backup, selecione a opção referente no menu Tools do Server Manager. Quando o Windows Server Backup for iniciado, você verá uma mensagem sobre o backup online. Se quiser usar backups online, é necessário inscrever-se no serviço, registrar o servidor e baixar o agente Microsoft Online Backup Service. Com o nó Windows Server Backup selecionado, clique no botão Continue para iniciar o processo.

No Windows Server Backup, mostrado na Figura 13-1, selecione o nó Local Backup para trabalhar com backups. Na primeira vez que você usar o Windows Server Backup você verá um aviso de que nenhum backup foi configurado para o computador. Esse aviso é eliminado quando você criar um backup usando o recurso Backup Once, que se encontra no menu Action, ou agendar backups para serem executados automaticamente usando o recurso Backup Schedule.

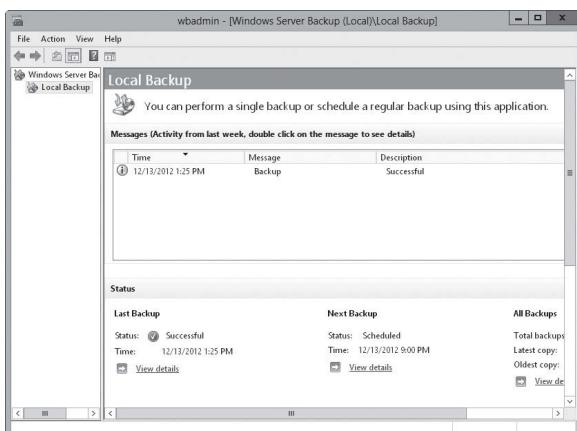


FIGURA 13-1 O Windows Server Backup oferece uma interface amigável para backup e restauração.

Para realizar operações de backup e recuperação é preciso ter determinadas permissões e direitos de usuário. Os membros dos grupos Administrators e Backup Operators têm autoridade total para fazer backup e restaurar qualquer tipo de arquivo, independentemente de quem é o proprietário do arquivo e das permissões configuradas. Os proprietários de arquivos e aqueles que receberam controle sobre arquivos também podem fazer backup desses arquivos, mas só daqueles dos quais são proprietários ou tenham recebido permissões dos tipos Read (Ler), Read & Execute (Ler e Executar), Modify (Modificar) ou Full Control (Controle Total).

OBSERVAÇÃO Lembre-se ainda de que contas locais só podem trabalhar com sistemas locais, já as contas de domínio possuem privilégios para todo o domínio. Sendo assim, um membro do grupo local Administrators só pode trabalhar com arquivos no sistema local, mas um membro do grupo Domain Admins pode trabalhar com todos os arquivos no domínio.

O Windows Server Backup oferece extensões para trabalhar com os seguintes tipos especiais de dados:

- **System state data (dados do estado do sistema)** Inclui arquivos de sistema essenciais necessários à recuperação do sistema local. Todos os computadores possuem dados do estado do sistema que devem sofrer backup, além de outros arquivos, para ser possível restaurar um sistema operacional completo.
- **Application data (dados de aplicativos)** Inclui arquivos de dados de aplicativos. É preciso fazer backup de dados de aplicativos se você quiser ter a possibilidade de recuperar aplicativos completamente. O Windows Server Backup cria backups em nível de bloco para dados de aplicativos usando o VSS.

Ele permite que você realize backup completo, de cópia e incremental. Ainda que se possa agendar um backup completo ou incremental para que seja realizado uma ou mais vezes ao dia, não é possível usar esse recurso para criar agendamentos de execuções separados para realizar tanto o backup completo quanto o incremental. Além disso, não é possível selecionar o dia ou os dias da semana quando são realizados os backups. Isso acontece porque cada servidor possui um único agendamento mestre configurado para execução uma ou mais vezes ao dia. Se os seus servidores possuem um único agendamento mestre, você pode contornar essa limitação. Configure o Windows Server Backup para realizar backups incrementais diários e depois crie uma tarefa agendada através do Task Scheduler, que utiliza o Wbadmin para criar um backup completo no dia da semana ou no dia do mês desejado.

Com o Windows Server Backup o primeiro backup de um servidor é sempre um backup completo. Isso ocorre porque o processo de backup completo limpa os bits archive nos arquivos para que o Windows Server Backup possa controlar quais arquivos serão atualizados depois. Se o Windows Server Backup realizará backups completos ou incrementais dali em diante dependerá das configurações de desempenho padrão que você configurar. Para definir as configurações de desempenho padrão, siga estas etapas:

1. Inicie o Windows Server Backup. No painel Actions ou no menu Action toque ou clique em Configure Performance Settings. A caixa de diálogo Optimize Backup Performance, mostrada na Figura 13-2, será exibida.
2. Execute um dos seguintes procedimentos e toque ou clique em OK:
 - Selecione Normal Backup Performance para realizar backups completos de todas as unidades anexadas.

- Selecione Faster Backup Performance para realizar backups incrementais de todas as unidades anexadas.
- Selecione Custom (Personalizado). Na lista de opções que aparece, escolha entre realizar backups completos ou incrementais para unidades anexadas individualmente.

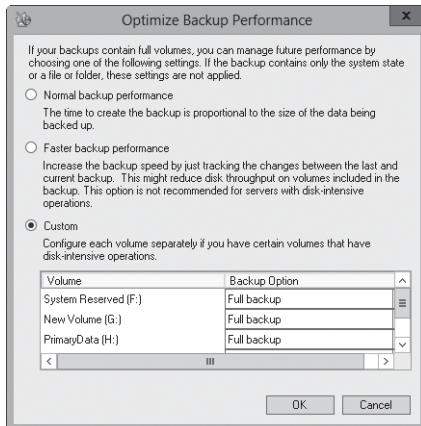


FIGURA 13-2 Em Optimize Backup Performance, defina as configurações padrão de backup.

3. Uma vez definidas as configurações de desempenho padrão, você pode iniciar um backup completo ou um backup de cópia. Para isso, toque ou clique em Backup Once no menu Action ou no painel Actions. Para configurar um agendamento de backup, toque ou clique em Backup Schedule no menu Action ou no painel Actions.

Como iniciar o trabalho com o utilitário de backup de linha de comando

O Wbadmin é a linha de comando equivalente para o Windows Server Backup. O Wbadmin é utilizado para gerenciar todos os aspectos da configuração do backup que seriam gerenciados com o Windows Server Backup. Isso quer dizer que você pode usar qualquer uma das duas ferramentas para gerenciar o backup e a recuperação.

Após a instalação do recurso Backup Command-Line Tools, como foi discutido anteriormente neste capítulo, pode-se usar o Wbadmin no gerenciamento de backup e recuperação. O Wbadmin se encontra no diretório %SystemRoot%\System32\. Essa faz parte do caminho de comando (command path) por padrão e, portanto, não é necessário adicioná-lo. Para executar o Wbadmin, siga estas etapas:

1. Abra um prompt de comando elevado com privilégio de administrador. Uma maneira de fazê-lo é digitando **cmd** na caixa Apps Search. Pressione e mantenha pressionado ou clique com o botão direito do mouse em Command Prompt na lista Apps e depois toque ou clique em Run As Administrator.

2. Na janela Command Prompt, insira o comando necessário ou execute um script que invoque o Wbadmin.

O Wbadmin possui diversos comandos associados, que estão resumidos na Tabela 13-2.

TABELA 13-2 Comandos de gerenciamento do Wbadmin

COMANDO	DESCRIÇÃO
DELETE SYSTEMSTATEBACKUP	Exclui o backup ou os backups do estado do sistema de um determinado local.
DISABLE BACKUP	Desabilita backups diários agendados para que deixem de ser executados.
ENABLE BACKUP	Habilita ou modifica um backup diário agendado.
GET DISKS	Lista os discos que estão online no momento para o computador local. Os discos são listados por nome do fabricante, tipo, número de disco, GUID, espaço total, espaço usado e volumes associados.
GET ITEMS	Lista os itens contidos em um determinado backup.
GET STATUS	Relata o status do job de backup ou de recuperação sendo executado no momento.
GET VERSIONS	Lista os detalhes sobre os backups disponíveis armazenados em um determinado local, incluindo o horário de backup e o destino de backup.
START BACKUP	Inicia um backup único usando os parâmetros especificados. Se houverem backups agendados habilitados e nenhum parâmetro <i>for</i> passado, o backup utiliza as configurações para backups agendados.
START RECOVERY	Inicia uma recuperação de volumes, aplicativos ou arquivos usando os parâmetros especificados.
START SYSTEMSTATEBACKUP	Inicia um backup de estado do sistema usando as opções especificadas.
START SYSTEMSTATERECOVERY	Inicia uma recuperação de estado do sistema usando os parâmetros especificados.
STOP JOB	Interrompe o job de backup ou de recuperação sendo executado no momento. Os trabalhos interrompidos não podem ser reiniciados do ponto onde foram interrompidos.

Se estiver trabalhando com o Wbadmin, obtenha ajuda em comandos disponíveis:

- Para visualizar uma lista de comandos de gerenciamento, digite **wbadmin /?** no prompt de comando.
- Para visualizar a sintaxe de um determinado comando de gerenciamento, digite **wbadmin *Command* /?**, onde *Command* é o nome do comando de gerenciamento que você quer analisar, como **wbadmin stop job /?**.

Ao usar o Wbadmin você verá que praticamente todos os comandos aceitam parâmetros e valores de parâmetros específicos que qualificam com o que você quer trabalhar. Para entender melhor como isso funciona, considere o seguinte exemplo de sintaxe:

```
wbadmin get versions [-backupTarget:{VolumeName | NetworkSharePath}]  
[-machine:BackupMachineName]
```

Os colchetes indicam que *-backupTarget* e *-machine* são opcionais. Assim, para obter informações sobre backups recuperáveis no computador local, poderia-se digitar o seguinte:

```
wbadmin get versions
```

Já para obter informações sobre backups recuperáveis armazenados na unidade F, poderia-se digitar o seguinte:

```
wbadmin get versions -backupTarget:f:
```

Ou para obter informações sobre backups recuperáveis armazenados na unidade F no Server96, poderia-se digitar o seguinte:

```
wbadmin get versions -backupTarget:f: -machine:server96
```

Muitos comandos Wbadmin utilizam os parâmetros *-backupTarget* e *-machine*. O destino do backup é o local de armazenamento onde você deseja trabalhar e pode ser expresso com um nome de volume local, como por exemplo F:, ou como um caminho de compartilhamento de rede, como \\FileServer32\backups\Server85. O parâmetro *-machine* identifica o computador no qual você quer trabalhar em operações de backup e recuperação.

Como trabalhar com os comandos do Wbadmin

Os comandos do Wbadmin são usados para gerenciar a configuração de backup dos servidores. Esses comandos trabalham com um conjunto específico de parâmetros. As seções a seguir oferecem uma visão geral sobre os comandos disponíveis e as sintaxes mais utilizadas.

Como usar comandos para fins gerais

Para a obtenção de informações sobre backups e sobre o sistema em que se está trabalhando, são oferecidos os seguintes comandos para fins gerais:

- **GET DISKS** Lista os discos que estão online no momento para o computador local. Os discos são listados por nome do fabricante, tipo, número de disco, GUID, espaço total, espaço usado e volumes associados.

```
wbadmin get disks
```

- **GET ITEMS** Lista os itens contidos em um determinado backup.

```
wbadmin get items -version:VersionIdentifier  
[-backupTarget:{VolumeName | NetworkSharepath}]  
[-machine:BackupMachineName]
```

- **GET STATUS** Relata o status do job de backup ou de recuperação sendo executado no momento.

```
wbadmin get status
```

- **GET VERSIONS** Lista os detalhes sobre os backups disponíveis armazenados em um determinado local, incluindo o horário de backup e o destino do backup.

```
wbadmin get versions [-backupTarget:{VolumeName | NetworkSharepath}] [-machine:BackupMachineName]
```

Como utilizar comandos de gerenciamento de backup

Para gerenciar backups e suas configurações, utilize os comandos e sintaxes de linha de comando a seguir:

- **DELETE SYSTEMSTATEBACKUP** Exclui o backup ou os backups do estado do sistema de um determinado local.

```
wbadmin delete systemstateBackup [-backupTarget:{VolumeName}] [-machine:BackupMachineName] [-keepVersions:NumberOfBackupsToKeep | -version:VersionIdentifier | -deleteOldest] [-quiet]
```

- **DISABLE BACKUP** Desabilita backups diários agendados para que deixem de ser executados.

```
wbadmin disable backup [-quiet]
```

- **ENABLE BACKUP** Habilita ou modifica um backup diário agendado.

```
wbadmin enable backup [-addTarget:{BackupTargetDisk}] [-removeTarget:{BackupTargetDisk}] [-schedule:TimeToRunBackup] [-include:VolumesToInclude] [-allCritical] [-quiet]
```

- **START BACKUP** Inicia um backup único usando os parâmetros especificados. Se houverem backups agendados habilitados e nenhum parâmetro for passado, o backup utiliza as configurações para backups agendados.

```
wbadmin start backup [-backupTarget:{TargetVolume | TargetNetworkShare}] [-include:VolumesToInclude] [-allCritical] [-noVerify] [-user:username] [-password:password] [-inheritAc1:InheritAc1] [-vssFull] [-quiet]
```

- **STOP JOB** Interrompe o job de backup ou de recuperação sendo executado no momento. Os trabalhos interrompidos não podem ser reiniciados do ponto onde foram cancelados.

```
wbadmin stop job [-quiet]
```

Como utilizar comandos de gerenciamento de recuperação

Para recuperar computadores e dados, utilize os comandos e sintaxes de linha de comando a seguir:

- **START RECOVERY** Inicia uma recuperação de volumes, aplicativos ou arquivos usando os parâmetros especificados.

```
wbadmin start recovery -version:VersionIdentifier
  -items:{VolumesToRecover | AppsToRecover | FilesOrFoldersToRecover}
  -itemType:{volume | app | file}
  [-backupTarget:{VolumeHostingBackup | NetworkShareHostingBackup}]
  [-machine:BackupMachineName]
  [-recoveryTarget:TargetVolumeForRecovery | TargetPathForRecovery]
  [-recursive]
  [-overwrite:{Overwrite | CreateCopy | skip}]
  [-notRestoreAcl]
  [-skipBadClusterCheck]
  [-noRollForward]
  [-quiet]
```

- **START SYSTEMSTATEBACKUP** Inicia um backup de estado do sistema usando as opções especificadas.

```
wbadmin start systemstateBackup -backupTarget:{VolumeName}
  [-quiet]
```

- **START SYSTEMSTATERECOVERY** Inicia uma recuperação de estado do sistema usando os parâmetros especificados.

```
wbadmin start systemstateRecovery -version:VersionIdentifier
  -showSummary
  [-backupTarget:{VolumeName | NetworkSharePath}]
  [-machine:BackupMachineName]
  [-recoveryTarget:TargetPathForRecovery]
  [-authSysvol]
  [-quiet]
```

Realização de backups do servidor

Como parte do planejamento para cada servidor do qual se quer fazer backup, você deve considerar quais volumes serão inclusos no backup e se os backups incluirão dados de recuperação do estado do sistema, dados de aplicativos ou ambos. Ainda que seja possível fazer backup manual para volumes compartilhados e mídias de DVD, é necessário um disco rígido separado dedicado à execução de backups agendados. Uma vez que você tenha configurado um disco para backups agendados, os utilitários de backup gerenciam o uso do disco e reutilizam o espaço de backups antigos ao

criarem novos backups automaticamente. Com os backups agendados, é preciso conferir periodicamente se os backups estão sendo realizados da maneira esperada e se o agendamento do backup atende às necessidades atuais.

Ao criar e agendar backups é preciso especificar os volumes a serem inclusos, o que afeta as formas com que se pode recuperar servidores e dados. Você tem as seguintes opções:

- **Full server (all volumes with application data)** Caso queira recuperar totalmente um servidor além de recuperar o estado do sistema e os dados de aplicativos, faça o backup de todos os volumes com dados de aplicativos. Como você optou pelo backup de todos os arquivos, estado do sistema e dados de aplicativos, será possível restaurar totalmente o servidor usando apenas as ferramentas de backup do Windows.
- **Full server (all volumes without application data)** Caso queira restaurar um servidor e os aplicativos separadamente, faça o backup de todos os volumes sem dados de aplicativos. Com essa técnica, será feito o backup do servidor usando as ferramentas de backup do Windows sem incluir os locais onde aplicativos e dados de aplicativos estão armazenados. Depois você pode fazer o backup dos aplicativos e dados relacionados usando ferramentas de terceiros ou ferramentas internas dos aplicativos. Pode-se recuperar totalmente um servidor com os utilitários de backup do Windows e, em um segundo momento, usar um utilitário de terceiros para restaurar backups de aplicativos e dados de aplicativos.
- **Critical volumes/bare metal recovery (recuperação bare-metal)** Faça o backup somente de volumes críticos caso queira recuperar apenas o sistema operacional.
- **Noncritical volumes** Faça o backup somente de volumes individuais caso queira recuperar apenas arquivos, aplicativos ou dados desses volumes.

Como parte do processo de backup, é preciso especificar um local de armazenamento para os backups. Ao escolher os locais de armazenamento, lembre-se do seguinte:

- Quando você utiliza um disco rígido interno para armazenar os backups, fica limitado em relação às possibilidades de recuperar o sistema. Você pode recuperar os dados de um volume mas não pode recompilar toda a estrutura do disco.
- Quando você utiliza um disco rígido externo para armazenar os backups, o disco será dedicado ao armazenamento de backups e não ficará visível no File Explorer. A escolha dessa opção formatará o disco ou discos selecionados, removendo qualquer dado existente.
- Quando você utiliza uma pasta compartilhada para armazenar os backups, o backup será substituído cada vez que um novo for criado. Não escolha essa opção caso queria armazenar vários backups para cada servidor.
- Quando você utiliza mídias removíveis ou DVDs para armazenar os backups, só é possível recuperar volumes inteiros, e não aplicativos ou arquivos individuais. A mídia utilizada deve ter ao menos 1 GB.

As seções a seguir apresentam técnicas para a realização de backups. Os procedimentos utilizados para fazer backup de servidores no Windows Server Backup e no Wbadmin são similares.

Configuração de backups agendados

Para agendar backups automatizados com o Windows Server Backup, siga estas etapas:

1. No Windows Server Backup, toque ou clique em Backup Schedule no menu Action ou no painel Actions. Isso iniciará o Backup Schedule Wizard (Assistente de Agendamento de Backup). Toque ou clique em Next.
2. Na página Select Backup Configuration observe o tamanho do backup listado sob a opção Full Server, como mostra a Figura 13-3. Esse é o espaço de armazenamento necessário para fazer backup dos dados do servidor, aplicativos e estado do sistema. Para fazer backup de todos os volumes no servidor, selecione a opção Full Server e toque ou clique em Next. Para fazer backup de volumes selecionados no servidor, toque ou clique em Custom e depois em Next.

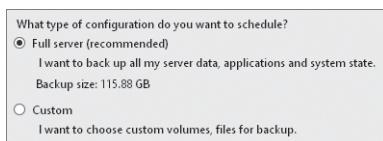


FIGURA 13-3 Observe o tamanho do backup.

OBSERVAÇÃO Os volumes que contêm arquivos ou aplicativos do sistema operacional são inclusos no backup por padrão e não podem ser excluídos. Infelizmente, isso significa que em um servidor com o Windows Server 2012 instalado na unidade D também é preciso fazer backup de toda a unidade C, que nesse caso inclui o gerenciador de inicialização e outros arquivos de inicialização.

3. Se você selecionou Custom, a página Select Items For Backup será exibida. Toque ou clique em Add Items. Como mostra a Figura 13-4, pode-se marcar as caixas de seleção para os volumes que quiser incluir no backup e desmarcar as caixas de seleção para os que devem ser deixados de fora. Selecione a opção Bare Metal Recovery se quiser recuperar completamente o sistema operacional. Toque ou clique em OK e depois em Next.

DICA Depois de selecionar os itens, é desejável tocar ou clicar em Advanced Settings antes de prosseguir. Use as opções da guia Exclusions para identificar locais e tipos de arquivo que não devem fazer parte do backup. Você também pode usar as opções na guia VSS Settings para especificar se você deseja criar um backup completo ou um backup de cópia.

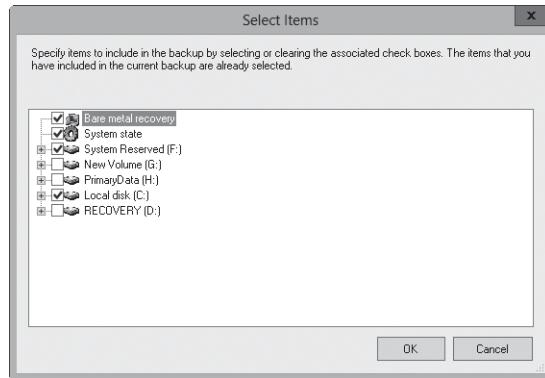


FIGURA 13-4 Selecione os itens a serem inclusos no backup.

4. Na página Specify Backup Time, mostrada na Figura 13-5, especifique com que frequência e quando você quer realizar backups. Para realizar backups diários em um determinado horário, selecione Once A Day e depois escolha a hora em que deve ter início o backup diário. Para realizar backups várias vezes ao dia, selecione More Than Once A Day. Depois, toque ou clique em uma hora de início sob Available Time. Toque ou clique em Add para mover a hora para Scheduled Time. Repita esse processo para cada hora de início que deseja adicionar. Toque ou clique em Next quando estiver pronto para prosseguir.

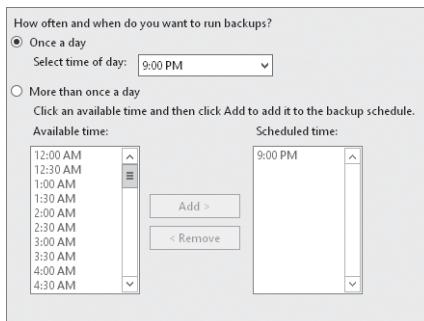


FIGURA 13-5 Selecione a hora de início do backup.

5. Na página Specify Destination Type são oferecidas as seguintes opções:

- **Back Up To A Hard Disk That Is Dedicated For Backups** Permite que você especifique um disco rígido dedicado a backups. Ainda que seja possível usar vários discos para backups, qualquer disco que for selecionado será formatado e depois dedicado apenas a backups. Essa opção é recomendável porque resulta no melhor desempenho. Se você escolheu essa opção, toque ou clique em Next, selecione o disco ou os discos a serem usados e toque ou clique em Next novamente.
 - **Back Up To A Volume** Permite a gravação de backups em volumes individuais em um disco rígido. Como um volume qualquer que seja selecionado não é dedicado a backups, ele pode ser usado para outros fins. Entretanto, o desempenho dos volumes selecionados é reduzido durante a gravação de backups. Se você escolheu essa opção, toque ou clique em Next, utilize as opções Add e Remove para selecionar os volumes a serem usados e toque ou clique em Next novamente.
 - **Back Up To A Shared Network Folder** Permite que você especifique uma pasta de rede compartilhada para backups. Com essa opção só é possível um backup por vez porque cada novo backup substitui o anterior. Se você escolheu essa opção, toque ou clique em Next. Quando for solicitado, toque ou clique em OK. Insira o caminho UNC para o compartilhamento de rede, como \\FileServer25\Backups\Exchange. Caso queira que o backup seja acessível a todos que tenham acesso à pasta compartilhada, selecione Inherit sob Access Control. Mas se você quiser restringir o acesso à pasta compartilhada ao usuário atual e aos membros dos grupos Administrators e Backup Operators, selecione Do Not Inherit sob Access Control. Toque ou clique em Next. Quando solicitado a fornecer as credenciais de acesso, insira o nome de usuário e a senha de uma conta autorizada para acessar e gravar na pasta compartilhada.
6. Na página Confirmation, confira os detalhes e toque ou clique em Finish. O assistente formata o disco. O processo de formatação pode levar apenas alguns minutos ou bem mais tempo, dependendo do tamanho do disco.
7. Na página Summary, toque ou clique em Close. Agora os backups estão agendados para o servidor.

Para agendar backups no Wbadmin utiliza-se o comando ENABLE BACKUP. O comando ENABLE BACKUP aceita os seguintes parâmetros:

- **-addTarget** Define o local de armazenamento para os backups de acordo com o GUID do disco que será usado. O GUID de um disco está listado como identificador do disco na saída do comando Wbadmin GET DISKS.
- **-removeTarget** Define o local de armazenamento a ser removido do agendamento de backup de acordo com o GUID do disco que será retirado. O GUID de um disco está listado como identificador do disco na saída do comando Wbadmin GET DISKS.
- **-include** Define uma lista delimitada por vírgula de letras de unidades de volume, pontos de montagem de volume e nomes de volume GUID para backup.
- **-allCritical** Inclui todos os volumes do sistema operacional no backup automaticamente.
- **-quiet** Especifica que você deseja executar o comando sem exibir avisos ao usuário.

Para ver como o ENABLE BACKUP é usado, considere os seguintes exemplos:

Agendar um backup para C e D às 21h diariamente

```
wbadmin enable backup -addTarget:{06d88776-0000-0000-0000-000000000000}
-schedule:18:00 -include:c:,d:
```

Agendar um backup para todos os volumes do sistema operacional às 6h e às 21h diariamente

```
wbadmin enable backup -addTarget:{06d88776-0000-0000-0000-000000000000}
-schedule:06:00,18:00 -allCritical
```

Alteração ou interrupção de backups agendados

Uma vez que você tenha backups agendados configurados em um servidor, é possível alterar ou interromper esses backups seguindo estas etapas:

1. Inicie o Windows Server Backup. Toque ou clique em Backup Schedule no menu Action ou no painel Actions. Isso iniciará o Backup Schedule Wizard. Toque ou clique em Next.
2. Na página Modify Scheduled Backup Settings, toque ou clique em Modify Backup se desejar adicionar ou remover itens, horas ou destinos de backup. Depois, siga as etapas de 3 a 7 da seção anterior “Configuração de backups agendados”. Se você quiser interromper os backups agendados, toque ou clique em Stop Backup, depois em Next e, por fim, em Finish. Quando for solicitado que você confirme, toque ou clique em Yes e depois em Close.

OBSERVAÇÃO A interrupção de backups libera os discos de backup para uso normal. Os arquivos de backup não são excluídos dos discos de backup, permanecendo disponíveis para uso na recuperação.

Para modificar backups agendados no Wbadmin utiliza-se o comando ENABLE BACKUP. Para destinos, utilize os parâmetros **-addTarget** e **-removeTarget** para modificar os discos de destino. Para o agendamento de execução e volumes inclusos, basta definir os novos valores que devem ser usados. Considere os exemplos a seguir:

Adição de um novo destino para backups agendados

```
wbadmin enable backup -addTarget:{41cd2567-0000-0000-0000-000000000000}
```

Remoção de um destino de backups agendados

```
wbadmin enable backup -removeTarget:{06d88776-0000-0000-0000-000000000000}
```

Modificação do agendamento de execução e volumes inclusos

```
wbadmin enable backup -schedule:03:00 -include:c:,d:,e:
```

Criação e agendamento de backups com o Wbadmin

Uma forma de criar backups manualmente é usando o comando Wbadmin START BACKUP. O comando START BACKUP aceita os seguintes parâmetros:

- **-backupTarget** Define o local de armazenamento para o backup como uma letra de unidade ou um caminho UNC para uma pasta compartilhada ou um servidor remoto.

- **-include** Define uma lista delimitada por vírgula de letras de unidades de volume, pontos de montagem de volume e nomes de volume GUID para backup.
- **-allCritical** Inclui todos os volumes do sistema operacional no backup automaticamente.
- **-inheritAcl** Especifica que você deseja que a pasta de backup na pasta compartilhada remota herde as permissões de segurança da pasta compartilhada. Se você não especificar esse parâmetro, a pasta de backup só estará acessível para o usuário especificado no parâmetro **-user**, administradores e operadores de backups.
- **-noVerify** Especifica que você não quer verificar backups gravados em mídias removíveis. Se você não especificar esse parâmetro, os backups gravados em mídias removíveis serão verificados.
- **-password** Define a senha a ser utilizada quando se conecta à pasta compartilhada remota.
- **-quiet** Especifica que você deseja executar o comando sem exibir avisos ao usuário.
- **-user** Define o nome de usuário a ser utilizado quando se conecta à pasta compartilhada remota.
- **-vssFull** Especifica que você quer realizar um backup completo usando o VSS, e isso garante que todos os dados do servidor e de aplicativos farão parte do backup. Não utilize esse parâmetro se estiver usando um utilitário de backup de terceiros para fazer backup de dados de aplicativos.

Para ver como o START BACKUP é usado, considere os seguintes exemplos:

Realização de um backup completo do servidor

```
wbadmin start backup -backupTarget:f: -vssfull
```

Backup de C e D para F

```
wbadmin start backup -backupTarget:f: -include:c:,d:
```

Backup de todos os volumes críticos

```
wbadmin start backup -backupTarget:f: -allCritical
```

Backup de C e D para uma pasta compartilhada remota

```
wbadmin start backup -backupTarget:\\fileserver27\\backups -include:c:,d:  
-user:williams
```

Se quiser criar um agendamento para executar backups em horários diferentes para dias diferentes, utilize o Task Scheduler para criar as tarefas necessárias à execução do comando no agendamento definido. Para agendar tarefas de execução de backups usando o Task Scheduler e Wbadmin siga estas etapas:

1. Em Computer Management, toque ou clique em Task Scheduler. Você está conectado ao computador local por padrão. Conforme necessário, conecte-se ao computador a ser acessado.
2. Pressione e mantenha pressionado ou clique com o botão direito do mouse no nó Task Scheduler e toque ou clique em Create Task. Isso abre a caixa de diálogo Create Task.

3. Na guia General insira o nome da tarefa e defina as opções de segurança para a execução da mesma.
 - Se a tarefa deve ser executada por um usuário que não o usuário atual, toque ou clique em Change User Or Group. Na caixa de diálogo Select User Or Group selecione o usuário ou o grupo pelo qual a tarefa deve ser executada. Forneça as credenciais adequadas quando for solicitado.
 - Defina outras opções conforme necessário. Por padrão, as tarefas só são executadas quando um usuário estiver logado. Se quiser executar a tarefa independentemente de haver um usuário logado, selecione Run Whether User Is Logged On Or Not. Pode-se também escolher executar com os privilégios mais altos e configurar a tarefa para versões anteriores do Windows.
4. Na guia Triggers, toque ou clique em New. Na caixa de diálogo New Trigger, selecione On A Schedule na lista Begin The Task. Utilize as opções oferecidas para definir o agendamento de execução e toque ou clique em OK.
5. Na guia Actions, toque ou clique em New. Na caixa de diálogo New Action, selecione Start A Program na lista Action.
6. Na caixa de texto Program/Script, insira **%windir%\System32\wbadmin.exe**.
7. Em Add Arguments, insira o comando START BACKUP que deseja utilizar, juntamente com os seus parâmetros, como no exemplo:

```
start backup -backupTarget:f: -include:c:,d:,e:\mountpoint,  
\\?\volume{be345a23-32b2-432d-43d2-7867ff3e3432}\
```
8. Toque ou clique em OK para fechar a caixa de diálogo New Action.
9. Na guia Conditions, especifique qualquer condição limitante para o início ou interrupção da tarefa.
10. Na guia Settings, escolha outras configurações opcionais para a tarefa.
11. Toque ou clique em OK para criar a tarefa.

Execução de backups manuais

Utilize o Windows Server Backup para fazer backup manualmente, seguindo estas etapas:

1. Inicie o Windows Server Backup. Toque ou clique em Backup Once no menu Action ou no painel Actions. Isso abrirá o Backup Once Wizard (Assistente de Backup Único).
2. Se você quiser fazer backup do servidor usando as mesmas opções utilizadas pelo Backup Schedule Wizard, selecione Scheduled Backup Options, toque ou clique em Next e toque ou clique em Backup para realizar o backup. Ignore as etapas restantes.
3. Caso queira fazer o backup do servidor usando outras opções, selecione Different Options e toque ou clique em Next.
4. Na página Select Backup Configuration, observe o tamanho do backup listado sob a opção Full Server. Esse é o espaço de armazenamento necessário para fazer backup dos dados do servidor, aplicativos e estado do sistema. Para fazer backup de todos os volumes no servidor, selecione a opção Full Server e toque ou clique em Next. Para fazer backup de volumes selecionados no servidor, toque ou clique em Custom e depois em Next.

5. Se você selecionou Custom, a página Select Items For Backup é exibida. Toque ou clique em Add Items. Marque as caixas de seleção dos volumes que você deseja fazer backup e desmarque as caixas daqueles volumes que não devem ser incluídos no backup. Selecione a opção Bare Metal Recovery se quiser recuperar completamente o sistema operacional. Toque ou clique em OK e depois em Next.

DICA Depois de selecionar os itens, é desejável tocar ou clicar em Advanced Settings antes de prosseguir. Use as opções da guia Exclusions para identificar locais e tipos de arquivo que não devem sofrer backup. Você também pode usar as opções na guia VSS Settings para especificar se você deseja criar um backup completo ou um backup de cópia.

6. Na página Specify Destination Type, realize uma das seguintes ações:

- Para fazer backup de unidades locais, selecione Local Drives e toque ou clique em Next. Na página Backup Destination, selecione o disco interno ou externo ou a unidade de DVD que será usada como destino de backup. Quando armazenados em um DVD, os backups são compactados e só é possível recuperar volumes completos. Como resultado, o tamanho do backup em um DVD pode ser menor do que o volume no servidor. Toque ou clique em Next.
- Para fazer backup em uma pasta compartilhada remota, selecione Remote Shared Folder e toque ou clique em Next. Na página Specify Remote Folder, insira o caminho UNC para a pasta compartilhada, como \\FileServer43\Backups. Caso queira que o backup seja acessível a todos que tenham acesso à pasta compartilhada, selecione Inherit sob Access Control. Mas se você quiser restringir o acesso à pasta compartilhada ao usuário atual, administradores e operadores de backup, selecione Do Not Inherit sob Access Control. Toque ou clique em Next. Quando solicitado a fornecer as credenciais de acesso, insira o nome de usuário e a senha de uma conta autorizada para acessar e gravar na pasta compartilhada.

7. Toque ou clique em Next e depois em Backup. A caixa de diálogo Backup Progress mostra o progresso do processo de backup. Se você tocar ou clicar em Close, o backup continuará a ser executado em segundo plano.

Como recuperar o servidor de falhas de hardware ou de inicialização

O Windows Server 2012 inclui uma arquitetura de diagnóstico e resolução extensa. Tais recursos podem ajudá-lo na recuperação de vários tipos de problemas envolvendo hardware, memória e desempenho, resolvendo-os automaticamente ou guiando os usuários no processo de solução.

O Windows Server 2012 inclui drivers de dispositivo mais confiáveis e de melhor desempenho para evitar as causas comuns de paradas e falhas. O cancelamento aprimorado de entrada/saída (I/O) para drivers de dispositivo garante que o sistema operacional possa recuperar-se normalmente de chamadas de bloqueio e que aconteçam menos operações de bloqueio de I/O de discos.

Para diminuir o tempo de inatividade e as reinicializações necessárias para instalações e atualizações de aplicativos, o Windows Server 2012 usa o processo de atualização para marcar arquivos em uso a serem atualizados e depois substitui automaticamente os arquivos na próxima vez que o aplicativo for iniciado. Em alguns casos, o Windows Server 2012 pode salvar os dados do aplicativo, fechar o aplicativo, atualizar os arquivos que estavam em uso e depois reiniciar o aplicativo. Para melhorar o de-

sempenho e a capacidade de resposta do sistema no geral, o Windows Server 2012 usa a memória com eficiência, oferece a execução ordenada para grupos de threads e fornece vários mecanismos de agendamento de processos. Ao otimizar o uso da memória e dos processos, o Windows Server 2012 assegura que os processos em segundo plano tenham menos impacto no desempenho do sistema.

O Windows Server 2012 traz diretrizes aprimoradas para as causas de condições sem resposta (unresponsive). Com a inclusão de detalhes adicionais no relatório de erros nos logs de eventos, o Windows Server 2012 facilita a identificação e a solução de problemas. Para se recuperar automaticamente de falhas no serviço, o Windows Server 2012 utiliza políticas de recuperação de serviços de forma mais extensa que os seus predecessores. Ao recuperar-se de uma falha no serviço, o Windows Server 2012 dá conta das dependências relativas a serviços ou não. Qualquer serviço dependente e componentes do sistema necessários serão iniciados antes do serviço em que ocorreu a falha.

Em versões anteriores do Windows, uma falha ou parada em um aplicativo é marcada como não respondendo, e é uma escolha do usuário sair e reiniciar o aplicativo. O Windows Server 2012 tenta solucionar problemas de aplicativos sem resposta usando o Restart Manager. O Restart Manager pode desligar e reiniciar aplicativos sem resposta automaticamente. Graças ao Restart Manager, você pode nem precisar intervir e tentar solucionar problemas com aplicativos congelados.

Instalações com falhas e condições sem resposta de aplicativos e drivers também são rastreadas pelo Action Center. O diagnóstico interno exibirá uma mensagem de aviso. Toque ou clique no ícone do Action Center na bandeja do sistema (system tray) para visualizar mensagens recentes. Toque ou clique em uma mensagem e o Windows Server 2012 abrirá a página Message Details no Action Center, que pode oferecer uma solução para o problema.

Para visualizar uma lista atual dos problemas no momento, siga estas etapas:

1. No Control Panel, sob o título System And Security, toque ou clique em Review Your Computer's Status.
2. No Action Center, uma lista de problemas conhecidos é exibida. Para alguns problemas é possível selecionar um botão View Message Details referente para exibir uma página Message Details. Se houver uma solução disponível, toque ou clique no link oferecido para baixar a solução ou visitar um site relacionado para obter mais informações.

Enquanto estiver trabalhando no Action Center, toque ou clique no link Check For Solutions no painel Maintenance para que o Windows Server busque soluções para você.

O Windows Server 2012 tenta solucionar problemas relacionados à pouca memória virtual oferecendo o Resource Exhaustion Detection And Recovery. Esse recurso monitora o limite de confirmação da memória virtual de todo o sistema e avisa se o computador estiver ficando com pouca memória virtual. Para ajudar na solução desse problema, ele também identifica o processo que está consumindo a maior parte da memória e possibilita que você feche a partir da caixa de diálogo Close Programs To Prevent Information Loss um ou todos os aplicativos que consomem mais recursos. O aviso de esgotamento de recursos também é registrado no log de eventos do sistema.

Em versões anteriores do Windows, os arquivos de sistema corrompidos eram uma das principais causas de falhas de inicialização. O Windows Server 2012 inclui um diagnóstico interno para detectar automaticamente durante a inicialização os arquivos de sistema corrompidos e guiar o usuário na recuperação automatizada ou manual. Para

resolver problemas de inicialização, o Windows Server 2012 utiliza a ferramenta Startup Repair (StR, Reparo de Inicialização), que é instalada automaticamente e iniciada se um sistema não puder ser inicializado. Uma vez instalado, o StR analisa os logs e relatórios de erros de inicialização para tentar determinar a causa da falha. Depois, o StR tenta corrigir o problema automaticamente. Se não for possível, ele restaura o sistema para o último estado operacional conhecido (Last Known Working State) e fornece informações de diagnóstico e opções de suporte para prosseguir a solução de problemas.

Alguns dos problemas de hardware reconhecidos no diagnóstico interno incluem detecção de erros e de falha de disco. Se um dispositivo estiver com problemas, o diagnóstico do hardware pode detectar condições de erro e reparar o problema automaticamente ou guiar o usuário pelo processo de recuperação. Com unidades de disco, o diagnóstico de hardware utiliza relatórios de falhas oferecidos por unidades de disco para detectar falhas possíveis e alertá-lo antes que elas ocorram. O diagnóstico de hardware também auxilia no processo de backup depois de exibir o alerta de que um disco pode estar com problemas.

Problemas de desempenho reconhecidos pelo diagnóstico interno incluem inicialização de aplicativos, inicialização lenta, em espera/retomar (Standby/resume) lento e desligamento lento. Se um computador estiver com um desempenho reduzido, o diagnóstico de desempenho pode detectar o problema e oferecer soluções possíveis para resolvê-lo. Para problemas de desempenho avançado, pode-se rastrear dados relacionados ao desempenho e à confiabilidade no console Diagnostics, que inclui um monitor de desempenho e um monitor de confiabilidade. (Isso é abordado no Capítulo 3, "Monitoramento de processos, serviços e eventos.")

Os problemas de memória reconhecidos pelo diagnóstico interno incluem vazamentos de memória e memória com falhas. Um vazamento de memória ocorre quando um aplicativo ou um componente do sistema não libera completamente as áreas de memória física depois de ter trabalhado com elas. Caso suspeite que um computador tem um problema na memória que não está sendo detectado automaticamente, selecione a opção relacionada e execute o Windows Memory Diagnostics manualmente durante a inicialização. Se a opção Windows Memory Diagnostics não aparecer na inicialização, siga estas etapas para executar o programa:

1. Inicie o Windows Memory Diagnostics. Uma maneira de fazê-lo é digitar **mdsched.exe** na caixa App Search e pressionar Enter.
2. Escolha se prefere reiniciar o computador neste momento e executar a ferramenta imediatamente ou agendar a ferramenta para conferir se há problemas no próximo reinício.
3. O Windows Memory Diagnostics é executado automaticamente depois que o computador reinicia, usando a combinação de testes padrão e realizando duas etapas de teste por padrão.

Para alterar as opções de execução, utilize a tecla F1. Podem ser realizados três níveis diferentes de testes de memória, incluindo Basic (básico), Standard (padrão) e Extended (estendido). Utilize um teste básico para fazer uma verificação rápida da memória. Utilize um teste padrão para realizar um teste padrão da memória. Utilize um teste estendido quando quiser realizar um teste mais extensivo. Use a opção Pass Count para definir o número de etapas do teste.

Para detectar falhas no sistema possivelmente causadas por falhas na memória, o diagnóstico da memória trabalha com a ferramenta Microsoft Online Crash Analysis.

Se um computador falhar por causa da memória e o diagnóstico detectar isso, será solicitado que você agende um teste de memória na próxima vez que o computador for reiniciado.

Como recuperar-se de um início com falhas

Se o Windows iniciar com falhas, o Windows Server 2012 entrará no modo Windows Error Recovery automaticamente. Nesse modo, você verá uma tela Recovery na próxima vez que tentar iniciar o servidor. As opções incluem:

- **Continue** Sair do menu reparar e continuar a carregar o sistema operacional
- **Use Another Operating System** Sair do menu reparar e permitir a seleção do sistema operacional a ser carregado (se houver vários sistemas operacionais instalados)
- **Troubleshoot** Exibir o menu Advanced Options
- **Turn Off Your PC** Sair do menu reparar e desligar o servidor

O menu Advanced Options apresenta três opções:

- **System Image Recovery** Permite que você recupere o servidor usando um arquivo de imagem do sistema. O arquivo de imagem não pode ser proveniente de um computador remoto.
- **Command Prompt** Permite que você acesse um prompt de comando e trabalhe com os comandos e ferramentas disponíveis no ambiente de recuperação.
- **Startup Settings** Permite que você altere o comportamento de inicialização e inicie o servidor no modo de segurança. Clique em Restart para reiniciar o computador no modo de segurança para que você possa desabilitar a imposição de assinatura de driver, a proteção antimalware de início antecipado e o reinício automático em falhas no sistema. Também possibilita a inicialização no modo de vídeo de baixa resolução (VGA Mode), modo de depuração, log de inicialização e modo de segurança.

Como iniciar um servidor no modo de segurança

Muitos problemas de inicialização ocorrem porque há alguma mudança no sistema, como um dispositivo instalado de forma incorreta, por exemplo. A configuração ou registro do sistema pode ter sido atualizada de forma inapropriada, causando um conflito. Muitas vezes é possível resolver problemas de inicialização usando o modo de segurança para recuperar ou solucionar problemas no sistema. Ao terminar de trabalhar com o modo de segurança, certifique-se de reiniciar o servidor usando a inicialização normal. Depois disso será possível utilizar o servidor normalmente.

No modo de segurança, o Windows Server 2012 só carrega arquivos, serviços e drivers básicos. Os drivers carregados incluem os relacionados ao mouse, monitor, teclado, armazenamento em massa e vídeo base. O driver de monitor define as configurações e modos básicos para o monitor do servidor e o vídeo base define as opções básicas para a placa gráfica do servidor. Nenhum serviço ou driver de rede será inicializado a menos que você escolha a opção Safe Mode With Networking (Modo de Segurança Com Rede). Como o modo de segurança carrega um conjunto limitado de informações de configuração, ele pode ajudá-lo na solução de problemas.

Para iniciar um servidor no modo de segurança, siga estas etapas:

1. Se o computador não iniciar normalmente, a tela Recovery é exibida durante a inicialização. Na tela Recovery, toque ou clique em Troubleshoot.
2. Na tela Advanced Options, toque ou clique em Startup Settings. Depois, na tela Windows Startup Settings, toque ou clique em Restart.
3. Utilize as teclas de direção para selecionar o modo de segurança desejado e pressione Enter. A opção de modo de segurança utilizada depende do tipo de problema que você está enfrentando. As opções-chave são as seguintes:
 - **Repair Your Computer** Carrega a ferramenta Startup Repair. Selecione essa opção para reiniciar o servidor e retornar à tela Recovery.
 - **Safe Mode** Carrega apenas arquivos, serviços e drivers básicos durante a sequência de inicialização. Os drivers carregados incluem mouse, monitor, teclado, armazenamento em massa e vídeo base. Nenhum serviço ou driver de rede é iniciado.
 - **Safe Mode With Networking** Carrega arquivos, serviços e drivers básicos, bem como serviços e drivers necessários para iniciar a rede.
 - **Safe Mode With Command Prompt** Carrega arquivos, serviços e drivers básicos e depois inicia um prompt de comando em vez da interface gráfica do Windows. Nenhum serviço ou driver de rede é iniciado.

DICA No Safe Mode With Command Prompt (Modo de Segurança com Prompt de Comando) pode-se iniciar o shell do Explorer a partir da interface da linha de comando. Para isso, pressione Ctrl+Shift+Esc e insira **explorer.exe** na janela New Process no menu File do Task Manager.

- **Enable Boot Logging** Permite a criação de um registro de todos os eventos de inicialização em um log de inicialização.
- **Enable Low-Resolution Video** Permite que o sistema seja iniciado no modo de exibição de baixa resolução 640 por 480, o que é útil se a exibição do sistema estiver configurada para um modo que não possa ser usado com o monitor atual.
- **Last Known Good Configuration** Inicia o computador no modo de segurança usando as informações de registro que o Windows salvou no último desligamento, incluindo o hive HKEY_CURRENT_CONFIG (HKCC). Esse hive de registro armazena informações sobre a configuração de hardware com a qual você obteve êxito ao iniciar o computador anteriormente.
- **Debugging Mode** Inicia o sistema no modo de depuração, o que só é útil para a solução de problemas de bugs (falhas) no sistema operacional.
- **Directory Services Restore Mode** Inicia o sistema no modo de segurança e permite a restauração do serviço de diretório. Essa opção está disponível no Windows Server 2008 R2 e em controladores de domínio posteriores.
- **Disable Automatic Restart On System Failure** Evita que o Windows Server reinicie automaticamente após uma falha no sistema operacional.
- **Disable Driver Signature Enforcement** Inicia o computador no modo de segurança sem a imposição de configurações de políticas de assinatura digital para drivers. Se um driver com uma assinatura digital inválida ou inexistente estiver

causando uma falha na inicialização, essa opção resolve o problema temporariamente para que você possa iniciar o computador e solucioná-lo, obtendo um novo driver ou alterando as configurações de imposição de assinatura do driver.

- **Disable Early Launch Anti-Malware Driver** Inicia o computador no modo de segurança sem executar o driver de inicialização do software antimalware do computador. Se o driver de inicialização do software antimalware do computador estiver impedindo a inicialização, é preciso procurar no site do desenvolvedor do software uma atualização que resolva o problema de inicialização ou então configurar o software removendo a proteção de inicialização.
 - **Start Windows Normally** Inicia o computador com as configurações normais.
4. Se um problema não voltar a aparecer quando você iniciar no modo de segurança, as configurações padrão e os drivers de dispositivos básicos podem ser eliminados da lista de causas possíveis. Se um dispositivo recém-adicionado ou um driver atualizado estiver causando problemas, pode-se usar o modo de segurança para remover o dispositivo ou reverter a atualização.

Backup e restauração do estado do sistema

Existem aproximadamente 50.000 arquivos de estado do sistema no Windows Server 2012, que usam em torno de 4 GB de espaço em disco na instalação padrão de um computador baseado em x64. A maneira mais rápida e fácil de fazer backup e restaurar o estado do sistema de um servidor é com o Wbadmin. Com o Wbadmin, pode-se usar o comando `START SYSTEMSTATEBACKUP` para criar um backup do estado do sistema para um computador e o comando `START SYSTEMSTATERECOVERY` para restaurar o estado do sistema de um computador.

DICA Ao selecionar a restauração de um estado de sistema em um controlador de domínio, é preciso estar no modo Directory Services Restore. Para aprender a restaurar o Active Directory, consulte a próxima seção.

Para fazer backup do estado do sistema de um servidor, insira o seguinte em um prompt de comando elevado:

```
wbadmin start systemstatebackup -backupTarget:VolumeName
```

Onde *VolumeName* é o local de armazenamento para o backup, como F:.

Para restaurar o estado do sistema de um servidor, insira o seguinte em um prompt de comando elevado:

```
wbadmin start systemstaterecovery -backupTarget:VolumeName
```

Onde *VolumeName* é o local de armazenamento que contém o backup que você deseja recuperar, como F:. Além disso, você pode fazer o seguinte:

- Usar o parâmetro `-recoveryTarget` para restaurar para um local alternativo.
- Usar o parâmetro `-machine` para especificar o nome do computador para recuperação caso o local de backup original contenha backups de vários computadores.
- Usar o parâmetro `-authSysvol` para realizar uma restauração autoritativa do SYSVOL.

Também é possível recuperar o estado do sistema usando um backup que inclua o estado do sistema ou realizando uma recuperação.

Restauração do Active Directory

Ao restaurar os dados do estado de um sistema para um controlador de domínio, é preciso escolher se você deseja realizar uma restauração autoritativa ou não autoritativa. O padrão é não autoritativa. Nesse modo, o Active Directory e os outros dados replicados são restaurados do backup e qualquer alteração é replicada de um outro controlador de domínio. Assim, pode-se restaurar um controlador de domínio com falhas de forma segura, sem sobreescriver as últimas informações do Active Directory. Por outro lado, se você estiver tentando restaurar o Active Directory para toda a rede usando dados do backup, é preciso fazer uma restauração autoritativa. Com uma restauração autoritativa os dados são restaurados no controlador de domínio atual e depois replicados para outros controladores de domínio.

ATENÇÃO Uma restauração autoritativa sobrescreve todos os dados do Active Directory do domínio. Antes de realizar uma restauração autoritativa, certifique-se de que os dados do arquivo são os dados corretos para propagar pelo domínio e de que os dados atuais em outros controladores de domínio estejam incorretos, ultrapassados ou corrompidos.

Para restaurar o Active Directory em um controlador de domínio e habilitar os dados restaurados para serem replicados pela rede, siga estas etapas:

1. Certifique-se de que o servidor que é controlador de domínio esteja desligado.
2. Reinicie o servidor que é controlador de domínio e entre no modo de segurança.
3. Selecione Directory Services Restore Mode (Modo de Restauração dos Serviços de Diretório).
4. Quando o sistema iniciar, use o utilitário Backup para restaurar os dados do estado do sistema e outros arquivos essenciais.
5. Após restaurar os dados mas antes de reiniciar o servidor, utilize a ferramenta Ntdsutil.exe para marcar objetos como autoritativos. Lembre-se de verificar com cuidado os dados do Active Directory.
6. Reinicie o servidor. Quando o sistema acabar a inicialização, os dados do Active Directory devem começar a ser replicados por todo o domínio.

Restauração do sistema operacional e do sistema completo

Como foi discutido anteriormente, o Windows Server 2012 inclui recursos de reparo de inicialização que podem recuperar um servidor em casos de arquivos do sistema corrompidos ou perdidos. O processo de reparo de inicialização também pode recuperar-se de alguns tipos de falhas envolvendo o gerenciador de inicialização. Se esses processos falharem e o gerenciador de inicialização for o fator que impede que você inicie o servidor, utilize o disco de instalação do Windows Server 2012 ou as opções de recuperação do sistema para restaurar o gerenciador e habilitar a inicialização.

As opções de recuperação do sistema estão disponíveis apenas em instalações de servidor completo e não em instalações Server Core. Com uma instalação Server Core é preciso usar o disco de instalação para iniciar a recuperação.

As opções de recuperação do sistema incluem as seguintes ferramentas:

- **System Image Recovery** Permite a recuperação do sistema operacional de um servidor ou a realização de uma recuperação do sistema completo. Em caso de

uma recuperação do sistema operacional ou do sistema completo, certifique-se de que os dados do backup estão disponíveis e de que você pode fazer logon com uma conta com as permissões apropriadas. Em uma recuperação de sistema completo, lembre-se de que os dados que não foram inclusos no backup original serão excluídos quando o sistema for recuperado, incluindo qualquer volume em uso que não tenha sido incluso no backup.

- **Windows Memory Diagnostics Tools** Permite que você faça o diagnóstico de um problema com a memória física do servidor. Podem ser realizados três níveis diferentes de testes de memória: básico, padrão e detalhado.

Você também pode acessar um prompt de comando. Esse prompt de comando dá acesso às ferramentas de linha de comando disponíveis durante a instalação bem como para os seguintes programas adicionais:

- **Startup Repair Wizard (X:\Sources\Recovery\StartRep.exe)** Normalmente, essa ferramenta é iniciada de forma automática em falhas de inicialização se o Windows detectar um problema com o setor de inicialização, com o gerenciador de inicialização ou com o armazenamento Boot Configuration Data (BCD, Dados de Configuração de Inicialização).
- **Startup Recovery Options (X:\Sources\Recovery\Recenv.exe)** Permite que você inicie o Startup Recovery Options Wizard. Se você inseriu configurações de recuperação incorretas em outra ocasião, pode fornecer opções diferentes.

Na posição de administrador você pode realizar a solução de problemas na linha de comando, seguindo estas etapas:

1. Se o computador não iniciar normalmente, a tela Recovery é exibida durante a inicialização. Na tela Recovery, toque ou clique em Troubleshoot.
2. Na tela Advanced Options, toque ou clique em Command Prompt.
3. Quando for solicitada a escolha de uma conta, toque ou clique na conta Administrator. Em seguida, insira a senha da conta Administrator e toque ou clique em Continue.
4. Utilize o prompt de comando para realizar a solução de problemas. Você poderia executar o Startup Repair Wizard, por exemplo, ao digitar **x:\sources\recovery\startrep.exe**.

Para recuperar o sistema operacional de um servidor ou realizar uma recuperação do sistema completo pode-se utilizar uma imagem de backup criada anteriormente com o Windows Server Backup. Com uma recuperação de sistema operacional você recupera todos os volumes críticos, mas não recupera volumes que não sejam do sistema. Se você recuperar o sistema completo, o Windows Server Backup reformata e reparticiona todos os discos ligados ao servidor. Portanto, utilize esse método apenas quando quiser recuperar os dados do servidor em um hardware separado ou se falharem todas as outras tentativas de recuperação no hardware existente.

OBSERVAÇÃO Ao recuperar o sistema operacional ou o sistema completo, certifique-se de que os dados de backup estão disponíveis e de que você pode fazer logon com uma conta com as permissões apropriadas. Com uma recuperação de sistema completo, lembre-se de que os dados que não foram inclusos no backup original serão excluídos quando o sistema for recuperado. Isso abrange qualquer volume em uso que não tenha sido incluso no backup.

Para recuperação um sistema operacional usando uma imagem de backup, siga as etapas:

1. Se o computador não iniciar normalmente, a tela Recovery é exibida durante a inicialização. Na tela Recovery, toque ou clique em Troubleshoot.
2. Na tela Advanced Options, toque ou clique em System Image Recovery.
3. Quando for solicitada a escolha de uma conta, toque ou clique na conta Administrator. Em seguida, insira a senha da conta Administrator e toque ou clique em Continue. Isso inicia o Re-Image Your Computer Wizard.
4. Na página Select A System Image Backup, toque ou clique em Use The Latest Available System Image (Recommended) e depois toque ou clique em Next. Ou então toque ou clique em Select A System Image e depois em Next.
5. Se você selecionar uma imagem para restauração, proceda de uma das seguintes maneiras na página Select The Location Of The Backup:
 - Toque ou clique no local que contém a imagem do sistema que você quer usar e depois toque ou clique em Next. Toque ou clique na imagem do sistema desejada e depois em Next.
 - Para procurar por uma imagem do sistema na rede, toque ou clique em Advanced e depois em Search For A System Image On The Network. Quando for solicitado que você confirme que deseja conectar-se à rede, toque ou clique em Yes. Na caixa de texto Network Folder, especifique o local do servidor e a pasta compartilhada em que a imagem está armazenada, como \\FileServer22\Backups, e toque ou clique em OK.
 - Para instalar um driver para um dispositivo de backup que não aparece na lista de locais, toque ou clique em Advanced e depois em Install A Driver. Insira a mídia de instalação do dispositivo e toque ou clique em OK. Depois que o Windows instalar o driver de dispositivo, o dispositivo de backup deve aparecer na lista de locais.
6. Na página Choose Additional Restore Options, faça as seguintes tarefas adicionais e toque ou clique em Next:
 - Marque a caixa de seleção Format And Repartition Disks para excluir partições existentes e reformatar os discos de destino para que sejam os mesmos que os do backup.
 - Selecione Only Restore System Drives para restaurar apenas as unidades do backup que são necessárias para executar o Windows: os volumes de inicialização, sistema e recuperação. Se o servidor possuir unidades de dados, elas não serão restauradas.
 - Toque ou clique em Install Drivers se quiser instalar drivers de dispositivos para o hardware para o qual se está fazendo a recuperação.
 - Toque ou clique em Advanced para determinar se o computador deve ser reiniciado e os erros em discos verificados imediatamente após o término da operação de recuperação.
7. Na página Confirmation, confira os detalhes da restauração e toque ou clique em Finish. O assistente restaurará o sistema operacional ou o sistema completo de acordo com as opções que você selecionou.

Restauração de aplicativos, volumes que não são do sistema e arquivos e pastas

O Windows Server 2012 oferece processos separados para a recuperação de estado do sistema e de servidor completo e para a recuperação de volumes e arquivos e pastas individuais. Você pode utilizar o Recovery Wizard no Windows Server Backup para recuperar volumes que não são do sistema e arquivos e pastas de um backup. Antes de começar, certifique-se de que o computador para o qual você está recuperando arquivos use o Windows Server 2012. Se desejar recuperar arquivos e pastas individuais, certifique-se de que exista ao menos um backup em um disco interno ou externo ou em uma pasta compartilhada remota. Não é possível recuperar arquivos e pastas de backups salvos em DVDs ou mídias removíveis.

Lembrando-se disso, pode-se recuperar volumes que não são do sistema, arquivos e pastas ou dados de aplicativos seguindo as etapas:

1. Inicie o Windows Server Backup. No painel Actions ou no menu Action toque ou clique em Recover. Isso iniciará o Recovery Wizard.
2. Na página Getting Started, especifique se você irá recuperar dados do computador local ou de um outro local e toque ou clique em Next.
3. Se estiver recuperando dados de um outro local, especifique se o backup que você deseja recuperar está em uma unidade local ou em uma pasta compartilhada remota. Depois, toque ou clique em Next e insira configurações específicas para o local. Ao recuperar de uma unidade local, selecione o local do backup na lista suspensa na página Select Backup Location. Ao recuperar de uma pasta compartilhada remota, insira o caminho para a pasta que contém o backup na página Specify Remote Folder. Na pasta remota, o backup deve estar armazenado em \\BackupServer\WindowsImageBackup\ComputerName.
4. Se estiver recuperando de um outro local, selecione na página Select Server de qual servidor são os dados que você gostaria de recuperar. Toque ou clique em Next.
5. Na página Select Backup Date, use o calendário e a lista de horários para selecionar a data e a hora do backup que você deseja recuperar. Os backups estão disponíveis para as datas que aparecem em negrito. Toque ou clique em Next.
6. Na página Select Recovery Type, realize uma das seguintes ações:
 - Para restaurar arquivos e pastas individuais, toque ou clique em Files And Folders e depois em Next. Na página Select Items To Recover, sob Available Items, toque ou clique no sinal de adição (+) para expandir a lista até que a pasta desejada esteja visível. Toque ou clique em uma pasta para exibir o seu conteúdo no painel adjacente. Toque ou clique em cada item a ser restaurado e depois em Next.
 - Para restaurar volumes não críticos ou que não são do sistema operacional, toque ou clique em Volumes e depois em Next. Na página Select Volumes, você verá uma lista de volumes de origem e de destino. Marque as caixas de seleção associadas aos volumes de origem que você quer recuperar e depois selecione o local para o qual deseja recuperá-los usando Destination Volume lists. Toque ou clique em Next. Se for solicitado que confirme a ação de recuperação, toque ou clique em Yes. Ignore as etapas 7 e 8.
 - Para restaurar dados de aplicativos, toque ou clique em Applications e depois em Next. Na página Select Application, sob Applications, toque ou clique no

aplicativo que deseja recuperar. Se o backup que está sendo usado é o mais recente, pode aparecer uma caixa de seleção com o rótulo Do Not Perform A RollForward Recovery Of The Application Databases. Marque essa caixa de seleção caso queira impedir que o Windows Server Backup role para frente o banco de dados do aplicativo que está no seu servidor no momento. Toque ou clique em Next. Tendo em vista que qualquer dado no volume de destino será perdido quando a recuperação for realizada, certifique-se de que o volume de destino esteja vazio ou não contenha informações das quais você pode precisar um dia.

7. Depois, especifique se deseja restaurar os dados para o local original (apenas arquivos que não são do sistema) ou para algum local alternativo. Para um local alternativo, insira o caminho para o local de restauração ou toque ou clique em Browse para selecioná-lo. Com aplicativos pode-se copiar os dados para um local alternativo. Entretanto, não se pode recuperar aplicativos para um local ou computador diferente.
8. Para a recuperação de arquivos e pastas, selecione uma técnica de recuperação a ser aplicada quando já existirem arquivos e pastas no local de recuperação. Você pode criar cópias para que tenha ambas as versões do arquivo ou pasta, substituir os arquivos existentes por arquivos recuperados ou ignorar arquivos e pastas duplicados para preservar arquivos existentes. Também é possível restaurar as permissões de segurança originais para os arquivos e pastas sendo recuperados.
9. Na página Confirmation, confira os detalhes e toque ou clique em Recover para restaurar os itens especificados.

Gerenciamento de políticas de recuperação de criptografia

Se você estiver na posição de administrador para uma organização que utiliza o Encrypting File System (EFS), o seu planejamento de recuperação de desastre deve conter procedimentos e preparações adicionais. É preciso considerar como lidar com tópicos relacionados aos certificados pessoais de criptografia, agente de recuperação do EFS e políticas de recuperação EFS. Essas questões são abordadas nas seções a seguir.

Noções básicas sobre certificados de criptografia e políticas de recuperação

Há suporte para criptografia de arquivos por pasta ou por arquivo. Qualquer arquivo que se encontre em uma pasta marcada para criptografia é criptografado automaticamente. Os arquivos em formato criptografado podem ser lidos somente pela pessoa que os criptografou. Para que outros usuários possam ler o arquivo criptografado, o usuário deve descriptografar o arquivo.

Cada arquivo criptografado possui uma chave de criptografia exclusiva. Isso significa que arquivos criptografados podem ser copiados, movidos ou renomeados como qualquer outro arquivo e, na maioria dos casos, essas ações não afetam a criptografia dos dados. O usuário que criptografou o arquivo sempre terá acesso a ele, desde que a chave privada do usuário esteja disponível no perfil do usuário no computador ou que o usuário tenha mobilidade de credenciais com o Digital Identification Management Service (DIMS). Para esse usuário, o processo de criptografia e descriptografia é automático e transparente.

O processo que controla a criptografia e a descriptografia é o EFS. A configuração padrão do EFS permite que os usuários criptografem os arquivos sem necessidade de uma permissão especial. Os arquivos são criptografados utilizando uma chave pública/privada que o EFS gera automaticamente para cada usuário. Por padrão, o Windows XP SP1 e versões posteriores do Windows utilizam o algoritmo Advanced Encryption Standard (AES) para a criptografia de arquivos com o EFS. Não há suporte para a criptografia AES no Windows 2000 ou em versões do Windows XP anteriores à SP1. Ao serem visualizados nesses computadores, os arquivos criptografados por AES podem parecer corrompidos quando não estão. O Internet Information Services 7 (Serviços de Informações da Internet 7) e versões posteriores podem usar um provedor AES para criptografar as senhas por padrão.

Os certificados de criptografia são armazenados como parte dos dados nos perfis de usuário. Se um usuário trabalhar com vários computadores e quiser utilizar a criptografia, um administrador precisa configurar um perfil móvel para ele. Um perfil móvel garante que os dados do perfil e os certificados de chave pública do usuário estejam acessíveis em outros computadores. Sem isso, os usuários não conseguirão acessar seus arquivos criptografados utilizando outros computadores.

DICA Uma alternativa para um perfil móvel é copiar o certificado de criptografia do usuário para os computadores que ele utiliza. Isso pode ser feito usando o backup de certificado e o processo de restauração discutidos em “Backup e restauração de dados criptografados e certificados” mais adiante neste capítulo. Simplesmente faça backup do certificado no computador original do usuário e o restaure em cada um dos computadores a que ele se conecta.

O EFS tem um sistema de recuperação de dados interno para proteção contra perdas de dados. Esse sistema de recuperação garante que os dados criptografados possam ser recuperados se o certificado da chave pública do usuário for perdido ou excluído. O cenário mais comum para isso é quando um usuário sai da empresa e a conta de usuário associada é excluída. Ainda que um gerente tenha conseguido fazer logon na conta do usuário, verificar os arquivos e salvar arquivos importantes para outras pastas, os arquivos criptografados só estarão disponíveis se a criptografia for removida pelo gerente que está atuando como o usuário que criptografou os arquivos ou se, estando logado como usuário, o gerente mover os arquivos para um volume FAT ou FAT32 (que não suportam a criptografia).

Para acessar os arquivos criptografados depois da conta de usuário ser excluída, é preciso utilizar um agente de recuperação. Os agentes de recuperação têm acesso à chave de criptografia de arquivo necessária para desbloquear os dados em arquivos criptografados. Para proteger dados confidenciais, no entanto, os agentes de recuperação não têm acesso à chave privada ou a qualquer informação de chave privada do usuário.

Os agentes de recuperação são designados automaticamente e os certificados de recuperação necessários também são gerados automaticamente. Isso assegura que os arquivos criptografados sempre possam ser recuperados.

Os agentes de recuperação do EFS estão configurados em dois níveis:

- **Domain** O agente de recuperação de um domínio é automaticamente configurado quando o primeiro controlador de domínio do Windows Server é instalado. Por padrão, o agente de recuperação é o administrador de domínio. Por meio de Group Policy, os administradores do domínio podem designar agentes de recuperação adicionais. Os administradores do domínio também podem delegar privilégios de agente de recuperação para administradores de segurança designados.

- **Local computer** Quando um computador faz parte de um grupo de trabalho ou em uma configuração autônoma, o agente de recuperação é o administrador do computador local por padrão. Pode-se designar agentes de recuperação adicionais. Além disso, se quiser ter agentes de recuperação locais em um ambiente de domínio, em lugar de agentes de recuperação no nível de domínio, você deve excluir a política de recuperação da Group Policy para o domínio.

Pode-se excluir as diretrivas de recuperação se não quiser que fiquem disponíveis.

Configuração da política de recuperação do EFS

As políticas de recuperação são configuradas automaticamente para controladores de domínio e estações de trabalho. Por padrão, os administradores de domínio são os agentes de recuperação designados para domínios e o administrador local é o agente de recuperação designado para uma estação de trabalho autônoma.

Por meio da Group Policy, pode-se visualizar, atribuir e excluir agentes de recuperação. Siga estas etapas:

1. Acesse o console da Group Policy para o computador local, site, domínio ou unidade organizacional com que queira trabalhar. Para detalhes sobre como trabalhar com a Group Policy, consulte o Capítulo 4 “Automatização de tarefas administrativas, políticas e procedimentos”.
2. Expanda Computer Configuration, Windows Settings, Security Settings e Public Key Policies e toque ou clique em Encrypting File System para acessar os Recovery Agents configurados na Group Policy.
3. O painel à direita lista os certificados de recuperação atribuídos atualmente. Os certificados de recuperação estão listados de acordo com quem os emitiu, para quem foram emitidos, data de validade, finalidade e mais.
4. Para designar um agente de recuperação adicional, pressione e mantenha pressionado ou clique com o botão direito do mouse em Encrypting File System e toque ou clique em Add Data Recovery Agent. Isso inicia o Add Data Recovery Agent Wizard, que é utilizado para selecionar um certificado gerado anteriormente que tenha sido atribuído a um usuário e marcá-lo como um certificado de recuperação designado. Toque ou clique em Next. Na página Select Recovery Agents, toque ou clique em Browse Directory e selecione o usuário com o qual você deseja trabalhar na caixa de diálogo Find Users, Contacts, And Groups. Toque ou clique em OK e depois em Next. Toque ou clique em Finish para adicionar o agente de recuperação.

OBSERVAÇÃO Antes de designar agentes de recuperação adicionais, você deve configurar uma autoridade de certificação-raiz (CA) no domínio. Depois disso, utilize o snap-in Certificates para gerar um certificado pessoal que utilize o modelo Recovery Agent do EFS. A CA raiz deve aprovar a solicitação do certificado para que ele possa ser utilizado. Você também pode usar Cipher.exe para gerar a chave e o certificado do agente de recuperação.

5. Para excluir um agente de recuperação, selecione o certificado referente no painel direito e pressione Delete. Quando for solicitado que confirme a ação, toque ou clique em Yes para excluir o agente permanente e irrevogavelmente. Se a política de recuperação estiver vazia (ou seja, não tiver qualquer outro agente de recuperação designado), o EFS será desativado para que os usuários não possam mais criptografar arquivos.

Backup e restauração de dados criptografados e certificados

Pode-se fazer backup e recuperar dados criptografados da mesma forma que se faz com qualquer outro dado. O importante é lembrar-se que você deve usar um software de backup que compreenda EFS, como o backup interno e as ferramentas de restauração. Entretanto, é preciso ter cuidado ao usar esse tipo de software.

O processo de backup ou de restauração não necessariamente faz backup ou restaura o certificado necessário para trabalhar com os dados criptografados. São os dados do perfil do usuário que contêm esse certificado. Se a conta de usuário existe e o perfil ainda contém o certificado necessário, o usuário pode trabalhar com os dados criptografados.

Se a conta de usuário existe e você fez o backup do perfil do usuário anteriormente e depois restaurou o perfil para recuperar um certificado excluído, o usuário ainda pode trabalhar com dados criptografados. Senão, não há outras maneiras de trabalhar com os dados. Será preciso que um agente de recuperação designado acesse os arquivos e remova a criptografia.

A possibilidade de fazer backup e restaurar os certificados é uma parte importante de qualquer plano de recuperação de desastre. As próximas seções analisam as técnicas que podem ser usadas na realização dessas tarefas.

Backup de certificados de criptografia

Para fazer backup e restaurar certificados pessoais, utiliza-se o snap-in Certificates. Os certificados pessoais são salvos no formato Personal Information Exchange (Troca de Informações Pessoais) (.pfx).

Para fazer backup de certificados pessoais, siga estas etapas:

1. Faça logon como o usuário no computador onde está armazenado o certificado pessoal com o qual você quer trabalhar. Toque ou clique em Start, digite **mmc** na caixa Search e pressione Enter. Isso abre o Microsoft Management Console (MMC, Console de Gerenciamento Microsoft).
2. No MMC, selecione File e depois Add/Remove Snap-In. A caixa de diálogo Add Or Remove Snap-Ins será aberta.
3. Na lista Available Snap-Ins, selecione Certificates e toque ou clique em Add. Selecione My User Account e toque ou clique em Finish. Isso adiciona o snap-in Certificates à lista Selected Snap-Ins. O foco do snap-in está configurado para a conta de usuário logada no momento.
4. Toque ou clique em OK para fechar a caixa de diálogo Add Or Remove Snap-Ins.
5. Expanda Certificates–Current User, expanda Personal e depois selecione Certificates. Pressione e mantenha pressionado ou clique com o botão direito do mouse no certificado que você deseja salvar. Toque ou clique em All Tasks e depois em Export. Isso inicia o Certificate Export Wizard. Toque ou clique em Next.
6. Selecione Yes, Export The Private Key. Toque ou clique em Next duas vezes.
7. Na página de segurança, utilize as opções oferecidas para especificar entidades de segurança que devem ter acesso ao certificado. A entidade de segurança padrão é a conta Administrator. Depois, insira e confirme uma senha para a abertura do certificado. Toque ou clique em Next.

8. Toque ou clique em Browse. Utilize a caixa de diálogo oferecida para especificar um local para o arquivo do certificado e toque ou clique em Save. Certifique-se de que o local é seguro para não comprometer a segurança do sistema. O arquivo é salvo com a extensão .pfx.
9. Toque ou clique em Next e em Finish. Se o processo de exportação for bem-sucedido, você verá uma caixa de mensagem com a confirmação. Toque ou clique em OK para fechar a caixa de mensagem.

Restauração de certificados de criptografia

Quando se tem o backup de um certificado, é possível restaurar o certificado para qualquer computador na rede e não apenas para o computador de origem. Na verdade, o processo de backup e restauração é a forma como os certificados são movidos de um computador para outro.

Para restaurar um certificado pessoal, siga estas etapas:

1. Copie o arquivo Personal Information Exchange (.pfx) para uma mídia removível, como uma unidade flash ou um disquete, e depois faça logon como usuário no computador em que deseja utilizar o certificado pessoal.
- OBSERVAÇÃO** Faça logon no computador de destino como o usuário do qual você está restaurando o certificado. Caso contrário, o usuário não conseguirá trabalhar com os seus dados criptografados.
2. Acesse o snap-in Certificates para My User Account, como foi descrito anteriormente.
 3. Expanda Certificates—Current User e pressione e mantenha pressionado ou clique com o botão direito do mouse em Personal. Toque ou clique em All Tasks e depois em Import. Isso inicia o Certificate Import Wizard.
 4. Toque ou clique em Next e insira a mídia removível.
 5. Toque ou clique em Browse. Na caixa de diálogo Open, localize o certificado pessoal na mídia removível. Certifique-se de selecionar Personal Information Exchange como o tipo de arquivo. Tendo localizado o arquivo, selecione-o e toque ou clique em Open.
 6. Toque ou clique em Next. Insira a senha para o certificado pessoal e toque ou clique em Next novamente.
 7. O certificado se encontra no armazenamento Personal por padrão. Toque ou clique em Next para aceitar o padrão. Toque ou clique em Finish. Se o processo de importação for bem-sucedido, você verá uma caixa de mensagem com a confirmação. Toque ou clique em OK.

PARTE IV

Administração de rede do Windows Server 2012

CAPÍTULO 14 Gerenciamento de redes TCP/IP **555**

CAPÍTULO 15 Como executar clientes e servidores DHCP **569**

CAPÍTULO 16 Otimização do DNS **610**

CAPÍTULO 14

Gerenciamento de redes

TCP/IP

- Como navegar por redes por meio do Windows Server 2012 **555**
- Como gerenciar redes no Windows 8 e no Windows Server 2012 **558**
- Como instalar redes TCP/IP **561**
- Como configurar redes TCP/IP **562**
- Como gerenciar conexões de rede **567**

Como administrador, é possível habilitar os computadores da rede para comunicarem-se por meio dos protocolos de rede básicos inclusos no Microsoft Windows Server 2012. O protocolo principal para isso é o TCP/IP. O TCP/IP é um pacote de protocolos e serviços usado para a comunicação dentro de uma rede e é o protocolo principal usado para a comunicação entre redes. Comparado às etapas de configuração de outros protocolos de rede, a configuração do TCP/IP é um tanto complicada; porém, o TCP/IP é o protocolo mais versátil disponível.

OBSERVAÇÃO As configurações da Group Policy afetam a permissão que você tem para instalar e gerenciar redes TCP/IP. As principais políticas que você deve analisar estão em User Configuration\Administrative Templates\Network\Network Connections e em Computer Configuration\Administrative Templates\System\Group Policy. A Group Policy é discutida no Capítulo 4 “Automatização de tarefas administrativas, políticas e procedimentos”.

Como navegar por redes por meio do Windows Server 2012

O Windows Server 2012 possui um conjunto abrangente de ferramentas de rede:

- **Network Explorer** Fornece um console central para pesquisas em computadores e dispositivos na rede
- **Network And Sharing Center** Fornece um console central para visualização e gerenciamento das configurações de rede e compartilhamento de um computador
- **Network Diagnostics** Fornece diagnósticos automáticos para ajudar a diagnosticar e resolver problemas de rede

Antes de descrever como essas ferramentas de rede são utilizadas, mostrarei os seguintes recursos do Windows Server 2012 com os quais essas ferramentas contam:

- **Network Discovery (Descoberta de Rede)** Recurso do Windows Server 2012 que controla a possibilidade de visualizar outros computadores e dispositivos
- **Network Awareness (Reconhecimento de Rede)** Recurso do Windows Server 2012 que reporta alterações na conectividade e configurações da rede

MUNDO REAL Computadores com Windows Vista SP1 ou mais recente, assim como versões mais recentes do Windows, dão suporte a extensões do reconhecimento de rede. Essas extensões permitem que um computador conectado a uma ou mais redes por meio de duas ou mais interfaces (independentemente de serem com ou sem fio) selecione a rota com melhor desempenho para uma transferência de dados específica. Como parte do processo de seleção da melhor rota, o Windows escolhe a melhor interface (com ou sem fio) para a transferência. Esse mecanismo intensifica a seleção de redes sem fio em relação às com fio quando ambas as interfaces estiverem presentes.

As configurações de descoberta de rede do computador com o qual você estiver trabalhando determinam os computadores e dispositivos que você pode pesquisar e visualizar nas ferramentas de rede do Windows Server 2012. As configurações de descoberta trabalham juntamente com as configurações do Windows Firewall de um computador para bloquearem ou permitirem o seguinte:

- Descoberta de computadores e dispositivos da rede
- Descoberta do seu computador por outros computadores

As configurações de descoberta de rede pretendem fornecer o nível adequado de segurança para cada uma das diversas categorias de rede às quais um computador pode conectar-se. Veja as três categorias definidas:

- **Domain network** Designa a rede na qual os computadores estão conectados ao domínio corporativo do qual fazem parte
- **Private network** Designa a rede na qual os computadores são configurados como membros de um grupo doméstico ou de trabalho e não estão conectados diretamente à Internet pública
- **Public network** Designa a rede na qual os computadores estão conectados a uma rede em um local público, como restaurantes ou aeroportos, e não a uma rede interna

Como o computador salva configurações separadamente para cada categoria de rede, diferentes configurações de bloqueio e permissão podem ser utilizadas para cada categoria de rede. Ao conectar o adaptador de rede de um computador a uma rede pela primeira vez, o Windows define a categoria de rede baseando-se nas configurações do computador. Baseado na categoria de rede, o Windows Server 2012 define automaticamente as configurações que ativam e desativam a opção de descoberta. O estado On (Ativado) significa que

- O computador pode descobrir outros computadores e dispositivos na rede.
- Outros computadores da rede podem descobrir o computador.

O estado Off (Desativado) significa que

- O computador não pode descobrir outros computadores e dispositivos na rede.
- Outros computadores da rede não podem descobrir o computador.

Normalmente, um adaptador de rede é configurado como público antes de você adicionar um computador ao domínio. O Network Explorer, mostrado na Figura 14-1, exibe uma lista de computadores e dispositivos descobertos na rede. Para acessar o Network Explorer, toque ou clique em File Explorer na tela Iniciar. No File Explorer, toque ou clique no botão para seleção de caminho de local e toque ou clique em Network.

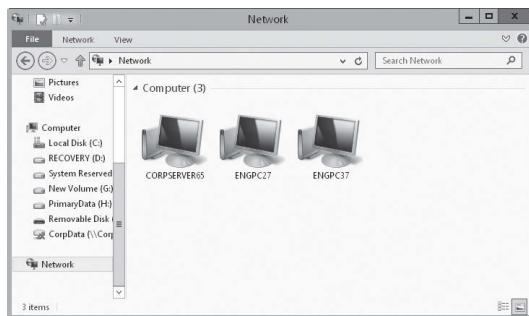


FIGURA 14-1 Use o Network Explorer para pesquisar recursos de rede.

Os computadores e dispositivos listados no Network Explorer dependem das configurações de descoberta de rede do computador, do sistema operacional e do computador ser ou não membro de um domínio. Se a descoberta estiver bloqueada e um servidor com Windows Server 2012 não for membro de um domínio, aparecerá um aviso com essa informação. Ao tocar ou clicar na mensagem de aviso e selecionar Turn On Network Discovery And File Sharing, você habilitará a descoberta de rede, o compartilhamento de arquivos e o compartilhamento de impressoras. Além disso, as portas relacionadas do Windows Firewall também serão abertas.

O Network And Sharing Center, mostrado na Figura 14-2, informa o estado atual da rede, assim como disponibiliza uma visão geral das configurações atuais da rede. Em Control Panel, é possível acessar o Network And Sharing Center tocando ou clicando em View Network Status And Tasks sob Network And Internet.

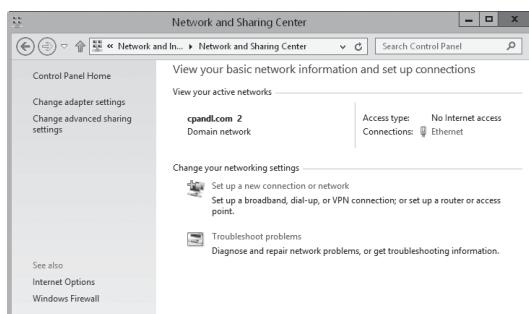


FIGURA 14-2 Visualize e gerencie as configurações de rede com o Network And Sharing Center.

O Network And Sharing Center disponibiliza uma visão geral da rede. O termo abaixo do nome da rede mostra a categoria da rede atual como Domain Network, Private Network ou Public Network. A caixa Access Type especifica se e como o computador está conectado à rede atual. Os termos para essa opção são No Network Access, No Internet Access ou Internet. Ao tocar ou clicar no nome de uma conexão de rede, é possível exibir a caixa de diálogo de status dessa rede.

Ao tocar ou clicar em Change Adapter Settings, a página Network Connections será exibida e pode ser utilizada para gerenciar as conexões de rede. Ao tocar ou clicar em Change Advanced Sharing Settings, aparecerão opções para alterar as configurações de compartilhamento e descoberta do computador para cada perfil de rede. Para gerenciar um perfil, expanda o painel de visualização do perfil tocando ou clicando no botão Expand (aquele com a seta para baixo), então toque ou clique nas configurações desejadas e depois em Save Changes. Para ativar ou desativar a descoberta de rede, toque ou clique em Turn On Network Discovery ou Turn Off Network Discovery conforme desejado e depois em Save Changes.

A partir do Network And Sharing Center, pode-se tentar diagnosticar um problema de rede. Para isso, toque ou clique em Troubleshoot Problems e depois em uma solução de problemas (troubleshooter) para executá-la (como Incoming Connections ou Network Adapter); siga as instruções. O Windows Network Diagnostics tentará identificar o problema da rede e fornecer uma solução possível.

Como gerenciar redes no Windows 8 e no Windows Server 2012

Em Group Policy, há políticas de gerenciamento de rede para redes com fio (IEEE 802.3) e redes sem fio (IEEE 802.11) sob Computer Configuration\Windows Settings\ Security Settings. Apenas uma política com fio e uma política sem fio podem ser criadas e aplicadas por vez. Ou seja, é possível estabelecer uma política com fio e uma sem fio para computadores com Windows Vista ou versão mais recente do Windows. Também é possível criar uma política sem fio para computadores com Windows XP.

Ao pressionar e manter pressionado ou clicar com o botão direito do mouse no nó Wired Network (IEEE 802.3), é possível criar uma política para o Windows Vista e versões mais recentes que especifique se o serviço de configuração automática de rede (Wire AutoConfig) será ou não utilizado para configurar e conectar esses clientes às redes Ethernet com fio 802.3. Para o Windows 7 e versões mais recentes do Windows, há opções para impedir o compartilhamento de credenciais do usuário e para especificar se deseja ou não proibir que os computadores façam tentativas de conexão automática à rede por um período de tempo especificado.

Ao pressionar e manter pressionado ou clicar com o botão direito do mouse no nó Wireless Network (IEEE 802.11), é possível criar políticas diferentes para computadores com Windows XP e computadores com versões mais recentes que possibilitem a configuração automática de WLAN, também é possível especificar as redes que podem ser utilizadas e definir as permissões de rede. Para o Windows 7 e versões mais recentes do Windows, há opções para impedir o compartilhamento de credenciais do usuário, para especificar se deseja ou não proibir que os computadores façam tentativas de conexão automática à rede por um período de tempo especificado e para impedir o uso de redes hospedadas.

O Windows Vista SP1 e versões mais recentes do Windows dão suporte a diversas melhorias para as redes com e sem fio. Essas alterações possibilitam que os usuários mudem suas senhas ao conectarem-se a uma rede com ou sem fio (em oposição a utilizar o recurso Winlogon para mudança de senha), corrijam uma senha incorreta inserida durante o logon e redefinam uma senha expirada; tudo como parte do processo de logon de rede.

As melhorias na segurança de rede incluem o seguinte:

- Secure Socket Tunneling Protocol (SSTP)
- Secure Remote Access (SRA)
- CryptoAPI Version 2 (CAPI2)
- Extensões do Online Certificate Status Protocol (OCSP)
- Preservação de porta para Teredo
- Assinatura de arquivo para Remote Desktop Protocol (RDP)

O protocolo SSTP possibilita a transmissão de dados na camada de link de dados por meio de um Hypertext Transfer Protocol sobre uma conexão Secure Sockets Layer (HTTPS). O SRA possibilita acesso seguro a redes remotas através de HTTPS. Em conjunto, essas tecnologias permitem que o usuário acesse uma rede privada com segurança utilizando uma conexão com a Internet. O SSTP e o SRA representam melhorias em relação aos protocolos Point-to-Point Tunneling Protocol (PPTP) e Layer Two Tunneling Protocol/Internet Protocol Security (L2TP/IPsec) porque utilizam as portas TCP/IP padrão para tráfego seguro na Web, e isso possibilita que eles atravessem a maioria dos firewalls, Network Address Translation (NAT) e proxies Web.

O SSTP utiliza o HTTP sobre SSL, que também é conhecido como Transport Layer Security (TLS). HTTP sobre SSL (porta TCP 443) é normalmente utilizado para proteger a comunicação entre sites. Sempre que os usuários conectam-se a um endereço Web que comece por *https://*, estão utilizando HTTP sobre SSL. Utilizar HTTP sobre SSL soluciona muitos dos problemas de conectividade da virtual private network (VPN, rede virtual privada). Como o SSTP dá suporte tanto a IPv4 quanto a IPv6, os usuários podem estabelecer túneis seguros usando qualquer uma dessas tecnologias de IP. Essencialmente, você obtém uma tecnologia VPN que funciona em qualquer lugar, fazendo com que você receba muito menos chamadas de suporte.

O CAPI2 estende suporte para a infraestrutura de chave pública (PKI, public key infrastructure) e para certificados X.509 e implementa uma funcionalidade adicional para validação de caminhos de certificados, repositório de certificados e verificação de assinatura. Uma das etapas da validação de caminho de certificado é a verificação de revogação, que envolve verificar o estado do certificado para garantir que ele não tenha sido revogado por seu emissor; é aqui que entra o Online Certificate Status Protocol (OCSP).

O OCSP é utilizado para verificar o estado de revogação dos certificados. O CAPI2 também dá suporte a cadeias de signatários OCSP independentes e à especificação de localizações adicionais de download OCSP com base em emissores individuais. Cadeias de signatários OCSP independentes modificam a implementação original do OCSP para que o OCSP funcione com respostas OCSP assinadas por signatários OCSP confiáveis que sejam separados do emissor do certificado que está sendo validado. Locais adicionais de download OCSP permitem especificar localizações de download OCSP para entidades emissoras de certificados (issuing CAs) como URLs que são adicionadas como propriedades ao certificado CA.

Para garantir a coexistência do IPv4 e do IPv6, o Windows permite que os aplicativos utilizem o IPv6 em uma rede IPv4 e também dá suporte a tecnologias relacionadas, como a preservação de portas para Teredo. O Teredo é uma tecnologia de encapsulamento baseada no User Datagram Protocol (protocolo UDP) que pode percorrer NATs. Esse recurso possibilita a comunicação Teredo entre NATs simétricas pela preservação de portas e outros tipos de NATs. Uma NAT é preservadora de portas se escolher utilizar o mesmo número de porta externo que o número de porta interno.

Versões atuais do Windows Server dão suporte ao descarregamento TCP Chimney. Esse recurso permite que o subsistema de rede transfira o processamento de uma conexão TCP/IP do processador de um servidor para seus adaptadores de rede, contanto que os adaptadores de rede suportem o processamento de TCP/IP offloading. Tanto conexões TCP/IPv4 quanto conexões TCP/IPv6 podem ser descarregadas. Por padrão, conexões TCP são descarregadas em adaptadores de rede de 10 gigabits por segundo (Gbps), mas não são descarregadas em adaptadores de rede de 1 Gbps. Para modificar essas configurações, utilize o Netsh.

A Network Diagnostic Framework (NDF, Estrutura de Diagnóstico de Rede) simplifica a solução de problemas da rede automatizando muitas etapas e soluções comuns de resolução de problemas. Ao executar o Windows Network Diagnostics, cada sessão de diagnóstico gera um relatório com os resultados do diagnóstico, e é possível visualizar essas informações no Action Center tocando ou clicando no link Troubleshooting e depois em View History. Na página Troubleshooting History, cada sessão de diagnóstico é listada por tipo e data de execução. Para informações mais detalhadas, selecione a sessão desejada e toque ou clique em View Details.

As informações de diagnóstico mostradas no Action Center provêm de um arquivo Event Trace Log (ETL, Log de Rastreamento de Eventos) criado como parte do diagnóstico. Se pressionar e manter pressionado ou clicar com o botão direito do mouse em uma sessão de diagnóstico e então selecionar Open File Location, verá os arquivos gerados como parte do diagnóstico para a sessão de diagnóstico selecionada.

Você pode utilizar o contexto Netsh Trace para realizar um rastreamento completo, assim como uma captura de pacote de rede e filtragem. Para realizar o rastreamento, são utilizados cenários e provedores predefinidos ou personalizados. Um cenário de rastreamento é uma coleção de provedores. Os provedores são os componentes na pilha de protocolo de rede com os quais você quer trabalhar, como TCP/IP, Windows Filtering Platform e Firewall, Wireless LAN Services, Winsock e NDIS. Normalmente, o Network Monitor (Netmon) é utilizado para analisar dados de rastreamento. Se você coletar dados de rastreamento em um computador no qual o Netmon não esteja instalado, pode simplesmente copiar o arquivo de rastreamento para um computador em que o Netmon esteja instalado, possibilitando a análise dos dados.

O Windows Vista SP1 e versões mais recentes do Windows utilizam um cliente compatível RDP 6.1 ou mais recente. Assim, arquivos RDP podem ser assinados digitalmente para impedir que os usuários abram ou executem arquivos RDP perigosos de fontes desconhecidas. Os administradores podem assinar arquivos RDP utilizando uma ferramenta de assinatura fornecida pela Microsoft. Três elementos relacionados podem ser configurados por meio da Group Policy ou por meio de edição do registro. Eles incluem uma lista de hashes de certificados separados por vírgula nos quais o administrador confia (conhecida como *lista de fornecedores confiáveis*), uma opção para permitir que os usuários decidam aceitar fornecedores não confiáveis (ativada por padrão) e uma opção para permitir que os usuários aceitem arquivos sem assinatura (ativada por padrão).

Como instalar redes TCP/IP

Para instalar uma rede em um computador, você deve instalar o protocolo de rede TCP/IP e um adaptador de rede. O Windows Server 2012 utiliza o TCP/IP como o protocolo padrão de rede de longa distância (WAN). Normalmente, instala-se o protocolo durante a instalação do Windows Server 2012. Você também pode instalar o protocolo TCP/IP por meio das propriedades de conexão de rede.

Para instalar o TCP/IP após instalar o Windows Server 2012, efetue o logon no computador utilizando uma conta com privilégios de administrador e siga estas etapas:

1. Em Control Panel, acesse o Network And Sharing Center tocando ou clicando em View Network Status And Tasks sob Network And Internet.
2. No Network And Sharing Center, toque ou clique em Change Adapter Settings.
3. Em Network Connections, pressione e mantenha pressionado ou clique com o botão direito do mouse na conexão com a qual deseja trabalhar, depois toque ou clique em Properties. A caixa de diálogo Ethernet Properties para a conexão é exibida, como mostra a Figura 14-3.

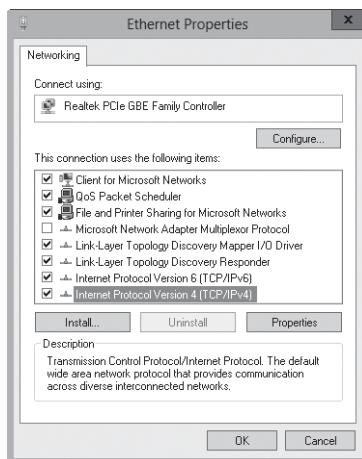


FIGURA 14-3 Instale e configure protocolo TCP/IP.

4. Se o Internet Protocol Version 6 (TCP/IPv6), o Internet Protocol Version 4 (TCP/IPv4) ou ambos não estiverem na lista de componentes instalados, é preciso instalá-los. Toque ou clique em Install. Toque ou clique em Protocol, depois em Add. Na caixa de diálogo Select Network Protocol, selecione o protocolo que deseja instalar e toque ou clique em OK. Se estiver instalando tanto o TCP/IPv6 quanto o TCP/IPv4, repita essa etapa para cada protocolo.

5. Na caixa de diálogo Properties para a conexão de rede, certifique-se de que o TCP/IPv6, o TCP/IPv4 ou ambos estão selecionados, então toque ou clique em OK.
6. Conforme necessário, siga as instruções na seção seguinte para configurar as conexões de rede do computador.

Como configurar redes TCP/IP

Uma conexão de rede é criada automaticamente se um computador possui um adaptador de rede e é conectado a uma rede. Se um computador possui mais de um adaptador de rede e for conectado a uma rede, uma conexão de rede é criada para cada adaptador. Se não houver conexão de rede disponível, é preciso conectar o computador à rede para criar um tipo diferente de conexão.

Os computadores utilizam endereços IP para comunicarem-se por meio do TCP/IP. O Windows Server 2012 disponibiliza as seguintes formas de configurar endereços IP:

- **Manualmente** Endereços IP atribuídos manualmente são chamados de *endereços IP estáticos*. Endereços IP estáticos são fixos e não mudam a menos que você altere-os. Geralmente, você atribui endereços IP estáticos a servidores Windows, e quando faz isso, precisa configurar informações adicionais para ajudar o servidor a navegar pela rede.
- **Dinamicamente** Um servidor DHCP (caso um esteja instalado na rede) atribui endereços IP dinâmicos durante a inicialização, e os endereços podem mudar com o tempo. O endereçamento IP dinâmico é a configuração padrão.
- **Endereços alternativos (somente IPv4)** Quando um computador é configurado para utilizar DHCPv4 e não houver servidor DHCPv4 disponível, o Windows Server 2012 atribuirá um endereço IP privado alternativo automaticamente. Por padrão, o endereço IPv4 alternativo encontra-se entre 169.254.0.1 e 169.254.255.254 com uma máscara de sub-rede de 255.255.0.0. Você também pode especificar um endereço IPv4 alternativo configurado manualmente, que é útil especialmente para usuários de laptops.

Como configurar endereços IP estáticos

Quando você atribui um endereço IP estático, precisa informar ao computador o endereço IP que deseja utilizar, a máscara de sub-rede para esse endereço IP e, se necessário, o gateway padrão a utilizar em comunicações entre redes. Um endereço IP é um identificador numérico de um computador. Esquemas de endereçamento IP variam de acordo com a forma como sua rede foi configurada, mas normalmente são atribuídos baseados em um segmento de rede particular.

Endereços IPv6 e endereços IPv4 são bastante diferentes. Com IPv6, os primeiros 64 bits representam o ID de rede e os últimos 64 bits representam a interface de rede. Com IPv4, um número variável de bits iniciais representa o ID de rede e o resto dos bits representam o ID do host. Por exemplo, se estiver trabalhando com IPv4 e um computador no segmento de rede 10.0.10.0 com uma máscara de sub-rede de 255.255.255.0, os primeiros três octetos (grupos de 8 bits) representam o ID de rede, e o intervalo de endereços disponível para hosts de computador é de 10.0.10.1 a 10.0.10.254. Nesse intervalo, o endereço 10.0.10.255 é reservado para difusões de rede.

Se estiver em uma rede privada que está indiretamente conectada à Internet, você deve utilizar endereços IPv4 privados. A Tabela 14-1 resume os endereços IPv4 de rede privada.

TABELA 14-1 Endereçamento IPv4 de rede privada

ID DE REDE PRIVADA	MÁSCARA DE SUB-REDE	INTERVALO DE ENDEREÇO DE REDE
10.0.0.0	255.0.0.0	10.0.0.0–10.255.255.255
172.16.0.0	255.240.0.0	172.16.0.0–172.31.255.255
192.168.0.0	255.255.0.0	192.168.0.0–192.168.255.255

Todos os outros endereços IPv4 de rede são públicos e devem ser locados ou comprados. Se a rede estiver conectada diretamente à Internet e você tiver obtido um intervalo de endereços IPv4 do seu provedor de serviços de Internet, pode utilizar os endereços IPv4 atribuídos a você.

Como utilizar o comando *ping* para verificar um endereço

Antes de atribuir um endereço IP estático, é preciso certificar-se de que o endereço não esteja em uso ou reservado para uso com DHCP. Com o comando *ping*, é possível verificar se um endereço está em uso. Abra um prompt de comando e digite **ping**, seguido pelo endereço IP desejado.

Para testar o endereço IPv4 10.0.10.12, utilizaria-se o seguinte comando:

```
ping 10.0.10.12
```

Para testar o endereço IPv6 FEC0::02BC:FF:BECB:FE4F:961D, utilizaria-se o seguinte comando:

```
ping FEC0::02BC:FF:BECB:FE4F:961D
```

Se o teste de ping der uma resposta de êxito, o endereço IP está em uso e é preciso tentar outro endereço. Se a solicitação chegar ao tempo limite para as quatro tentativas de ping, o endereço IP não está ativo na rede nesse momento e provavelmente não está em uso. Entretanto, um firewall pode estar bloqueando sua solicitação de ping. O administrador de rede de sua empresa também pode confirmar se um endereço IP está em uso.

Como configurar um endereço IPv4 ou IPv6 estático

Uma conexão de rede local (LAN) é disponibilizada para cada adaptador de rede instalado. Essas conexões são criadas automaticamente. Para configurar endereços IP estáticos para uma conexão específica, siga estas etapas:

1. No Network And Sharing Center, toque ou clique em Change Adapter Settings. Em Network Connections, pressione e mantenha pressionado ou clique com o botão direito do mouse na conexão com a qual deseja trabalhar, depois toque ou clique em Properties.
2. Toque ou clique duas vezes em Internet Protocol Version 6 (TCP/IPv6) ou em Internet Protocol Version 4 (TCP/IPv4) de acordo com o tipo de endereço IP que estiver configurando.

3. Para endereços IPv6, faça o seguinte:

- Toque ou clique em Use The Following IPv6 Address, e digite o endereço IPv6 na caixa de texto IPv6 Address. O endereço IPv6 atribuído ao computador não pode estar em uso em qualquer outra parte da rede.
- A opção Subnet Prefix Length garante que o computador comunique-se adequadamente por meio da rede. O Windows Server 2012 deve inserir um valor padrão para o prefixo de sub-rede na caixa de texto Subnet Prefix Length. Se a rede não utilizar sub-redes de comprimentos variáveis, o valor padrão deve ser o suficiente, mas se a rede utilizar sub-redes de comprimentos variáveis, é preciso alterar esse valor conforme adequado para a sua rede.

4. Para endereços IPv4, faça o seguinte:

- Toque ou clique em Use The Following IPv4 Address, e digite o endereço IPv4 na caixa de texto IPv4 Address. O endereço IPv4 atribuído ao computador não pode estar em uso em qualquer outra parte da rede.
- A opção Subnet Mask garante que o computador comunique-se adequadamente por meio da rede. O Windows Server 2012 deve inserir um valor padrão para a máscara de sub-rede na caixa de texto Subnet Mask. Se a rede não utilizar sub-redes de comprimentos variáveis, o valor padrão deve ser o suficiente, mas se a rede utilizar sub-redes de comprimentos variáveis, é preciso alterar esse valor conforme adequado para a sua rede.

5. Se o computador precisar de acesso a outras redes TCP/IP, à Internet ou a outras sub-redes, é preciso especificar um gateway padrão. Digite o endereço IP do roteador padrão da rede na caixa de texto Default Gateway.

6. O Domain Name System (DNS) é necessário para a resolução de nomes de domínio. Digite um endereço preferencial e um endereço alternativo para o servidor DNS nas caixas de texto fornecidas.

7. Quando tiver terminado, toque ou clique em OK duas vezes. Repita esse processo para os outros adaptadores de rede e protocolos IP que deseja configurar.

8. Com o endereçamento IPv4, configure o WINS conforme necessário.

Como configurar endereços IP dinâmicos e endereçamento IP alternativo

Embora a maioria dos servidores possuam endereços IP estáticos, é possível configurar os servidores para que utilizem o endereçamento dinâmico, endereçamento IP alternativo ou ambos. Para configurar o endereçamento dinâmico e alternativo, siga estas etapas:

- 1.** No Network And Sharing Center, toque ou clique em Change Adapter Settings. Em Network Connections, uma conexão LAN é mostrada para cada adaptador de rede instalado. Essas conexões são criadas automaticamente. Se você não visualizar uma conexão LAN para um adaptador instalado, verifique o driver do adaptador na unidade. Talvez esteja instalado incorretamente. Pressione e mantenha pressionado ou clique com o botão direito do mouse na conexão com a qual deseja trabalhar e toque ou clique em Properties.

2. Toque ou clique duas vezes em Internet Protocol Version 6 (TCP/IPv6) ou em Internet Protocol Version 4 (TCP/IPv4) de acordo com o tipo de endereço IP que estiver configurando.
3. Selecione Obtain An IPv6 Address Automatically (Obter um endereço IPv6 automaticamente) ou Obtain An IP Address Automatically (Obter um endereço IP automaticamente) conforme apropriado para o tipo de endereço IP que está configurando. Você pode selecionar Obtain DNS Server Address Automatically (Obter o endereço dos servidores DNS automaticamente), ou pode selecionar Use The Following DNS Server Addresses (Usar os seguintes endereços de servidor DNS) e então digitar um endereço de servidor DNS preferencial e um alternativo nas caixas de texto fornecidas.
4. Quando utiliza o endereçamento IPv4 dinâmico, você pode configurar um endereço alternativo automático ou configurar manualmente um endereço alternativo. Para utilizar uma configuração automática, na guia Alternate Configuration, selecione Automatic Private IP Address. Toque ou clique em OK, depois em Close e então pule a última etapa.
5. Para utilizar uma configuração manual, na guia Alternate Configuration, selecione User Configured e digite na caixa de texto IP Address o endereço IP que deseja utilizar. O endereço IP que atribuir ao computador deve ser um endereço IP privado, como mostrado anteriormente na Tabela 14-1, e não pode estar em uso em qualquer outra parte da rede quando as configurações forem aplicadas. Conclua a configuração alternativa definindo as configurações de máscara de sub-rede, gateway padrão, servidor DNS e WINS. Quando tiver terminado, toque ou clique em OK e em Close.

Como configurar múltiplos gateways

Para fornecer tolerância a falhas no caso de ocorrer uma interrupção no roteador, você pode configurar computadores com Windows Server 2012 de forma que eles usem múltiplos gateways padrão. Quando você atribui múltiplos gateways, o Windows Server 2012 utiliza uma métrica de gateway para definir qual gateway será utilizado em cada momento. A métrica de gateway indica o custo de roteamento para a utilização de cada gateway. O gateway com o menor custo de roteamento, ou métrica, é usado primeiro. Se o computador não conseguir se comunicar com esse gateway, o Windows Server tentará utilizar o próximo gateway com métrica mais baixa.

A melhor maneira de configurar múltiplos gateways depende da configuração de sua rede. Se os computadores de sua empresa utilizam DHCP, provavelmente você desejará configurar os gateways adicionais por meio de configurações no servidor DHCP. Se os computadores utilizarem endereços IP estáticos ou se você quiser configurar os gateways separadamente, atribua-os seguindo estas etapas:

1. No Network And Sharing Center, toque ou clique em Change Adapter Settings. Em Network Connections, pressione e mantenha pressionado ou clique com o botão direito do mouse na conexão com a qual deseja trabalhar, depois toque ou clique em Properties.
2. Toque ou clique duas vezes em Internet Protocol Version 6 (TCP/IPv6) ou em Internet Protocol Version 4 (TCP/IPv4) de acordo com o tipo de endereço IP que estiver configurando.

3. Toque ou clique em Advanced para abrir a caixa de diálogo Advanced TCP/IP Settings, mostrada na Figura 14-4.

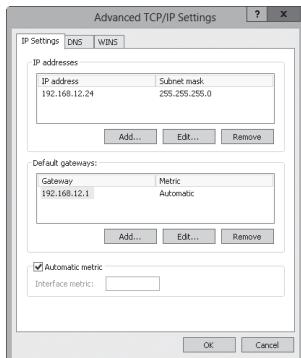


FIGURA 14-4 Configure múltiplos endereços IP e gateways na caixa de diálogo Advanced TCP/IP Settings.

4. O painel Default Gateways mostra os gateways atuais que foram configurados manualmente (se houver). Você pode inserir gateways padrão adicionais conforme necessário.
- Toque ou clique em Add e digite o endereço do gateway na caixa de texto Gateway.
 - Por padrão, o Windows Server 2012 atribui automaticamente uma métrica ao gateway. Você também pode atribuir a métrica. Para isso, limpe a caixa de seleção Automatic Metric, insira uma métrica na caixa de texto fornecida e toque ou clique em Add.
 - Repita as etapas a-c para cada gateway que deseja adicionar.
5. Toque ou clique em OK e em Close.

Como configurar a rede para Hyper-V

Após instalar o Hyper-V e criar uma rede virtual externa, seu servidor utilizará um adaptador de rede virtual para conectar-se à rede física. Quando trabalhar com a página Network Connections, você verá o adaptador de rede original e um novo adaptador de rede virtual. O adaptador de rede original não terá nada ligado a ele exceto o Microsoft Virtual Network Switch Protocol, e o adaptador de rede virtual terá todos os protocolos e serviços padrão ligados a ele. O adaptador de rede virtual que aparecer sob Network Connections terá o mesmo nome que o switch de rede virtual com o qual está associado.

OBSERVAÇÃO Como parte da configuração do Hyper-V, você pode criar uma rede virtual interna, o que possibilita a comunicação somente entre o servidor e as máquinas virtuais hospedadas. Essa configuração expõe um adaptador de rede virtual ao servidor físico sem a necessidade de ter um adaptador de rede físico associado a ele. O Hyper-V só associa o serviço de rede virtual a um adaptador de rede físico quando uma rede virtual externa é criada.

Depois disso, quando você instalar o Hyper-V em um servidor e habilitar a rede virtual externa, verá que a comutação (switching) de rede virtual está sendo utilizada. Como mostra a Figura 14-5, o servidor possui uma conexão de rede com o Hyper-V Extensible Virtual Switch Protocol habilitado e com todos os outros componentes de rede não habilitados e uma entrada para um conexão virtual com os principais componentes de rede habilitados e o Hyper-V Extensible Virtual Switch Protocol desabilitado. Essa é a configuração recomendada para garantir uma comunicação apropriada para o servidor e para qualquer máquina virtual hospedada que esteja utilizando a rede. Se essa configuração for alterada, as máquinas virtuais não conseguirão conectar-se à rede externa.

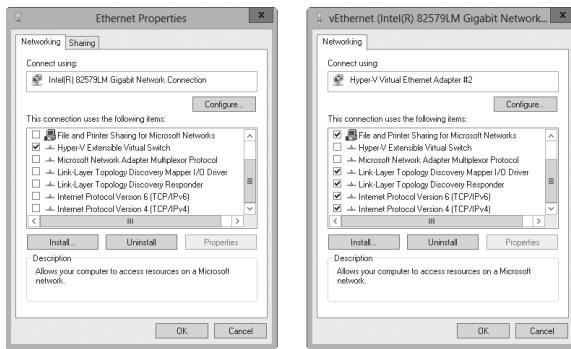


FIGURA 14-5 Use a comutação de rede virtual para garantir a comunicação com máquinas virtuais hospedadas.

Como gerenciar conexões de rede

As conexões de rede possibilitam que os computadores acessem recursos da rede e da Internet. Uma conexão de rede é criada automaticamente para cada adaptador de rede instalado em um computador. Esta seção analisa as possíveis técnicas de gerenciamento dessas conexões.

Como verificar o estado, velocidade e atividade das conexões de rede

Para verificar o estado de uma conexão de rede, siga estas etapas:

1. No Network And Sharing Center, toque ou clique em Change Adapter Settings. Em Network Connections, pressione e mantenha pressionado ou clique com o botão direito do mouse na conexão com a qual deseja trabalhar, depois toque ou clique em Status.
2. A caixa de diálogo Status da conexão de rede será exibida. Se a conexão estiver desabilitada ou se a mídia estiver desconectada, não será possível ter acesso a essa caixa de diálogo. Habilite a conexão ou conecte o cabo de rede para resolver o problema, então tente exibir a caixa de diálogo Status novamente.

Como habilitar e desabilitar conexões de rede

As conexões de rede são criadas e conectadas automaticamente. Se quiser desabilitar a conexão para que ela não seja utilizada, siga estas etapas:

1. No Network And Sharing Center, toque ou clique em Change Adapter Settings. Em Network Connections, pressione e mantenha pressionado ou clique com o botão direito do mouse na conexão, toque ou clique em Disable para desativar a conexão e desabilitá-la.
2. Se quiser habilitar a conexão mais tarde, pressione e mantenha pressionado ou clique com o botão direito do mouse na conexão em Network Connections e toque ou clique em Enable.

Se quiser desconectar-se de uma rede, siga estas etapas:

1. No Network And Sharing Center, toque ou clique em Change Adapter Settings. Em Network Connections, pressione e segure ou clique com o botão direito do mouse na conexão e toque ou clique em Disconnect. Normalmente, somente conexões de acesso remoto possuem uma opção Disconnect.
2. Se quiser ativar a conexão mais tarde, pressione e mantenha pressionado ou clique com o botão direito do mouse na conexão em Network Connections e toque ou clique em Connect.

Como renomear conexões de rede

O Windows Server 2012 inicialmente atribui nomes padrão a conexões de rede. Em Network Connections, você pode renomear uma conexão a qualquer momento pressionando e mantendo pressionada ou clicando com o botão direito do mouse na conexão, tocando ou clicando em Rename e então digitando um novo nome. Se um computador tiver múltiplas conexões de rede, um nome descritivo pode ajudar você e os outros a entender os usos de uma conexão em particular.

CAPÍTULO 15

Como executar clientes e servidores DHCP

- Introdução ao DHCP **569**
- Instalação de servidores DHCP **575**
- Configuração de servidores DHCP **580**
- Gerenciamento dos escopos do DHCP **588**
- Gerenciamento do pool de endereços, das concessões e das reservas **601**
- Como fazer backup e restaurar o banco de dados do DHCP **606**

Você pode usar o protocolo Dynamic Host Configuration Protocol (DHCP) para simplificar a administração de domínios do Active Directory. Neste capítulo, você aprenderá como colocar isso em prática. O DHCP é usado para atribuir dinamicamente informações de configuração TCP/IP a clientes de rede. Além de tornar a configuração do sistema mais rápida, isso também fornece um mecanismo centralizado para atualizar a configuração. Para habilitar o DHCP na rede, é preciso instalar e configurar um servidor DHCP. Esse servidor é responsável por atribuir as informações de rede necessárias.

Introdução ao DHCP

O DHCP fornece controle centralizado sobre o endereçamento IP e outros elementos. Após a instalação do DHCP, você passa a contar com o servidor DHCP para oferecer as informações básicas necessárias para a rede TCP/IP, o que pode incluir: endereço IP, máscara de sub-rede e gateway padrão; servidores Domain Name System (DNS, Sistema de Nomes de Domínio) primários e secundários; servidores Windows Internet Name Service (WINS) primários e secundários; e o nome de domínio DNS. Os servidores DHCP podem atribuir um endereço IP versão 4 (IPv4) dinâmico, um endereço IP versão 6 (IPv6) ou ambos os endereços a qualquer placa de interface de rede (NIC, network interface card) de um computador.

Uso de endereçamento e configuração IPv4 dinâmico

Um computador que usa endereçamento e configuração IPv4 dinâmico é chamado de *cliente DHCPv4*. Quando um cliente DHCPv4 é iniciado, um endereço IPv4 de 32 bits pode ser recuperado de um pool de endereços IPv4 definido no servidor DHCP da rede. O endereço é atribuído ao cliente por um determinado período de tempo conhecido como *concessão*. Quando a concessão tiver decorrido aproximadamente 50%, o cliente tentará renová-la. Se o cliente não conseguir renová-la nesse momento, ele fará uma nova tentativa antes que a concessão expire. Se a tentativa falhar, o cliente tentará entrar em contato com um servidor DHCP alternativo. Os endereços IPv4 que não são renovados, retornam ao pool de endereços. Se o cliente conseguir entrar em

contato com o servidor DHCP, mas o endereço IP atual não puder ser reatribuído, o servidor DHCP atribuirá um novo endereço IPv4 ao cliente.

A disponibilidade de um servidor DHCP não afeta a inicialização ou o logon (na maioria dos casos). Os clientes DHCPv4 poderão ser iniciados e os usuários poderão efetuar logon no computador local mesmo se um servidor DHCP não estiver disponível. Durante a inicialização, o cliente DHCPv4 procura por um servidor DHCP. Se um servidor DHCP estiver disponível, o cliente obterá suas informações de configuração a partir do servidor. Se um servidor DHCP não estiver disponível e a concessão anterior do cliente ainda estiver válida, o cliente executará ping no gateway padrão listado na concessão. Um ping bem-sucedido avisa o cliente que ele está provavelmente na mesma rede em que estava quando a concessão foi emitida, e o cliente continua a usar a concessão como descrito anteriormente. Um ping com falha avisa o cliente que ele pode estar em uma rede diferente. Nesse caso, o cliente usa a autoconfiguração do IPv4. O cliente também usará a autoconfiguração do IPv4 se um servidor DHCP não estiver disponível e a concessão anterior estiver expirada.

A autoconfiguração do IPv4 funciona assim:

1. O computador cliente seleciona um endereço IP da sub-rede classe B 169.254.0.0 reservada para a Microsoft e usa a máscara de sub-rede 255.255.0.0. Antes de usar o endereço IPv4, o cliente realiza um teste com o protocolo Address Resolution Protocol (ARP) para certificar-se de que nenhum outro cliente está usando esse endereço IPv4.
2. Se o endereço IPv4 estiver em uso, o cliente repetirá a etapa 1, testando até dez endereços IPv4 antes de relatar uma falha. Quando um cliente estiver desconectado da rede, o teste do ARP sempre obterá sucesso. Como resultado, o cliente usa o primeiro endereço IPv4 que selecionar.
3. Se o endereço IPv4 estiver disponível, o cliente fará a configuração da NIC com esse endereço. Após, o cliente tentará entrar em contato com o servidor DHCP, enviando uma difusão à rede a cada cinco minutos. Quando o cliente contatar o servidor com sucesso, o cliente obterá uma concessão e fará a reconfiguração da interface de rede.

Como parte de seu planejamento, você precisa considerar quantos servidores DHCP devem estar instalados na rede. Normalmente, é recomendável que permaneçam instalados ao menos dois servidores DHCP em cada segmento de rede física. O Windows Server 2012 inclui failover de DHCP para IPv4. O failover de DHCP permite a alta disponibilidade de serviços de DHCP sincronizando as concessões de endereços IPv4 entre dois servidores DHCP por meio de um dos dois modos a seguir:

- **Load Balance** Quando o balanceamento de carga é feito nos servidores, a porcentagem da carga com que cada servidor deve lidar deve ser especificada. Normalmente, usa-se uma abordagem de 50/50 para que a carga seja dividida igualmente entre cada servidor. Você também pode usar outras abordagens, como 60/40 para fazer com que um servidor ocupe-se de 60% da carga e outro de 40%.
- **Hot Standby** Com a espera ativa, um dos servidores atua como o servidor primário e controla os serviços de DHCP. O outro atua como um servidor em espera para entrar em ação caso o servidor primário falhe ou esgote seus endereços para concessão. Uma porcentagem específica de endereços IP disponíveis é reservada para a espera ativa – 5% por padrão.

A configuração do failover de DHCP é simples, direta e não requer cluster ou qualquer configuração avançada. Para configurar o failover de DHCP, basta completar estas etapas:

1. Instale e configure dois servidores DHCP. Os servidores devem estar na mesma rede física.
2. Crie um escopo DHCPv4 em um dos servidores. Os escopos são pools de endereços IPv4 ou IPv6 que você pode atribuir a clientes por meio de concessões.
3. Quando o outro servidor é estabelecido como um parceiro de failover para o escopo DHCPv4, o escopo é replicado para o parceiro.

Uso de endereçamento e configuração IPv6 dinâmico

Tanto o IPv4 quanto o IPv6 estão disponíveis por padrão quando algum hardware de rede é detectado durante a instalação. Como discutido no Capítulo 1, "Visão geral da administração do Windows Server 2012" e no Capítulo 14, "Gerenciamento de redes TCP/IP", o IPv4 é a versão principal do IP usada na maioria das redes, enquanto o IPv6 é a versão do IP de última geração. O IPv6 usa endereços de 128 bits. Em uma configuração padrão, os primeiros 64 bits representam o ID de rede e os últimos 64 bits representam a interface de rede no computador.

Você pode usar o DHCP para configurar o endereçamento IPv6 de duas maneiras:

- **Modo com informações de estado DHCPv6 (Stateful)** Neste modo, um cliente adquire seu endereço IPv6 e seus parâmetros de configuração da rede por meio do DHCPv6.
- **Modo sem informações de estado DHCPv6 (Stateless)** Neste modo, um cliente usa a autoconfiguração para adquirir seu endereço IP e obtém seus parâmetros de configuração adicionais da rede por meio do DHCPv6.

Um computador que usa endereçamento IPv6 dinâmico, configuração IPv6 dinâmico ou ambos os mecanismos é chamado de *cliente DHCPv6*. Assim como ocorre com o DHCPv4, os componentes da infraestrutura DHCPv6 consistem em clientes DHCPv6 que requerem configuração, servidores DHCPv6 que fornecem configuração e agentes de retransmissão DHCPv6 que transmitem mensagens entre clientes e servidores quando os clientes estão em sub-redes que não possuem um servidor DHCPv6.

Diferentemente do DHCPv4, você também deve configurar seus roteadores IPv6 para comportarem DHCPv6. Um cliente DHCPv6 realiza autoconfiguração com base nos sinalizadores da mensagem Router Advertisement enviada por um roteador adjacente. São eles:

- Managed Address Configuration, sinalizador também conhecido como *M flag*. Quando configurado em 1, o sinalizador instrui o cliente a usar um protocolo de configuração para obter endereços com informações de estado.
- Other Stateful Configuration, sinalizador também conhecido como *O flag*. Quando configurado em 1, o sinalizador instrui o cliente a usar um protocolo de configuração para obter outras definições de configuração.

O Windows inclui um cliente DHCPv6. O cliente DHCPv6 tenta uma configuração baseada em DHCPv6 dependendo dos valores do *M flag* e do *O flag* das mensagens Router Advertisement que receber. Se houver mais de um roteador de anúncio para

uma determinada sub-rede, o roteador ou roteadores adicionais devem ser configurados para anunciar os mesmos prefixos de endereço sem informações de estado e os mesmos valores para M flag e O flag. Os clientes IPv6 com Microsoft Windows XP ou Windows Server 2003 não incluem um cliente DHCPv6 e, portanto, ignoram os valores do M flag e do O flag de anúncios de roteador que receberem.

Você pode configurar um roteador IPv6 para definir o M flag como 1 em anúncios de roteador inserindo o comando a seguir em um prompt de comando elevado, no qual *InterfaceName* é o nome real da interface:

```
netsh interface ipv6 set interface InterfaceName managedaddress=enabled
```

Da mesma forma, você pode definir o O flag como 1 em anúncios de roteador inserindo o comando a seguir em um prompt de comando elevado:

```
netsh interface ipv6 set interface InterfaceName otherstateful=enabled
```

Se o nome da interface apresentar espaços, coloque o valor relacionado entre aspas, como mostrado no exemplo a seguir:

```
netsh interface ipv6 set interface "Wired Ethernet Connection 2"  
managedaddress=enabled
```

Ao trabalhar com M flags e O flags, lembre-se do seguinte:

- Se tanto o M flag quanto o O flag estiverem definidos como 0, será considerado que a rede não tem uma infraestrutura DHCPv6. Os clientes usam anúncios de roteador para endereços não link-local e configuração manual para definir outras configurações.
- Se tanto o M flag quanto o O flag estiverem definidos como 1, o DHCPv6 será usado para endereçamento IP e outras definições de configuração. Essa combinação é conhecida como *modo com informações de estado DHCPv6*, em que o DHCPv6 atribui endereços com informações de estado a clientes IPv6.
- Se o M flag estiver definido como 0 e o O flag como 1, o DHCPv6 será usado apenas para atribuir outras definições de configuração. Os roteadores adjacentes são configurados para anunciar prefixos de endereço não link-local dos quais clientes IPv6 derivam endereços sem informações de estado. Essa combinação é conhecida como *modo sem informações de estado DHCPv6*.
- Se o M flag estiver definido como 1 e o O flag como 0, o DHCPv6 será usado para configuração de endereço IP, mas não para outras configurações. Como os clientes IPv6 normalmente precisam ser configurados com outras definições, como os endereços IPv6 de servidores DNS, essa combinação geralmente não é usada.

O Windows obtém endereços IPv6 dinâmicos por meio de um processo parecido com os endereços IPv4 dinâmicos. Normalmente, a autoconfiguração IPv6 para clientes DHCPv6 em modo com informações de estado opera da seguinte maneira:

1. O computador cliente seleciona um endereço IPv6 unicast link-local. Antes de usar o endereço IPv6, o cliente realiza um teste usando ARP para certificar-se de que nenhum outro cliente está usando esse endereço IPv6.
2. Se o endereço IPv6 estiver em uso, o cliente repete a etapa 1. Lembre-se de que quando um cliente estiver desconectado da rede, o teste usando ARP sempre obtém sucesso. Como resultado, o cliente usa o primeiro endereço IPv6 que selecionar.

3. Se o endereço IPv6 estiver disponível, o cliente fará a configuração da NIC com esse endereço. Após, o cliente tentará entrar em contato com o servidor DHCP, enviando uma difusão à rede a cada cinco minutos. Quando o cliente contatar o servidor com sucesso, o cliente obterá uma concessão e fará a reconfiguração da interface de rede.

No entanto, a autoconfiguração IPv6 não opera dessa forma para clientes DHCPv6 em modo sem informações de estado. No modo sem informações de estado, os clientes DHCPv6 configuram tanto endereços link-local quanto endereços não link-local adicionais trocando mensagens Router Solicitation e Router Advertisement com roteadores adjacentes.

Como o DHCPv4, o DHCPv6 usa mensagens User Datagram Protocol (UDP). Os clientes DHCPv6 ouvem mensagens de DHCP na porta UDP 546. Os servidores e agentes de retransmissão DHCPv6, por sua vez, ouvem mensagens de DHCPv6 na porta UDP 547. A estrutura para mensagens de DHCPv6 é muito mais simples que para DHCPv4, que tinha suas origens no protocolo Bootstrap Protocol (BOOTP) para dar suporte a estações de trabalho sem disco.

As mensagens de DHCPv6 começam com o campo Msg-Type de 1 byte que indica o tipo de mensagem de DHCPv6. Esse campo é seguido pelo campo Transaction-ID de 3 bytes determinado por um cliente e usado para agrupar as mensagens de uma troca de mensagens de DHCPv6. Após o campo Transaction-ID, opções do DHCPv6 são usadas para indicar a identificação de clientes e servidores, endereços e outras definições de configuração.

Três campos são associados com cada opção do DHCPv6. O campo Option-Code de 2 bytes indica uma opção específica. O campo Option-Len de 2 bytes indica o comprimento do campo Option-Data em bytes. O campo Option-Data contém os dados para a opção.

As mensagens trocadas entre agentes de retransmissão e servidores usam uma estrutura de mensagens diferente para transferir informações adicionais. O campo Hop-Count de 1 byte indica o número de agentes de retransmissão que receberam a mensagem. Um agente de retransmissão que receber uma mensagem, pode descartá-la caso ela exceda uma contagem de saltos máxima já configurada. O campo Link-Address de 15 bytes contém um endereço não link-local que é atribuído a uma interface conectada à rede em que o cliente está localizado. Com base no campo Link-Address, o servidor pode determinar o escopo de endereço correto do qual atribuir um endereço. O campo Peer-Address de 15 bytes contém o endereço IPv6 do cliente que originalmente enviou a mensagem ou do agente de retransmissão que retransmitiu a mensagem. Após o campo Peer-Address estão as opções do DHCPv6. Uma opção muito importante é a chamada Relay Message. Essa opção fornece um encapsulamento das mensagens que estão sendo trocadas entre o cliente e o servidor.

O IPv6 não apresenta endereços de difusão. O uso do endereço de difusão limitado para algumas mensagens de DHCPv4 foi substituído pelo uso do endereço All_DHCP_Relay_Agents_and_Servers do FF02::1:2 para o DHCPv6. Um cliente DHCPv6 que está tentando descobrir a localização do servidor DHCPv6 na rede envia uma mensagem *Solicit* a partir de seu endereço link-local para FF02::1:2. Se houver um servidor DHCPv6 na sub-rede do cliente, ele receberá a mensagem *Solicit* e enviará uma resposta apropriada. Se o cliente e o servidor estiverem em sub-redes diferentes, um agente de retransmissão DHCPv6 da sub-rede do cliente que receber a mensagem *Solicit* a encaminhará para um servidor DHCPv6.

Como verificar a atribuição de endereço IP

Você pode usar o comando `Ipconfig` para verificar o endereço IP atualmente atribuído e outras informações de configuração. Para obter informações para todos os adaptadores de rede do computador, digite o comando `ipconfig /all` no prompt de comando. Se o endereço IP tiver sido atribuído automaticamente, você verá uma entrada para Autoconfiguration IP Address. No exemplo a seguir, o endereço IPv4 autoconfigurado é 169.254.98.59:

```
Windows IP Configuration
  Host Name .....: DELTA
  Primary DNS Suffix .....: microsoft.com
  Node Type .....: Hybrid
  IP Routing Enabled.....: No
  WINS Proxy Enabled.....: No
  DNS Suffix Search List.....: microsoft.com
Ethernet adapter Ethernet:
  Connection-specific DNS Suffix...:
  Description .....: Intel Pro/1000 Network Connection
  Physical Address.....: 23-15-C6-F8-FD-67
  DHCP Enabled.....: Yes
  Autoconfiguration Enabled...: Yes
  Autoconfiguration IP Address: 169.254.98.59
  Subnet Mask .....: 255.255.0.0
  Default Gateway .....:
  DNS Servers .....
```

Noções básicas sobre escopos

Os *escopos* são pools de endereços IPv4 ou IPv6 que você pode atribuir a clientes por meio de concessões. O DHCP também fornece uma maneira de atribuir permanentemente uma concessão de endereço. Para isso, é necessário criar uma reserva especificando o endereço IPv4 a ser reservado e o endereço de controle de acesso à mídia (MAC, media access control) do computador que reterá o endereço IPv4. Depois disso, a reserva garantirá que o computador cliente com o endereço MAC especificado sempre obtenha o endereço IPv4 designado. Com o IPv6, você pode determinar se uma concessão é temporária ou permanente. Uma concessão permanente é similar a uma reserva.

Os escopos são criados para especificar os intervalos de endereços IP que estão disponíveis para clientes DHCP. Por exemplo, você poderia atribuir o intervalo de endereços IP 192.168.12.2 a 192.168.12.250 a um escopo chamado Enterprise Primary. Os escopos podem usar endereços IPv4 públicos ou privados nestas redes:

- **Redes classe A** Endereços IP de 1.0.0 a 126.255.255.255
- **Redes classe B** Endereços IP de 128.0.0.0 a 191.255.255.255
- **Redes classe C** Endereços IP de 192.0.0.0 a 223.255.255.255
- **Redes classe D** Endereços IP de 224.0.0.0 a 239.255.255.255

OBSERVAÇÃO O endereço IP 127.0.0.1 é usado para loopback local.

Os escopos também podem usar endereços IPv6 unicast link-local, unicast global e multicast. Os endereços unicast link-local começam com FE80. Os endereços IPv6 multicast começam com FF00. Os endereços unicast global (site-local) incluem todos os outros endereços exceto endereços :: (não especificado) e ::1 (loopback).

Um servidor DHCP único pode gerenciar vários escopos. Com endereços IPv4, estão disponíveis quatro tipos de escopo:

- **Normal** Usado para atribuir pools de endereços IPv4 a redes classe A, B e C.
- **Multicast** Usado para atribuir pools de endereços IP a redes classe D de IPv4. Os computadores usam endereços IP multicast como endereços IP secundários além de um endereço IP padrão.
- **Superescopos** Contêineres para outros escopos. Eles são usados para simplificar o gerenciamento de vários escopos e também dar suporte a clientes DHCP em uma rede física única em que várias redes IP lógicas são usadas.
- **Failover** Escopos divididos entre dois servidores DHCP para aumentar a tolerância a falhas, fornecer redundância e permitir o balanceamento de carga.

Com o IPv6, apenas os escopos normais estão disponíveis. Embora você possa criar escopos em vários segmentos de rede, normalmente é recomendável que esses segmentos estejam na mesma classe de rede, como todos os endereços IP de classe C.

DICA Lembre-se que você deve configurar as retransmissões DHCPv4 e DHCPv6 para retransmitir solicitações de difusão de DHCPv4 e DHCPv6 entre segmentos de rede. Você pode configurar agentes de retransmissão com o Routing and Remote Access Service (RRAS) e o DHCP Relay Agent Service. Também é possível configurar alguns roteadores como agentes de retransmissão.

Instalação de servidores DHCP

O endereçamento IP dinâmico se torna disponível apenas se um servidor DHCP estiver instalado na rede. Com o Add Roles And Features Wizard, você pode instalar o servidor DHCP como um serviço de função, fazer suas configurações iniciais e autorizar o servidor no Active Directory. Somente servidores DHCP autorizados podem fornecer endereços IP dinâmicos a clientes.

Instalação de componentes DHCP

Em um servidor com Windows Server 2012, siga estas etapas para permitir que o servidor opere como um servidor DHCP:

1. Um endereço IPv4 estático e outro IPv6 estático devem ser atribuídos aos servidores DHCP em cada sub-rede para a qual ele prestará serviços e com a qual estiver conectado. Certifique-se de que o servidor tenha endereços IPv4 e IPv6 estáticos.
2. No Server Manager, toque ou clique em Manage e em Add Roles And Features, ou selecione Add Roles And Features no painel Quick Start. O Add Roles And Features Wizard será iniciado. Se o assistente exibir a página Before You Begin, leia o texto Welcome e toque ou clique em Next.

3. Na página Installation Type, a opção Role-Based Or Feature-Based Installation está selecionada por padrão. Toque ou clique em Next.
4. Na página Server Selection, você pode escolher instalar funções e recursos em servidores ou virtual hard disks (VHD, discos rígidos virtuais) em execução. Selecione um servidor do pool de servidores ou do pool de servidores no qual montar um VHD. Se estiver adicionando funções e recursos a um VHD, toque ou clique em Browse e depois use a caixa de diálogo Browse For Virtual Hard Disks para localizá-lo. Quando estiver pronto para prosseguir, toque ou clique em Next.

OBSERVAÇÃO Apenas servidores com Windows Server 2012 e que foram adicionados para gerenciamento no Server Manager constam na lista.

5. Na página Select Roles, selecione DHCP Server. Se recursos adicionais forem necessários para instalar uma função, você verá uma caixa de diálogo adicional. Toque ou clique em Add Features para fechar a caixa de diálogo e adicionar os recursos necessários para a instalação do servidor. Quando estiver pronto para prosseguir, toque ou clique em Next três vezes.
6. Se o servidor em que você quer instalar a função DHCP Server não tiver todos os arquivos de origem binários necessários, o servidor os obterá via Windows Update por padrão ou de uma localização especificada na Group Policy (política de grupo).

OBSERVAÇÃO Também é possível especificar um caminho alternativo para os arquivos de origem necessários. Para isso, clique no link Specify An Alternate Source Path, digite o caminho alternativo na caixa exibida e toque ou clique em OK. Para compartilhamentos de rede, digite o caminho UNC para o compartilhamento, como \\CorpServer82\WinServer2012\. Para imagens montadas do Windows, insira o caminho do WIM com o prefixo WIM: e inclua o índice da imagem a ser usada, como WIM:\\CorpServer82\Win-Server2012\install.wim:4.

7. Após examinar as opções de instalação e salvá-las conforme necessário, toque ou clique em Install para começar o processo de instalação. A página Installation Progress monitora o progresso da instalação. Se fechar o assistente, toque ou clique no ícone Notifications no Server Manager e no link fornecido para reabri-lo.
8. Quando o Setup terminar de instalar a função DHCP Server, a página Installation Progress será atualizada para refletir isso. Examine os detalhes da instalação para se assegurar de que todas as fases da instalação foram concluídas com sucesso.
9. Como informado no painel de tarefas Post-Deployment Configuration, é necessária uma configuração adicional para o servidor DHCP. Toque ou clique no link Complete DHCP Configuration. O DHCP Post-Install Configuration Wizard será iniciado.
10. A página Description informa que os grupos DHCP Administrators e DHCP Users serão criados no domínio para a delegação da administração de DHCP Server. Além disso, se o servidor DHCP tiver ingressado em um domínio, ele será autorizado no Active Directory. Toque ou clique em Next.
11. Na página Authorization, execute uma das opções a seguir para especificar as credenciais a serem usadas na autorização do servidor DHCP no Active Directory:
 - Seu nome de usuário atual é exibido na caixa de texto User Name. Se você possuir privilégios de administrador no domínio do qual o servidor DHCP é membro e desejar usar suas credenciais atuais, toque ou clique em Commit para tentar autorizar o servidor com essas credenciais.

- Se você preferir usar credenciais alternativas ou não conseguir autorizar o servidor com suas credenciais atuais, selecione Use Alternate Credentials e toque ou clique em Specify. Na caixa de diálogo Windows Security, insira o nome de usuário e senha da conta autorizada e toque ou clique em OK. Em seguida, toque ou clique em Commit para tentar autorizar o servidor com essas credenciais.
 - Se você quiser autorizar o servidor DHCP mais tarde, selecione Skip AD Authorization e toque ou clique em Commit. Lembre-se de que nos domínios, somente servidores DHCP autorizados podem fornecer endereços IP dinâmicos a clientes.
12. Quando o assistente terminar a configuração de pós-instalação, examine os detalhes da instalação para garantir que as tarefas tenham sido concluídas com sucesso e toque ou clique em Close.
13. Em seguida, será necessário reiniciar o serviço DHCP Server no servidor DHCP para que os grupos DHCP Administrators e DHCP Users possam ser usados. Para isso, toque ou clique em DHCP no painel esquerdo do Server Manager. Após, no painel principal, no painel Servers, selecione o servidor DHCP. Por fim, no painel Services, pressione e mantenha pressionada ou clique com o botão direito do mouse na entrada do DHCP Server e toque ou clique em Restart Service.
14. Para concluir a instalação, é necessário que você:
- Se o servidor tiver várias placas de rede, analise as associações do servidor e especifique as conexões que o servidor DHCP comporta para prestar serviços aos clientes. Consulte “Configuração das associações de servidor” mais adiante neste capítulo.
 - Configure as opções do servidor para atribuir definições de configuração comuns a clientes DHCPv4, inclusive 003 Router, 006 DNS Servers, 015 DNS Domain Name e 044 WINS/NBNS Servers. Consulte “Configuração das opções de escopo” mais adiante neste capítulo.
 - Configure as opções do servidor para atribuir definições de configuração comuns a clientes DHCPv4 e DHCPv6, inclusive 003 Router, 006 DNS Servers, 015 DNS Domain Name e 044 WINS/NBNS Servers. Consulte “Configuração das opções de escopo” mais adiante neste capítulo.
 - Crie e ative todos os escopos do DHCP que o servidor usará, como discutido em “Criação e gerenciamento de escopos” mais adiante neste capítulo.

Como iniciar e usar o console DHCP

Após instalar um servidor DHCP, o console DHCP é usado para configurar e gerenciar o endereçamento IP dinâmico. No Server Manager, toque ou clique em Tools e em DHCP para abrir o console DHCP. A janela principal do console DHCP é mostrada na Figura 15-1. Como você pode ver, a janela principal é dividida em dois painéis. O painel esquerdo lista os servidores DHCP do domínio de acordo com o fully qualified domain name (FQDN, nome de domínio totalmente qualificado) de cada um. A listagem de um servidor pode ser expandida para mostrar os subnós IPv4 e IPv6. Se expandir os nós IP, você verá as opções e os escopos definidos para a versão de IP relacionada. O painel direito mostra a exibição expandida da seleção atual.

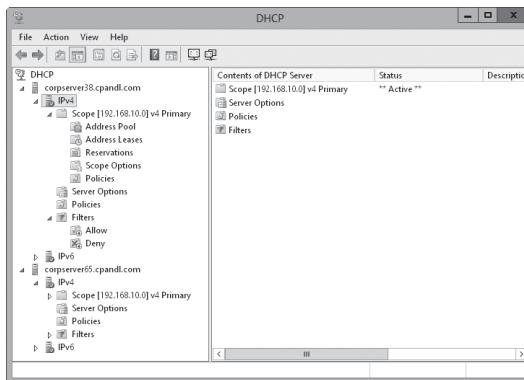


FIGURA 15-1 Use o console DHCP para criar e gerenciar as configurações do servidor DHCP.

Os ícones dos diversos nós mostram o status atual dos nós. Para nós de servidor e IP, talvez os seguintes ícones sejam exibidos:

- Um ícone de servidor com um círculo verde e uma marca de verificação indica que o serviço de DHCP está em execução e o servidor está ativo.
- Um ícone de servidor com um círculo vermelho e um X indica que o console não consegue se conectar ao servidor. O serviço de DHCP foi interrompido ou o servidor está inacessível.
- Uma seta vermelha para baixo indica que o servidor DHCP não foi autorizado.
- Um ícone de aviso azul indica que o estado do servidor foi alterado ou que um aviso foi emitido.

Para escopos, talvez os seguintes ícones sejam exibidos:

- Uma seta vermelha para baixo indica que o escopo não foi ativado.
- Um ícone de aviso azul indica que o estado do escopo foi alterado ou que um aviso foi emitido.

Como se conectar a servidores DHCP remotos

Quando o console DHCP é iniciado, você é diretamente conectado a um servidor DHCP local, mas não verá entradas para servidores DHCP remotos. Para se conectar a servidores remotos, siga estas etapas:

1. Pressione e mantenha pressionado ou clique com o botão direito do mouse em DHCP na árvore de console e toque ou clique em Add Server. A caixa de diálogo mostrada na Figura 15-2 será aberta.
2. Selecione This Server e digite o endereço IP ou o nome do computador do servidor DHCP a ser gerenciado.
3. Toque ou clique em OK. Uma entrada para o servidor DHCP é adicionada à árvore de console.

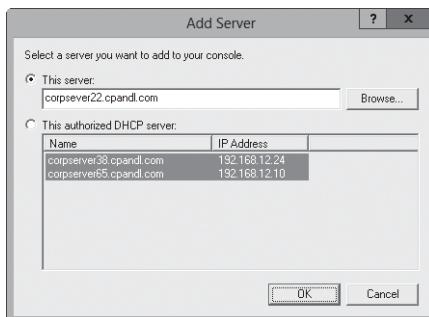


FIGURA 15-2 Se seu servidor DHCP não estiver listado, você precisará adicioná-lo ao console DHCP por meio da caixa de diálogo Add Server.

DICA Ao trabalhar com servidores remotos, talvez certas opções não possam ser selecionadas. Isso pode ser solucionado com uma simples atualização das informações do servidor: pressione e mantenha pressionado ou clique com o botão direito do mouse no nó do servidor e selecione Refresh.

Como iniciar e interromper um servidor DHCP

Os servidores DHCP são gerenciados por meio do serviço DHCP Server. Como com qualquer outro serviço, você pode iniciar, interromper, pausar e retomar o serviço DHCP Server no nó Services do Computer Management ou a partir da linha de comando. Também é possível gerenciar o serviço DHCP Server no console DHCP. Pressione e mantenha pressionado ou clique com o botão direito do mouse no servidor a ser gerenciado no console DHCP, aponte o cursor para All Tasks e toque ou clique em Start, Stop, Pause, Resume ou Restart, conforme apropriado.

OBSERVAÇÃO Você também pode usar o Server Manager para iniciar e interromper um servidor DHCP. Toque ou clique em DHCP no painel esquerdo do Server Manager. Após, no painel principal, no painel Servers, selecione o servidor DHCP. Por fim, no painel Services, pressione e mantenha pressionada ou clique com o botão direito do mouse na entrada de DHCP Server e toque ou clique em Start Service, Stop Service, Pause Service, Resume Service ou Restart Service, conforme apropriado.

Como autorizar um servidor DHCP no Active Directory

Antes de poder usar um servidor DHCP em um domínio, você deve autorizá-lo no Active Directory. Com a autorização do servidor, você especifica que ele está autorizado para fornecer endereçamento IP dinâmico no domínio. O Windows Server 2012 requer autorização para impedir que servidores DHCP não autorizados prestem serviços a clientes do domínio. Isso, por sua vez, garante que as operações de rede sejam executadas sem problemas.

Para autorizar um servidor DHCP no console DHCP, pressione e mantenha pressionada ou clique com o botão direito do mouse na entrada do servidor no modo de exibição de árvore e selecione Authorize. Para remover a autorização, pressione e mantenha pressionado ou clique com o botão direito do mouse no servidor e selecione Unauthorized.

Configuração de servidores DHCP

Após instalar um novo servidor DHCP, você precisa configurá-lo e otimizá-lo para o ambiente de rede. Um conjunto de opções diferente é fornecido para IPv4 e IPv6.

Configuração das associações de servidor

Um servidor com várias NICs tem várias conexões de rede local e pode fornecer serviços de DHCP a qualquer uma dessas conexões de rede. No entanto, talvez você não queira que o DHCP faça ofertas por todas as conexões disponíveis. Por exemplo, se um servidor tiver uma conexão de 100 megabits por segundo (Mbps) e outra de 1 gigabit por segundo (Gbps), talvez você prefira que todo o tráfego DHCP passe pela conexão de 1 Gbps.

Para associar o DHCP a uma conexão específica de rede, siga estas etapas:

1. No console DHCP, pressione e mantenha pressionado ou clique com o botão direito do mouse no servidor com o qual você deseja trabalhar e toque ou clique em Add/Remove Bindings.
2. Selecione a guia IPv4 ou IPv6 conforme apropriado para o tipo de associação com a qual você deseja trabalhar.
3. A caixa de diálogo Bindings exibe uma lista de conexões de rede disponíveis para o servidor DHCP. Se você quiser que o serviço DHCP Server use uma conexão para prestar serviços aos clientes, marque a caixa de seleção dessa conexão. Caso contrário, desmarque a caixa de seleção relacionada. Se não houver conexões de rede listadas para o protocolo com o qual você está trabalhando, certifique-se de que o servidor tenha um endereço estático para esse protocolo.
4. Toque ou clique em OK ao terminar.

Atualização de estatísticas do DHCP

O console DHCP fornece estatísticas relacionadas à disponibilidade e uso de endereços IPv4 e IPv6. Para visualizar essas estatísticas, expanda no console DHCP o nó do servidor com o qual você deseja trabalhar, pressione e mantenha pressionado ou clique com o botão direito do mouse em IPv4 ou IPv6 conforme apropriado para o tipo de endereço a ser usado e toque ou clique em Display Statistics.

Por padrão, essas estatísticas são atualizadas apenas quando você inicia o console DHCP ou seleciona o servidor e toca ou clica no botão Refresh da barra de ferramentas.

Se você monitorar periodicamente o DHCP, é recomendável que as estatísticas sejam atualizadas automaticamente. Para isso, siga estas etapas:

1. No console DHCP, expanda o nó do servidor com o qual você deseja trabalhar, pressione e mantenha pressionado ou clique com o botão direito do mouse em IPv4 ou IPv6 conforme apropriado para o tipo de endereço a ser usado e toque ou clique em Properties.
2. Na guia General, selecione Automatically Update Statistics Every e insira um intervalo de atualização em horas e minutos. Toque ou clique em OK.

Auditoria e solução de problemas do DHCP

O Windows Server 2012 é configurado para auditar processos de DHCP por padrão. A auditoria monitora processos e solicitações de DHCP em arquivos de log.

Você pode usar logs de auditoria para ajudá-lo a solucionar problemas com um servidor DHCP. Embora você possa habilitar e configurar o registro em log separadamente para IPv4 e IPv6, os dois protocolos usam os mesmos arquivos de log por padrão. O local padrão para logs de DHCP é %SystemRoot%\System32\DHCP. Nessa pasta, você encontrará um arquivo de log diferente para cada dia da semana. O arquivo de log para segunda-feira é nomeado DhcpSrvLog-Mon.log, o arquivo de log para terça-feira é chamado de DhcpSrvLog-Tue.log e assim por diante.

Ao iniciar o servidor DHCP ou a cada novo dia que começar, uma mensagem de cabeçalho é gravada no arquivo de log. Esse cabeçalho fornece um resumo dos eventos de DHCP e seus significados. Interromper e iniciar o serviço DHCP Server não limpa necessariamente o arquivo de log. Os dados de log são limpos somente quando um log não tiver recebido gravação nas últimas 24 horas. Você não precisa monitorar o espaço usado pelo serviço DHCP Server. Esse serviço está configurado para monitorar a si mesmo e restringe o uso de espaço em disco por padrão.

Você pode habilitar ou desabilitar a auditoria do DHCP seguindo estas etapas:

1. No console DHCP, expanda o nó do servidor com o qual você deseja trabalhar, pressione e mantenha pressionado ou clique com o botão direito do mouse em IPv4 ou IPv6 conforme apropriado para o tipo de endereço a ser usado e toque ou clique em Properties.
2. Na guia General, marque ou desmarque a caixa de seleção Enable DHCP Audit Logging e toque ou clique em OK.

Por padrão, os logs de DHCP são armazenados em %SystemRoot%\System32\DHCP. Você pode alterar o local dos logs de DHCP seguindo estas etapas:

1. No console DHCP, expanda o nó do servidor com o qual você deseja trabalhar, pressione e mantenha pressionado ou clique com o botão direito do mouse em IPv4 ou IPv6 conforme apropriado para o tipo de endereço a ser usado e toque ou clique em Properties.
2. Toque ou clique na guia Advanced. O Audit Log File Path exibe o local atual da pasta para arquivos de log. Insira um novo local para a pasta ou, para selecionar um novo local, toque ou clique em Browse.
3. Toque ou clique em OK. Neste ponto, o Windows Server 2012 precisa reiniciar o serviço DHCP Server. Quando solicitado que o serviço seja reiniciado, toque ou clique em Yes. O serviço será interrompido e iniciado novamente.

O servidor DHCP apresenta um sistema de automonitoramento que verifica o uso de espaço em disco. Por padrão, o tamanho máximo de todos os logs do servidor DHCP é de 70 megabytes (MB), com cada log individual sendo limitado a um sétimo desse espaço. Se o servidor atingir o limite de 70 MB ou um log individual ocupar mais que o espaço alocado, o registro em log da atividade do DHCP é interrompido até que os arquivos de log sejam limpos ou que seja disponibilizado espaço. Normalmente, isso acontece no início do dia quando o servidor limpa o arquivo de log da semana anterior para esse dia.

As chaves de registro que controlam o uso de log e outras configurações do DHCP estão localizadas sob HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters.

As chaves a seguir controlam o registro em log:

- **DhcpLogFilesMaxSize** Determina o tamanho de arquivo máximo para todos os logs. O padrão é 70 MB.
- **DhcpLogDiskSpaceCleanupInterval** Determina com que frequência o DHCP verifica o uso de espaço em disco e faz a limpeza conforme necessário. O intervalo padrão é de 60 minutos.
- **DhcpLogMinSpaceOnDisk** Determina o limite mínimo de espaço livre para gravar o log. Se o disco apresentar menos espaço livre que o valor especificado, o registro em log é temporariamente desabilitado. O valor padrão é 20 MB.

DhcpLogMinSpaceOnDisk é considerada uma chave opcional e sua criação não é automática. Essa chave deve ser criada conforme necessário e configurada com valores apropriados para sua rede.

Integração do DHCP e do DNS

O DNS é usado para resolver nomes de computadores em domínios do Active Directory e na Internet. Graças ao protocolo de atualização dinâmica do DNS, você não precisa registrar manualmente clientes DHCP no DNS. O protocolo permite que o cliente ou o servidor DHCP registre a entrada nas zonas de pesquisa direta e pesquisa inversa no DNS conforme necessário. Quando configurados com a configuração padrão para DHCP, os clientes DHCP atuais automaticamente atualizam seus próprios registros de DNS após receberem uma concessão de endereço IP, e o servidor DHCP atualiza registros para clientes novos após emitir uma concessão. Você pode modificar esse comportamento globalmente para cada servidor DHCP ou por escopo.

A proteção de nome é um recurso adicional do Windows Server 2012. Com ela, o servidor DHCP realiza registros em nome do cliente apenas se nenhum outro cliente com essas informações de DNS estiver registrado. A proteção de nome pode ser configurada para IPv4 e IPv6 no nível do adaptador de rede ou no nível de escopo. As configurações da proteção de nome determinadas no nível de escopo têm precedência sobre a configuração no nível de IPv4 ou IPv6.

A proteção de nome é projetada para impedir a prática de name squatting. O name squatting ocorre quando um computador não baseado em Windows registra um nome no DNS que já está registrado para um computador com sistema operacional Windows. Com a habilitação da proteção de nome, você pode impedir que computadores não baseados em Windows façam name squatting. Embora, de modo geral, o name squatting não apresente um problema quando o Active Directory é usado para reservar um nome para um usuário ou computador único, normalmente é recomendável que a proteção de nome seja habilitada em todas as redes Windows.

A proteção de nome é baseada no Dynamic Host Configuration Identifier (DHCID) e é compatível com o DHCID RR (registro de recurso) no DNS. O DHCID é um registro de recurso armazenado no DNS que mapeia nomes para impedir registros duplicados. O DHCP usa o registro de recurso do DHCID para armazenar um identificador para um computador juntamente com informações relacionadas para o nome, como os registros A e AAAA do computador. O servidor DHCP pode solicitar um registro DHCID

que tenha correspondência e recusar o registro de um computador com um endereço diferente na tentativa de registrar um nome com um registro DHCID existente.

Você pode visualizar e alterar as configurações globais da integração de DNS seguindo estas etapas:

1. No console DHCP, expanda o nó do servidor com o qual você deseja trabalhar, pressione e mantenha pressionado ou clique com o botão direito do mouse em IPv4 ou IPv6 e toque ou clique em Properties.
2. Toque ou clique na guia DNS. A Figura 15-3 mostra as configurações padrão de integração de DNS para o DHCP. Como essas configurações são definidas por padrão, normalmente não é necessário que elas sejam modificadas.

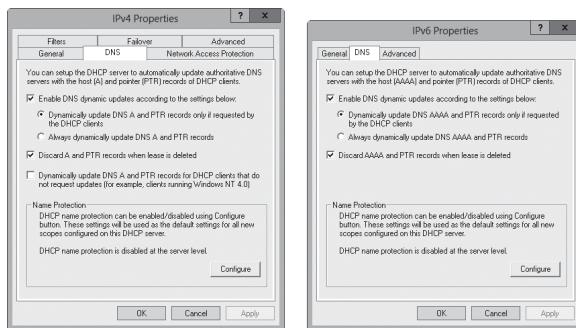


FIGURA 15-3 A guia DNS mostra as configurações padrão para a integração do DNS com o DHCP.

3. Se desejar, você pode habilitar ou desabilitar o recurso de proteção de nome. Com ele, o servidor DHCP realiza registros em nome do cliente apenas se nenhum outro cliente com essas informações de DNS estiver registrado. Para habilitar ou desabilitar a proteção de nome, toque ou clique em Configure. Na caixa de diálogo Name Protection, marque ou desmarque a opção Enable Name Protection e toque ou clique em OK.

Você pode visualizar e alterar as configurações por escopo da integração de DNS seguindo estas etapas:

1. No console DHCP, expanda o nó do servidor com o qual você deseja trabalhar e também o IPv4 ou IPv6.
2. Pressione e mantenha pressionado ou clique com o botão direito do mouse no escopo com o qual você deseja trabalhar e toque ou clique em Properties.
3. Toque ou clique na guia DNS. As opções disponíveis são as mesmas opções mostradas na Figura 15-3. Como essas configurações são definidas por padrão, normalmente não é necessário que elas sejam modificadas.
4. Se desejar, você pode habilitar ou desabilitar o recurso de proteção de nome. Toque ou clique em Configure. Na caixa de diálogo Name Protection, marque ou desmarque a opção Enable Name Protection e toque ou clique em OK.

Integração do DHCP e da NAP

A Network Access Protection (NAP, Proteção de Acesso à Rede) é projetada para proteger a rede contra clientes que não apresentam as configurações de segurança apropriadas. A maneira mais fácil de habilitar a NAP com o DHCP é configurando o servidor DHCP como um Network Policy Server. Para isso, você precisa instalar a função Network Policy And Access Services, configurar uma política compatível para integração de NAP e DHCP no servidor e habilitar a NAP para DHCP. Esse processo habilita a NAP para os computadores de rede que usam DHCP, mas não configura completamente a NAP para uso.

Você pode criar uma política de integração de NAP e DHCP seguindo estas etapas:

1. No servidor que você deseja que atue como o Network Policy Server, use o Add Roles And Features Wizard para instalar a função Network Policy And Access Services. É necessário que ao menos o serviço de função Network Policy Server seja instalado.
2. No Network Policy Server Console, disponível a partir do menu Tools no Server Manager, selecione o nó NPS (Local) na árvore de console e toque ou clique em Configure NAP no painel principal. O Configure NAP Wizard será iniciado.
3. Na lista Network Connection Method, escolha o Dynamic Host Configuration Protocol (DHCP) como o método de conexão a ser implantado na rede para clientes compatíveis com NAP. Como mostrado na Figura 15-4, o nome da diretiva é configurado como NAP DHCP por padrão. Toque ou clique em Next.

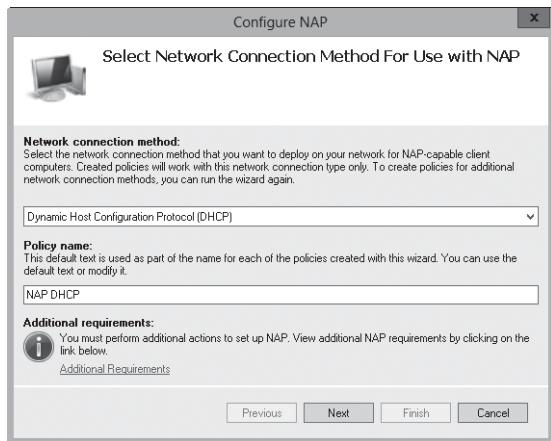


FIGURA 15-4 Configure a política Network Access Protection para o servidor DHCP local.

4. Na página Specify NAP Enforcement Servers Running DHCP Server, é necessário identificar todos os servidores DHCP remotos de sua rede executando o seguinte processo:

- Toque ou clique em Add. Na caixa de diálogo New RADIUS Client, digite um nome amigável para o servidor remoto na caixa de texto Friendly Name. Após, digite o nome de host DNS do servidor DHCP remoto na caixa de texto Address. Toque ou clique em Verify para assegurar que o nome de host DNS é válido.
 - No painel Shared Secret, selecione Generate e toque ou clique no botão Generate para criar uma frase-chave longa de segredo compartilhado. Você precisa inserir essa frase-chave na política NAP DHCP em todos os servidores DHCP remotos. Certifique-se de anotar essa frase-chave. Se preferir, copie-a no Notepad e salve-a em um arquivo armazenado em local seguro. Toque ou clique em OK.
5. Toque ou clique em Next. Na página Specify DHCP Scopes, você pode identificar os escopos de DHCP para os quais essa política deve ser aplicada. Se nenhum escopo for especificado, a política será aplicada a todos os escopos habilitados para NAP nos servidores DHCP selecionados. Toque ou clique em Next duas vezes para passar a página Configure Machine Groups.
 6. Na página Specify A NAP Remediation Server Group And URL, selecione um Remediation Server ou toque ou clique em New Group para definir um grupo de atualização e especificar servidores para lidarem com a correção. Os servidores de atualizações armazenaam atualizações de software para clientes NAP que precisem delas. Na caixa de texto exibida, digite a URL de uma página da Web que forneça aos usuários instruções de como fazer com que seus computadores fiquem em conformidade com a política de integridade da NAP. Certifique-se de que todos os clientes DHCP possam acessar essa URL. Toque ou clique em Next para continuar.
 7. Na página Define NAP Health Policy, use as opções fornecidas para determinar o modo de operação da política de integridade da NAP. Na maioria dos casos, as configurações padrão são satisfatórias. Com as configurações padrão, o acesso de clientes incompatíveis com NAP à rede é negado, enquanto clientes compatíveis com NAP são verificados quanto à conformidade e automaticamente corrigidos, permitindo que eles obtenham as atualizações de software necessárias que foram disponibilizadas por você. Toque ou clique em Next e em Finish.

Você pode modificar as configurações da NAP globalmente para cada servidor DHCP ou por escopo. Para visualizar ou alterar as configurações globais de NAP, siga estas etapas:

1. No console DHCP, expanda o nó do servidor com o qual você deseja trabalhar, pressione e mantenha pressionado ou clique com o botão direito do mouse em IPv4 e toque ou clique em Properties.
2. Na guia Network Access Protection, mostrada na Figura 15-5, toque ou clique em Enable On All Scopes ou Disable On All Scopes para habilitar ou desabilitar a NAP para todos os escopos do servidor.

OBSERVAÇÃO Quando o servidor DHCP local também for um Network Policy Server, o Network Policy Server estará sempre acessível. Se você não configurou o servidor como um Network Policy Server ou o servidor DHCP não estiver conseguindo contatar o Network Policy Server designado, você verá um erro com essa informação na guia Network Access Protection.

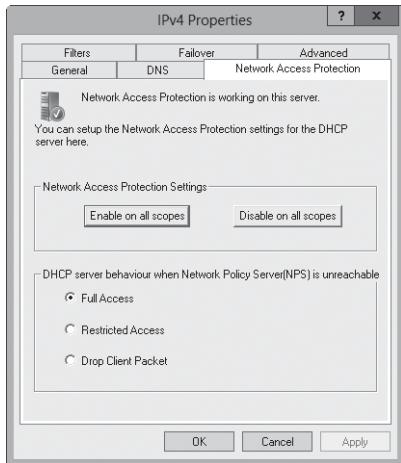


FIGURA 15-5 A guia Network Access Protection controla as opções de proteção para o DHCP.

3. Escolha uma das opções a seguir para especificar como o servidor DHCP se comporta se o Network Policy Server estiver inacessível e toque ou clique em OK para salvar suas configurações:

- **Full Access** Concede aos clientes DHCP acesso completo (irrestrito) à rede. Isso significa que os clientes poderão realizar qualquer ação permitida.
- **Restricted Access** Concede aos clientes DHCP acesso restrito à rede. Isso significa que os clientes poderão trabalhar somente com o servidor com o qual estiverem conectados.
- **Drop Client Packet** Bloqueia as solicitações dos clientes e impede que eles acessem a rede. Isso significa que os clientes não terão acesso aos recursos da rede.

Você pode visualizar e alterar as configurações da NAP para escopos individuais seguindo estas etapas:

1. No console DHCP, expanda o nó do servidor com o qual você deseja trabalhar e também o IPv4.
2. Pressione e mantenha pressionado ou clique com o botão direito do mouse no escopo com o qual você deseja trabalhar e toque ou clique em Properties.
3. Na guia Network Access Protection, toque ou clique em Enable For This Scope or Disable For This Scope para habilitar ou desabilitar a NAP para esse escopo.
4. Se você estiver habilitando a NAP e desejar usar um perfil de NAP diferente do padrão, toque ou clique em Use Custom Profile na guia Network Access Protection e digite o nome do perfil, como **Alternate NAP DHCP**.
5. Toque ou clique em OK para salvar suas configurações.

Como evitar conflitos de endereço IP

Os conflitos de endereço IPv4 são uma causa comum de problemas com o DHCP. Dois computadores na mesma rede não podem ter o mesmo endereço IP unicast. Se o mesmo endereço IPv4 unicast for atribuído a mais de um computador, ao menos um deles pode ser desconectado da rede. Mais especificamente, o computador que já estiver usando o endereço IPv4 terá permissão para continuar a usá-lo, enquanto qualquer outro computador que tentar usar esse mesmo endereço IPv4 terá o uso bloqueado.

Para melhor detectar e evitar possíveis conflitos, você pode habilitar a detecção de conflitos de endereço IPv4 seguindo estas etapas:

1. No console DHCP, expanda o nó do servidor com o qual você deseja trabalhar, pressione e mantenha pressionado ou clique com o botão direito do mouse em IPv4 e toque ou clique em Properties.
2. Na guia Advanced, defina um valor diferente de 0 para Conflict Detection Attempts. O valor que você inserir determina a quantidade de vezes que um servidor DHCP verifica um endereço IP antes de concedê-lo a um cliente. O servidor DHCP verifica os endereços IP enviando uma solicitação de ping pela rede.

MUNDO REAL Um endereço IPv4 unicast é um endereço IP padrão para redes classe A, B e C. Quando um cliente DHCP solicita uma concessão, um servidor DHCP verifica seu pool de endereços disponíveis e atribui ao cliente uma concessão em um endereço IPv4 disponível. Por padrão, o servidor verifica apenas a lista de concessões atuais para determinar se um endereço está disponível. Ele não consulta a rede de fato para investigar se um endereço está em uso. Infelizmente, em um ambiente de rede com muita utilização, um administrador pode ter atribuído esse endereço IPv4 a outro computador ou um computador offline pode ter se conectado com uma concessão que acredita não estar expirada, mesmo que o servidor DHCP acredite que a concessão expirou. De qualquer maneira, há um conflito de endereço que causará problemas na rede. Para reduzir esses tipos de conflito, configure a detecção de conflitos com um valor maior que 0.

Como salvar e restaurar a configuração de DHCP

Após definir todas as configurações de DHCP necessárias, é recomendável que você salve a configuração do DHCP para que ela possa ser restaurada em um servidor DHCP. Para salvar a configuração, insira o comando a seguir no prompt de comando:

```
netsh dump DHCP >dhcpconfig.dmp
```

Nesse exemplo, *dhcpconfig.dmp* é o nome do script de configuração a ser criado. Após criar o script, você poderá restaurar a configuração inserindo o comando a seguir no prompt de comando:

```
netsh exec dhcpconfig.dmp
```

DICA Você também pode usar essa técnica para configurar um outro servidor DHCP com a mesma configuração. Basta copiar o script de configuração para uma pasta no computador de destino e executá-lo.

Você pode salvar ou restaurar a configuração de DHCP também com o console DHCP. Para salvar a configuração, pressione e mantenha pressionada ou clique com o botão direito do mouse na entrada do servidor DHCP, toque ou clique em Backup, use a caixa de diálogo exibida para selecionar a pasta para o backup e toque ou clique em OK. Para restaurar a configuração, pressione e mantenha pressionada ou clique com o botão direito do mouse na entrada do servidor DHCP, toque ou clique em Restore, use

a caixa de diálogo exibida para selecionar a pasta de backup e toque ou clique em OK. Quando solicitada a confirmação, toque ou clique em Yes.

Gerenciamento dos escopos do DHCP

Após instalar um servidor DHCP, você precisará configurar os escopos que o servidor DHCP usará. Os escopos são grupos de endereços IP que você pode conceder a clientes. Como explicado anteriormente em “Noções básicas sobre escopos”, é possível criar superescopos, escopos normais, escopos de multicast e escopos de failover com endereços IPv4, mas apenas escopos normais podem ser criados com endereços IPv6.

Criação e gerenciamento de superescopos

Um superescopo é um contêiner de escopos IPv4 similar em muitos aspectos com o fato de uma unidade organizacional ser um contêiner de objetos do Active Directory. Os superescopos ajudam você a gerenciar os escopos disponíveis para a rede e também a dar suporte a clientes DHCP em uma rede física única em que várias redes IP lógicas são usadas. Em outras palavras, você pode criar superescopos para distribuir endereços IP de redes lógicas diferentes para o mesmo segmento de rede física. Com um superescopo, você pode ativar ou desativar vários escopos com uma ação única. Você também pode visualizar estatísticas para todos os escopos do superescopo, em vez de precisar verificar as estatísticas para cada escopo.

Criação de superescopos

Após criar ao menos um escopo IPv4 normal ou de multicast, você poderá criar um superescopo seguindo estas etapas:

1. No console DHCP, expanda o nó do servidor com o qual você deseja trabalhar, pressione e mantenha pressionado ou clique com o botão direito do mouse em IPv4 e toque ou clique em New Superscope. O New Superscope Wizard será iniciado. Toque ou clique em Next.
2. Insira um nome para o superescopo e toque ou clique em Next.
3. Selecione os escopos a serem adicionados ao superescopo. Selecione escopos individuais tocando ou clicando em suas entradas apresentadas na lista Available Scopes. Selecione vários escopos tocando ou clicando nas entradas mantendo pressionada a tecla Shift ou a tecla Ctrl.
4. Toque ou clique em Next e em Finish.

Como adicionar escopos a um superescopo

Você pode adicionar escopos a um superescopo ao criá-lo ou posteriormente. Para adicionar um escopo a um superescopo, siga estas etapas:

1. Pressione e mantenha pressionado ou clique com o botão direito do mouse no escopo que você deseja adicionar a um superescopo e toque ou clique em Add To Superscope.
2. Na caixa de diálogo Add Scope To A Superscope, selecione um superescopo.
3. Toque ou clique em OK. O escopo é adicionado ao superescopo.

Como remover escopos de um superescopo

Para remover um escopo de um superescopo, siga estas etapas:

1. Pressione e mantenha pressionado ou clique com o botão direito do mouse no escopo que você deseja remover de um superescopo e toque ou clique em Remove From Superscope.
2. Quando solicitado, toque ou clique em Yes para confirmar a ação. Se esse escopo for o último do superescopo, o superescopo é automaticamente excluído.

Como ativar e desativar um superescopo

Ao ativar ou desativar um superescopo, você torna todos os escopos de dentro do superescopo ativos ou inativos. Para ativar um superescopo, pressione e mantenha pressionado ou clique com o botão direito do mouse no superescopo e selecione Activate. Para desativar um superescopo, pressione e mantenha pressionado ou clique com o botão direito do mouse no superescopo e selecione Deactivate.

Como excluir um superescopo

A exclusão de um superescopo remove o contêiner do superescopo, mas não exclui os escopos que ele contém. Se você deseja excluir os escopos membros, precisará fazer isso separadamente. Para excluir um superescopo, pressione e mantenha pressionado ou clique com o botão direito do mouse no superescopo e selecione Delete. Quando solicitado, toque ou clique em Yes para confirmar a ação.

Criação e gerenciamento de escopos

Os escopos fornecem um pool de endereços IP a clientes DHCP. Um escopo normal apresenta endereços de rede classe A, B ou C. Um escopo de multicast apresenta endereços de rede classe D. Embora os escopos normais e de multicast sejam criados de maneiras diferentes, eles são gerenciados da mesma forma em vários aspectos. As principais diferenças são que os escopos de multicast não podem usar reservas e você não pode configurar opções adicionais para WINS, DNS, roteamento e assim por diante.

Como criar escopos normais para endereços IPv4

Você pode criar um escopo normal para endereços IPv4 seguindo estas etapas:

1. No console DHCP, expanda o nó do servidor com o qual você deseja trabalhar e selecione, pressione e mantenha pressionado ou clique com o botão direito do mouse em IPv4. Se você deseja adicionar o novo escopo a um superescopo automaticamente, selecione e pressione e mantenha pressionado ou clique com o botão direito do mouse no superescopo.
2. No menu de atalho, toque ou clique em New Scope. O New Scope Wizard será iniciado. Toque ou clique em Next.
3. Insira um nome e uma descrição para o escopo e toque ou clique em Next.
4. As caixas Start IP Address e End IP Address definem o intervalo de endereços IP válido para o escopo. Na página IP Address Range, insira um endereço inicial e um endereço final nessas caixas.

OBSERVAÇÃO De modo geral, o escopo não inclui os endereços x.x.x.0 e x.x.x.255, que são os normalmente reservados para endereços de rede e mensagens de difusão, respectivamente. Portanto, você usaria um intervalo como 192.168.10.1 a 192.168.10.254 em vez de 192.168.10.0 a 192.168.10.255.

- Quando o intervalo de endereços IP é inserido, a quantidade de bits e a máscara de sub-rede são preenchidos automaticamente (como mostrado na Figura 15-6). A menos que use sub-redes, você deve manter os valores padrão.

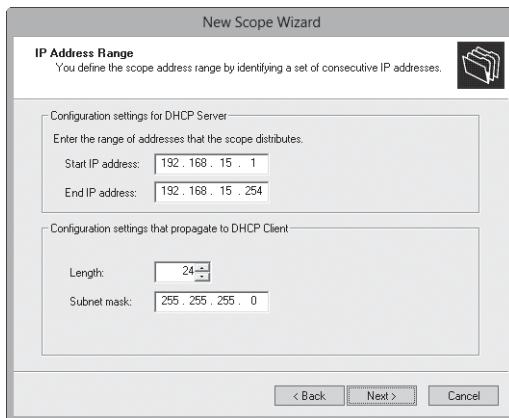


FIGURA 15-6 No New Scope Wizard, insira o intervalo de endereços IP para o escopo.

- Toque ou clique em Next. Se o intervalo de endereços IP inserido estiver em várias redes, você recebe a oportunidade de criar um superescopo que contenha escopos separados para cada rede. Nesse caso, selecione o botão de opção Yes para prosseguir e passar para a etapa 8. Caso tenha se enganado em alguma ação, toque ou clique em Back e modifique o intervalo de endereços IP inserido.
- Use as caixas Start IP Address e End IP Address da página Add Exclusions And Delay para definir intervalos de endereços IP a serem excluídos do escopo. Você pode excluir vários intervalos de endereços conforme descrito a seguir:
 - Para definir um intervalo de exclusão, digite um endereço inicial e um endereço final nas caixas Start IP Address e End IP Address de Exclusion Range e toque ou clique em Add. Para excluir um endereço IP único, use esse endereço tanto como endereço IP inicial quanto endereço IP final.
 - Para rastrear quais intervalos de endereços são excluídos, use a lista Excluded Address Range.
 Para excluir um intervalo de exclusão, selecione o intervalo na lista Excluded Address Range e toque ou clique em Remove.
- Toque ou clique em Next. Especifique a duração das concessões para o escopo com as caixas Day(s), Hour(s) e Minutes. A duração padrão é de oito dias. Toque ou clique em Next.

OBSERVAÇÃO Uma duração de concessão configurada para ser muito longa pode reduzir a efetividade do DHCP e pode causar eventualmente que você esgote seus endereços IP disponíveis, especialmente em redes com usuários móveis ou outros tipos de computador que não sejam membros fixos da rede. Uma boa duração de concessão para a maioria das redes é de um a três dias.

9. Você tem a oportunidade de configurar opções de DHCP comuns para DNS, WINS, gateways, entre outros. Se desejar configurar essas opções nesse momento, selecione Yes, I Want To Configure These Options Now. Caso contrário, selecione No, I Will Configure These Options Later e não realize as etapas de 10 a 15.
10. Toque ou clique em Next. A primeira opção que pode ser configurada é o gateway padrão. Na caixa IP Address, insira o endereço IP do gateway padrão primário e toque ou clique em Add. Repita esse processo para outros gateways padrão.
11. O primeiro gateway listado é o que os clientes tentam usar primeiramente. Se o gateway não estiver disponível, os clientes tentam usar o próximo gateway e assim por diante. Use os botões Up e Down para alterar a ordem dos gateways, conforme necessário.
12. Toque ou clique em Next. Como mostrado na Figura 15-7, defina as configurações padrão de DNS para clientes DHCP. Insira o nome do domínio pai a ser usado para a resolução de DNS de nomes de computador que não são totalmente qualificados.

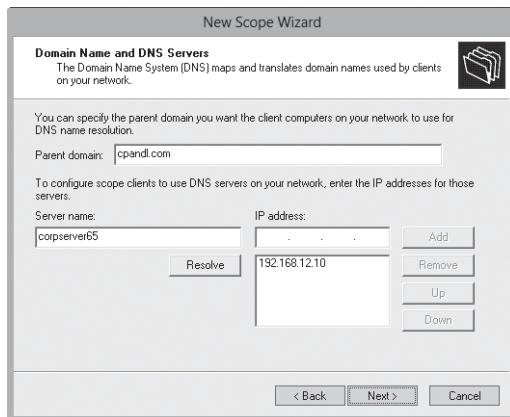


FIGURA 15-7 Use a página Domain Name And DNS Servers para configurar as configurações padrão de DNS para clientes DHCP.

13. Na caixa IP Address, insira o endereço IP do servidor DNS padrão primário e toque ou clique em Add. Repita esse processo para especificar servidores DNS adicionais. Novamente, a ordem das entradas determinam qual endereço IP é usado primeiro. Altere a ordem conforme necessário com os botões Up e Down. Toque ou clique em Next.

DICA Se você sabe o nome de um servidor em vez de seu endereço IP, insira o nome na caixa Server Name e toque ou clique em Resolve. O endereço IP é inserido na caixa IP Address, se possível. Adicione o servidor tocando ou clicando em Add.

14. Determine as configurações padrão de WINS para os clientes DHCP. As técnicas usadas são as mesmas descritas anteriormente. Toque ou clique em Next.
15. Se você deseja ativar o escopo, selecione Yes, I Want To Activate This Scope Now e toque ou clique em Next. Caso contrário, selecione No, I Will Activate This Scope Later e toque ou clique em Next.
16. Toque ou clique em Finish para concluir o processo.

Como criar escopos normais para endereços IPv6

Os escopos normais para endereços IPv6 são criados com o New Scope Wizard. Ao configurar o DHCP para endereços IPv6, você deve inserir o ID de rede e um valor de preferência. Normalmente, os primeiros 64 bits de um endereço IPv6 identificam a rede, e o New Scope Wizard espera que você insira um valor de 64 bits. O valor de preferência define a prioridade do escopo em relação aos outros escopos. O escopo com o valor de preferência mais baixo será usado primeiro. O escopo com a segunda menor preferência será o segundo a ser usado e assim por diante.

Você pode criar um escopo normal para endereços IPv6 seguindo estas etapas:

1. No console DHCP, expanda o nó do servidor com o qual você deseja trabalhar.
2. Selecione e pressione e mantenha pressionado ou clique com o botão direito do mouse em IPv6. No menu de atalho, toque ou clique em New Scope. O New Scope Wizard será iniciado. Toque ou clique em Next.
3. Insira um nome e uma descrição para o escopo e toque ou clique em Next.
4. Na página Scope Prefix, mostrada na Figura 15-8, insira o prefixo de rede de 64 bits e defina um valor de preferência. Toque ou clique em Next.

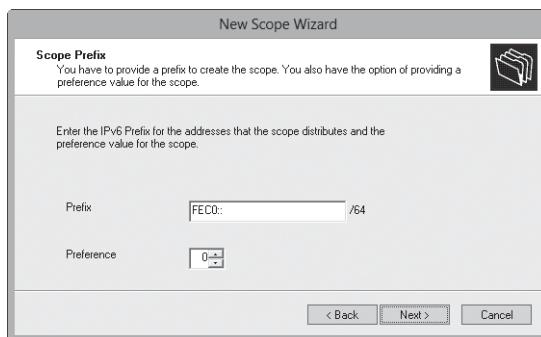


FIGURA 15-8 No New Scope Wizard, insira o prefixo de rede e o valor de preferência.

5. Use as caixas Start IP Address e End IP Address da página Add Exclusions para definir intervalos de endereços IPv6 a serem excluídos do escopo. Você pode excluir vários intervalos de endereços conforme descrito a seguir:

- Para definir um intervalo de exclusão, digite um endereço inicial e um endereço final nas caixas Start IPv6 Address e End IPv6 Address de Exclusion Range e toque ou clique em Add. Para excluir um endereço IPv6 único, use esse endereço como o endereço IPv6 inicial e toque ou clique em Add.
- Para rastrear quais intervalos de endereços são excluídos, use a lista Excluded Address Range.

Para excluir um intervalo de exclusão, selecione o intervalo na lista Excluded Address Range e toque ou clique em Remove.

6. Toque ou clique em Next. Os endereços IPv6 dinâmicos podem ser temporários ou permanentes. Um endereço permanente é similar a uma reserva. Na página Scope Lease, mostrada na Figura 15-9, especifique a duração das concessões para endereços permanentes com as caixas Days, Hours e Minutes sob Preferred Life Time e Valid Life Time. A caixa Preferred Life Time define o tempo que você prefere que a concessão permaneça válida. A caixa Valid Life Time define o tempo máximo que a concessão permanece válida. Toque ou clique em Next.

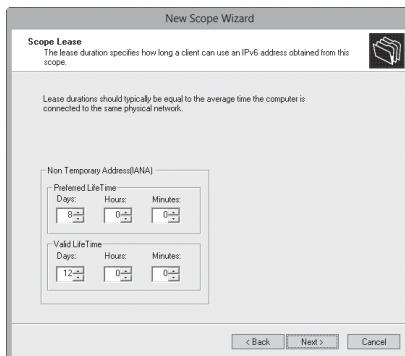


FIGURA 15-9 Especifique a duração das concessões permanentes.

OBSERVAÇÃO Um tempo de vida de concessão configurado para ser muito longo pode reduzir a efetividade do DHCP e pode causar eventualmente que você esgote seus endereços IP disponíveis, especialmente em redes com usuários móveis ou outros tipos de computador que não sejam membros fixos da rede. Uma boa duração de concessão para concessões permanentes é de oito a 30 dias.

7. Se você deseja ativar o escopo, selecione Yes sob Activate Scope Now e toque ou clique em Finish. Caso contrário, selecione No sob Activate Scope Now e toque ou clique em Finish.

Como criar escopos de multicast

Para criar um escopo de multicast, siga estas etapas:

1. No console DHCP, expanda o nó do servidor com o qual você deseja trabalhar. Selecione e pressione e mantenha pressionado ou clique com o botão direito do mouse em IPv4. Se você deseja adicionar o novo escopo a um superescopo, selecione e pressione e mantenha pressionado ou clique com o botão direito do mouse no superescopo.
 2. No menu de atalho, toque ou clique em New Multicast Scope. O New Multicast Scope Wizard será iniciado. Toque ou clique em Next.
 3. Insira um nome e uma descrição para o escopo e toque ou clique em Next.
 4. As caixas Start IP Address e End IP Address definem o intervalo de endereços IP válido para o escopo. Insira um endereço inicial e um endereço final nessas caixas. Você deve definir escopos de multicast por meio de endereços IP de classe D. Isso significa que o intervalo de endereços IP válido é de 224.0.0.0 a 239.255.255.255.
 5. As mensagens enviadas por computadores com endereços IP de multicast apresentam um valor específico de time-to-live (TTL, tempo de vida). O valor de TTL especifica o número máximo de roteadores pelo qual a mensagem pode passar. O valor padrão de 32 é suficiente para a maioria das redes. Se você tiver uma rede grande, talvez precisará aumentar esse valor para refletir o número real de roteadores que pode ser usado.
 6. Toque ou clique em Next. Caso tenha se enganado em alguma ação, toque ou clique em Back e modifique o intervalo de endereços IP inserido.
 7. Use o intervalo de exclusão para definir os intervalos de endereços IP a serem excluídos do escopo. Você pode excluir vários intervalos de endereços:
 - Para definir um intervalo de exclusão, insira um endereço inicial e um endereço final nas caixas Start IP Address e End IP Address e toque ou clique em Add.
 - Para rastrear quais intervalos de endereços são excluídos, use a lista Excluded Addresses.Para excluir um intervalo de exclusão, selecione o intervalo na lista Excluded Addresses e toque ou clique em Remove.
 8. Toque ou clique em Next. Especifique a duração das concessões para o escopo com as caixas Day(s), Hour(s) e Minutes. A duração padrão é de 30 dias. Toque ou clique em Next.
- DICA** Se você tiver trabalhado pouco com multicast, não deverá alterar o valor padrão. As concessões de multicast não são usadas da mesma forma que as concessões normais. Vários computadores podem usar um endereço IP de multicast e todos eles podem ter uma concessão do endereço IP. Uma boa duração de concessão de multicast para a maioria das redes é de 30 a 60 dias.
9. Se você deseja ativar o escopo, selecione Yes e toque ou clique em Next. Caso contrário, selecione No e toque ou clique em Next.
 10. Toque ou clique em Finish para concluir o processo.

Configuração das opções de escopo

As opções de escopo permitem que você controle precisamente o funcionamento de um escopo e defina as configurações padrão TCP/IP para clientes que usam o escopo. Por exemplo, você pode usar as opções de escopo para permitir que os clientes encontrem automaticamente servidores DNS na rede. Você também pode definir configurações para gateways padrão, WINS, entre outros. As opções de escopo se aplicam apenas a escopos normais e não a escopos de multicast.

Você pode configurar as opções de escopo por meio destas maneiras:

- Globalmente para todos os escopos configurando opções padrão de servidor
- Por escopo configurando opções de escopo
- Por cliente configurando opções de reserva
- Por classe de clientes configurando classes específicas de usuário ou fornecedores

O IPv4 e o IPv6 apresentam opções de escopo diferentes. As opções de escopo usam uma hierarquia para determinar quando certas opções são aplicadas. A lista anterior mostra a hierarquia. Basicamente, isso significa que:

- As opções por escopo sobrescrevem as opções globais.
- As opções por cliente sobrescrevem as opções por escopo e globais.
- As opções por classe de clientes sobrescrevem todas as demais opções.

VISUALIZAÇÃO E ATRIBUIÇÃO DE OPÇÕES DE SERVIDOR

As opções de servidor são aplicadas a todos os escopos configurados em um determinado servidor DHCP. Para visualizar e atribuir opções de servidor, siga estas etapas:

1. No console DHCP, dê um toque duplo ou clique duas vezes no servidor com o qual você deseja trabalhar e expanda suas pastas de IPv4 e IPv6 no modo de exibição de árvore.
2. Para visualizar as configurações atuais, selecione o nó Server Options sob IPv4 ou IPv6, dependendo do tipo de endereço com o qual você deseja trabalhar. As opções que estão configuradas no momento são exibidas no painel direito.
3. Para atribuir novas configurações, pressione e mantenha pressionado ou clique com o botão direito do mouse em Server Options e toque ou clique em Configure Options. A caixa de diálogo Server Options será aberta. Sob Available Options, marque a caixa de seleção da primeira opção a ser configurada. Com a opção selecionada, insira as informações solicitadas no painel Data Entry. Repita esta etapa para configurar outras opções.
4. Toque ou clique em OK para salvar suas alterações.

VISUALIZAÇÃO E ATRIBUIÇÃO DE OPÇÕES DE ESCOPO

As opções de escopo são específicas a um escopo individual e sobrescrevem as opções padrão de servidor. Para visualizar e atribuir opções de escopo, siga estas etapas:

1. No console DHCP, expanda a entrada do escopo com o qual você deseja trabalhar.
2. Para visualizar as configurações atuais, selecione Scope Options. As opções que estão configuradas no momento são exibidas no painel direito.

3. Para atribuir novas configurações, pressione e mantenha pressionado ou clique com o botão direito do mouse em Scope Options e toque ou clique em Configure Options. A caixa de diálogo Scope Options será aberta. Sob Available Options, marque a caixa de seleção da primeira opção a ser configurada. Com a opção selecionada, insira as informações solicitadas no painel Data Entry, como mostrado na Figura 15-10. Repita esta etapa para configurar outras opções.

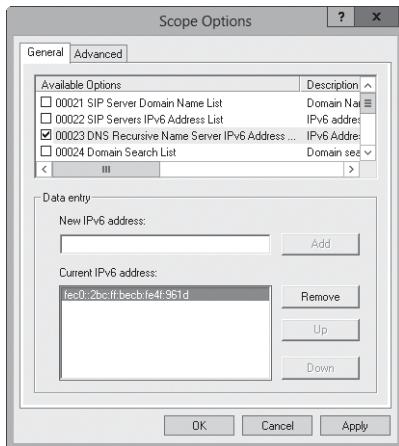


FIGURA 15-10 Selecione a opção a ser configurada na caixa de diálogo Scope Options e insira as informações solicitadas no painel Data Entry.

4. Toque ou clique em OK.

VISUALIZAÇÃO E ATRIBUIÇÃO DE OPÇÕES DE RESERVA

As opções de reserva podem ser atribuídas a um cliente que tenha um endereço IPv4 ou IPv6 reservado. Essas opções são específicas a um cliente individual e sobrescrevem as opções específicas ao servidor e ao escopo. Para visualizar e atribuir opções de reserva, siga estas etapas:

1. No console DHCP, expanda a entrada do escopo com o qual você deseja trabalhar.
2. Dê um toque duplo ou clique duas vezes na pasta Reservations do escopo.
3. Para visualizar as configurações atuais, toque ou clique na reserva a ser examinada. As opções que estão configuradas no momento são exibidas no painel direito.
4. Para atribuir novas configurações, pressione e mantenha pressionada ou clique com o botão direito do mouse na reserva e toque ou clique em Configure Options. A caixa de diálogo Reservation Options será aberta. Sob Available Options, marque a caixa de seleção da primeira opção a ser configurada. Com a opção selecionada, insira as informações solicitadas no painel Data Entry. Repita esta etapa para configurar outras opções.

Como modificar escopos

Você pode modificar um escopo existente seguindo estas etapas:

1. No console DHCP, dê um toque duplo ou clique duas vezes no servidor com o qual você deseja trabalhar e expanda suas pastas de IPv4 e IPv6 no modo de exibição de árvore. Essa ação deve exibir os escopos atualmente configurados para o servidor.
2. Pressione e mantenha pressionado ou clique com o botão direito do mouse no escopo a ser modificado e toque ou clique em Properties.
3. Nesse momento, você pode modificar as propriedades do escopo. Lembre-se do seguinte:
 - Quando você modifica escopos IPv4 normais, há a opção de configurar um tempo de expiração da concessão ilimitado. Se optar por isso, você criará concessões permanentes que reduzirão a efetividade dos pools de endereços IP com o DHCP. As concessões permanentes não são liberadas a menos que você as libere fisicamente ou desative o escopo. Como resultado, você pode eventualmente esgotar seus endereços, principalmente à medida que sua rede cresce. Uma alternativa melhor para concessões ilimitadas é usar reservas de endereços apenas para clientes específicos que precisem de endereços IP fixos.
 - Quando você modifica escopos de multicast, há a opção de configurar um tempo de vida para o escopo. O tempo de vida do escopo determina o tempo que ele permanece válido. Por padrão, os escopos de multicast são válidos enquanto estiverem ativados. Para alterar essa configuração, toque ou clique na guia Lifetime, selecione Multicast Scope Expires On e determine uma data de vencimento.

Como ativar e desativar escopos

No console DHCP, os escopos inativos são exibidos com um ícone que apresenta uma seta vermelha para baixo. Os escopos ativos exibem um ícone de pasta normal.

Você pode ativar um escopo desativado pressionando e mantendo pressionado ou clicando com o botão direito do mouse no escopo desejado, no console DHCP, e selecionando Activate. Você pode desativar um escopo ativado pressionando e mantendo pressionado ou clicando com o botão direito do mouse no console DHCP e selecionando Deactivate.

DICA A desativação desliga um escopo, mas não finaliza as concessões atuais de clientes. Se você deseja finalizar concessões, siga as instruções de “Liberação de endereços e concessões” mais adiante neste capítulo.

Como habilitar o Bootstrap Protocol

O BOOTP é um protocolo de endereçamento IPv4 dinâmico anterior ao DHCP. Os escopos normais não comportam o BOOTP. Para tornar um escopo compatível com BOOTP, siga estas etapas:

1. Pressione e mantenha pressionado ou clique com o botão direito do mouse no escopo normal para endereços IPv4 a ser modificado e toque ou clique em Properties.
2. Na guia Advanced, toque ou clique em Both para dar suporte a clientes DHCP e BOOTP.
3. Conforme necessário, defina uma duração de concessão para clientes BOOTP e toque ou clique em OK.

Como remover um escopo

Remover um escopo exclui permanentemente o escopo do servidor DHCP. Para isso, siga estas etapas:

1. No console DHCP, pressione e mantenha pressionado ou clique com o botão direito do mouse no escopo que você deseja remover e toque ou clique em Delete.
2. Quando solicitada a confirmação de que você deseja excluir o escopo, toque ou clique em Yes.

Configuração de vários escopos em uma rede

Você pode configurar vários escopos em uma rede única. Um servidor DHCP único ou vários servidores DHCP podem prestar serviços a esses escopos. No entanto, todas as vezes que você trabalhar com vários escopos, é extremamente importante que os intervalos de endereços usados por escopos diferentes não se sobreponham. Cada escopo deve ter um intervalo de endereços exclusivo. Caso contrário, o mesmo endereço IP pode ser atribuído a clientes DHCP diferentes, o que pode causar problemas graves na rede.

Para entender como vários escopos podem ser usados, considere o cenário a seguir, em que cada servidor tem seu intervalo de endereços IP de escopos do DHCP na mesma sub-rede:

- **Servidor A** 192.168.10.1 a 192.168.10.99
- **Servidor B** 192.168.10.100 a 192.168.10.199
- **Servidor C** 192.168.10.200 a 192.168.10.254

Todos esses servidores respondem a mensagens de descoberta do DHCP e podem atribuir endereços IP a clientes. Se um dos servidores falhar, os demais podem continuar a fornecer serviços de DHCP à rede. Para incluir tolerância a falhas e fornecer redundância, você pode usar escopos de failover conforme discutido na próxima seção.

Criação e gerenciamento de escopos de failover

Os escopos de failover são divididos entre dois servidores DHCP para aumentar a tolerância a falhas, fornecer redundância por usar mais de um servidor DHCP e permitir o平衡amento de carga. Com um escopo de failover, você identifica os dois servidores DHCP que dividem o escopo. Se um dos servidores ficar indisponível ou sobre-carregado, o outro servidor pode ocupar seu lugar continuando a conceder novos endereços IP e renovar concessões existentes. Um escopo de failover também pode ajudar a balancear carga de servidores.

Como criar escopos de failover

Os escopos de failover aplicam-se apenas a endereços IPv4. Você pode dividir um escopo único ou um superescopo que contenha vários escopos.

Um escopo de failover é criado no servidor DHCP que você quer que atue como o servidor primário dividindo um escopo ou superescopo existente. Durante o pro-

cesso de criação de um escopo de failover, é necessário especificar o servidor parceiro com o qual você deseja dividir o escopo do servidor primário. Esse servidor adicional atua como o servidor secundário do escopo. Como os escopos de failover são um aprimoramento do servidor, nenhuma configuração adicional é necessária para clientes DHCP.

O modo com que a divisão de escopo funciona depende das configurações definidas no escopo de failover. Siga uma das ações a seguir:

- **Otimizar para balanceamento de carga** Um escopo de failover otimizado para balanceamento de carga apresenta um tempo de espera muito curto ou nulo configurado em suas propriedades de escopo. Sem tempo de espera, tanto o servidor primário quanto o servidor secundário pode responder a solicitações DHCP DISCOVER de clientes DHCP. Isso permite que o servidor mais rápido responda e aceite um DHCPOFFER primeiro. A tolerância a falhas continua sendo parte do escopo. Se um dos servidores ficar indisponível ou sobrecarregado e não conseguir responder a solicitações, o outro servidor fará isso e continuará a distribuir endereços até que o processo normal seja restaurado. Para o balanceamento de carga, configure Load Balance como o modo de failover.
- **Otimizar para tolerância a falhas** Um escopo de failover otimizado para tolerância a falhas apresenta um tempo de espera estendido configurado em suas propriedades de escopo. O tempo de espera no servidor DHCP secundário faz com que o servidor responda com atraso a solicitações DHCP DISCOVER de clientes DHCP. Esse atraso do servidor secundário permite que o servidor DHCP primário responda e aceite DHCPOFFER primeiro. No entanto, se o servidor primário ficar indisponível ou sobrecarregado e não conseguir responder a solicitações, o servidor secundário fará isso e continuará a distribuir endereços até que o servidor primário esteja disponível novamente para prestar serviços aos clientes. Para tolerância a falhas, configure Hot Standby como o modo de failover.

Você pode criar um escopo de failover completando as etapas a seguir:

1. No console DHCP, conecte-se ao servidor DHCP primário para o escopo de failover. Dê um toque duplo ou clique duas vezes na entrada do servidor primário e expanda sua pasta IPv4 no modo de exibição de árvore.
2. O escopo com o qual você deseja trabalhar já deve estar definido. Pressione e mantenha pressionado ou clique com o botão direito do mouse no escopo ou superescopo que você deseja configurar para failover e toque ou clique em Configure Failover. O Configure Failover Wizard será iniciado. Toque ou clique em Next.
3. Em seguida, você precisará especificar o servidor parceiro a ser usado para failover. Toque ou clique em Add Server. Use as opções da caixa de diálogo Add Server para selecionar o servidor DHCP secundário para o escopo de failover e toque ou clique em OK. Desmarque a caixa de seleção Reuse Existing Failover Relationships e toque ou clique em Next para prosseguir.
4. Na página Create A New Failover Relationship, mostrada na Figura 15-11, use a lista Mode para configurar o modo de failover como Load Balance ou Hot Standby.

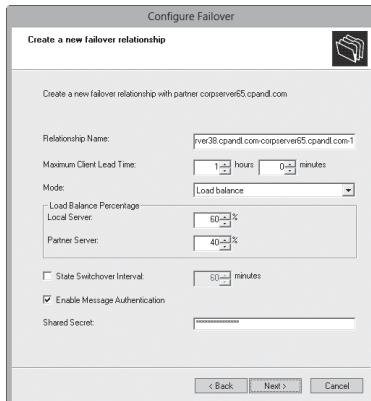


FIGURA 15-11 Especifique a porcentagem da divisão.

5. Se você configurar o modo de failover como Load Balance, use as caixas de combinação sob Load Balance Percentage para especificar a porcentagem relativa de como alocar os endereços IP para cada servidor. Seguem alguns exemplos de configuração:
 - Uma divisão de 80/20 funciona melhor quando você deseja que um servidor lide com a maior parte da carga de trabalho, enquanto o outro permanece disponível conforme necessário.
 - Uma divisão de 60/40 funciona melhor quando você deseja que um servidor lide com uma parte um pouco maior da carga de trabalho do que outro, mas que os dois servidores tenham cargas de trabalho regulares.
 - Uma divisão de 50/50 funciona melhor quando você deseja平衡ear igualmente a carga entre os dois servidores.
6. Se você configurar o modo de failover como Hot Standby, defina a função do parceiro como Active ou Standby e especifique a porcentagem relativa de endereços IP a ser reservada. Por padrão, 5% dos endereços IP são reservados para o servidor em espera.
7. Digite um segredo compartilhado para os parceiros. O segredo compartilhado é uma senha que os parceiros usam ao sincronizar o banco de dados do DHCP e realizar outras tarefas relacionadas à manutenção da parceria de failover do DHCP. Quando estiver pronto para prosseguir, toque ou clique em Next.
8. Toque ou clique em Finish. Examine o resumo da configuração do escopo de failover. Se algum erro for encontrado, talvez você precise corrigi-lo. Toque ou clique em Close.

Como modificar ou remover escopos de failover

Os escopos de failover não são identificados como tal no console DHCP. Você pode identificar um escopo de failover pelo seu ID de rede e pool de endereços IP. Nor-

malmente, você encontrará um escopo com o mesmo ID de rede em dois servidores DHCP, e as propriedades do escopo incluirão informações sobre a parceria de failover. Para visualizar essas informações, pressione e mantenha pressionado ou clique com o botão direito do mouse no escopo e selecione Properties. Na caixa de diálogo Properties, selecione a guia Failover.

A parceria pode ser gerenciada de diversas formas:

- Se você suspeitar que os detalhes de configuração relacionados à parceria não estão sincronizados, pressione e mantenha pressionado ou clique com o botão direito do mouse no escopo e selecione Replicate Partnership.
- Se você suspeitar que o banco de dados do DHCP que os parceiros compartilham não está sincronizado, pressione e mantenha pressionado ou clique com o botão direito do mouse no escopo e selecione Replicate Scope.
- Se você não quiser mais que o escopo execute failover, é possível desconfigurar o failover pressionando e mantendo pressionado ou clicando com o botão direito do mouse no escopo e selecionando Deconfigure Failover.

Após o estabelecimento da parceria, as configurações de failover não podem ser modificadas. No entanto, você pode desconfigurar o failover e, em seguida, reconfigurá-lo.

Gerenciamento do pool de endereços, das concessões e das reservas

Os escopos têm pastas separadas para pools de endereços, concessões e reservas. Acessando essas pastas, você pode visualizar estatísticas atuais para os dados relacionados e gerenciar entradas existentes.

Visualização de estatísticas do escopo

As estatísticas do escopo fornecem informações resumidas sobre o pool de endereços para o escopo ou superescopo atual. Para visualizar as estatísticas, pressione e mantenha pressionado ou clique com o botão direito do mouse no escopo ou superescopo e selecione Display Statistics.

As principais colunas da caixa de diálogo Scope Statistics são apresentadas da seguinte forma:

- **Total Scopes** Exibe o número de escopos de um superescopo.
- **Total Addresses** Exibe o número total de endereços IP atribuídos ao escopo.
- **In Use** Exibe o número total (como um valor numérico e como uma porcentagem do total de endereços disponíveis) dos endereços em uso. Se o total chegar a 85% ou mais, é recomendável considerar a atribuição de endereços adicionais ou a liberação de endereços para o uso.
- **Available** Exibe o número total (como um valor numérico e como uma porcentagem do total de endereços disponíveis) dos endereços disponíveis para o uso.

Como habilitar e configurar a filtragem de endereços MAC

A filtragem de endereços MAC (também conhecida como *filtragem de camada de enlace*) é um recurso para endereços IPv4 que permite a você incluir ou excluir computadores e dispositivos com base em seu endereço MAC. Quando você configura a filtragem de endereços MAC, pode especificar os tipos de hardware que não serão incluídos na filtragem. Por padrão, todos os tipos de hardware definidos na RFC 1700 não são incluídos na filtragem. Para modificar as exceções quanto ao tipo de hardware, siga estas etapas:

1. No console DHCP, pressione e mantenha pressionado ou clique com o botão direito do mouse no nó IPv4 e toque ou clique em Properties.
2. Na guia Filters, toque ou clique em Advanced. Na caixa de diálogo Advanced Filter Properties, marque a caixa de seleção dos tipos de hardware a serem excluídos da filtragem. Desmarque a caixa de seleção dos tipos de hardware a serem filtrados.
3. Toque ou clique em OK para salvar suas alterações.

Antes de poder configurar a filtragem de endereços MAC, você deve:

- Habilitar e definir uma lista de permissões explícita. O servidor DHCP fornece serviços de DHCP apenas a clientes cujos endereços MAC estão na lista de permissões. Qualquer cliente que anteriormente tenha recebido endereços IP tem sua renovação de endereço negada se seu endereço MAC não estiver na lista de permissões.
- Habilitar e definir uma lista de negações explícita. O servidor DHCP nega serviços de DHCP apenas a clientes cujos endereços MAC estão na lista de negações. Qualquer cliente que anteriormente tenha recebido endereços IP tem sua renovação de endereço negada se seu endereço MAC estiver na lista de negações.
- Habilitar e definir uma lista de permissões e uma lista de bloqueios. A lista de bloqueios tem precedência sobre a lista de permissões. Isso significa que o servidor DHCP fornece serviços de DHCP apenas a clientes cujos endereços MAC estão na lista de permissões, desde que não haja correspondências na lista de bloqueios. Se um endereço MAC foi negado, o endereço será sempre bloqueado mesmo se estiver na lista de permissões.

Para habilitar uma lista de permissões, uma lista de negações ou ambas, siga estas etapas:

1. No console DHCP, pressione e mantenha pressionado ou clique com o botão direito do mouse no nó IPv4 e toque ou clique em Properties.
2. Na guia Filters são exibidos os detalhes de configuração atuais de filtro. Para usar uma lista de permissões, selecione Enable Allow List. Para usar uma lista de negações, selecione Enable Deny List.
3. Toque ou clique em OK para salvar suas alterações.

OBSERVAÇÃO Como alternativa, você pode simplesmente pressionar e manter pressionado ou clicar com o botão direito do mouse no nó Allow ou Deny sob o nó Filters e selecionar Enable para habilitar as listas de permissões ou negações. Se você pressionar e manter pressionado ou clicar com o botão direito do mouse nos nós Allow ou Deny e selecionar Disable, você desabilitará as listas de permissões ou negações.

Após habilitar a filtragem, você define seus filtros usando o endereço MAC para o computador cliente ou adaptador de rede do dispositivo. Em um computador cliente, você pode obter o endereço MAC digitando o comando **ipconfig /all** no prompt de comando. A entrada Physical Address exibe o endereço MAC do cliente. Você deve digitar esse valor de maneira exata para que o filtro de endereços funcione.

Um endereço MAC é definido por oito emparelhamentos de números hexadecimais de dois dígitos separados por um hifen, como mostrado no exemplo a seguir:

FE-01-56-23-18-94-EB-F2

Ao definir um filtro, você pode especificar o endereço MAC com ou sem os hifens. Isso significa que é possível inserir FE-01-56-23-18-94-EB-F2 ou FE0156231894EBF2.

Você também pode usar um asterisco (*) como um curinga para correspondência de padrões. Para permitir que qualquer valor corresponda a uma parte específica do endereço MAC, você pode inserir * onde os valores normalmente estariam, como mostrado no exemplo a seguir:

FE-01-56-23-18-94-*-*F2

FE-*56-23-18-94-*-*

FE-01-56-23-18-*-*-*

FE01*

Para configurar um filtro de endereços MAC, siga estas etapas:

1. No console DHCP, dê um toque duplo ou clique duas vezes no nó IPv4 e, após, no nó Filters.
2. Pressione e mantenha pressionado ou clique com o botão direito do mouse em Allow ou Deny, conforme for apropriado para o tipo de filtro que estiver sendo criado, e toque ou clique em New Filter.
3. Insira o endereço MAC a ser filtrado e adicione um comentário na caixa de texto Description, se desejar. Toque ou clique em Add. Repita esta etapa para adicionar outros filtros.
4. Toque ou clique em Close ao terminar.

Configuração de um novo intervalo de exclusão

Você pode excluir endereços IPv4 ou IPv6 de um escopo definindo um intervalo de exclusão. Os escopos podem apresentar vários intervalos de exclusão. Para definir um intervalo de exclusão para um escopo com endereços IPv4, siga estas etapas:

1. No console DHCP, expanda o escopo com o qual você deseja trabalhar e pressione e mantenha pressionada ou clique com o botão direito do mouse na pasta Address Pool ou na pasta Exclusions. No menu de atalho, toque ou clique em New Exclusion Range.
2. Insira um endereço inicial e um endereço final nas caixas Start IP Address e End IP Address e toque ou clique em Add. O intervalo especificado deve ser um subconjunto do intervalo definido para o escopo atual e não deve estar em uso. Repita esta etapa para adicionar outros intervalos de exclusão.
3. Toque ou clique em Close ao terminar.

Para definir um intervalo de exclusão para um escopo com endereços IPv6, siga estas etapas:

1. No console DHCP, expanda o escopo com o qual você deseja trabalhar e pressione e mantenha pressionada ou clique com o botão direito do mouse na pasta Exclusions. No menu de atalho, toque ou clique em New Exclusion Range.
2. Insira um endereço inicial e um endereço final nas caixas Start IPv6 Address e End IPv6 Address e toque ou clique em Add. O intervalo especificado deve ser um subconjunto do intervalo definido para o escopo atual e não deve estar em uso. Repita esta etapa para adicionar outros intervalos de exclusão.
3. Toque ou clique em Close ao terminar.

Se a exclusão não for mais necessária, você pode excluí-la. Selecione Address Pool ou Exclusions conforme apropriado. No painel principal, pressione e mantenha pressionada ou clique com o botão direito do mouse na exclusão, selecione Delete e toque ou clique em Yes para responder à mensagem de confirmação.

Reserva de endereços DHCP

O DHCP disponibiliza várias maneiras de atribuir endereços permanentes a clientes. Uma opção é usar a configuração Unlimited na caixa de diálogo Scope para atribuir endereços permanentes a todos os clientes que usem o escopo. Outra, é reservar endereços DHCP para cliente. Ao reservar um endereço DHCP, o servidor DHCP sempre atribui o mesmo endereço IP ao cliente e você não precisa sacrificar para isso os recursos de gerenciamento centralizado que tornam o DHCP tão atraente.

Para reservar um endereço IPv4 para um cliente, siga estas etapas:

1. No console DHCP, expanda o escopo com o qual você deseja trabalhar e pressione e mantenha pressionada ou clique com o botão direito do mouse na pasta Reservations. No menu de atalho, toque ou clique em New Reservation.
2. Na caixa de texto Reservation Name, digite um nome curto e ao mesmo tempo descriptivo para a reserva. Esse nome é usado apenas para fins de identificação.
3. Na caixa IP Address, insira o endereço IPv4 que você deseja reservar para o cliente.

OBSERVAÇÃO Esse endereço IP deve estar dentro do intervalo de endereços válido para o escopo selecionado no momento.

4. A caixa MAC Address especifica o endereço MAC para a NIC do computador cliente. Você pode obter o endereço MAC digitando o comando **ipconfig /all** no prompt de comando do computador cliente. A entrada Physical Address exibe o endereço MAC do cliente. Você deve digitar esse valor de maneira exata para que a reserva de endereço funcione.
5. Se desejar, insira um comentário na caixa de texto Description.
6. Por padrão, tanto clientes DHCP quanto BOOTP são suportados. Essa opção é satisfatória e você precisará alterá-la apenas se desejar excluir um tipo específico de cliente.
7. Toque ou clique em Add para criar uma reserva de endereço. Repita esta etapa para adicionar outras reservas de endereço.
8. Toque ou clique em Close ao terminar.

Para reservar um endereço IPv6 para um cliente, siga estas etapas:

1. No console DHCP, expanda o escopo com o qual você deseja trabalhar e pressione e mantenha pressionada ou clique com o botão direito do mouse na pasta Reservations. No menu de atalho, toque ou clique em New Reservation.
2. Na caixa de texto Reservation, digite um nome curto e ao mesmo tempo descriptivo para a reserva. Essa informação é usada apenas para fins de identificação.
3. Na caixa IPv6 Address, insira o endereço IPv6 que você deseja reservar para o cliente.

OBSERVAÇÃO Esse endereço IP deve estar dentro do intervalo de endereços válido para o escopo selecionado no momento.

4. A caixa Device Unique Identifier (DUID, identificador exclusivo do dispositivo) especifica o endereço MAC para a NIC do computador cliente. Você pode obter o endereço MAC digitando o comando **ipconfig /all** no prompt de comando do computador cliente. A entrada Physical Address exibe o endereço MAC do cliente. Você deve digitar esse valor de maneira exata para que a reserva de endereço funcione.
5. O Identity Association Identifier (IAID) define um prefixo de identificador exclusivo para o cliente. Normalmente, esse valor apresenta nove dígitos.
6. Se desejar, insira um comentário na caixa de texto Description.
7. Toque ou clique em Add para criar uma reserva de endereço. Repita esta etapa para adicionar outras reservas de endereço.
8. Toque ou clique em Close ao terminar.

Liberação de endereços e concessões

Ao trabalhar com endereços reservados, é necessário observar duas questões com cuidado:

- Os endereços reservados não são automaticamente reatribuídos. Se o endereço já estiver em uso, você precisará liberá-lo para garantir que o cliente apropriado possa obtê-lo. Você pode forçar um cliente a liberar um endereço finalizando a concessão do cliente ou efetuando logon no cliente e digitando o comando **ipconfig /release** no prompt de comando.
- Os clientes não alternam automaticamente para o endereço reservado. Se o cliente estiver usando um endereço IP diferente, você precisará forçar o cliente a liberar a concessão atual e solicitar uma nova. Você pode fazer isso finalizando a concessão do cliente ou efetuando logon no cliente e digitando o comando **ipconfig /renew** no prompt de comando.

Como modificar as propriedades de reservas

Você pode modificar as propriedades de reservas seguindo estas etapas:

1. No console DHCP, expanda o escopo com o qual você deseja trabalhar e toque ou clique na pasta Reservations.
2. Pressione e mantenha pressionada ou clique com o botão direito do mouse na reserva e toque ou clique em Properties. Nesse momento, você pode modificar as propriedades da reserva. As opções sombreadas não podem ser modificadas, mas as outras podem. Essas opções são as mesmas descritas na seção anterior.

Como excluir concessões e reservas

Você pode excluir concessões e reservas ativas seguindo estas etapas:

1. No console DHCP, expanda o escopo com o qual você deseja trabalhar e toque ou clique na pasta Address Leases ou na pasta Reservations, conforme apropriado.
2. Pressione e mantenha pressionada ou clique com o botão direito do mouse na concessão ou reserva que você deseja excluir e toque ou clique em Delete.
3. Confirme a exclusão tocando ou clicando em Yes.
4. A concessão ou reserva é removida do DHCP. No entanto, o cliente não é forçado a liberar o endereço IP. Para forçar o cliente a liberar o endereço IP, efetue logon no cliente que possui a concessão ou a reserva e digite o comando **ipconfig /release** no prompt de comando.

Como fazer backup e restaurar o banco de dados do DHCP

Os servidores DHCP armazenam informações sobre concessões e reservas do DHCP em arquivos de banco de dados. Por padrão, esses arquivos são armazenados no diretório %SystemRoot%\System32\DHCP. Os arquivos mais importantes desse diretório são usados da seguinte maneira:

- **Dhcp.mdb** O arquivo de banco de dados primário para o servidor DHCP
- **J50.log** Um arquivo de log de transações usado para recuperar transações incompletas no caso de um servidor apresentar mau funcionamento
- **J50.chk** Um arquivo de ponto de verificação usado para determinar quais entradas do log de transações já foram efetivadas na base de dados do servidor DHCP
- **J500000A.log** Um arquivo de log reservado para o servidor DHCP
- **J500000B.log** Um arquivo de log reservado para o servidor DHCP
- **J500000C.log** Um arquivo de log reservado para o servidor DHCP
- **J500000D.log** Um arquivo de log reservado para o servidor DHCP
- **J500000E.log** Um arquivo de log reservado para o servidor DHCP
- **J500000F.log** Um arquivo de log reservado para o servidor DHCP
- **Tmp.edb** Um arquivo de trabalho temporário para o servidor DHCP

Como fazer backup do banco de dados do DHCP

A pasta %SystemRoot%\System32\DHCP\Backup contém as informações de backup para a configuração de DHCP e o banco de dados do DHCP. Por padrão, o backup do banco de dados do DHCP é feito a cada 60 minutos automaticamente. Para fazer backup manualmente do banco de dados do DHCP a qualquer momento, siga estas etapas:

1. No console DHCP, pressione e mantenha pressionado ou clique com o botão direito do mouse no servidor do qual você deseja fazer backup e toque ou clique em Backup.

2. Na caixa de diálogo Browse For Folder, selecione a pasta que conterá o banco de dados do DHCP de backup e toque ou clique em OK.

As chaves de registro que controlam o local e a frequência dos backups do DHCP, bem como outras configurações de DHCP, estão localizadas sob: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters.

As chaves a seguir controlam a configuração do banco de dados e do backup do DHCP:

- **BackupDatabasePath** Determina o local do banco de dados do DHCP. Essa opção deve ser configurada por meio da caixa de diálogo Properties do DHCP. Toque ou clique na guia Advanced e defina o Database Path conforme apropriado.
- **DatabaseName** Determina o nome do arquivo de banco de dados primário do DHCP. O valor padrão é DHCP.mdb.
- **BackupInterval** Determina a frequência com que é feito o backup do banco de dados das informações dos clientes DHCP. O padrão é 60 minutos.
- **DatabaseCleanupInterval** Determina com que frequência o serviço de DHCP exclui registros expirados do banco de dados das informações dos clientes DHCP. O valor padrão é de 4 horas.

Como restaurar o banco de dados do DHCP a partir do backup

No caso de uma falha e posterior recuperação do servidor, talvez você precise restaurar e reconciliar o banco de dados do DHCP. Para forçar o DHCP a restaurar o banco de dados a partir do backup, siga estas etapas:

1. Se necessário, restaure uma cópia íntegra da pasta %SystemRoot%\System32\DHCP\Backup do arquivo morto. Após, inicie o console DHCP, pressione e mantenha pressionado ou clique com o botão direito do mouse no servidor que você deseja restaurar e toque ou clique em Restore.
2. Na caixa de diálogo Browse For Folder, selecione a pasta que contém o backup a ser restaurado e toque ou clique em OK.
3. Durante a restauração do banco de dados, o serviço DHCP Server é interrompido.

Como resultado, os clientes DHCP permanecem temporariamente incapazes de contatar o servidor DHCP para obter endereços IP.

Como usar backup e restauração para mover um banco de dados do DHCP para um novo servidor

Se você precisa remontar um servidor que esteja fornecendo serviços de DHCP, talvez queira mover os serviços de DHCP a outro servidor antes de remontar o servidor. Para isso, você precisa realizar diversas tarefas nos servidores de origem e destino. No servidor de destino, faça o seguinte:

1. Instale o serviço DHCP Server no servidor de destino e reinicie o servidor.
2. Interrompa o serviço DHCP Server no console Services.
3. Exclua o conteúdo da pasta %SystemRoot%\System32\DHCP.

No servidor original, faça o seguinte:

1. Interrompa o serviço DHCP Server no console Services.
2. Após a interrupção do serviço DHCP Server, desabilite o serviço para que ele não possa mais ser iniciado.
3. Copie todo o conteúdo da pasta %SystemRoot%\System32\DHCP para a pasta %SystemRoot%\System32\DHCP do servidor de destino.

Agora, todos os arquivos necessários estão no servidor de destino. Inicie o serviço DHCP Server no servidor de destino para completar a migração.

Como forçar o serviço DHCP Server a gerar o banco de dados do DHCP novamente

Se o banco de dados do DHCP for corrompido e o Windows não conseguir repará-lo quando você interrompe e reinicia o serviço DHCP Server, você poderá tentar restaurar o banco de dados conforme descrito em “Como restaurar o banco de dados do DHCP a partir do backup” anteriormente neste capítulo. Se essa ação falhar ou você preferir iniciar com uma nova cópia do banco de dados do DHCP, siga estas etapas:

1. Interrompa o serviço DHCP Server no console Services.
2. Exclua o conteúdo da pasta %SystemRoot%\System32\DHCP. Se desejar forçar uma nova geração completa do banco de dados e impedir que o servidor faça sua restauração a partir de um backup anterior, você também deve excluir o conteúdo da pasta Backup.

ATENÇÃO Mantenha os arquivos DHCP se as chaves de registro DHCPServer não estiverem intactas. Essas chaves devem estar disponíveis para restaurar o banco de dados do DHCP.

3. Reinicie o serviço DHCP Server.
4. Nenhuma concessão ativa ou outra informação para escopos é exibida no console DHCP. Para recuperar as concessões ativas para cada escopo, você deve reconciliar os escopos do servidor conforme discutido na próxima seção.
5. Para impedir que haja conflitos com concessões anteriormente atribuídas, você deve manter habilitada a detecção de conflitos de endereços por alguns dias, conforme discutido anteriormente em “Como evitar conflitos de endereço IP” neste capítulo.

Como reconciliar concessões e reservas

A reconciliação verifica as concessões e reservas de clientes comparando-as ao banco de dados do DHCP no servidor. Se forem encontradas inconsistências entre o que está gravado no registro do Windows e o que está gravado no banco de dados do servidor DHCP, você pode selecionar e reconciliar qualquer entrada inconsistente. Após a reconciliação das entradas selecionadas, o DHCP restaura o endereço IP ao proprietário original ou cria uma reserva temporária para o endereço IP. Quando o tempo de concessão expira, o endereço é recuperado para uso futuro.

Você pode reconciliar escopos individualmente ou em conjunto no servidor. Para reconciliar um escopo individualmente, siga estas etapas:

1. No console DHCP, pressione e mantenha pressionado ou clique com o botão direito do mouse no escopo com o qual você deseja trabalhar e toque ou clique em Reconcile.
2. Na caixa de diálogo Reconcile, toque ou clique em Verify.
3. As inconsistências são relatadas na janela de status. Selecione os endereços exibidos e toque ou clique em Reconcile para corrigir as inconsistências.
4. Se não forem encontradas inconsistências, toque ou clique em OK.

Para reconciliar todos os escopos de um servidor, siga estas etapas:

1. No console DHCP, expanda a entrada do servidor, pressione e mantenha pressionado ou clique com o botão direito do mouse no nó IPv4 e toque ou clique em Reconcile All Scopes.
2. Na caixa de diálogo Reconcile All Scopes, toque ou clique em Verify.
3. As inconsistências são relatadas na janela de status. Selecione os endereços exibidos e toque ou clique em Reconcile para corrigir as inconsistências.
4. Se não forem encontradas inconsistências, toque ou clique em OK.

CAPÍTULO 16

Otimização do DNS

- Introdução ao DNS **610**
- Configuração de resolução de nomes em clientes DNS **615**
- Instalação de servidores DNS **616**
- Gerenciamento de servidores DNS **626**
- Gerenciamento de registros de DNS **631**
- Atualização de propriedades de zona e o registro SOA **636**
- Gerenciamento da configuração e da segurança do servidor DNS **640**

Este capítulo mostra as técnicas utilizadas para instalar e gerenciar o Domain Name System (DNS, Sistema de Nomes de Domínio) em uma rede. O DNS é o serviço de resolução de nomes que resolve nomes de computadores para endereços IP. Quando se utiliza o DNS, um nome de host totalmente qualificado – omega.microsoft.com, por exemplo – pode ser resolvido para um endereço IP, permitindo que os computadores localizem uns aos outros. O DNS opera na pilha de protocolo TCP/IP e pode ser integrado com o Windows Internet Name Service (WINS), o Dynamic Host Configuration Protocol (protocolo DHCP) e o Active Directory. A integração total do DNS com esses recursos de rede do Windows permite otimizá-lo para domínios do Microsoft Windows Server.

Introdução ao DNS

O DNS organiza grupos de computadores em domínios. Esses domínios são organizados em uma estrutura hierárquica, que pode ser definida na Internet para redes públicas ou na empresa para redes privadas (também chamadas, respectivamente, de *extranets* e *intranets*). Os vários níveis da hierarquia identificam computadores específicos, domínios organizacionais e domínios de primeiro nível. Para o nome de host totalmente qualificado omega.microsoft.com, *omega* representa o nome do host de um computador específico, *microsoft* é o domínio organizacional e *com* é o domínio de primeiro nível.

Os domínios de primeiro nível são a raiz da hierarquia DNS e também são chamados de *root domains* (domínios-raiz). Esses domínios são organizados geograficamente, por tipo de organização e por função. Os domínios normais, como microsoft.com, também são chamados de *parent domains* (domínios-pai), pois são os pais de uma estrutura organizacional. Pode-se dividir os domínios-pai em subdomínios que serão utilizados para grupos ou departamentos dentro da empresa.

Os subdomínios são muitas vezes chamados de *child domains* (domínios-filho). Por exemplo, o fully qualified domain name (FQDN, nome de domínio totalmente qualificado) de um computador de um grupo de recursos humanos poderia ser de-

signado jacob.hr.microsoft.com. Aqui, *jacob* é o nome do host, *hr* é o domínio-filho e *microsoft.com* é o domínio-pai.

Integração do Active Directory com o DNS

Como afirmado no Capítulo 6, “Como utilizar o Active Directory”, os domínios do Active Directory utilizam o DNS para implementar sua estrutura e hierarquia de nomenclatura. O Active Directory e o DNS são integrados, tanto que é preciso instalar o DNS na rede antes de instalar o Active Directory Domain Services (AD DS).

Durante a instalação do primeiro controlador de domínio em uma rede do Active Directory, tem-se a oportunidade de instalar o DNS automaticamente se um servidor DNS não puder ser encontrado na rede. Também é possível especificar se o DNS e o Active Directory devem ser totalmente integrados. Na maioria dos casos, é aconselhável responder afirmativamente a ambas as perguntas. Com a integração total, as informações de DNS serão armazenadas diretamente no Active Directory, o que permite aproveitar a capacidade do Active Directory.

Entender a diferença entre as integrações parcial e total é muito importante:

- **Integração parcial** Com a integração parcial, o domínio utiliza o armazenamento de arquivos padrão. As informações de DNS são armazenadas em arquivos baseados em texto que terminam com a extensão .dns. A localização padrão desses arquivos é %SystemRoot%\System32\DNS. As atualizações para o DNS são controladas por meio de um único servidor DNS autoritativo. Esse servidor é designado como o servidor DNS primário para o domínio específico ou para uma parte desse domínio chamada zona. Os clientes que utilizam atualizações dinâmicas do DNS por meio do DHCP devem estar configurados para utilizar o servidor DNS primário da zona. Se não estiverem, as informações no DNS não serão atualizadas. Da mesma forma, as atualizações dinâmicas por meio do DHCP não podem ser feitas se o servidor DNS primário estiver offline.
- **Integração total** Com a integração total, o domínio utiliza o armazenamento integrado ao diretório. As informações de DNS são armazenadas diretamente no Active Directory e ficam disponíveis por meio do contêiner do objeto *dnsZone*. Como as informações fazem parte do Active Directory, qualquer controlador de domínio pode acessar os dados e é possível utilizar uma abordagem de vários mestres para as atualizações dinâmicas por meio do DHCP. Isso permite que qualquer controlador de domínio com o serviço DNS Server receba as atualizações dinâmicas. Além disso, os clientes que utilizam as atualizações dinâmicas no DNS por meio do DHCP podem usar qualquer servidor DNS dentro da zona. Um benefício adicional da integração ao diretório é a capacidade de utilizar a segurança do diretório para controlar o acesso às informações de DNS.

Se observar a forma como as informações de DNS são replicadas pela rede, verá mais vantagens na integração total com o Active Directory. Com a integração parcial, as informações de DNS são armazenadas e replicadas separadamente do Active Directory. Tendo-se duas estruturas separadas, a eficácia do DNS e do Active Directory é reduzida e a administração se torna mais complexa. Como o DNS é menos eficiente que o Active Directory em replicar alterações, você também poderia aumentar o tráfego da rede e a quantidade de tempo necessária para replicar as alterações de DNS por ela.

Em versões anteriores do serviço DNS Server para servidores do Windows, a reinicialização de um servidor DNS poderia levar uma hora ou mais em grandes empresas com zonas extremamente grandes integradas ao AD DS. A operação demorava tanto tempo porque os dados de zona eram carregados em primeiro plano enquanto o servidor estava iniciando o serviço DNS. Para garantir que os servidores DNS possam responder mais rapidamente após uma reinicialização, o serviço DNS Server para o Windows Server 2008 R2 e posteriores foi aprimorado para carregar os dados de zona do AD DS em segundo plano enquanto o serviço é reiniciado. Isso assegura que o servidor DNS responda às solicitações de dados de zonas e possa controlá-las.

Na inicialização, os servidores DNS com o Windows Server 2008 R2 e posteriores realizam as seguintes tarefas:

- Enumeram todas as zonas a ser carregadas
- Carregam dicas de raiz de arquivos ou do armazenamento do AD DS
- Carregam todas as zonas que estejam armazenadas em arquivos, e não no AD DS
- Começam a responder às consultas e chamadas de procedimento remoto (RPCs, Remote Procedure Calls)
- Criam uma ou mais threads para carregar as zonas que estejam armazenadas no AD DS

Como as threads separadas carregam os dados de zona, o servidor DNS pode responder às consultas enquanto o carregamento de zona está em andamento. Se um cliente DNS realizar uma consulta para um host em uma zona que já tenha sido carregada, o servidor DNS responderá apropriadamente. Se a consulta for para um host que ainda não tenha sido carregado na memória, o servidor DNS irá ler os dados do host a partir do AD DS e atualizar sua lista de registro de modo adequado.

Como habilitar o DNS na rede

Para habilitar o DNS na rede, é preciso configurar os clientes e servidores DNS. Quando se configura os clientes DNS, informa-se aos clientes os endereços IP dos servidores DNS da rede. Utilizando esses endereços, os clientes podem se comunicar com os servidores DNS em qualquer parte da rede, mesmo se os servidores estiverem em sub-redes diferentes.

OBSERVAÇÃO A configuração de um cliente DNS é explicada no Capítulo 14, “Gerenciamento de redes TCP/IP”. A configuração de um servidor DNS será explicada na próxima seção deste capítulo.

O cliente DNS integrado em computadores com o Microsoft Windows 7 e posteriores, bem como o Windows Server 2008 R2 ou posteriores, dá suporte ao tráfego DNS pelo IPv4 (Internet Protocol version 4) e pelo IPv6 (Internet Protocol version 6). Por padrão, o IPv6 configura os endereços site-local conhecidos (well-known) dos servidores DNS em FEC0:0:0:FFFF::1, FEC0:0:0:FFFF::2 e FEC0:0:0:FFFF::3. Para adicionar os endereços IPv6 de seus servidores DNS, utilize as propriedades do componente TCP/IPv6 (Internet Protocol Version 6) em Network Connections ou o seguinte comando:

```
netsh interface IPV6 ADD DNS
```

Os servidores DNS com o Windows Server 2008 R2 ou posteriores dão aos endereços IPv6 um suporte tão completo quanto aos endereços IPv4. No console DNS Ma-

nager, os endereços do host são exibidos como endereços IPv4 ou IPv6. A ferramenta de linha de comando Dnscmd também aceita endereços em ambos os formatos. Além disso, os servidores DNS agora podem enviar consultas recursivas somente a servidores IPv6 e a lista de encaminhadores do servidor pode conter endereços IPv4 e IPv6. Por fim, os servidores DNS agora dão suporte ao namespace de domínio `ip6.arpa` para pesquisas inversas.

Quando a rede utiliza o DHCP, deve-se configurá-lo para trabalhar com o DNS. Os clientes DHCP podem registrar os endereços IPv6 em conjunto com os endereços IPv4 ou em lugar deles. Para garantir a integração adequada do DHCP com o DNS, é preciso definir as opções de escopo do DHCP como especificado em “Configuração das opções de escopo” no Capítulo 15, “Como executar clientes e servidores DHCP”. Para o IPv4, deve-se definir as opções de escopo 006 DNS Servers e 015 DNS Domain Name. Para o IPv6, deve-se definir as opções de escopo 00023 DNS Recursive Name Server IPV6 Address List e 00024 Domain Search List. Além disso, se os computadores da rede precisarem estar acessíveis a partir de outros domínios do Active Directory, é necessário criar registros para eles no DNS. Os registros de DNS são organizados em zonas, sendo uma *zona* simplesmente uma área dentro de um domínio.

Os computadores clientes DNS com o Windows 7 ou posterior, bem como o Windows Server 2008 R2 ou posterior, podem utilizar a Link-Local Multicast Name Resolution (LLMNR) para resolver nomes em um segmento de rede local quando um servidor DNS não estiver disponível. Eles também procuram periodicamente um controlador de domínio no domínio a que pertencem. Essa funcionalidade ajuda a evitar problemas de desempenho que poderiam ocorrer se uma falha de rede ou servidor fizesse com que um cliente DNS criasse uma associação com um controlador de domínio distante, localizado em um link lento, em lugar de um controlador de domínio local. Anteriormente, essa associação continuava até que o cliente fosse forçado a buscar um novo controlador de domínio, como quando o computador cliente era desconectado da rede por um longo período de tempo. Ao renovar periodicamente sua associação com um controlador de domínio, o cliente DNS pode reduzir a probabilidade de vir a ser associado a um controlador de domínio inadequado.

O serviço de cliente DNS para o Windows 8 e o Windows Server 2012 tem várias melhorias de interoperabilidade e segurança específicas para LLMNR e NetBIOS. Para melhorar a segurança da rede móvel, o serviço:

- Não envia consultas LLMNR de saída pela banda larga móvel ou interfaces VPN
- Não envia consultas NetBIOS de saída pela banda larga móvel

Para uma melhor compatibilidade com os dispositivos em modo de economia de energia, o tempo limite da consulta LLMNR foi aumentado para 410 milissegundos (ms) para a primeira nova tentativa e 410 ms para a segunda, perfazendo o valor de tempo limite total de 820 ms, em vez de 300 ms. Para melhorar os tempos de resposta para todas as consultas, o serviço de cliente DNS faz o seguinte:

- Emite consultas LLMNR e NetBIOS em paralelo e otimiza o IPv4 e o IPv6
- Divide interfaces em redes para enviar consultas DNS paralelas
- Utiliza o armazenamento em cache de DNS assíncrono com um tempo de resposta otimizado

OBSERVAÇÃO Pode-se configurar um computador cliente DNS com o Windows 7 ou posteriores, bem como com o Windows Server 2008 R2 ou posteriores, para localizar o controlador de domínio mais próximo, em vez de pesquisar aleatoriamente. Isso pode melhorar o desempenho em redes contendo domínios que se conectam através de links lentos. Contudo, por causa do tráfego de rede que esse processo gera, a localização do controlador de domínio mais próximo pode ter um impacto negativo no desempenho da rede.

O Windows Server 2008 e posteriores dão suporte a zonas primárias somente leitura e à zona GlobalNames. Para dar suporte a read-only domain controllers (RODCs, controladores de domínio somente leitura), a zona somente leitura primária será criada automaticamente. Quando um computador se torna um RODC, ele replica uma cópia somente leitura completa de todas as partições de aplicativos que o DNS utiliza, incluindo a partição de domínio, ForestDNSZones e DomainDNSZones. Isso assegura que o servidor DNS em execução no RODC tenha uma cópia somente leitura completa de qualquer zona DNS. Como administrador de um RODC, você pode visualizar o conteúdo de uma zona somente leitura primária. No entanto, não é possível alterar o conteúdo de uma zona no RODC. Pode-se alterar o conteúdo da zona somente em um controlador de domínio padrão.

Para dar suporte a todos os ambientes DNS e à resolução de nomes de rótulo único, pode-se criar uma zona chamada *GlobalNames*. Para um desempenho ideal e suporte entre florestas, deve-se integrar essa zona com o AD DS e configurar cada servidor DNS autoritativo com uma cópia local. Quando se utiliza os registros de recursos Service Location (SRV) para publicar a localização da zona GlobalNames, ela fornece nomes de computadores exclusivos e de rótulo único pela floresta. Diferentemente do WINS, a zona GlobalNames se destina a fornecer a resolução de nomes de rótulo único para um subconjunto de nomes de host – normalmente, os registros de recursos CNAME para seus servidores corporativos. A zona GlobalNames não se destina a ser utilizada para a resolução de nomes ponto a ponto, como a resolução de nomes para estações de trabalho. A LLMNR serve para isso.

Quando a zona GlobalNames está configurada apropriadamente, a resolução de nomes de rótulo único funciona como se segue:

1. O sufixo DNS primário do cliente é acrescentado ao nome de rótulo único que o cliente estiver pesquisando e a consulta é submetida ao servidor DNS.
2. Se o nome completo desse computador não estiver resolvido, o cliente solicitará a resolução utilizando suas listas de pesquisa de sufixo DNS, se tiver alguma.
3. Se nenhum desses nomes puder ser resolvido, o cliente solicitará a resolução utilizando o nome de rótulo único.
4. Se o nome de rótulo único aparecer na zona GlobalNames, o servidor DNS hospedando-a o resolverá. Caso contrário, a consulta recorrerá ao WINS.

A zona GlobalNames fornece a resolução de nomes de rótulo único somente quando todos os servidores DNS autoritativos tiverem o Windows Server 2008 R2 ou posteriores. No entanto, outros servidores DNS que não são autoritativos para qualquer zona podem ter outros sistemas operacionais. As atualizações dinâmicas na zona GlobalNames não têm suporte.

Configuração de resolução de nomes em clientes DNS

A melhor maneira de configurar a resolução de nomes para clientes DNS dependerá da configuração de sua rede. Se os computadores utilizarem o DHCP, provavelmente será desejável configurar o DNS por meio de configurações no servidor DHCP. Se os computadores utilizarem endereços IP estáticos ou você quiser configurar o DNS especificamente para um determinado sistema, deve-se configurar o DNS manualmente.

É possível fazer as configurações do DNS na guia DNS da caixa de diálogo Advanced TCP/IP Settings. Para acessar essa caixa de diálogo, siga estas etapas:

1. Abra Network And Sharing Center e toque ou clique em Change Adapter Settings.
2. Em Network Connections, pressione e segure ou clique com o botão direito do mouse na conexão com a qual quer trabalhar e toque ou clique em Properties.
3. Toque ou clique duas vezes em Internet Protocol Version 6 (TCP/IPv6) ou Internet Protocol Version 4 (TCP/IPv4), dependendo do tipo de endereço IP que estiver configurando.
4. Se o computador estiver utilizando o DHCP e você quiser que ele especifique o endereço do servidor DNS, selecione Obtain DNS Server Address Automatically. Caso contrário, selecione Use The Following DNS Server Addresses e digite os endereços primário e alternativo do servidor DNS nas caixas de texto fornecidas.
5. Toque ou clique em Advanced para exibir a caixa de diálogo Advanced TCP/IP Settings. Nessa caixa de diálogo, toque ou clique na guia DNS.

Utilize as opções da guia DNS como a seguir:

- **DNS Server Addresses, In Order Of Use** Utilize esta área para especificar o endereço IP de cada servidor DNS que seja utilizado para a resolução de nomes de domínios. Toque ou clique em Add se quiser adicionar um endereço IP de servidor à lista. Toque ou clique em Remove para remover um endereço de servidor selecionado da lista. Toque ou clique em Edit para editar uma entrada selecionada. Pode-se especificar vários servidores para a resolução de DNS. A prioridade deles é determinada pela ordem. Se o primeiro servidor não estiver disponível para responder a uma solicitação de resolução de nome do host, o próximo servidor DNS na lista será acessado e assim por diante. Para alterar a posição de um servidor na caixa da lista, selecione-o e utilize o botão de seta para cima ou para baixo.
- **Append Primary And Connection Specific DNS Suffixes** Normalmente, esta opção está selecionada por padrão. Selecione-a para resolver nomes de computadores não qualificados do domínio primário. Por exemplo, se o nome de computador Gandolf for utilizado e o domínio-pai for microsoft.com, o nome do computador tentará ser resolvido para gandolf.microsoft.com. Se o nome do computador totalmente qualificado não existir no domínio-pai, a consulta irá falhar. O domínio-pai utilizado é o definido na guia Computer Name da caixa de diálogo System Properties. (Toque ou clique em System And Security\System no Control Panel, em Change Settings e exiba a guia Computer Name para verificar as configurações.)
- **Append Parent Suffixes Of The Primary DNS Suffix** Esta opção está selecionada por padrão. Selecione-a para resolver nomes de computadores não qualificados utilizando a hierarquia de domínio-pai/filho. Se uma consulta falhar no

domínio-pai imediato, o sufixo do pai do domínio-pai será utilizado para tentar resolver a consulta. Esse processo continuará até que o topo da hierarquia de domínio DNS seja alcançado. Por exemplo, se o nome de computador Gandolf fosse utilizado no domínio dev.microsoft.com, o DNS tentaria resolver o nome do computador para gandolf.dev.microsoft.com. Se isso não funcionasse, o DNS tentaria resolver o nome do computador para gandolf.microsoft.com.

- **Append These DNS Suffixes (In Order)** Seleciona esta opção para definir sufixos DNS específicos a utilizar, em lugar da resolução por meio do domínio-pai. Toque ou clique em Add se quiser adicionar um sufixo de domínio à lista. Toque ou clique em Remove para remover um sufixo de domínio selecionado na lista. Toque ou clique em Edit para editar a entrada selecionada. Pode-se especificar vários sufixos de domínio, que serão utilizados em ordem. Se o primeiro sufixo não for resolvido adequadamente, o DNS tentará utilizar o próximo na lista. Se isso falhar, o próximo sufixo será utilizado e assim por diante. Para alterar a ordem dos sufixos de domínio, selecione o sufixo e utilize o botão de seta para cima ou para baixo para alterar sua posição.
- **DNS Suffix For This Connection** Esta opção define um sufixo DNS específico para a conexão que substituirá os nomes DNS já configurados para uso nela. Geralmente, se define o nome de domínio DNS na guia Computer Name da caixa de diálogo System Properties.
- **Register This Connection's Addresses In DNS** Seleciona esta opção se quiser que todos os endereços IP desta conexão sejam registrados no DNS sob o nome de domínio totalmente qualificado do computador. Esta opção está selecionada por padrão.

OBSERVAÇÃO As atualizações dinâmicas do DNS são utilizadas em conjunto com o DHCP para permitir que um cliente atualize seu registro A (Host Address) caso seu endereço IP mude e para permitir que o servidor DHCP atualize o registro PTR (Pointer) para o cliente do servidor DNS. Pode-se configurar os servidores DHCP para atualizar os registros A e PTR em nome do cliente. As atualizações dinâmicas do DNS têm suporte nos servidores DNS com BIND 8.2.1 ou superiores, bem como no Windows 2000 Server, Windows Server 2003 e versões de servidores posteriores do Windows.

- **Use This Connection's DNS Suffix In DNS Registration** Seleciona esta opção se quiser que todos os endereços IP desta conexão sejam registrados no DNS sob o domínio-pai.

Instalação de servidores DNS

Pode-se configurar qualquer servidor com Windows Server 2012 como um servidor DNS. Quatro tipos de servidores DNS estão disponíveis:

- **Servidor primário integrado ao Active Directory** Um servidor DNS que está totalmente integrado ao Active Directory. Todos os dados do DNS são armazenados diretamente no Active Directory.
- **Servidor primário** O principal servidor DNS de um domínio que esteja parcialmente integrado ao Active Directory. Esse servidor armazena uma cópia mestra dos registros de DNS e os arquivos de configuração do domínio. Esses arquivos são armazenados como arquivos de texto com a extensão .dns.

- **Servidor secundário** Um servidor DNS que fornece serviços de backup para o domínio. Esse servidor armazena uma cópia dos registros do DNS obtidos de um servidor primário e depende das transferências de zona para atualizações. Os servidores secundários obtêm suas informações de DNS de um servidor primário quando são iniciados e as mantêm até que elas sejam atualizadas ou percam a validade.
- **Servidor somente de encaminhamento** Um servidor que armazena em cache as informações de DNS após pesquisas e sempre repassa as solicitações para outros servidores. Esses servidores mantêm as informações de DNS até que sejam atualizadas ou percam a validade, ou até que o servidor seja reiniciado. Diferentemente dos servidores secundários, os servidores somente de encaminhamento não solicitam cópias completas dos arquivos de banco de dados de uma zona. Isso significa que, ao iniciar um servidor somente de encaminhamento, seu banco de dados não contém informações.

Antes de configurar um servidor DNS, é preciso instalar o serviço DNS Server. A seguir, é possível configurar o servidor para fornecer serviços DNS integrados, primários, secundários ou somente de encaminhamento.

Instalação e configuração do serviço DNS Server

Todos os controladores de domínio podem agir como servidores DNS e talvez seja solicitado que você instale e configure o DNS durante a instalação do controlador de domínio. Se responder afirmativamente às solicitações, o DNS já será instalado e a configuração padrão será definida automaticamente. Não será preciso reinstá-lo.

Se estiver trabalhando com um servidor membro em vez de um controlador de domínio, ou se não tiver instalado o DNS, siga estas etapas para fazê-lo:

1. No Server Manager, toque ou clique em Manage e em Add Roles And Features, ou selecione Add Roles And Features no painel Quick Start. O Add Roles And Features Wizard será iniciado. Se o assistente exibir a página Before You Begin, leia o texto Welcome e toque ou clique em Next.
2. Na página Installation Type, a opção Role-Based Or Feature-Based Installation está selecionada por padrão. Toque ou clique em Next.
3. Na página Server Selection, pode-se escolher instalar funções e recursos em servidores ou discos rígidos virtuais em execução. Selecione um servidor do pool de servidores ou um do pool de servidores no qual montar um virtual hard disk (VHD, disco rígido virtual). Se estiver adicionando funções e recursos a um VHD, toque ou clique em Browse e depois use a caixa de diálogo Browse For Virtual Hard Disks para localizá-lo. Quando estiver pronto para continuar, toque ou clique em Next.

OBSERVAÇÃO Somente servidores com o Windows Server 2012 e que tenham sido adicionados para gerenciamento no Server Manager serão listados.

4. Na página Server Roles, selecione DNS Server. Se recursos adicionais forem necessários para instalar uma função, você verá uma caixa de diálogo adicional. Toque ou clique em Add Features para fechar a caixa de diálogo e adicionar os recursos necessários para a instalação do servidor. Quando estiver pronto para continuar, toque ou clique em Next três vezes.

5. Se o servidor em que quer instalar a função DNS Server não tiver todos os arquivos de origem binários necessários, o servidor os obterá via Windows Update por padrão ou de uma localização especificada via Group Policy.

OBSERVAÇÃO Também é possível especificar um caminho alternativo para os arquivos de origem necessários. Para fazê-lo, clique no link Specify An Alternate Source Path, digite o caminho alternativo na caixa fornecida e toque ou clique em OK. Para compartilhamentos de rede, digite o caminho UNC para o compartilhamento, como \\CorpServer82\WinServer2012\. Para imagens montadas do Windows, digite o caminho do WIM prefixado com WIM: e incluindo o índice da imagem a utilizar, como WIM:\\CorpServer82\WinServer2012\install.wim:4.

6. Toque ou clique em Install para começar o processo de instalação. A página Installation Progress acompanha o progresso da instalação. Se fechar o assistente, toque ou clique no ícone Notifications no Server Manager e depois no link fornecido para reabri-lo.
7. Quando o Setup terminar de instalar a função DNS Server, a página Installation Progress será atualizada para refleti-lo. Examine os detalhes da instalação para garantir que tenha sido bem-sucedida.
8. A partir de agora, o serviço DNS Server deverá iniciar automaticamente toda vez que o servidor for reinicializado. Se não for iniciado, será preciso fazê-lo manualmente. (Consulte "Como iniciar e interromper um servidor DNS" posteriormente neste capítulo.)
9. Depois de instalar um servidor DNS, o console do DNS será utilizado para o configurar e gerenciar. No Server Manager, toque ou clique em Tools e em DNS para abrir o console DNS Manager, mostrado na Figura 16-1.

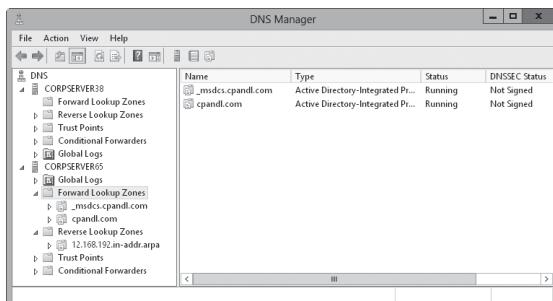


FIGURA 16-1 Utilize o console DNS Manager para gerenciar os servidores DNS na rede.

10. Se o servidor que quiser configurar não estiver listado no modo de exibição de árvore, será preciso se conectar a ele. Pressione e segure ou clique com o botão direito do mouse em DNS no modo de exibição de árvore e toque ou clique em Connect To DNS Server. Faça uma das opções a seguir:
 - Se estiver tentando se conectar a um servidor local, selecione This Computer e toque ou clique em OK.

- Se estiver tentando se conectar a um servidor remoto, selecione The Following Computer, digite o nome ou o endereço IP do servidor e toque ou clique em OK.
- 11.** Uma entrada do servidor DNS deve ser listada no painel do modo de exibição de árvore de console DNS Manager. Pressione e segure ou clique com o botão direito do mouse na entrada do servidor e toque ou clique em Configure A DNS Server. O Configure A DNS Server Wizard será iniciado. Toque ou clique em Next.
- 12.** Na página Select Configuration Action, mostrada na Figura 16-2, selecione Configure Root Hints Only para especificar que somente as estruturas básicas do DNS devem ser criadas neste momento.



FIGURA 16-2 Configure as dicas de raiz para instalar somente as estruturas de base do DNS.

- 13.** Toque ou clique em Next. O assistente irá procurar estruturas existentes do DNS e modificá-las conforme necessário.
- 14.** Toque ou clique em Finish para concluir o processo.

MUNDO REAL Se o assistente não tiver conseguido configurar as dicas de raiz, talvez seja necessário configura-las manualmente ou copiá-las de outro servidor. Contudo, um conjunto padrão de dicas de raiz está incluído no DNS Server e elas devem ser adicionadas automaticamente. Para confirmar, pressione e segure ou clique com o botão direito do mouse na entrada do servidor no console DNS e selecione Properties. Na caixa de diálogo Properties, as dicas de raiz atualmente configuradas serão mostradas na guia Root Hints.

Configuração de um servidor DNS primário

Todo o domínio deve ter um servidor DNS primário. É possível integrar esse servidor com o Active Directory, ou ele pode agir como um servidor primário padrão. Os servidores primários podem ter zonas de pesquisa direta e inversa. Utiliza-se pesquisas diretas para resolver nomes de domínio para endereços IP. As pesquisas inversas (ou reversas) são necessárias para autenticar solicitações DNS resolvendo endereços IP para nomes de domínio ou hosts.

Depois de instalar o serviço DNS Server no servidor, poderá configurar um servidor primário seguindo estas etapas:

1. Inicie o console DNS Manager. Se o servidor que quiser configurar não for listado, conecte-se a ele conforme descrito anteriormente.
2. Uma entrada do servidor DNS deve estar listada no painel do modo de exibição de árvore de console DNS Manager. Pressione e segure ou clique com o botão direito do mouse na entrada do servidor e toque ou clique em New Zone. O New Zone Wizard será iniciado. Toque ou clique em Next.
3. Como mostra a Figura 16-3, pode-se agora selecionar o tipo de zona. Se estiver configurando um servidor primário integrado ao Active Directory (em um controlador de domínio), selecione Primary Zone e certifique-se de que a caixa de seleção Store The Zone In Active Directory esteja marcada. Se não quiser integrar o DNS com o Active Directory, selecione Primary Zone e desmarque a caixa de seleção Store The Zone In Active Directory. Toque ou clique em Next.

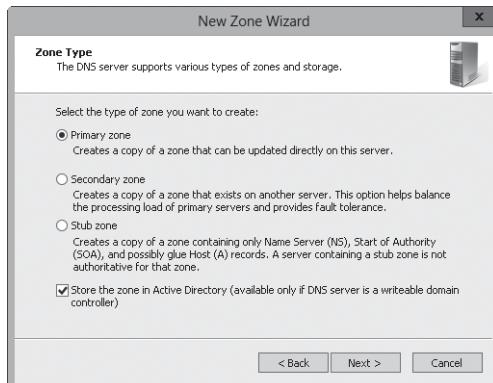


FIGURA 16-3 No New Zone Wizard, selecione o tipo de zona.

4. Se estiver integrando a zona com o Active Directory, escolha uma das estratégias de replicação a seguir; caso contrário, avance para a etapa 6.
 - **To All DNS Servers Running On Domain Controllers In This Forest** Escolha esta estratégia se quiser a estratégia de replicação mais ampla. Lembre-se, a floresta do Active Directory inclui todas as árvores de domínio que compartilhem os dados de diretório com o domínio atual.
 - **To All DNS Servers Running On Domain Controllers In This Domain** Escolha esta estratégia se quiser replicar as informações de DNS dentro do domínio atual.
 - **To All Domain Controllers In This Domain (For Windows 2000 Compatibility)** Escolha esta estratégia se quiser replicar as informações de DNS para todos os controladores de domínio do domínio atual, conforme necessário para a compatibilidade com o Windows 2000. Embora essa estratégia proporcione

uma replicação mais ampla para as informações de DNS dentro do domínio e dê suporte à compatibilidade com o Windows 2000, nem todo controlador de domínio também é um servidor DNS (nem é preciso configurar todo controlador de domínio como um servidor DNS).

5. Toque ou clique em Next. Selecione a opção Forward Lookup Zone e toque ou clique em Next.
6. Digite o nome completo DNS da zona. O nome da zona deve ajudar a determinar como o servidor ou a zona se encaixam na hierarquia de domínio DNS. Por exemplo, se estivesse criando o servidor primário para o domínio microsoft.com, você digitaria **microsoft.com** como o nome da zona. Toque ou clique em Next.
7. Se estiver configurando uma zona primária que não esteja integrada ao Active Directory, é preciso definir o nome do arquivo da zona. Um nome padrão para o arquivo de banco de dados DNS da zona deve estar preenchido. Você pode utilizá-lo ou digitar um novo nome de arquivo. Toque ou clique em Next.
8. Especifique se as atualizações dinâmicas são permitidas. Você tem três opções:
 - **Allow Only Secure Dynamic Updates** Quando a zona está integrada ao Active Directory, pode-se utilizar access control lists (ACLs, listas de controle de acesso) para restringir quais clientes podem realizar as atualizações dinâmicas. Com esta opção selecionada, somente clientes com contas de computadores autorizadas e ACLs aprovadas poderão atualizar seus registros de recursos no DNS quando modificações ocorrerem.
 - **Allow Both Nonsecure And Secure Dynamic Updates** Escolha esta opção para permitir que qualquer cliente atualize seus registros de recursos no DNS quando modificações ocorrerem. Os clientes podem ser seguros ou não.
 - **Do Not Allow Dynamic Updates** A escolha desta opção desabilita as atualizações dinâmicas no DNS. Você só deve utilizar esta opção quando a zona não estiver integrada ao Active Directory.
9. Toque ou clique em Next e em Finish para concluir o processo. A nova zona foi adicionada ao servidor e os registros de DNS básicos foram automaticamente criados.
10. Um único servidor DNS pode prover serviços para vários domínios. Se tiver vários domínios-pai, como microsoft.com e msn.com, poderá repetir esse processo para configurar outras zonas de pesquisa direta. Também é necessário configurar as zonas de pesquisa inversa. Siga as etapas listadas em "Configuração de pesquisas inversas" mais adiante neste capítulo.
11. É preciso criar registros adicionais para qualquer computador que queira tornar acessível para outros domínios DNS. Para fazê-lo, siga as etapas listadas em "Gerenciamento de registros de DNS" mais adiante neste capítulo.

MUNDO REAL A maioria das empresas tem áreas privadas e públicas de sua rede. As áreas de rede pública podem ser onde estão localizados servidores web e de email externo. As áreas de rede pública de sua empresa não devem permitir o acesso irrestrito. Em vez disso, as áreas de rede pública devem ser configuradas como parte de redes de perímetro. (As redes de perímetro também são conhecidas como *DMZs*, zonas desmilitarizadas, e *sub-redes filtradas*. Essas são áreas protegidas pelo firewall de sua empresa que têm acesso externo restrito e nenhum acesso à rede interna.) Caso contrário, as áreas de rede pública devem estar em uma área completamente separada e protegida por firewall.

As áreas de rede privada são onde os servidores internos e as estações de trabalho da empresa estão localizados. Nas áreas de rede pública, suas configurações DNS estão em um espaço público da Internet. Aqui, pode-se utilizar um nome de DNS .com, .org ou .net que tenha sido registrado com um registrador da Internet e os endereços IP públicos que tenham sido adquiridos ou concedidos. Nas áreas de rede privada, suas configurações DNS estão no espaço da rede privada. Aqui, pode-se utilizar adatum.com como o nome de DNS e os endereços IP da empresa, conforme abordado no Capítulo 14.

Configuração de um servidor DNS secundário

Os servidores secundários fornecem serviços DNS de backup na rede. Se estiver utilizando a integração completa com o Active Directory, não será realmente necessário configurar os secundários. Em vez disso, você deve configurar vários controladores de domínio para controlar os serviços DNS. A replicação do Active Directory irá então controlar a replicação de informações de DNS para seus controladores de domínio. Por outro lado, se estiver utilizando uma integração parcial, talvez queira configurar os secundários para diminuir a carga no servidor primário. Em uma rede de porte pequeno ou médio, talvez consiga utilizar os servidores de nomes de seu Internet Service Provider (ISP, provedor de serviços de Internet) como secundários. Nesse caso, você deve contatar seu ISP para configurar os serviços DNS secundários para você.

Como os servidores secundários utilizam zonas de pesquisa direta para a maioria dos tipos de consultas, talvez não precise de zonas de pesquisa inversa. Mas os arquivos da zona de pesquisa inversa são essenciais para os servidores primários e deve-se configurá-los para a resolução de nomes de domínio adequada.

Se quiser configurar seus próprios secundários para serviços de backup e平衡amento de carga, siga estas etapas:

1. Inicie o console DNS Manager. Se o servidor que quiser configurar não for listado, conecte-se a ele conforme descrito anteriormente.
2. Pressione e segure ou clique com o botão direito do mouse na entrada do servidor e toque ou clique em New Zone. O New Zone Wizard será iniciado. Toque ou clique em Next.
3. Para Zone Type, selecione Secondary Zone. Toque ou clique em Next.
4. Os servidores secundários podem utilizar os arquivos de zona de pesquisa direta e inversa. A zona de pesquisa direta será criada primeiro, portanto, selecione Forward Lookup Zone e toque ou clique em Next.
5. Digite o nome completo de DNS para a zona e toque ou clique em Next.
6. Toque ou clique na lista Master Servers, digite o endereço IP do servidor primário da zona e pressione Enter. O assistente tentará validar o servidor. Se um erro ocorrer, certifique-se de que o servidor está conectado à rede e de que digitou o endereço IP correto. Se quiser copiar os dados de zona de outros servidores em caso do servidor primário não estar disponível, repita esta etapa.
7. Toque ou clique em Next e em Finish. Em uma rede grande ou com ampla utilização, talvez seja necessário configurar as zonas secundárias de pesquisa inversa. Caso afirmativo, siga as etapas listadas na próxima seção.

Configuração de pesquisas inversas

As pesquisas diretas são utilizadas para resolver nomes de domínio para endereços IP. As pesquisas inversas são utilizadas para resolver endereços IP para nomes de domínio. Cada segmento em sua rede deve ter uma zona de pesquisa inversa. Por exemplo, se tiver as sub-redes 192.168.10.0, 192.168.11.0 e 192.168.12.0, deverá ter três zonas de pesquisa inversa.

A convenção de nomenclatura padrão para zonas de pesquisa inversa é digitar o ID de rede na ordem inversa e utilizar o sufixo *in-addr.arpa*. Com o exemplo anterior, se teria zonas de pesquisa inversa chamadas 10.168.192.in-addr.arpa, 11.168.192.in-addr.arpa e 12.168.192.in-addr.arpa. Os registros na zona de pesquisa inversa devem estar em sincronia com a zona de pesquisa direta. Se as zonas saírem de sincronia, a autenticação pode falhar para o domínio.

As zonas de pesquisa inversa são criadas seguindo estas etapas:

1. Inicie o console DNS Manager. Se o servidor que quiser configurar não for listado, conecte-se a ele conforme descrito anteriormente.
2. Pressione e segure ou clique com o botão direito do mouse na entrada do servidor e toque ou clique em New Zone. O New Zone Wizard será iniciado. Toque ou clique em Next.
3. Se estiver configurando um servidor primário integrado ao Active Directory (em um controlador de domínio), selecione Primary Zone e certifique-se de que Store The Zone In Active Directory esteja selecionado. Se não quiser integrar o DNS com o Active Directory, selecione Primary Zone e desmarque a caixa de seleção Store The Zone In Active Directory. Toque ou clique em Next.
4. Se estiver configurando uma zona de pesquisa inversa para um servidor secundário, selecione Secondary Zone e toque ou clique em Next.
5. Se estiver integrando a zona com o Active Directory, escolha uma das estratégias de replicação a seguir:
 - **To All DNS Servers Running On Domain Controllers In This Forest** Escolha esta estratégia se quiser a estratégia de replicação mais ampla. Lembre-se, a floresta do Active Directory inclui todas as árvores de domínio que compartilham os dados de diretório com o domínio atual.
 - **To All DNS Servers Running On Domain Controllers In This Domain** Escolha esta estratégia se quiser replicar as informações de DNS dentro do domínio atual.
 - **To All Domain Controllers In This Domain (For Windows 2000 Compatibility)** Escolha esta estratégia se quiser replicar as informações de DNS para todos os controladores de domínio do domínio atual, conforme necessário para a compatibilidade com o Windows 2000. Embora esta estratégia proporcione uma replicação mais ampla para as informações de DNS dentro do domínio, nem todo controlador de domínio também é um servidor DNS (e não é preciso configurar todo controlador de domínio como um servidor DNS).
6. Selecione a opção Reverse Lookup Zone e toque ou clique em Next.

7. Escolha se quer criar uma zona de pesquisa inversa para endereços IPv4 ou IPv6 e toque ou clique em Next. Faça uma das seguintes opções:
 - Se estiver configurando uma zona de pesquisa inversa para IPv4, digite o ID de rede para a zona de pesquisa inversa. Os valores digitados definirão o nome padrão para a zona de pesquisa inversa. Toque ou clique em Next.
 - Se tiver várias sub-redes na mesma rede, como 192.168.10 e 192.168.11, poderá digitar somente a parte da rede para o nome da zona. Por exemplo, neste caso, você iria utilizar 168.192.in-addr.arpa e permitir que o console DNS Manager criasse as zonas de sub-rede quando fosse necessário.
 - Se estiver configurando uma zona de pesquisa inversa para IPv6, digite o prefixo de rede para a zona de pesquisa inversa. Os valores digitados serão utilizados para gerar automaticamente os nomes de zona relacionados. Dependendo do prefixo digitado, será possível criar até oito zonas. Toque ou clique em Next.
8. Se estiver configurando um servidor primário ou secundário que não esteja integrado ao Active Directory, é preciso definir o nome de arquivo da zona. Um nome padrão para o arquivo de banco de dados DNS da zona deve estar preenchido para você. Você pode utilizá-lo ou digitar um novo nome de arquivo. Toque ou clique em Next.
9. Especifique se as atualizações dinâmicas são permitidas. Você tem três opções:
 - **Allow Only Secure Dynamic Updates** Quando a zona está integrada ao Active Directory, pode-se utilizar ACLs para restringir quais clientes podem realizar as atualizações dinâmicas. Com esta opção selecionada, somente clientes com contas de computadores autorizadas e ACLs aprovadas poderão atualizar seus registros de recursos no DNS quando modificações ocorrerem.
 - **Allow Both Nonsecure And Secure Dynamic Updates** Escolha esta opção para permitir que qualquer cliente atualize seus registros de recursos no DNS quando modificações ocorrerem. Os clientes podem ser seguros ou não.
 - **Do Not Allow Dynamic Updates** A escolha desta opção desabilita as atualizações dinâmicas no DNS. Você só deve utilizar esta opção quando a zona não estiver integrada ao Active Directory.
10. Toque ou clique em Next e em Finish. A nova zona foi adicionada ao servidor e os registros de DNS básicos foram automaticamente criados.

Depois de definir as zonas de pesquisa inversa, é preciso garantir que a delegação para elas seja adequadamente controlada. Contate sua equipe de rede ou seu ISP para garantir que as zonas sejam registradas com o domínio-pai.

Configuração de nomes globais

A zona GlobalNames é uma zona de pesquisa direta especialmente nomeada que deve estar integrada ao AD DS. Quando todos os servidores DNS para suas zonas tiverem o Windows Server 2008 ou versões mais recentes, implantar uma zona GlobalNames criará registros globais estáticos com rótulo único, sem depender do WINS. Isso permite que os usuários acessem os hosts utilizando nomes de rótulo único em vez de nomes de domínio totalmente qualificados. Deve-se utilizar a zona GlobalNames quando a resolução de nomes depender do DNS, como quando a empresa não estiver mais utilizando o WINS e se planeje implantar apenas o IPv6. Como as atualizações

dinâmicas não podem ser utilizadas para registrar atualizações na zona GlobalNames, deve-se configurar a resolução de nomes de rótulo único somente para os servidores principais (primários).

Você pode implantar uma zona GlobalNames completando as seguintes etapas:

1. No console DNS Manager, selecione um servidor DNS que também seja um controlador de domínio. Se o servidor que quiser configurar não for listado, conecte-se a ele conforme descrito anteriormente.
2. Pressione e segure ou clique com o botão direito do mouse no nó Forward Lookup Zones e toque ou clique em New Zone. No New Zone Wizard, toque ou clique em Next para aceitar os padrões para criar uma zona primária integrada ao AD DS. Na página Active Directory Zone Replication Scope, escolha replicar a zona por toda a floresta e toque ou clique em Next. Na página Zone Name, digite **GlobalNames** como o nome da zona. Toque ou clique em Next duas vezes e em Finish.
3. Em todo servidor DNS autoritativo da floresta agora e no futuro, será preciso digitar o seguinte em um prompt de comandos com privilégios elevados: **dnscmd ServerName /enableglobalnamessupport 1**, em que *ServerName* é o nome do servidor DNS que hospeda a zona GlobalNames. Para especificar o computador local, utilize um ponto (.) em vez do nome do servidor, como **dnscmd . /enableglobalnamessupport 1**.
4. Para cada servidor que quiser que os usuários possam acessar utilizando um nome de rótulo único, adicione um registro de alias (CNAME) à zona GlobalNames. No console DNS Manager, pressione e segure ou clique com o botão direito do mouse no nó GlobalNames, selecione New Alias (CNAME) e utilize a caixa de diálogo fornecida para criar o novo registro de recurso.

OBSERVAÇÃO Um servidor DNS autoritativo tenta resolver as consultas na seguinte ordem: utilizando os dados de zona local, a zona GlobalNames, os sufixos DNS e o WINS. Para as atualizações dinâmicas, um servidor DNS autoritativo verifica a zona GlobalNames antes de verificar os dados de zona local.

DICA Se quiser que os clientes DNS de outra floresta utilizem a zona GlobalNames para resolver nomes, é preciso adicionar um registro de recurso do serviço (SRV) com o nome _globalnames._msdcs para a partição DNS dessa floresta. O registro deve especificar o FQDN do servidor DNS que hospeda a zona GlobalNames.

Gerenciamento de servidores DNS

O console DNS Manager é a ferramenta utilizada para gerenciar os servidores DNS locais e remotos. Como mostrado na Figura 16-4, a janela principal do console DNS Manager é dividida em dois painéis. O painel esquerdo permite acessar os servidores DNS e suas zonas. O painel direito mostra os detalhes do item selecionado no momento. Pode-se trabalhar com o console DNS Manager de três maneiras:

- Tocar ou clicar duas vezes na entrada no painel esquerdo para expandir a lista de arquivos dela.
- Selecionar uma entrada no painel esquerdo para exibir os detalhes como o status da zona e os registros do domínio no painel direito.
- Pressionar e segurar ou clicar com o botão direito do mouse em uma entrada para exibir um menu de contexto.

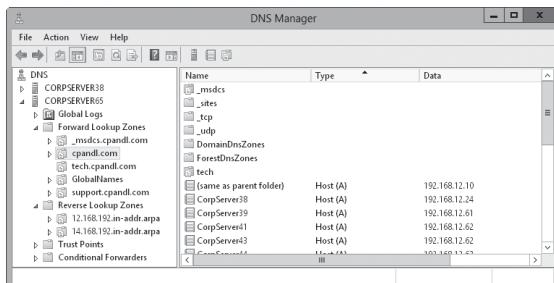


FIGURA 16-4 Gerencie os servidores DNS locais e remotos utilizando o console DNS Manager.

As pastas Forward Lookup Zones e Reverse Lookup Zones fornecem acesso aos domínios e zonas configurados para uso nesse servidor. Quando as pastas de domínio ou sub-rede são selecionadas no painel esquerdo, pode-se gerenciar os registros de DNS do domínio ou da sub-rede.

Como adicionar e remover servidores para gerenciamento

Pode-se utilizar o console DNS Manager para gerenciar os servidores com o DNS seguindo estas etapas:

1. Pressione e segure ou clique com o botão direito do mouse em DNS na árvore de console e toque ou clique em Connect To DNS Server.
2. Se estiver tentando se conectar ao computador local, selecione This Computer. Caso contrário, selecione The Following Computer e digite o endereço IP ou o nome de host totalmente qualificado do computador remoto ao qual quer se conectar.
3. Toque ou clique em OK. O Windows Server 2012 tentará contatar o servidor. Se o fizer, adicionará o servidor ao console.

OBSERVAÇÃO Se um servidor estiver offline ou inacessível de alguma outra forma por causa de restrições de segurança ou problemas com o serviço Remote Procedure Call (RPC, chamada de procedimento remoto), a conexão irá falhar. Ainda será possível adicionar o servidor ao console tocando ou clicando em Yes quando for solicitado.

No console DNS Manager, pode-se excluir um servidor selecionando sua entrada e pressionando Delete. Quando for solicitado, toque ou clique em Yes para confirmar a exclusão. A exclusão de um servidor apenas remove da lista de servidores na árvore de console. Ela não exclui realmente a função do servidor.

Como iniciar e interromper um servidor DNS

Para gerenciar os servidores DNS, utiliza-se o serviço DNS Server. Pode-se iniciar, interromper, pausar, continuar e reiniciar o serviço DNS Server no nó Services do Server Manager ou através de uma linha de comando. Também é possível gerenciar o serviço DNS Server no console DNS Manager. Pressione e segure ou clique com o botão direito do mouse no servidor que quer gerenciar no console DNS Manager, aponte para All Tasks e toque ou clique em Start, Stop, Pause, Resume ou Restart, conforme apropriado.

OBSERVAÇÃO No Server Manager, sob o nó DNS Server, expanda o nó DNS e pressione e segure ou clique com o botão direito do mouse no servidor com o qual quer trabalhar. No menu de atalho, selecione Start Service, Stop Service, Pause Service, Resume Service ou Restart Service, conforme apropriado.

Utilização de DNSSEC e assinatura de zonas

O Windows 7 ou versões posteriores, bem como o Windows Server 2008 R2 ou posteriores, dão suporte ao DNS Security Extensions (DNSSEC). O DNSSEC é definido em várias Request For Comments (RFCs), incluindo as RFCs 4033, 4034 e 4035. Essas RFCs adicionam autoridade de origem, integridade dos dados e negação autenticada de existência para o DNS. Com o DNSSEC, deve-se aprender sobre os seguintes registros de recursos adicionais:

- DNSKEY (Domain Name System Key)
- RRSIG (Resource Record Signature)
- NSEC (NextSECure)
- DS (Domain Services)

O cliente DNS com esses sistemas operacionais pode enviar consultas que indiquem suporte para o DNSSEC, processem registros relacionados e determinem se um servidor DNS possui registros válidos em seu nome. Em servidores com o Windows, o DNSSEC permite que os servidores DNS assinem zonas com segurança, hospedem zonas assinadas pelo DNSSEC, processem registros relacionados e realizem validação e autenticação. A maneira como um cliente DNS trabalha com o DNSSEC é configurada por meio da Name Resolution Policy Table (NRPT), que armazena as configurações que definem o comportamento do cliente DNS. Normalmente, a NRPT é gerenciada por meio da Group Policy.

Quando um servidor DNS hospedando uma zona assinada recebe uma consulta, ele retorna as assinaturas digitais, além dos registros solicitados. Um resolvedor ou outro servidor configurado com uma âncora de confiança para uma zona assinada ou para um pai de uma zona assinada pode obter a chave pública do par de chaves pública/privada e validar que as respostas são autênticas e não foram adulteradas.

Como parte de seu planejamento pré-implantação, é preciso identificar as zonas DNS a proteger com assinaturas digitais. O DNS Server para o Windows Server 2012 tem as seguintes melhorias significativas para o DNSSEC:

- Suporte para atualizações dinâmicas nas zonas integradas ao Active Directory. Anteriormente, se uma zona de domínio do Active Directory fosse assinada, era preciso atualizar manualmente todos os registros SRV e outros registros de recursos. Isso não é mais necessário, pois o DNS Server agora o faz automaticamente.
- Suporte para assinatura online, gerenciamento de chave automatizado e distribuição de âncora de confiança automatizada. Anteriormente, era preciso configurar e gerenciar as assinaturas, chaves e âncoras de confiança. Isso não é mais necessário, pois o DNS Server agora o faz automaticamente.
- Suporte para validações de registros assinados com padrões DNSSEC atualizados (padrões NSEC3 e RSA/SHA-2). Anteriormente, não se podia assinar registros com o NSEC3 e o RSA/SHA-2.

Além disso, lembre-se do seguinte:

- Para zonas armazenadas em arquivos, o servidor primário e todos os servidores secundários hospedando uma zona com DNSSEC devem ser um servidor DNS com o Windows Server 2008 R2 ou posteriores ou um servidor compatível com o DNSSEC que esteja em execução em um sistema operacional diferente do Windows.
- Para zonas integradas ao Active Directory, todo controlador de domínio que seja um servidor DNS no domínio deve ter o Windows Server 2008 R2 ou posteriores se a zona assinada estiver configurada para replicar para todos os servidores DNS do domínio. Todo controlador de domínio que seja um servidor DNS na floresta deve ter o Windows Server 2008 R2 ou posteriores se a zona assinada estiver configurada para replicar para todos os servidores DNS da floresta.
- Para ambientes mistos, todos os servidores que forem autoritativos para uma zona assinada com o DNSSEC devem ser servidores compatíveis com ele. Os clientes Windows compatíveis com o DNSSEC que solicitarem dados e validação DNSSEC devem estar configurados para emitir consultas DNS para um servidor compatível com ele. Os clientes Windows não compatíveis com o DNSSEC podem ser configurados para emitir consultas DNS a servidores compatíveis com o DNSSEC. Os servidores compatíveis com o DNSSEC podem ser configurados para enviar consultas recursivamente a um servidor DNS não compatível com o DNSSEC.

A proteção de zonas DNS com assinaturas digitais é um processo com várias etapas. Como parte desse processo, é preciso designar um *key master* (mestre de chave). Qualquer servidor autoritativo que hospede uma cópia primária de uma zona pode agir como o mestre de chave. A seguir, é preciso gerar uma Key Signing Key e uma Zone Signing Key. Uma Key Signing Key (chave KSK), que é uma chave de autenticação, tem uma chave privada e uma chave pública associada a ela. A chave privada é utilizada para assinar todos os registros de DNSKEY na raiz da zona. A chave pública é utilizada como uma âncora de confiança para validar respostas do DNS. Uma Zone Signing Key (chave ZSK) é utilizada para assinar os registros de zona.

Depois de gerar as chaves, crie os registros de recursos para negação autenticada de existência utilizando o padrão NSEC3 mais seguro ou o padrão NSEC menos se-

guro. Como as âncoras de confiança são utilizadas para validar as respostas do DNS, também é preciso especificar como elas serão atualizadas e distribuídas. Normalmente, será desejável atualizar e distribuir as âncoras de confiança automaticamente. Por padrão, os registros são assinados com a criptografia SHA-1 e SHA-256. Você também pode selecionar outros algoritmos de criptografia.

Não é preciso percorrer o processo de configuração toda vez que assinar uma zona. As chaves e outros parâmetros de assinatura estarão disponíveis para reutilização.

Para assinar uma zona enquanto personaliza os parâmetros de assinatura, siga estas etapas:

1. No console DNS Manager, pressione e segure ou clique com o botão direito do mouse na zona que quer proteger. No menu de atalho, selecione DNSSEC e Sign The Zone. O Zone Signing Wizard será iniciado. Se o assistente exibir a página de boas-vindas, leia o texto Welcome e toque ou clique em Next.
2. Na página Signing Options, selecione Customize Zone Signing Parameters e toque ou clique em Next.
3. Selecione um mestre de chave para a zona. Qualquer servidor autoritativo que hospede uma cópia primária de uma zona pode agir como o mestre de chave. Quando estiver pronto para continuar, toque ou clique em Next duas vezes.
4. Na página Key Signing Key, configure uma KSK tocando ou clicando em Add, aceitando ou alterando os valores padrão para as propriedades e substituição da chave e toque ou clique em OK. Quando estiver pronto para continuar, toque ou clique em Next duas vezes.
5. Na página Zone Signing Key, configure uma ZSK tocando ou clicando em Add, aceitando ou alterando os valores padrão para as propriedades e substituição da chave e toque ou clique em OK. Quando estiver pronto para continuar, toque ou clique em Next cinco vezes.
6. Depois do assistente assinar a zona, clique em Finish.

Para assinar uma zona e utilizar os parâmetros de assinatura existentes, siga estas etapas:

1. No console DNS Manager, pressione e segure ou clique com o botão direito do mouse na zona que quer proteger. No menu de atalho, selecione DNSSEC e Sign The Zone. O Zone Signing Wizard será iniciado. Se o assistente exibir a página de boas-vindas, leia o texto Welcome e toque ou clique em Next.
2. Na página Signing Options, selecione Sign The Zone With Parameters Of An Existing Zone. Digite o nome de uma zona assinada existente, como **cpandl.com**. Toque ou clique em Next.
3. Na página Key Master, selecione um mestre de chave para a zona. Qualquer servidor autoritativo que hospede uma cópia primária de uma zona pode agir como o mestre de chave. Toque ou clique em Next duas vezes.
4. Depois do assistente assinar a zona, clique em Finish.

Criação de domínios-filho dentro de zonas

Utilizando o console DNS Manager, pode-se criar domínios-filho dentro de uma zona. Por exemplo, se criar a zona primária microsoft.com, poderá criar os subdomínios

hr.microsoft.com e mis.microsoft.com para ela. Os domínios-filho são criados seguindo estas etapas:

1. No console DNS Manager, expanda a pasta Forward Lookup Zones do servidor com o qual quer trabalhar.
2. Pressione e segure ou clique com o botão direito do mouse na entrada do domínio-pai e toque ou clique em New Domain.
3. Digite o nome do novo domínio e toque ou clique em OK. Para hr.microsoft.com, você digitaria **hr**. Para mis.microsoft.com, digitaria **mis**.

Criação de domínios-filho em zonas separadas

Conforme a empresa crescer, talvez se deseje organizar o namespace do DNS em zonas separadas. Na sede da empresa, você poderia ter uma zona para o domínio-pai microsoft.com. Nas filiais, poderia ter zonas para cada escritório, como memphis.microsoft.com, newyork.microsoft.com e la.microsoft.com.

Os domínios-filho são criados em zonas separadas seguindo estas etapas:

1. Instale um servidor DNS em cada domínio-filho e crie as zonas de pesquisa direta e inversa necessárias para ele, conforme descrito anteriormente em "Instalação de servidores DNS".
2. No servidor DNS autoritativo do domínio-pai, delegue autoridade a cada domínio-filho. A delegação de autoridade permite que o domínio-filho resolva consultas DNS e responda a elas a partir de computadores dentro e fora da sub-rede local.

Delega-se autoridade a um domínio-filho seguindo estas etapas:

1. No console DNS Manager, expanda a pasta Forward Lookup Zones do servidor com o qual quer trabalhar.
2. Pressione e segure ou clique com o botão direito do mouse na entrada do domínio-pai e toque ou clique em New Delegation. O New Delegation Wizard será iniciado. Toque ou clique em Next.
3. Como mostrado na Figura 16-5, digite o nome do domínio delegado, como **service**, e toque ou clique em Next. O nome digitado atualizará o valor da caixa de texto Fully Qualified Domain Name.



FIGURA 16-5 Digitar o nome do domínio delegado define o nome de domínio totalmente qualificado (FQDN).

4. Toque ou clique em Add. A caixa de diálogo New Name Server Record será exibida.
5. Na caixa de texto Server Fully Qualified Domain Name, digite o nome do host totalmente qualificado de um servidor DNS para o domínio-filho, como **corpserver01.memphis.adatum.com**, e toque ou clique em Resolve. O servidor irá realizar uma consulta de pesquisa e adicionar os endereços IP resolvidos à lista IP Address.
6. Repita a etapa 5 para especificar servidores de nomes adicionais. A ordem das entradas determina qual endereço IP será utilizado primeiro. Altere a ordem conforme necessário utilizando os botões Up e Down. Quando estiver pronto para continuar, toque ou clique em OK para fechar a caixa de diálogo New Name Server Record.
7. Toque ou clique em Next e em Finish.

Exclusão de um domínio ou de uma sub-rede

Excluir um domínio ou uma sub-rede permanentemente os removerá do servidor DNS. Para excluir um domínio ou uma sub-rede, siga estas etapas:

1. No console DNS Manager, pressione e segure ou clique com o botão direito do mouse na entrada do domínio ou da sub-rede.
2. No menu de atalho, toque ou clique em Delete e confirme a ação tocando ou clicando em Yes.
3. Se o domínio ou a sub-rede estiverem integrados ao Active Directory, um prompt de aviso será exibido. Confirme que quer excluir o domínio ou a sub-rede integrada ao Active Directory tocando ou clicando em Yes.

OBSERVAÇÃO A exclusão de um domínio ou de uma sub-rede exclui todos os registros de DNS no arquivo de zona, mas não exclui realmente o arquivo de zona em um servidor primário ou secundário que não esteja integrado ao Active Directory. O arquivo de zona real permanecerá no diretório %SystemRoot%\System32\DNS. Pode-se excluir esse arquivo depois de ter excluído as zonas do console DNS Manager.

Gerenciamento de registros de DNS

Depois de criar os arquivos de zonas necessários, você pode adicionar registros a elas. Os computadores que precisem ser acessados a partir do Active Directory e de domínios DNS devem ter registros de DNS. Embora haja muitos tipos de registros de DNS, a maioria deles não é utilizada normalmente. Então, em vez de focar em tipos de registro que você provavelmente não irá usar, vamos focar naqueles que utilizará:

- **A (IPv4 address)** Mapeia um nome de host para um endereço IPv4. Quando um computador tiver vários endereços IPv4, placas de adaptador, ou ambos, deverá ter vários registros de endereço.
- **AAAA (IPv6 address)** Mapeia um nome de host para um endereço IPv6. Quando um computador tiver vários endereços IPv6, placas de adaptador, ou ambos, deverá ter vários registros de endereço.
- **CNAME (canonical name)** Define um alias para um nome de host. Por exemplo, utilizando esse registro, zeta.microsoft.com pode ter o alias de www.microsoft.com.

- **MX (mail exchanger)** Especifica um servidor de email para o domínio, permitindo que mensagens de email sejam enviadas para os servidores de email corretos do domínio.
- **NS (name server)** Especifica um servidor de nomes para o domínio, o que permite pesquisas DNS dentro de várias zonas. Cada servidor de nomes primário e secundário deve estar declarado por meio deste registro.
- **PTR (pointer)** Cria um ponteiro que mapeia um endereço IP para um nome de host para pesquisas inversas.
- **SOA (start of authority)** Declara o host que é mais autoritativo para a zona e, como tal, é a melhor fonte de informações de DNS sobre ela. Cada arquivo de zona deve ter um registro SOA (que é criado automaticamente quando uma zona é adicionada). Também declara outras informações sobre a zona, como a pessoa responsável, o intervalo de atualização, o intervalo de repetição e assim por diante.

Como adicionar registros de endereço e ponteiro

Utiliza-se os registros A e AAAA para mapear um nome de host para um endereço IP e o registro PTR cria um ponteiro para o host para pesquisas inversas. Você pode criar registros de endereço e ponteiro ao mesmo tempo ou separadamente.

Uma nova entrada de host com registros de endereço e ponteiro é criada seguindo estas etapas:

1. No console DNS Manager, expanda a pasta Forward Lookup Zones do servidor com o qual você deseja trabalhar.
2. Pressione e segure ou clique com o botão direito do mouse no domínio que quer atualizar e toque ou clique em New Host (A Or AAAA). A caixa de diálogo mostrada na Figura 16-6 será aberta.

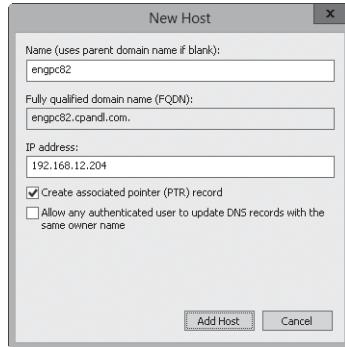


FIGURA 16-6 Crie registros de endereço e registros de ponteiro simultaneamente com a caixa de diálogo New Host.

3. Digite o nome de computador de rótulo único, como **servicespc85**, e o endereço IP, como **192.168.10.58**.

-
4. Marque a caixa de seleção Create Associated Pointer (PTR) Record.

OBSERVAÇÃO Você pode criar registros PTR somente se a zona de pesquisa inversa correspondente estiver disponível. É possível criar esse arquivo seguindo as etapas listadas em “Configuração de pesquisas inversas” anteriormente neste capítulo. A opção Allow Any Authenticated User só estará disponível quando um servidor DNS estiver configurado em um controlador de domínio.

5. Toque ou clique em Add Host e em OK. Repita essas etapas conforme necessário para adicionar outros hosts.
6. Toque ou clique em Done quando tiver terminado.

Como incluir um registro PTR posteriormente

Se for preciso adicionar um registro PTR posteriormente, pode-se fazê-lo seguindo estas etapas:

1. No console DNS Manager, expanda a pasta Reverse Lookup Zones do servidor com o qual quer trabalhar.
2. Pressione e segure ou clique com o botão direito do mouse na sub-rede que quer atualizar e toque ou clique em New Pointer (PTR).
3. Digite o endereço IP do host, como **192.168.1.95**, e o nome do host, como **servicespc54**. Toque ou clique em OK.

Como adicionar aliases para registros DNS com CNAME

Especifica-se aliases de hosts utilizando registros CNAME. Os aliases permitem que um único computador host pareça ser vários. Por exemplo, pode-se fazer com que o host gamma.microsoft.com pareça ser www.microsoft.com e ftp.microsoft.com.

Para criar um registro CNAME, siga estas etapas:

1. No console DNS Manager, expanda a pasta Forward Lookup Zones do servidor com o qual você deseja trabalhar.
2. Pressione e segure ou clique com o botão direito do mouse no domínio que quer atualizar e toque ou clique em New Alias (CNAME).
3. Na caixa de texto Alias Name, digite o alias. O alias é um nome de host de rótulo único, como *www* ou *ftp*.
4. Na caixa de texto Fully Qualified Domain Name (FQDN) For Target Host, digite o nome de host completo do computador para o qual o alias será criado.
5. Toque ou clique em OK.

Como adicionar servidores de email

Os registros MX identificam servidores de email para o domínio. Esses servidores são responsáveis pelo processamento ou encaminhamento de emails dentro do domínio. Quando um registro MX é criado, deve-se especificar um número de preferência para o servidor de email. Um número de preferência é um valor de 0 a 65.535 que denota a prioridade do servidor de email dentro do domínio. O servidor de email com o número de preferência mais baixo tem a maior prioridade e será o primeiro a receber emails. Se a distribuição de email falhar, o servidor de email com o próximo número de preferência mais baixo será tentado.

Para criar um registro MX, siga estas etapas:

1. No console DNS Manager, expanda a pasta Forward Lookup Zones do servidor com o qual quer trabalhar.
2. Pressione e segure ou clique com o botão direito do mouse no domínio que quer atualizar e toque ou clique em New Mail Exchanger (MX).
3. Agora você poderá criar um registro para o servidor de email preenchendo estas caixas de texto:

- **Host Or Child Domain** Utilizando um nome de rótulo único, digite o nome do subdomínio pelo qual o servidor especificado neste registro será responsável. Na maioria dos casos, esta caixa será deixada em branco, o que especifica que não há um subdomínio e o servidor será responsável pelo domínio em que este registro foi criado.
- **Fully Qualified Domain Name (FQDN)** Digite o FQDN do domínio ao qual este registro MX deva ser aplicado, como **cpndl.com**.
- **Fully Qualified Domain Name (FQDN) Of Mail Server** Digite o FQDN do servidor de email que deva controlar o recebimento e a distribuição de emails, como **corpmail.cpndl.com**. O domínio de email especificado anteriormente será roteado para este servidor de email para distribuição.
- **Mail Server Priority** Digite um número de preferência para o host de 0 a 65.535.

OBSERVAÇÃO Atribua números de preferência que deixem espaço para crescimento. Por exemplo, utilize 10 para o servidor de email de prioridade mais alta, 20 para o próximo e 30 para o seguinte.

MUNDO REAL Não é possível digitar um nome com vários rótulos na caixa de texto Host Or Child Domain. Se for preciso digitar um nome com várias partes, estará criando o registro MX no nível errado da hierarquia DNS. Crie ou acesse o nível de domínio adicional necessário e adicione um registro MX nele para o subdomínio.

4. Toque ou clique em OK.

Como adicionar servidores de nomes

Os registros NS especificam os servidores de nomes do domínio. Cada servidor de nomes primário e secundário deve estar declarado por meio desse registro. Se utilizar servidores de nome secundários de um ISP, certifique-se de inserir os registros NS apropriados.

Para criar um registro NS, siga estas etapas:

1. No console DNS Manager, expanda a pasta Forward Lookup Zones do servidor com o qual quer trabalhar.
2. Exiba os registros de DNS do domínio selecionando a pasta do domínio no modo de exibição de árvore.
3. Pressione e segure ou clique com o botão direito do mouse no registro NS existente no painel de visualização e toque ou clique em Properties. A caixa de diálogo Properties do domínio será aberta com a guia Name Servers selecionada, como mostrado na Figura 16-7.

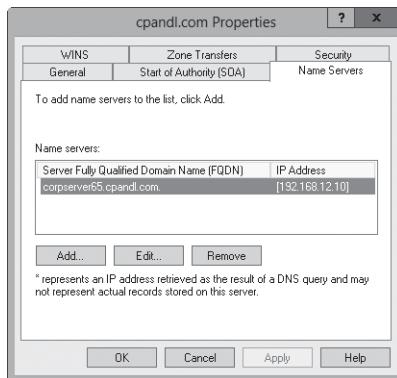


FIGURA 16-7 Configure os servidores de nomes do domínio por meio da caixa de diálogo Properties do domínio.

4. Toque ou clique em Add. A caixa de diálogo New Name Server Record será exibida.
5. Na caixa de texto Server Fully Qualified Domain Name, digite o nome de um servidor DNS para o domínio-filho, como **corpserver01.cpandl.com**, e toque ou clique em Resolve. O servidor irá realizar uma consulta de pesquisa e adicionar os endereços IP resolvidos à lista IP Address.
6. Repita a etapa 5 para especificar servidores de nomes adicionais. A ordem das entradas determina qual endereço IP será utilizado primeiro. Altere a ordem conforme necessário utilizando os botões Up e Down. Quando estiver pronto para continuar, toque ou clique em OK para fechar a caixa de diálogo New Name Server Record.
7. Toque ou clique em OK para salvar suas alterações.

Visualização e atualização de registros de DNS

Para visualizar ou atualizar os registros de DNS, siga estas etapas:

1. Toque ou clique duas vezes na zona com a qual quer trabalhar. Os registros da zona devem ser exibidos no painel direito.
2. Toque ou clique duas vezes no registro DNS que quer visualizar ou atualizar. A caixa de diálogo Properties do registro será aberta. Faça as alterações necessárias e clique ou toque em OK.

Atualização de propriedades de zona e o registro SOA

Cada zona tem propriedades separadas que podem ser configuradas. Essas propriedades definem os parâmetros gerais da zona utilizando o registro SOA, a notificação de alterações e a integração com o WINS. No console DNS Manager, defina as propriedades de zona fazendo uma das opções a seguir:

- Pressione e segure ou clique com o botão direito do mouse na zona que quer atualizar e toque ou clique em Properties.
- Selecione a zona e toque ou clique em Properties no menu Action.

As caixas de diálogo Properties para as zonas de pesquisa direta e inversa são idênticas, exceto pelas guias WINS e WINS-R. Nas zonas de pesquisa direta, utiliza-se a guia WINS para configurar as pesquisas para nomes de computador NetBIOS. Nas zonas de pesquisa inversa, utiliza-se a guia WINS-R para configurar as pesquisas inversas para nomes de computador NetBIOS.

Modificação do registro SOA

Um registro SOA designa o servidor de nomes autoritativo para uma zona e define as propriedades gerais dela, como os intervalos de repetição e atualização. Você pode modificar essas informações seguindo estas etapas:

1. No console DNS Manager, pressione e segure ou clique com o botão direito do mouse na zona que quer atualizar e toque ou clique em Properties.
2. Toque ou clique na guia Start Of Authority (SOA) e atualize as caixas de texto mostradas na Figura 16-8.

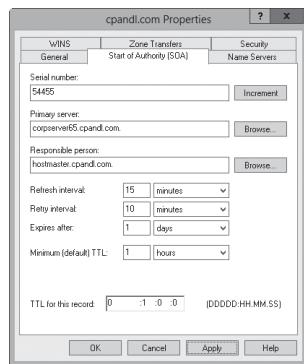


FIGURA 16-8 Na caixa de diálogo Properties da zona, defina as propriedades gerais dela e atualize o registro SOA.

As caixas de texto na guia Start Of Authority (SOA) são utilizadas da seguinte forma:

- **Serial Number** Um número de série que indica a versão dos arquivos de banco de dados DNS. Esse número é atualizado automaticamente sempre que são

feitas alterações nos arquivos da zona. Você também pode atualizar o número manualmente. Os servidores secundários utilizam esse número para determinar se os registros de DNS da zona foram alterados. Se o número de série do servidor primário for maior do que o do servidor secundário, os registros foram alterados e o servidor secundário pode solicitar os registros de DNS da zona. Também é possível configurar o DNS para notificar os servidores secundários sobre alterações (o que pode agilizar o processo de atualização).

- **Primary Server** O FQDN de um servidor de nomes seguido de um ponto. O ponto é utilizado para terminar o nome e garantir que as informações do domínio não sejam anexadas à entrada.
- **Responsible Person** O endereço de email da pessoa encarregada do domínio. A entrada padrão é *hostmaster* seguida de um ponto, isto é, *hostmaster@your_domain.com*. Se alterar essa entrada, substitua o símbolo @ por um ponto no endereço de email e termine o endereço com um ponto.
- **Refresh Interval** O intervalo em que um servidor secundário procura atualizações da zona. Se o intervalo estiver definido para 60 minutos, as alterações de registro NS podem não ser propagadas para um servidor secundário por até uma hora. O tráfego de rede será reduzido aumentando esse valor.
- **Retry Interval** O tempo que o servidor secundário aguarda após uma falha para baixar o banco de dados da zona. Se o intervalo estiver definido para 10 minutos e a transferência do banco de dados da zona falhar, o servidor secundário irá aguardar 10 minutos antes de solicitar novamente o banco de dados da zona.
- **Expires After** O período de tempo em que as informações da zona são válidas no servidor secundário. Se o servidor secundário não puder baixar os dados de um servidor primário dentro desse período, ele irá deixar os dados em seu cache perderem a validade e então para de responder a consultas DNS. A configuração de Expires After para sete dias permite que os dados em um servidor secundário sejam válidos por sete dias.
- **Minimum (Default) TTL** O valor de time-to-live (TTL, tempo de vida) mínimo para registros armazenados em cache em um servidor secundário. O valor pode ser definido em dias, horas, minutos ou segundos. Quando esse valor é alcançado, o servidor secundário faz com que o registro associado perca a validade e o descarta. A próxima solicitação para o registro precisa ser enviada ao servidor primário para resolução. Defina o tempo de vida mínimo para um valor relativamente alto, como 24 horas, para reduzir o tráfego na rede e aumentar a eficiência. Lembre-se de que um valor mais alto reduz a propagação das atualizações pela Internet.
- **TTL For This Record** O valor de TTL para este registro SOA específico. O valor é definido no formato Dias : Horas : Minutos : Segundos e geralmente deve ser o mesmo que o tempo de vida mínimo para todos os registros.

Permissão e restrição de transferências de zona

As transferências de zona enviam uma cópia das informações da zona para outros servidores DNS. Esses servidores podem estar no mesmo domínio ou em outros. Por razões de segurança, o Windows Server 2012 desabilita as transferências de zona. Para

habilitá-las para secundários que tenha configurado internamente ou com ISPs, é preciso permitir as transferências de zona e especificar os tipos de servidores para os quais elas podem ser feitas.

Embora se possa permitir transferências de zona com qualquer servidor, isso abre o servidor a possíveis problemas de segurança. Em vez de abrir o caminho, você deve restringir o acesso às informações da zona de modo que apenas os servidores identificados possam solicitar atualizações do servidor primário da zona. Isso permitirá canalizar as solicitações por meio de um grupo seletivo de servidores secundários, como os servidores de nomes secundários de seu ISP, e ocultar os detalhes de sua rede interna do mundo externo.

Para permitir as transferências de zona e restringir o acesso ao banco de dados da zona primária, siga estas etapas:

1. No console DNS Manager, pressione e segure ou clique com o botão direito do mouse no domínio ou na sub-rede que quer atualizar e toque ou clique em Properties.
2. Toque ou clique na guia Zone Transfers, como mostrado na Figura 16-9.

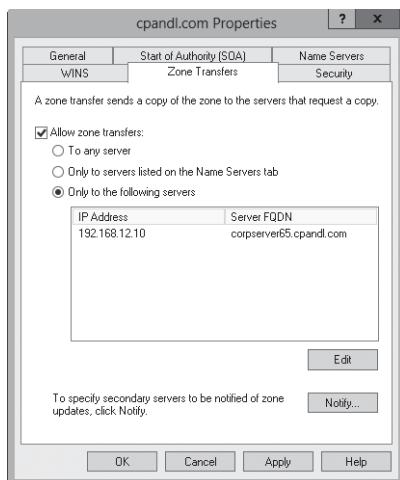


FIGURA 16-9 Utilize a guia Zone Transfers para permitir as transferências de zona para qualquer servidor ou para servidores designados.

3. Para restringir as transferências aos servidores de nomes listados na guia Name Servers, marque a caixa de seleção Allow Zone Transfers e escolha Only To Servers Listed On The Name Servers Tab.
4. Para restringir as transferências aos servidores designados, marque a caixa de seleção Allow Zone Transfers e escolha Only To The Following Servers. Toque ou clique em Edit conforme apropriado para exibir a caixa de diálogo Allow Zone Transfers. Toque ou clique na lista IP Address, digite o endereço IP do servidor

secundário da zona e pressione Enter. O Windows tentará validar o servidor. Se um erro ocorrer, certifique-se de que o servidor está conectado à rede e de que digitou o endereço IP correto. Se quiser copiar os dados de zona de outros servidores em caso do primeiro servidor não estar disponível, também pode adicionar endereços IP de outros servidores. Toque ou clique em OK.

5. Toque ou clique em OK para salvar suas alterações.

Notificação de alterações para secundários

Você define as propriedades de uma zona com seu registro SOA. Essas propriedades controlam como as informações de DNS são propagadas na rede. Também é possível especificar que o servidor primário deve notificar os servidores de nomes secundários quando forem feitas alterações no banco de dados da zona. Para fazê-lo, siga estas etapas:

1. No console DNS Manager, pressione e segure ou clique com o botão direito do mouse no domínio ou na sub-rede que quer atualizar e toque ou clique em Properties.
2. Na guia Zone Transfers, toque ou clique em Notify. A caixa de diálogo mostrada na Figura 16-10 será exibida.

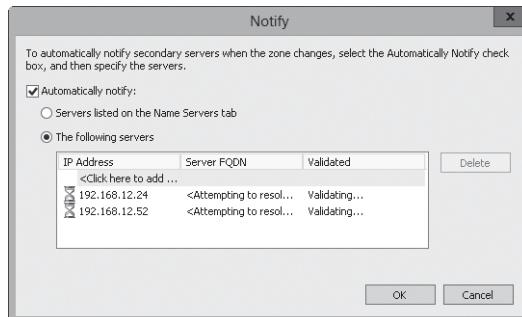


FIGURA 16-10 Na caixa de diálogo Notify, notifique todos os secundários listados na guia Name Servers ou servidores específicos que você designar.

3. Para notificar os servidores secundários listados na guia Name Servers, marque a caixa de seleção Automatically Notify e escolha Servers Listed On The Name Servers Tab.
4. Se quiser designar servidores específicos a notificar, marque a caixa de seleção Automatically Notify e escolha The Following Servers. Toque ou clique na lista IP Address, digite o endereço IP do servidor secundário da zona e pressione Enter. O Windows tentará validar o servidor. Se um erro ocorrer, certifique-se de que o servidor está conectado à rede e de que digitou o endereço IP correto. Se quiser notificar outros servidores, adicione os endereços IP deles também.
5. Toque ou clique em OK duas vezes.

Configuração do tipo de zona

Ao criar zonas, elas serão designadas como tendo um tipo específico de zona e um modo de integração ao Active Directory. Você pode alterar o tipo e o modo de integração a qualquer momento seguindo estas etapas:

1. No console DNS Manager, pressione e segure ou clique com o botão direito do mouse no domínio ou na sub-rede que quer atualizar e toque ou clique em Properties.
2. Sob Type na guia General, toque ou clique em Change. Na caixa de diálogo Change Zone Type, selecione o novo tipo da zona.
3. Para integrar a zona com o Active Directory, marque a caixa de seleção Store The Zone In Active Directory.
4. Para remover a zona do Active Directory, desmarque a caixa de seleção Store The Zone In Active Directory.
5. Toque ou clique em OK duas vezes.

Como habilitar e desabilitar as atualizações dinâmicas

As atualizações dinâmicas permitem que os clientes DNS registrem e mantenham seus próprios registros de endereço e ponteiro. Isso é útil principalmente para computadores configurados dinamicamente por meio do DHCP. Habilitando as atualizações dinâmicas, os computadores configurados dinamicamente localizam uns aos outros com mais facilidade na rede. Quando uma zona está integrada ao Active Directory, você tem a opção de exigir atualizações seguras. Com atualizações seguras, pode-se utilizar ACLs para controlar quais computadores e usuários podem atualizar o DNS dinamicamente.

Você pode habilitar e desabilitar as atualizações dinâmicas seguindo estas etapas:

1. No console DNS Manager, pressione e segure ou clique com o botão direito do mouse no domínio ou na sub-rede que quer atualizar e toque ou clique em Properties.
2. Utilize as opções a seguir na lista Dynamic Updates da guia General para habilitar ou desabilitar as atualizações dinâmicas:
 - **None** Desabilitar as atualizações dinâmicas.
 - **Nonsecure And Secure** Habilitar as atualizações dinâmicas não seguras e seguras.
 - **Secure Only** Habilitar atualizações dinâmicas com a segurança do Active Directory. Esta opção só estará disponível com a integração ao Active Directory.
3. Toque ou clique em OK.

OBSERVAÇÃO As configurações de integração do DNS também precisam estar definidas para o DHCP. Consulte “Integração do DHCP e do DNS” no Capítulo 15.

Gerenciamento da configuração e da segurança do servidor DNS

Utiliza-se a caixa de diálogo Server Properties para gerenciar a configuração geral dos servidores DNS. Por meio dela, você pode habilitar e desabilitar endereços IP para o

servidor e controlar o acesso a servidores DNS fora da empresa. Também é possível configurar o monitoramento, o registro em log e as opções avançadas.

Como habilitar e desabilitar endereços IP para um servidor DNS

Por padrão, os servidores DNS com hospedagem múltipla respondem a solicitações DNS em todas as interfaces de rede disponíveis e os endereços IP que estão configurados para utilizar.

Por meio do console DNS Manager, você pode especificar que o servidor pode responder a solicitações somente em endereços IP específicos. Geralmente, será desejável garantir que um servidor DNS tenha ao menos uma interface IPv4 e uma IPv6.

Para especificar quais endereços IP serão utilizados para responder às solicitações, siga estas etapas:

1. No console DNS Manager, pressione e segure ou clique com o botão direito do mouse no servidor que quer configurar e toque ou clique em Properties.
2. Na guia Interfaces, selecione Only The Following IP Addresses. Selecione um endereço IP que deva responder às solicitações DNS ou desmarque um endereço IP que não deva fazê-lo. Somente os endereços IP selecionados serão utilizados para o DNS. Todos os outros endereços IP no servidor serão desabilitados para o DNS.
3. Toque ou clique em OK.

Controle do acesso a servidores DNS fora da empresa

A restrição do acesso a informações de zona permite especificar quais servidores internos e externos podem acessar o servidor primário. Para os servidores externos, isso controla quais servidores podem entrar a partir do mundo externo. Você também pode controlar quais servidores DNS de sua empresa podem acessar servidores fora dela. Para fazê-lo, é preciso configurar o encaminhamento DNS no domínio.

Para o encaminhamento DNS, configura-se os servidores DNS dentro do domínio com uma das seguintes opções:

- **Não encaminhadores (Nonforwarders)** Servidores que devem repassar consultas DNS que não puderem resolver a servidores de encaminhamento designados. Esses servidores agem essencialmente como clientes DNS para seus servidores de encaminhamento (forwarders).
- **Somente encaminhamento (Forwarding-only)** Servidores que só podem armazenar em cache respostas e passar solicitações aos encaminhadores. Também são conhecidos como servidores DNS *caching-only* (somente para armazenamento em cache).
- **Encaminhadores (Forwarders)** Servidores que recebem as solicitações de servidores não encaminhadores e de somente encaminhamento. Os encaminhadores utilizam métodos de comunicação DNS normais para resolver consultas e enviar respostas de volta aos outros servidores DNS.
- **Encaminhadores condicionais (Conditional Forwarders)** Servidores que encaminham solicitações com base no domínio DNS. O encaminhamento condicional será útil se a empresa tiver vários domínios internos.

OBSERVAÇÃO Não se pode configurar o servidor raiz de um domínio para encaminhamento (exceto para o encaminhamento condicional utilizado com resolução de nomes interna). Todos os outros servidores podem ser configurados para encaminhamento.

Criação de servidores sem encaminhamento e somente de encaminhamento

Para criar um servidor DNS sem encaminhamento ou somente de encaminhamento, siga estas etapas:

1. No console DNS Manager, pressione e segure ou clique com o botão direito do mouse no servidor que quer configurar e toque ou clique em Properties.
2. Toque ou clique na guia Advanced. Para configurar o servidor como um não encaminhador, assegure que a caixa de seleção Disable Recursion esteja desmarcada, toque ou clique em OK e pule as etapas restantes. Para configurar o servidor como um servidor somente de encaminhamento, certifique-se de que a caixa de seleção Disable Recursion esteja marcada.
3. Na guia Forwarders, toque ou clique em Edit. A caixa de diálogo Edit Forwarders será exibida.
4. Toque ou clique na lista IP Address, digite o endereço IP de um encaminhador para a rede e pressione Enter. O Windows tentará validar o servidor. Se um erro ocorrer, certifique-se de que o servidor está conectado à rede e de que digitou o endereço IP correto. Repita esse processo para especificar os endereços IP de outros encaminhadores.
5. Defina o intervalo de Forward Queries Time Out. Esse valor controla por quanto tempo o não encaminhador tenta consultar o encaminhador atual se não obtiver resposta. Quando o intervalo de Forward Queries Time Out passa, o não encaminhador tenta o próximo encaminhador na lista. O padrão é três segundos. Toque ou clique em OK.

Criação de servidores de encaminhamento

Qualquer servidor DNS que não seja designado como um não encaminhador ou um servidor somente de encaminhamento agirá como um encaminhador. Portanto, nos encaminhadores designados da rede você deve estar seguro de que a opção Disable Recursion não esteja selecionada e de que não configurou o servidor para encaminhar solicitações para outros servidores DNS do domínio.

Configuração de encaminhamento condicional

Se tiver vários domínios internos, talvez queira considerar o encaminhamento condicional, que permite direcionar as solicitações para domínios específicos a servidores DNS específicos para resolução. O encaminhamento condicional será útil se a empresa tiver vários domínios internos e for preciso resolver as solicitações entre eles.

Para configurar o encaminhamento condicional, siga estas etapas:

1. No console DNS Manager, selecione e pressione e segure ou clique com o botão direito do mouse na pasta Conditional Forwarders do servidor com o qual quer trabalhar. Toque ou clique em New Conditional Forwarder no menu de atalho.
2. Na caixa de diálogo New Conditional Forwarder, digite o nome de um domínio para o qual as consultas devam ser encaminhadas, como **adatum.com**.

3. Toque ou clique na lista IP Address, digite o endereço IP de um servidor DNS autoritativo no domínio especificado e pressione Enter. Repita esse processo para especificar endereços IP adicionais.
4. Se estiver integrando o DNS com o Active Directory, marque a caixa de seleção Store This Conditional Forwarder In Active Directory e escolha uma das seguintes estratégias de replicação:
 - **All DNS Servers In This Forest** Escolha esta estratégia se quiser a estratégia de replicação mais abrangente. Lembre-se, a floresta do Active Directory inclui todas as árvores de domínio que compartilhem os dados de diretório com o domínio atual.
 - **All DNS Servers In This Domain** Escolha esta estratégia se quiser replicar as informações do encaminhador (forwarder) dentro do domínio atual e de seus domínios-filho.
 - **All Domain Controllers In This Domain** Escolha esta estratégia se quiser replicar as informações do encaminhador para todos os controladores de domínio dentro do domínio atual e de seus domínios-filho. Embora esta estratégia proporcione uma replicação mais ampla para as informações do encaminhador dentro do domínio, nem todo controlador de domínio também é um servidor DNS (e não é preciso configurar todo controlador de domínio como um servidor DNS).
5. Defina o intervalo de Forward Queries Time Out. Esse valor controla por quanto tempo o servidor tenta consultar o encaminhador até definir que não obteve resposta. Quando o intervalo de Forward Queries Time Out passa, o servidor tenta o próximo servidor autoritativo na lista. O padrão é cinco segundos. Toque ou clique em OK.
6. Repita esse procedimento para configurar o encaminhamento condicional para outros domínios.

Como habilitar e desabilitar o log de eventos

Por padrão, o serviço DNS rastreia todos os eventos de DNS, registrando-os no log de eventos do DNS Server. Esse log registra todos os eventos DNS aplicáveis e está acessível por meio do nó Event Viewer no Computer Management. Isso significa que todos os eventos informativos, de aviso e de erro, serão registrados. Pode-se alterar as opções de registro em log seguindo estas etapas:

1. No console DNS Manager, pressione e segure ou clique com o botão direito do mouse no servidor que quer configurar e toque ou clique em Properties.
2. Utilize as opções na guia Event Logging para configurar o registro em log do DNS. Para desabilitar totalmente o registro em log, escolha No Events.
3. Toque ou clique em OK.

Uso da depuração do registro em log para monitorar a atividade do DNS

Normalmente, se utiliza o log de eventos do DNS Server para monitorar a atividade do DNS em um servidor. Esse log registra todos os eventos DNS aplicáveis e está acessível por meio do nó Event Viewer no Computer Management. Se estiver tentando solucionar problemas do DNS, algumas vezes será útil configurar um log de depuração

temporário para monitorar certos tipos de eventos do DNS. Contudo, não se esqueça de desmarcar esses eventos depois de terminar a depuração.

Para configurar a depuração, siga estas etapas:

1. No console DNS Manager, pressione e segure ou clique com o botão direito do mouse no servidor que quer configurar e toque ou clique em Properties.
2. Na guia Debug Logging, mostrada na Figura 16-11, marque a caixa de seleção Log Packets For Debugging e as caixas de seleção para os eventos que quiser monitorar temporariamente.

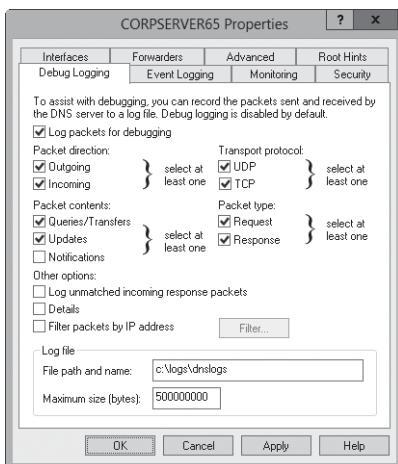


FIGURA 16-11 Utilize a guia Debug Logging para selecionar os eventos que quer registrar em log.

3. Na caixa de texto File Path And Name, digite o nome do arquivo de log, como **dns.logs**. Os logs são armazenados na pasta %SystemRoot%\System32\DNS por padrão.
4. Toque ou clique em OK. Quando terminar a depuração, desative o registro em log desmarcando a caixa de seleção Log Packets For Debugging.

Monitoramento de um servidor DNS

O Windows Server 2012 tem uma funcionalidade interna para monitoramento de um servidor DNS. O monitoramento é útil para garantir que a resolução de DNS esteja adequadamente configurada.

Pode-se configurar o monitoramento para ocorrer manual ou automaticamente seguindo estas etapas:

1. No console DNS Manager, pressione e segure ou clique com o botão direito do mouse no servidor que quer configurar e toque ou clique em Properties.
2. Toque ou clique na guia Monitoring, mostrada na Figura 16-12. Você pode realizar dois tipos de testes. Para testar a resolução de DNS no servidor atual, marque

a caixa de seleção A Simple Query Against This DNS Server. Para testar a resolução de DNS no domínio, marque a caixa de seleção A Recursive Query To Other DNS Servers.

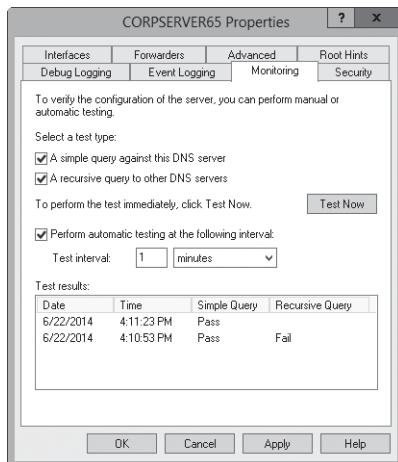


FIGURA 16-12 Configure um servidor DNS para monitoramento manual ou automático na guia Monitoring.

3. Pode-se realizar um teste manual tocando ou clicando em Test Now. O servidor pode ser agendado para monitoramento automático marcando a caixa de seleção Perform Automatic Testing At The Following Interval e definindo um intervalo de tempo em segundos, minutos ou horas.
4. O painel Test Results mostrará os resultados do teste. Você verá um carimbo de data e hora indicando quando o teste foi realizado e um resultado, como Pass ou Fail. Embora uma única falha possa ser o resultado de uma interrupção temporária, várias falhas normalmente indicam um problema de resolução de DNS.

OBSERVAÇÃO Se todos os testes de consulta recursiva falharem, a opção de servidor avançado Disable Recursion pode estar selecionada. Toque ou clique na guia Advanced e verifique as opções de servidor.

MUNDO REAL Se estiver solucionando um problema do DNS ativamente, talvez queira configurar o teste para ocorrer a cada 10-15 segundos. Esse intervalo proporcionará uma sucessão rápida de resultados de testes. Se estiver monitorando problemas no DNS como parte de seus deveres administrativos diários, um intervalo de tempo mais longo, como duas ou três horas, será desejável.

Índice

Símbolos e números

\$ (símbolo de compartilhamento especial), 471–472
32 bits, processos de, 89–91
64 bits, sistemas de, 5–6, 42–44

A

Account Lockout Policy, 192–193, 319–320, 323–324
ACEs (access control entries), 295
acesso direto à memória de rede (Net-DMA), 13–14
ACLs (listas de controle de acesso), 250
ACPI (Advanced Configuration and Power Interface), 8–12
Action Center, 539, 560
Active Directory
 adiamento da criação de índice, 219
 Administration Tool, 250 *Consulte também LDAP (Lightweight Directory Access Protocol)*
 Administrative Center. *Consulte Active Directory Administrative Center*
 árvore, domínios, 223–225
 auditoria de objetos, 499–501
 CAs (autoridades de certificação), 14–16, 32, 74–75
 Certificate Services, 14–16, 32
 clonagem de computadores de domínio virtuais, 221
 comando Adprep, 248
 comando Ntdsutil, 249
 Configuration Wizard, 216–217
 contas gerenciadas, 218
 controladores de domínio somente leitura, 16–17
 controles de políticas com base em declarações, 219
 diagnosticar problemas, ferramenta, 250, 287–289
 Directory Services Restore Mode, 16–18
 distribuição de dados atualizados. *Consulte replicação*
 Domain Services, 15–16, 32
 domínios, visão geral da estrutura, 221–222. *Consulte também domínios*
 esquemas. *Consulte esquemas*
 estrutura fornecida por, 221
 exportar contas, 370
 Federation Services, 15–16, 32
ferramenta de, snap-ins, 247–248
ferramenta de suporte, tabela de 249–250
ferramenta Users And Computers. *Consulte Active Directory Users And Computers*
florestas, domínio, 223–225, 315
funções de operações flutuantes de mestre único (FSMO), 70–71, 271, 274
Garantia de mecanismo de autenticação, 218
Group Policy, relação, 135–136
Grupo de contas de serviço gerenciado, 220
importação de contas, 370
ingresso remoto no domínio, 220
instalação, 216, 268–270
integração de DNS, 18–21, 215–216, 610–612, 620–621, 623
integração do Server Manager, 221
integração parcial com o DNS, 18–20
integração total com o DNS, 19–20
interoperabilidade com outros serviços de diretório, 240
Kerberos. *Consulte Kerberos*
LDAP. *Consulte LDAP (Lightweight Directory Access Protocol)*
Lightweight Directory Services, 15–16, 32
Limite de software de ID relativo e avisos, 221
lista de comandos de DS, 249
Lixeira do Active Directory, 218, 220, 242–246
manutenção enquanto pausado, 16–18
mecanismo, visão geral, 234–236
múltiplos controladores de domínio, 14–15
níveis funcionais de domínio, 223–225, 229–235
opções de implantação do DHCP, 19–21. *Consulte também DHCP (Dynamic Host Configuration Protocol)*
permissões, configuração, 378–379
pesquisar objetos de diretório, 252–254, 256
pesquisar usuários e grupos, 348–349
Política refinada de senha aprimorada, 220
portas utilizadas, 290–292
PowerShell, módulo, 218–219, 257
Problemas com Windows Firewall, 248
publicar compartilhamentos, 466–467
recuperação de objetos excluídos, 243–246
recurso de ativação, 219
recurso de ingresso offline no domínio, 218

- recursos, tabela dos principais, 219–221
recursos 2008 R2, 218–219
repositórios de dados, 14–15
requisitos do computador cliente, 228
Restartable Active Directory Domain Services, 16–18
restaurar, 544
resumo das ferramenta de linha de comando, 248–249
Rights Management Services, 15–16, 32
RODC com problemas de DNS, 19–20
serviços Web, 219, 257
servidores. *Consulte* controladores de domínio
sites, 135–136
snap-in Domains And Trusts, 224–225
solução de problemas, 290–292
uso do ADSI para comunicação, 240
- Active Directory Administrative Center
adição de membros a grupos, 337–338
capacidades, 219, 254
criar contas de computador, 258–259
criar contas de usuário de domínio, 331–332
criar grupos globais, 334–335
desbloqueio de contas, 371–372
domínios, conectar, 255–256
editar as propriedades das contas de computador, 261
excluir, desabilitar e habilitar contas de computador, 262
habilitar contas desabilitadas, 372
informações de contato, configuração, 347–348
mover contas de computador, 264
OUs (unidades organizacionais), gerenciamento, 279
paineis Organization, 347
pesquisar, 256–257
redefinir contas de computador bloqueadas, 262–264
regras de acesso central, 297–299
seleção de grupo primário, 338
várias contas de usuário, gerenciamento, 373–376
- Active Directory Domain Services, 228
Active Directory Domain Services Installation Wizard, 280
Active Directory Federation Services (AD FS), 15–16, 32, 295
Active Directory Installation Wizard, 268–270
Active Directory Lightweight Directory Services (AD LDS), 15–16, 32
Active Directory Rights Management Services (AD RMS), 15–16, 32
Active Directory Service Interface (ADSI), 240
- Active Directory Sites And Services, 227–228, 278–288
Active Directory Users And Computers
abrir, 250
adição de membros a grupos, 337–338
Advanced Features, 251
auditoria de objetos, 499–501
configurações do horário de logon, 353–355
conjunto de pastas, 250–251
copiar contas de usuário de domínio, 369
criar contas de computador, 259–261
criar contas de usuário de domínio, 328–332
criar grupos globais, 334
domínios e controladores, conectar, 252–253
editar as propriedades do computador, 261
escopo, selecionar para um novo grupo, 334, 335
especificações da pasta base, 352–353
excluir, desabilitar e habilitar contas de computador, 262
habilitar contas desabilitadas, 372
informações de contato, configuração para contas de usuário, 345–347
listagem de contas e recursos, 366–367
 mestres de operações, visualizar, 271–272
mover contas de computador, 264
múltiplas contas, trabalhar com, 371
OUs (unidades organizacionais), gerenciamento, 226, 251, 279–280
perfil do usuário, definir para várias contas, 374–375
permissões, configuração, 378–379
pesquisar objetos de diretório, 252–254
pesquisar usuários e grupos, 348–349
redefinir contas de computador bloqueadas, 262–263
renomear contas de usuários, 367–369
seleção de grupo primário, 338
várias contas de usuário, gerenciamento, 373–376
- Active Directory Web Services (ADWS), 257
AD CS (Active Directory Certificate Services), 14–16, 32
AD DS (Active Directory Domain Services). *Consulte também* Active Directory
adicionar a um servidor, 216
centralidade ao Active Directory, 15–16
Configuration Wizard, 216–217, 269–270
descrição da função, 32
DNS, instalação, 610–611
Group Policy. *Consulte GPMC (Group Policy Management Console)*
instalar controladores de domínio, 268–270
Restartable AD Domain Services, 16–18

- adaptadores de rede
adicionar, avaliar a necessidade, 97
associações de servidor DHCP, configurar, 580
conexões de rede, 567–568
configurações de descoberta, 556–557
endereços MAC, 13–15
estatísticas de utilização, 96
instalação de TCP/IP, 561–562
NIC Teaming, 60
problemas de desempenho, 132
virtuais, para Hyper-V, 566–567
- Add Roles And Features Wizard, 69–72, 523–524
- administrators, 313–315, 483–484
- Adsedit.msc, 250
- Advanced Configuration and Power Interface (ACPI), 8–12
- Advanced Encryption Standard (AES), 359, 549
- Aero, Windows, 4–5
- ajuste de desempenho. *Consulte* desempenho
- ajuste de desempenho de I/O de disco, 131
- alertas, contadores de desempenho, 127–128
- ambiente de pré-inicialização, 4–5
- ambiente de pré-instalação, 4–5
- Analizador de Melhores Práticas, 58–59
- aplicativos
- Apps, 6–7, 134–135, 361
 - atualizações, 538–539
 - backups de arquivos de dados, 525, 530–531
 - configurações de desempenho, 76
 - instalação Server Core sem intuito de executar, 39–40
 - logs de aplicativo, 106
 - restauração, 547–548
- aplicativos Web, internos, 15–16
- apoio DNS64, 13–14
- apoio NAT64/DNS64, 13–14
- Application Server, 32
- armazenamento. *Consulte* também unidades de disco rígido
- ajuste de desempenho de I/O, 131
 - anexoado, 417
 - BitLocker Drive Encryption, 34, 134, 402–403
 - contadores PhysicalDisk, 131
 - dispositivos de armazenamento removíveis, 394–396
 - Enhanced Storage, 35
 - estatísticas de uso de disco Resource Monitor, 118
 - iSNS Server Service, 35
 - mídias removíveis, 441–442
 - serviço de função Storage Services, 385
 - subsistemas, 434–435, 437
- técnica tradicional vs. baseada em padrões, 417
- Windows Standards-Based Storage Management, 37
- armazenamento anexado, técnicas baseadas em padrões, 417
- armazenamento baseado em padrões
- abstração, 433–434
 - armazenamento tradicional, comparação, 417–418
 - camadas, 434–435
 - compartilhamentos, criação, 435–436
 - criação de disco virtual em espaços de armazenamento, 438–440
 - eliminação de duplicação, 434–435
 - espaços de armazenamento, 433–434
 - gerenciamento de volume, 434–436, 439–442
 - opções do nó Disks, Server Manager, 435–436
 - pools de armazenamento, 433–434, 436–439
 - subsistemas, 434–435, 437
- Windows Standards-Based Storage Management, 37, 434–435
- arquivos
- compactação, 410–411
 - criptografia, 413–414, 548–550. *Consulte* também EFS (Encrypting File System)
 - expandir compactados, 411–412
 - opções de herança, 492
 - permissões básicas, 488–491
 - permissões especiais, 487, 490–492
 - pesquisar, 6–7
 - restauração, 547–548
- arquivos, logs de evento, 114–116
- arquivos de despejo, 82–84
- arquivos do sistema
- fazer backup, 525, 530–531
 - Startup Repair, 542
- arquivos ZAW (.zap), 180–181
- árvore, domínios, 223–225
- assistência remota, 5–6, 36, 134
- ativação, 44–45, 72–74, 219
- atributo archive, 518
- atualizações
- aplicativos, 538–539
 - comando Wusa.exe, 42–43
 - com Group Policy, 183–185
 - Windows Server Update Services, 34
- atualizações dinâmicas. *Consulte* também DHCP (Dynamic Host Configuration Protocol)
- atualizar Group Policy, 156–160, 164
- áudio, 36
- auditoria
- configuração de políticas de, 208, 495–501
 - de registro, 499–500

- direitos exigidos para fazer alterações, 495
específica de arquivo ou pasta, 497–500
falhas de logon, 377–378
objetos do Active Directory, 499–501
privilegio Generate Security Audits, 309
servidor DHCP, 581–582
- autenticação. *Consulte também* contas; senhas
controles de acesso baseados em
declarações, 493–495
função Active Directory Domain Services,
15–16
garantia de mecanismo de autenticação do
Active Directory, 218
identidade Authenticated Users, 315
Kerberos. *Consulte Kerberos*
políticas de segurança, 207–208
problemas no gerenciamento de servidor
remoto, 26–28
protocolos, 294–295
Rights Management Services, 15–16
autenticação baseada em impressão digital,
37
autenticação de rede, 294–295
autenticação do LAN Manager, 207–208
autenticação NTLM, 294
autocorreção do NTFS, 448–449
Automatic Updates, 133–134, 185–188
autoridades de certificação (CAs), 14–16, 32,
74–75
- B**
- Background Intelligent Transfer Service (BITS),
34
backup
agendar backup automático, 531–537
atributo archive, 518
backups de cópia, 518
backups diferenciais, 518–519, 522–523
backups fora do local, 516–517
backups incrementais, 518–519, 522–523,
525–526
baseado em nuvem, 522–524
certificados de criptografia, 551–552
completo, 518, 522–523, 525–526
configurando, 524–530
considerações de planejamento, 516–518
considerações para o agendamento, 516–
517
considerações sobre hardware, 516–517,
519–522
cópias de sombra como suplementos para,
478–482, 516–517
dados de aplicativos, 525, 530–531
de cópia, 518
de GPOs (Group Policy Objects), 163
diário, 518, 529
diferencial, 518–519, 522–523
DVDs, 522–523, 531–532, 538
especificação do local de armazenamento,
530–532
estado do sistema, 525, 543
incremental, 518–519, 522–523, 525–526
manual, 537–538
Microsoft Online Backup Service, 522–524
normal, 518
opção somente volumes críticos, 530–531
opções de mídia, 521–522
opções de volume para, 530–531
pastas compartilhadas remotas, 530–531,
536, 538
permissões, 525
privilegio Back Up Files And Directories,
308
restauração de dados por. *Consulte*
restaurar
unidades LTO, 520–521
utilitários para, lista de, 522–523
Wbadmim. *Consulte comando Wbadmim*
backup
Windows Server Backup. *Consulte Windows*
Server Backup
- balanceamento de carga
escopos de failover, 598–601
Network Load Balancing (NLB), 36, 62
- barras de tarefas, políticas de modelo,
148–149
- BCD Editor, 431–433
- bibliotecas de vínculo dinâmico (DLLs), 38, 50
- binários, 24–25, 56, 62–64, 71–72, 216
- binários da pasta USNs, 63–64
- BitLocker Drive Encryption, 34, 134, 402–403
- BITS (Background Intelligent Transfer Service),
34
- BOOTP (Bootstrap Protocol), 597
- BranchCache, 35, 384
- BranchCache for Network Files, 33
- C**
- c-states, 10–12
- cadeias de espera, visualizar, 90–91
- caixa de diálogo System Properties, 74–84
- caixa Search, painel de opções Start, 6–7
- caminhos de arquivo, modelos de segurança,
196–199
- caminhos de unidade, 405, 441–442
- capacidades internas para grupos, 311–313
- CAPI2 (CryptoAPI Version 2), 559
- cartões inteligentes, 300, 318, 358
- CAs (autoridades de certificação), 14–16, 32,
74–75

- catálogos globais
 atribuição de controlador de domínio, 236–238
 cache da associação de grupo universal, 279
 configurar, 236–237, 278
 função de autenticação, 229
 portas utilizadas, 290–291
- certificados
 Active Directory Certificate Services (AD CS), 14–16
 CAs (autoridades de certificação), 14–16, 32, 74–75
 criptografia de arquivos, 412
 DNSSEC, 627–630
 fazendo backup, 551–552
 perfis móveis, 360
 recuperação, 548–550
 registro automático, 184–186
 Rights Management Services, 15–16
 serviços de função, 32
- Character Map (Mapa de caracteres), 4–6
- charms, 5–7
- chaves de produto, 44–46, 72–74
- Check Disk, 48, 448–451
- chkdsk, 48, 448–451
- Claims-Aware Agent (Agente de reconhecimento de declaração), 32
- Client for NFS, 35
- clustering, 35
- cmdlet get-help, 25–26
- cmdlets, 24–26. *Consulte também Windows PowerShell 3.0*
- cmdlets disable-, 25–26
- cmdlets enable-, 25–26
- cmdlets get-, 25–26
- cmdlets new-, 25–26
- cmdlets remove-, 25–26
- cmdlets set-, 25–27
- comando Adprep, 230–233, 248–249
- comando ARP, 47
- comando CALL, 48
- comando CHKNTFS, 48
- comando COPY, 48
- comando Cscript, 41–42
- comando DATE, 48
- comando DEL, 48
- comando DISKPART, 48
- comando ECHO, 48
- comando End Task, 87–88, 92–93
- comando EXIT, 48
- comando FIND, 48
- comando FOR, 48
- comando FORMAT, 48
- comando FTP, 48
- comando get-service, 26–27
- comando get-smbshare, 458–459
- comando gpedit.msc, 142
- comando Gresult, 169–171
- comando LABEL, 49
- comando Netsh, 41–42, 45, 50, 560, 587
- comando ntdsutil, 249, 274
- comando ping, 50, 563
- comando PROMPT, 50
- comando Scwcmd, 204, 210
- comando SystemInfo, 42–43
- comando Wbadmin de backup
 agendar backup automático, 535–537
 ajuda, 527
 comandos disponíveis, 527–530, 534–536
 comparados a outros utilitários de backup, 522–523
 desabilitar backup diário, 529
 em execução, 526
 especificação do local de armazenamento, 530–532
 estado do sistema, 543
 excluir backups de estado do sistema, 529
 habilitar backup diário, 529
 modificar backups agendados, 535
 opção somente volumes críticos, 530–531
 opções de volume, 530–531
 parâmetros, 528
 Task Scheduler, 536–537
- comando Wecutil, 42–43
- comando Wevutil, 42–43
- comandos. *Consulte também comandos específicos*
 abrir novos prompts de comando, 40–41
 comando NET HELP, 23–24
 console. *Consulte Windows PowerShell 3.0*
 executar caixa Search, 134–135
 Mini Windows PC, tabela, 47–51
 modo de segurança com prompt, 542
 comandos de Ds, lista, 249
 comandos Dsquery, 240–241, 249
 comandos MINWINPC, 47–51
- comandos NET
 comando net help, 23–24
 comando net session, 473–474
 comando net share, 458–459
 lista, 49–50
- comandos Netdom, 41–42, 250, 263–264, 277–278
- comandos SET, 51
- comandos Slmgr, 41–42
- comandos Wmic, 42–43
- Comma-Separated Value Directory Exchange (CSVDE), 370
- compactação de arquivo, 48, 408–411, 423
- compartilhamento
 compartilhamento de pasta pública, 454–455
 compartilhamentos administrativos, 471–474

- compartilhamentos especiais, 471–474
compartilhamentos ocultos, 461, 471–474
cópias de sombra de pastas
compartilhadas, 478–482
modelo de arquivo padrão, 454–455
opções de rede, 12–13
permissões. *Consulte* permissões de compartilhamento
compartilhamento de arquivos
Advanced Sharing Settings, 457–459
clientes que estão acessando atualmente, visualizar número, 459–460
cmdlet get-smbshare, 458–459
comando net session, 473–474
comando net share, 458–459
compartilhamento de pasta pública, 454–458
compartilhamentos administrativos, 471–474
compartilhamentos especiais, 471–474
compartilhamentos múltiplos em pastas únicas, 462–464
compartilhamentos ocultos, 461, 471–474
controles de acesso baseados em declarações, 456–457
criar pastas compartilhadas, 460–466
fechar compartilhamentos abertos, 475
File And Printer Sharing, habilitar/ desabilitar, 458–459
interromper compartilhamento de pastas, 475–476
modelos de cotas, 465–466
modificar configurações para pastas, 465–467
NFS, 33, 35, 460–461, 463–464, 476–479
nomear compartilhamentos, 461, 463–464
opção Enable Access-Based Enumeration, 464
opções de configuração offline, 461–464
padrão, 454–466
permissões. *Consulte* permissões de compartilhamento
permissões NTFS, visualizar, 485
políticas de acesso central, 456–457
problemas com o Hyper-V, 465–466
propriedades de gerenciamento avançado, 465–466
protocolo SMB, 207, 454, 456–459, 463–466
publicar compartilhamentos, 466–467
suporte para sistemas de arquivos, 454–455
visualizar compartilhamentos existentes, 458–461
visualizar sessões, 473–475
compartilhamento Driveletter\$, 472
compartilhamento FAX\$, 471
compartilhamento IPC\$, 471
compartilhamento NETLOGON, 471
compartilhamento SYSVOL, 472
compartilhamentos administrativos, 471–474
compartilhamentos ocultos, 471–474
componentes, removibilidade, 4–5
computadores Apple, 338, 460–461, 476–479
computadores primários
para redirecionamento de pasta, 171–172
para restrição de mobilidade, 361
Computer Management
abrir, 100, 265
arquivar logs de eventos, 114–116
compartilhamento de arquivos, visualizar sessões, 473–475
compartilhamentos de arquivos, visualizar, 459–460
configuração de serviços, 99–105
configurar permissões de compartilhamento, 467–469
criar pastas compartilhadas, 460–464
desabilitar serviços, 105
Event Viewer, 109–110, 114–115
fechar compartilhamentos de arquivos, 475
ingresso de computadores a domínios ou grupos de trabalho, 265–268
iniciar serviços, 101
interromper compartilhamento de pastas, 475–476
interromper serviços, 101
limpar logs de eventos, 114
nó Open Files, 474–475
opções de logs de eventos, configuração, 113–114
pausar serviços, 101
publicar compartilhamentos, 466–467
servidores remotos, trabalha com, 100
sessões, terminar, 474
conexões de rede, 567–568, 580
confiança
relações de confiança transitivas, 228
Rights Management Services, 15–16
configuração de dispositivos de rede, 5–6
configuração de recuperação do serviço Group Policy Client, 104
configurações de Restricted Groups, 193–194
configurações do sistema, modelo, 148–149
configurar direitos globais do usuário, 326–327
conjuntos de coletores de dados, 122–128
conjuntos de volumes. *Consulte também* volumes estendidos
atribuição de letra de unidade, 423
criar, 422–423
definição, 418
dimensionar segmentos por disco, 422–423
exclusão, 424
problemas de status, tabela de, 420–421
vantagens, 420
conjuntos espelhados, 424–433

- console DNS Manager
 configuração DNSSEC, 627–630
 configurações de atualização dinâmica, 640
 configurações de log de eventos, 643–644
 configurar servidores, 618–622
 console para adicionar/remover servidores, 626–627
 criar domínio filho, 629–631
 depuração, registro em log, 643–644
 designação de servidor primário, 636–637
 editar registros, 635
 endereços IP, desabilitar, 641–642
 estrutura, 626
 excluir domínios ou sub-redes, 631
 gerenciamento de registros com, 631–635
 iniciar ou interromper servidores DNS, 627
 intervalos de atualização, 636–637
 modificação de registro SOA, 636–637
 monitorar opções, 644–645
 números de série, 636–637
 opções de encaminhamento, configuração, 641–644
 parâmetro de expiração, 636–637
 parâmetros de TTL, 636–637
 propriedades de zona, configuração, 636–640
 registros CNAME, adicionar, 633
 registros de endereço e ponteiro, adicionar, 631–633
 registros MX (mail exchange), 632–634
 responsible persons, 636–637
 servidores de nome, adicionar, 634–635
 visualizar registros, 635
- console System, 72–84
- conta Administrator, 305–306, 315
- conta Guest, 306
- conta LocalService, 305, 501
- conta LocalSystem, 305
- conta NetworkService, 305, 501
- contadores, desempenho, 120–125, 127–131
- contas
 Administrator, 305–306, 315
 associações de grupo, gerenciamento, 337–338
 atualizar, 366–367
 computador. *Consulte contas de computador*
 conta Guest, 306
 contas bloqueadas, 371–372
 contas de serviço gerenciado, 339–343
 contas virtuais, 344
 cotas de disco, 501
 data de validade, alterar, 373, 376
 direitos de logon, 310–311
 domínio. *Consulte contas de domínio*
 excluir, 371
 exportar, 370
- ferramentas para criação, 315–316
 grupo. *Consulte contas de grupo*
 importar, 370
 opções de segurança, 358–359
 padrão e predefinidas, 304–306
 políticas de bloqueio, 192–193, 319–320, 323–324
 políticas de nomeação, 316–318
 senhas. *Consulte senhas*
 usuário. *Consulte contas de usuário*
 contas bloqueadas, 371–372, 377–378
 contas de computador
 associações de grupo, 493
 auditoria, 500–501
 contas de computador gerenciado, 260–261
 controles de acesso baseados em declarações, 493–495
 criação de, 257–261
 editar propriedade de, 261
 gerenciamento, 262
 grupos, adicionar computadores, 337–338
 listagem, 366–367
 mover, 264
 objetos, 229
 permissões, configuração, 378–379
 privilégio Create Account Objects, 266
 proteção de nome, 582
 protegidas, 262
 redefinir contas de computador
 bloqueadas, 262–264
 senhas, 262–264
- contas de domínio
 criar, 328–332
 data de validade, alterar, 373
 exibir nomes, 316–317
 listagem, 366–367
- contas de grupo
 capacidades internas, 311–313
 contas de usuário, comparação, 298–300
 criação, 333–336
 direitos de logon, 310–311
 excluir, 371
 ferramentas para criação, 315–316
 globais, criar, 334–335
 grupos implícitos, 315–316
 grupos padrão, 313–316
 locais, criar, 335–336
 nomes, 300
 operação básica, 300–301
 privilégios disponíveis, tabela de, 308–310
 SIDs, 302–303
- contas de serviço gerenciado, 339–342
- contas de serviço gerenciado de grupo, 220
- contas de usuário
 associação de grupo, gerenciamento, 337–338, 373
 atualizar, 366–367

- caminho de script de logon, definir, 349
caminhos de perfis, definir, 349, 369
capacidades, tipos, 307–308
cartões inteligentes, 300
certificados públicos, 300
configuração de direitos locais do usuário, 328
configurar direitos globais do usuário, 326–327
contas bloqueadas, 371–372, 377–378
contas de grupo, comparação, 298–300
credenciais, impedir que deleguem, 359
direitos de logon, 310–311
domínio. *Consulte* contas de usuário de domínio
efeitos da exclusão, 300
ferramentas para criação, 315–316
gerenciamento, 371, 373–379
gerenciamento de direitos, 325–328
habilitar contas desabilitadas, 372
informações de contato, definir, 345–348
internas, 305
locais. *Consulte* contas de usuário locais
nome de script de logon, renomear, 369
nomes de logon identificados, 299–300
opções de segurança, 358–359
pastas base, definir, 349, 369
permissões, configuração, 378–379
políticas de nomeação, 316–318. *Consulte* também nomes de usuário
predefinidas, 305–306
privilegios, 307–310
propriedades, configuração, 373–376
renomear, 367–369
senhas, 300
SIDs (security identifiers), 300
status Disabled, 358, 376–379
tipos, 299–300
variáveis de ambiente, 350–351
contas de usuário de domínio
copiar para criar nova, 369
criar, 328–332
definição, 299–300
excluir, 371
propriedades, configuração, 373–376
solução de problemas de logon, 377–378
contas de usuário locais
atribuir a grupos locais, 335–336
criar novas, 332–333
definição, 299–300
contas expiradas, 373
contas implícitas, 304
contas integradas, 304
contas predefinidas, 304
contas virtuais, 344
contatos, adicionar a grupos, 338
contêineres, 135–137
contextos de nomenclatura, 287–289
Control Panel, 6–7, 23–24, 148–149, 539
controladores de disco, duplicar, 427
controladores de domínio
AD DS (Active Directory Domain Services), 15–16
agrupar, 57
atualizar Group Policy, 156–160, 164
catálogos globais, designação, 236–238
clonagem de controladores de domínio virtuais, 221
criar com o Active Directory Domain Services, 228
Directory Services Restore Mode, 16–18
estados do Active Directory, 17–18
finalidade, 609
GPOs padrão, 144–145
grupo Domain Controllers, 337
instalação, 268–271
instalação do DNS, 617–618
mestre de infraestrutura, 236–237, 241, 271–278
 mestres de operações, 228–229
modelo de replicação multimestre, 14–15
níveis funcionais, 223–225
nomes, alterar, 74–75
políticas com base em declarações, 494
portas utilizadas, 290–292
privilegio Synchronize Directory Service Data, 310
rebaixar, 270–271
replicação de dados de diretório, 228–229
restaurar estado do sistema, 544
servidores bridgehead, 289–292
sites, associar, 283
somente leitura (RODC, 16–17, 19–20, 217, 614
verificar instalação, 216–217
controles de acesso, 295–299. *Consulte* também permissões
controles de acesso baseados em declarações, 295–298, 493–495
cópias de sombra, 478–482, 516–517
cotas de disco
NTFS. *Consulte* cotas de disco NTFS
problemas de aplicação, 501
Resource Manager, 500–501, 511–515
cotas de disco do Resource Manager, 500–501, 511–515
cotas de disco NTFS
gerenciar, 507–511
Group Policy, 502–505
habilitar com base em volumes individuais, 505–507
importar e exportar, 509–511

- limites, 501
 vs. cotas de disco do Resource Manager, 500–501
 cotas de disco para contas do sistema, 501
 credenciais, impedir delegação, 359
 credenciais alternativas, 57
 criptografia
 AES (Advanced Encryption Standard), 359
 BitLocker Drive Encryption, 34
 compactação não permitida, 411–412
 copiar arquivos criptografados, 414
 criptografia de hardware de unidade, 389
 descriptografar arquivos e diretórios, 416
 EFS. *Consulte EFS (Encrypting File System)*
 etapas para criptografar arquivos, 413–414
 fazer backup de certificados, 551–552
 mecanismo, 412
 NTFS, 411–412, 414
 perfis de usuário para certificados, 412
 política de recuperação, 548–550
 restaurar certificados, 552
 sistema de recuperação de dados para arquivos, 412–413, 415
 SMB, 454, 456–457
 CryptoAPI Version 2 (CAPI2), 559
 CSVDE (Comma-Separated Value Directory Exchange), 370
- D**
- D states, 11–12
 Data Center Bridging, 35
 Data Execution Prevention (DEP), 79–80, 89–90
 Dcgpofox, 170–172
 DCOM Server Process Launcher, 104
 declarações de usuário, 493–494
 Default Domain Controller Policy GPO, 144–145, 170–172
 Default Domain Controllers GPO, 494
 Default Domain Policy GPO, 170–172
 delegação, 309, 359
 DEP (Data Execution Prevention), 79–80, 89–90
 descoberta, rede, 12–13, 556–558
 descrições, usuário, 346
 descriptografar arquivos e diretórios, 416
 descritores de segurança, 295, 301
 desempenho
 ajuste de rede, 132
 alertas, 58–59, 127–128
 c-states, 10–12
 conjuntos de coletores de dados, 122–128
 diagnósticos internos, 540
 efeitos das opções de energia, 8–12
 estatísticas de uso da CPU, 94–95
 faixa de disco para velocidade de I/O, 424–427
 ferramenta de monitoramento. *Consulte Performance Monitor*
 gráficos, 75–76, 93–94
 guia Task Manager Performance, 93–97
 memória, ajuste, 128–130
 memória virtual, configurar, 76–79
 monitoramento, metas, 116
 opções da Data Execution Prevention, 79–80
 opções de aplicativos, 76
 p-states, 10–12
 paginação, configurar, 76–79
 painel Server Manager Performance, 58–59
 privilégios Profile, 310
 processadores, ajuste, 130–131
 desfragmentar unidades, 451–453
 desktop, 6–7, 148–149
 Desktop Experience, 3–6, 38, 55, 134
 desligamento
 comando shutdown, 46
 métodos, 6–9
 privilegio Shut Down The System, 310
 scripts, 176–177
 detecção de links lentos, 157–158, 165–168
 DFS (Distributed File System), 33, 107, 140, 148–149, 250, 384–385
 DHCP (Dynamic Host Configuration Protocol)
 agentes de transmissão, 571, 573, 575
 concessões, 569–570, 573–574, 587, 590–594, 597, 605
 configuração IPv6, 571–573
 conflictos de endereços IP, evitar, 587
 DHCLIDs, 582
 DNS, 19–21
 endereçamento IPv4, 569–571
 escopos, 574–575, 578
 integração de DNS, 582–583, 610–611, 613
 mensagens de anúncio de roteador, 572–573
 modo com informações de estado, 571–573
 modo Hot Standby, 569–571
 modo Load Balance, 569–570
 modo sem informações de estado, 571–573
 NAP, 584–587
 número de servidores necessários, 569–570
 proteção de nome, 582
 reservar endereços, 604–605
 responsabilidades, 569
 Server Core padrão, 45
 serviço failover, 569–571
 servidor. *Consulte servidor DHCP*
 WINS, 21–22
 DirectAccess, 13–14, 33
 Directory Services Access Control Lists Utility, 250
 Directory Services Restore Mode, 16–18
 direito Add Workstations To Domain, 265–266

- direitos, 15–16, 325–328. *Consulte também* permissões
direitos de logon, 310–311
diretórios, arquivo, 48, 410–414. *Consulte também* pastas
diretórios, domínio. *Consulte* Active Directory
Disable Automatic Restart On System Failure, 542
discos básicos, 393, 399–403, 419
discos virtuais
 criar em pools de armazenamento, 437–440
 criar pool de armazenamento, 436–439
 exibição Server Manager, 435–436
 funções, adicionar/remover, 69–73
 iSCSI, 434–435
 localização em armazenamento baseado em padrões, 433–435
 opções de layout, 437–439
 volumes padrão, criar, 439–442
Disk Cleanup, 4–5
Disk Management
 atribuir letra da unidade, 441–442
 comando Rescan Disks, 396, 403–404
 converter discos básicos em discos dinâmicos, 400–402
 criar conjuntos distribuídos, 426–427
 criar cópias de sombra, 479–480
 criar partições, 405–408
 criar volumes, 405–408, 422–423
 discos com permutação automática, 396
 espelhamento de disco, 427–429
 esquema de codificação de cores de partição, 405
 excluir partições, 443
 expandir volumes, 447
 faixa de disco com paridade, 429
 gerenciamento de caminho de unidade, 441–442
 inicializar discos, 397
 limitações do gerenciamento remoto, 392, 394
 modos de exibição, 392
 mover discos dinâmicos para novos sistemas, 402–404
 Optimize Drives, 451–453
 partições ativas, marcar, 400–401
 problemas de estados de unidade, tabela de, 420–421
 propriedades, visualizar, 393–394
 redimensionar partições, 445–447
 reduzir volumes, 446–447
 remover um espelho, 432–433
 valores de status de unidade, tabela de, 397–398
VHDs (virtual hard disks), gerenciar, 403–404
volumes, visualizar propriedades, 418–419
Diskraid.exe, 41–42
dispositivos
 contas. *Consulte* contas de computador
 declarações, 492–495
 estados de energia, 11–12
dispositivos de armazenamento removíveis, 393–396, 441–442
Distributed File System (DFS), 33, 107, 140, 148–149, 250, 384–385
DLLs (dynamic-link libraries), 38, 50
DNS (Domain Name System)
 Active Directory, integrar, 610–612, 620–621, 623
 Active Directory, uso, 215–216
 aliases, 633
 atribuir para configuração de endereço IP, 564–565
 clientes, 612–616
 configurar em Advanced TCP/IP Settings, 615–616
 console Manager. *Consulte* console DNS Manager
 DHCP integração, 19–20, 582–583, 610–611, 613
 DNSSEC, 19–21, 627–630
 domínios de DNS vs. domínios do Active Directory, 228
 domínios filhos, 18–19, 279, 610–611
 domínios país, 18–19, 216, 610–611
 estrutura, 610–611
 estrutura de nome de host, 610
 FQDNs, 216–217, 610–611
 habilitar em uma rede, 612–614
 integração parcial com o Active Directory, 18–20, 610–611
 integração total com o Active Directory, 19–20, 610–611
 intranets, relação, 610
 IPv6, 612–613
 LLMNR, 613
 log, Servidor DNS, 107
 opções de atualização dinâmica, 621, 640
 organização do, 18–21
 porta utilizada, 291–292
 problemas de segurança, 621–622, 627–630
 proteção de nome, 582
 registros de SOA (start of authority), 632, 636–637
 replicação por redes, 610–612
 resolução de nomes de rótulo único, 614
 RODCs, 19–20, 217, 614
 servidores. *Consulte* servidores DNS
 tipos de registro, 631–632
 zona GlobalNames, 614, 624–625
 zonas 610–612, 620–625
Dnscmd.exe, 250

- DNSSEC (DNS Security Extensions), 19–21, 627–630
- Domain Name System (DNS). *Consulte DNS (Domain Name System)*
- domínios
- AD DS. *Consulte Active Directory; AD DS (Active Directory Domain Services)*
 - árvores, 223–225
 - CAs (autoridades de certificação), 14–16, 32, 74–75
 - controladores. *Consulte controladores de domínio*
 - definição, 5–6
 - DNS vs. Active Directory, 228
 - domínios filhos, 18–19, 216, 629–631
 - domínios-raiz, 18–19
 - florestas, 223–225
 - FQDNs (fully qualified domain names), 99, 216–217, 299–300, 610–611
 - gerenciamento remoto, 64
 - GPOs padrão, 144–145
 - ingresso de computadores, 74–75, 265–268
 - níveis funcionais, 223–225
 - nó GPMC Domains, 146–147
 - país, 216
 - permissões para gerenciar a Group Policy, 153
 - problemas de GPO local, 141–142
 - servidores membros, 14–15
 - sincronização de horário, 134–135
 - sistema de nomes. *Consulte DNS (Domain Name System)*
 - subdomínios, 18–19
 - tipo de rede Domain, 12–13
 - top-level (TLDs), 216
 - visão geral da estrutura, 221
- Windows Domain Manager, 250
- domínios filhos, 18–19, 216, 610–611, 629–631
- domínios pais, 18–19, 216, 610–611
- domínios virtuais, 221
- domínios-raiz, 18–19
- drivers de dispositivos, 41–42, 52, 74–76, 309, 542
- Dsacls.exe, 250
- DVDs para backups, 522–523, 531–532, 538
- Dynamic Host Configuration Protocol. *Consulte DHCP (Dynamic Host Configuration Protocol)*
- E**
- edição da Web, 5–6
- edições do Windows Server 2012, 5–6
- editores de políticas. *Consulte GPMC (Group Policy Management Console)*
- EFS (Encrypting File System)
- conceder acesso especial a arquivos criptografados, 414
 - copiar arquivos criptografados, 414
 - descriptografar arquivos e diretórios, 416
 - etapas para criptografar arquivos, 413–414
 - fazer backup de certificados, 551–552
 - mechanismo, 412
 - NTFS, 411–412
 - perfis móveis, 360
 - política de recuperação, configurar, 415, 548–550
 - posse de arquivos, 412
 - restaurar certificados, 552
 - sistema de recuperação de dados, 412–413, 415
 - eliminação de duplicação, 33, 384, 434–435, 439–440
 - email
- configurações para contas de usuário, 346
 - grupos de distribuição, 301
 - SMTP Server, 36
- emulação Windows NT PDC, 241
- endereçamento IP alternativo, 564–565
- endereçamento IP dinâmico, 564–565
- endereços IP
- conexões discadas, atribuir estático, 357–358
 - configuração dinâmica. *Consulte DHCP (Dynamic Host Configuration Protocol)*
 - conflitos, evitar, 587
 - desabilitar para DNS, 641–642
 - endereços estáticos, 562–564
 - escopos, 574–575, 578, 595–597
 - escopos de multicast, 594
 - escopos normais, 589–594
 - intervalos de exclusão, definir, 603–605
 - IP Address Management Server, 35
 - métodos de atribuição, 562
 - registros DNS para mapeamento, 631–632
 - reservar DHCP, 603–607
 - resolução de nomes. *Consulte resolução de nomes*
 - servidores IPAM para gerenciamento, 134–135
 - superescopos, 575, 587–590
- endereços IP estáticos, 562–564
- endereços IPv4
- BOOTP (Bootstrap Protocol), 597
 - configurar, 560–565, 569–571, 587
 - endereçamento dinâmico, 569–571
 - endereços conflitantes, evitar, 587
 - escopos de failover, 598–601
 - escopos normais para endereços, 589–593
 - expressões decimais, 13–15
 - filtrar endereço MAC, 602–604
 - reservar endereços, 604–605

- endereços IPv6
configuração, 130, 560–565
endereçamento dinâmico, 571–573
escopos normais, 575, 592–594
expressões decimais, 13–15
habilitar para computadores clientes, 612–613
LLMNR para resolução de nome, 22–24
reservar endereços, 604–605
endereços MAC, 13–15
Enhanced Storage, 35, 384
erros. *Consulte também* eventos
 erros de parada, 82–84
 melhorias nos mecanismos de recuperação, 538–539
 Microsoft Online Crash Analysis, 540–541
 níveis de eventos, 110
 erros de parada, 82–84
eSATA, 395
escopo, grupo, 334–335
escopos de endereços IP
 classes e tipos, 574–575
 escopos de failover, 575, 598–601
 escopos normais, 589–594
 estatísticas, visualizar, 601
 gerenciar, 597–598
 indicadores de ícone, 578
 intervalos de exclusão, 603–605
 opções de escopo, 595–597
 superescopos, 575, 587–590
escopos de multicast, 575, 594
escopos normais, 575, 589–594
espelhamento de disco, 424–433
esquemas
 função de mestre, 240, 242, 272–278
 grupo Schema Admins, 313–315
 Lixeira do Active Directory, preparação, 242–243
 níveis funcionais necessários para suporte de recurso, 218–219
 padrão, 236–237
estado de suspensão, ausência, 4–5
estado máximo de processador, 8–12
estado mínimo do processador, 8–12
estado Sleep, servidor, 4–5
estados de suspensão, processador, 10–12
estados ociosos de processador, 10–12
estatística Cached, 96
estruturas físicas, domínio, 221
estruturas lógicas, domínio, 221
Event Viewer, 3–4, 109–113
eventos
 Audit Success/Failure, 110
 categorias de tarefas, 110
 comandos de linha de comando para configurar, 42–43
 Critical, 110
 Error, 110
 Event Viewer, 109–113
 Events, Server Manager, 58–59
 IDs, 108, 110
 informativos, 109
 níveis, 109–110
 propriedades, 108
 rastreamento, conjuntos de coletores de dados, 123–124
 Server Manager para visualização, 107–113
 Warning, 110
eventos Critical, 110
examinar, 33
executar funções de servidor, 274–278
exibição, 6–7, 75–76
exportar contas, 370
- ## F
- Failover Clustering, 35
faixa de disco, 424–427, 429, 432–434, 438–439
falhas
 erros de parada, 82–84
 melhorias nos mecanismos de recuperação, 538–539
 Microsoft Online Crash Analysis, 540–541
 partições crash dump, 400–401
 reinicialização automática após erro fatal, 82–83
falhas, sistema, mecanismos de recuperação, 538–541
falhas de página, 89–90, 129
Fax Server, 3–4, 33
ferramenta ADSI Edit, 250, 287–289
ferramenta do Windows Software Licensing Management, 41–42, 73–74
ferramentas do Windows Server Migration, 46
File And Storage Services, 33, 392, 465–467
File Explorer
 acesso ao Control Panel, 6–7
 compartilhamentos especiais, conectar, 472–474
 criptografia de arquivos, 413–414
 descriptografar arquivos e diretórios, 416
 permissões, configuração, 484–485, 488–492
 posse de objeto, 483–484
 restaurar cópias de sombra, 479–481
 unidades de rede, 481–482
 visualizar permissões, 485–486
File Server Resource Manager (FSRM), 385, 510–515
File Server VSS Agent Service, 385
filtragem de camada de link, 602–604
filtrar endereço MAC, 602–604

- FireWire, 394–395
 firmware, conformidade com versão ACPI, 10–11
 florestas, domínio, 145–146, 223–225, 315
 formatar partições, 405, 407–409, 423
 formato ADMX, 139–140
 FQDN (fully qualified domain name)
 estrutura, 216–217, 610–611
 nomes de conta de grupo utilizando, 300
 nomes de logon utilizando, 299–300
 serviços, identificando, 99
 FSRM (File Server Resource Manager), 385
 Fsutil, 387
 função de emulador PDC, 241–242, 271–272, 274–278
 função de mestre de ID relativo
 executar, 274–278
 finalidade, 240
 gerenciar, 271–272
 localização, 242
 tarefa gerar SID, 300
 transferência, 274
 função de mestre de nomeação de domínios, 240, 242, 272–278
 função FSMO (flexible single-master operation), 70–71, 271, 274. *Consulte também* mestres de operações
 funções de servidor
 Add Roles And Features Wizard, 57, 69–72
 binários, 71–72
 configuração de política de segurança, 206
 considerações sobre requisitos de hardware, 31
 definição, 31
 gerenciamento com módulo ServerManager, 62
 gerenciamento com Server Manager, 69–73
 Ocsetup.exe para configuração, 41–42
 paineis Roles And Features, Server Manager, 58–59
 Remove Roles and Features Wizard, 70–73
 tabela de disponíveis, 32–34
- G**
- G states, 11–12
 Gadgets do Windows, 4–5
 gateways, 564–566
 gerenciamento remoto
 adicionar servidores ao Server Manager, 66–67
 bloquear para o servidor local, 65
 capacidades do Disk Management, 392, 394
 cliente web WinRM IIS Extension, 26–27
 credenciais requeridas, 65–66
 ferramentas disponíveis, 64
 grupos, 67–70
 independência do Remote Desktop, 66
 PowerShell, 69–70
 PowerShell Web Access, 24–25
 propriedades, 60
 RSAT, 36, 64, 133, 254
 tarefas disponíveis, 64–66
 Windows Firewall, aplicativos habilitados, 65–66
 WinRM, 25–29
- GPMC (Group Policy Management Console)
 abrir, 145–146
 abrir políticas locais, 144
 Active Directory, uso, 146–147
 atalhos, 147–148
 atribuição de script, 176–179
 atualizar Group Policy, 156–160, 164
 auditoria, configuração, 495–497
 bloquear herança, 154–156
 comando Add Forest, 145–146
 comando gpmc.msc, 145–146
 configurações do processamento de loopback, 165
 copiar GPOs, 162
 criar GPOs, 149–151
 criar políticas locais, 144
 delegação de privilégios para gerenciar, 151–153
 desabilitar GPOs, 142, 164
 detecção de links lentos, configurar, 165–168
 editar uma GPO, 142–143, 146–147
 escolhas Editor, 139
 estrutura de nós, 145–146
 excluir GPOs, 168–170
 fazer backup de GPOs, 163
 formato ADMX, 139–140
 gerenciamento do Automatic Update, 185–188
 GPOs de início, 139, 150–151
 GPOs locais, 141–144
 Group Policy Object Editor, 139
 herança, gerenciar, 153–156
 implantação de software, 181
 implantar modelos de segurança, 203
 importar GPOs, 162–163
 imposição de herança, 155–156
 instalação, 139
 links vs. acessar GPOs reais, 146–147
 Local Object Editor, 139
 Modeling Wizard, 159–161
 modelos administrativos, 147–150
 nó Computer Configuration, 146–148
 nó Domains, 146–147
 nó Group Policy Modeling, 146–147
 nó Group Policy Results, 146–147
 nó Policies, 147–148

- nó Preferences, 147–148
nó Results, 164, 169–170
nó Sites, 146–147
nó Software Settings, 147–148
nó User Configuration, 147–148
nó Windows Settings, 147–148
ordem de vinculação, alterar, 154
permissões para gerenciar a Group Policy, conceder, 153
preferência por precedência, configuração, 154, 165
problemas de versão do OS, 139–142
redirecionar pastas especiais, 172–175
registro automático, 184–186
remoção de link, 168–170, 211
repositório central, 140
restaurar GPOs, 163–164
RSOP (Resultant Set of Policy), 164, 169–171
solução de problemas, 169–171
vincular GPOs a contêineres, 149–151
- GPOE (Group Policy Object Editor). Consulte GPMC (Group Policy Management Console)
- GPOs (Group Policy Objects)
atribuição de script de desligamento, 176–177
atribuição de script de início, 176–177
atribuição de script de logon/logoff, 178–179
atribuições de direitos do usuário, 326
atualizar, 156–160, 164
auditoria, configuração, 495–501
bloquear herança, 154–156
camada GPO local específica para usuário, 142, 144
camada local Administrators and Non-Administrators, 141–142, 144
comando gpedit.msc, 142
configurações do processamento de loopback, 165
contêineres, 135–137
copiar, 162
criar, 149–151
definição de, 135–136
delegação de privilégios para gerenciar, 151–153
desabilitar local, 142
desabilitar partes não utilizadas, 164
editar. Consulte GPMC (Group Policy Management Console)
excluir, 168–170
fazer backup, 163
Folder Redirection, editar, 171–175
GPOs de início, 150–151
herança, 135–137, 153–156
implantação de modelos de segurança, 202–203
- implantação de políticas baseadas em declarações, 297–299
importar, 162–163
locais, 141–144
log de eventos, 141–142
modelos administrativos, 148–150
objetos de Group Policy locais, 141–144
ordem de vinculação, alterar, 153–154
pasta Machine, 143–146
pasta para políticas de domínio, 145–146
pasta User, 143–146
políticas de conta, definir, 319–320
políticas de domínio padrão, 144–145, 170–172
políticas de segurança, incluindo, 210
precedência, 149–150, 153–156, 165
prioridade de GPOs locais, 142
remoção de link, 168–170
replicação, 140
repositórios centrais, 140
resolução de conflitos, 142
restauração, 163–164
RSOP (Resultant Set of Policy), 169–171
vincular a contêineres, 149–151
- GPOs de início, 150–151
GPT (GUID partition table), 390, 397, 401–402, 405
Gupdate, 159–160
Graphical Management Tools And Infrastructure, 56
Graphical Shell, 3–4, 55
gravações, desempenho de disco, 131
- Group Policy
Active Directory, relação, 135–136
agentes de recuperação EFS, 550
atribuição de script, 176–179
atualizações manuais, 159–160
atualizar, 138, 156–160, 164
auditoria, configuração, 495–501
Automatic Update, gerenciamento, 185–188
bloquear herança, 154–156
capacidades, 135–136
comando gpedit.msc, 142
compatibilidade com versões OS, 138
configuração da política de recuperação, 415
configurações de grupos restritos, 193–194
configurações do processamento de loopback, 165
console. Consulte GPMC (Group Policy Management Console)
contêineres, 135–137
delegação de privilégios para gerenciar, 151–153
desabilitar partes não utilizadas, 164

- deteção de links lentos, 165–168
 direitos do usuário, 325–328
 dispositivos móveis, 166
 excluir, 168–170
 gerenciamento, 139–160
 gerenciamento de redirecionamento de pasta, 171–175
GPMC. Consulte GPMC (Group Policy Management Console)
 herança, 153–156
 implantação de modelos de segurança, 202–203
 implantar software, 179–187
 links, 146–147, 149–151, 154, 168–170
 locais, 135–136, 325–328
Management Console, 35
Modeling Wizard, 159–161
 modelos administrativos, 148–150
 modelos de segurança. *Consulte* modelos de segurança
 nó *Wired Network*, 558
 nó *Wireless Network*, 558–559
 ordem de aplicativos, 136–137
 permissões para gerenciar, 151–153
 política de cota de disco NTFS, 502–505
 objetos. *Consulte* GPOs (Group Policy Objects)
 políticas com base em declarações, 296
 políticas de usuário vs. de computador, 136–138
 precedência, 149–150, 153–156, 165
 problemas com cotas de disco, 501
 registro automático, 184–186
 registro em log, 141–142
 replicação, 140
 requisitos, 138
RSOP (Resultant Set of Policy), 151–152, 164, 169–171
 sequência de aplicativos, 136–137
 solução de problemas, 169–171
 Windows Update para payloads, 63–64
- Group Policy Management Console (GPMC). Consulte GPMC (Group Policy Management Console)*
- Group Policy Management Editor, 319–320
Group Policy Object Editor (GPOE), 139. *Consulte também* GPMC (Group Policy Management Console)
 grupo Administrators, 313–315, 483
 grupo de programa Administrative Tools, 23–24
 grupo Domain Admins, 307, 313–315
 grupo Domain Computers, 337
 grupo Domain Users, 336
 grupo Enterprise Admins, 313–315
- grupo Everyone
 associação conta Guest, 306
 permissão de compartilhamento Full Control padrão, 465–466
- grupo Guest, 306
- grupos
 adicionar membros, 337–338, 373
 auditoria, 499–501
 capacidades internas, 311–313
 configurar por escopo, 304
 contas. *Consulte* contas de grupo
 controles de acesso baseados em declarações, 493–495
 de computadores, 337–338, 500–501
 de distribuição, 52, 301
 de segurança, 301, 303
 direitos dos membros, 325
 encontrar no Active Directory, 348–349
 escopos, 301–302
 grupo Guest, 306
 internos, 306–307
 listagem, 366–367
 permissões, configuração, 378–379
 política. *Consulte* Group Policy primários, 338
 servidores, gerenciamento remoto, 67–70
 tipos de grupos, 300
 uso recomendado dos tipos, 303–304 universais, 229, 236–239, 279, 302–304
- grupos de trabalho
Active Directory Lightweight Directory Services, 15–16
 CAs (autoridades de certificação), 15–16
 contas Administrator, 306
 definição, 5–6
 gerenciamento remoto, 64
 ingresso de computadores, 74–75, 265–268
 sincronização de horário, 134–135
- grupos globais
 capacidades de escopo, 302
 contas, criar, 334–335
 definição, 301
 uso recomendado, 303–304
- grupos implícitos
 função dos, 307
 grupo Everyone, 306
 lista de, 315–316
- grupos locais
 adicionar usuários, 336
 criar, 335–336
 GPOs locais, 141–144
Local Group Policy Editor, 311–313
 modelos de segurança para políticas locais, 191–193
 políticas locais, 325–328
 tipos, 301

grupos locais de domínio, 301–304
grupos locais internos, 301
guia Advanced, caixa de diálogo System Properties, 75–84
guia Computer Name
guia Computer Name, 73–75
GUIDs (globally unique identifiers), 260

H

hardware
 backups, opções, 519–522
 configuração, 5–6
 CPUs. *Consulte processadores*
 diagnósticos internos, 540
 discos. *Consulte unidades de disco rígido*
 guia Hardware, acesso para configuração, 74–76
 independência, modularização, 4–5
 log Hardware Events, 107
herança
 ACEs, 295
 GPOs, 135–137, 153–156
 opções, 492
 permissões de objetos, 484–485
horário
 comando TIME, 51
 propriedade Time Zone, 60–61
 recurso Windows Time, 134–135
hotfixes, 42–43
Hyper-V
 compartilhamentos de arquivos, problemas, 465–466
 configuração da rede, 566–567
 Descrição de serviço, 33

I

identidade de logon anônimo, 315
identidade Everyone, 315–316
identidade Interactive, 315–316
identidade Proxy, 315–316
identidade Restricted, 315–316
identidade Self, 315–316
identidade Service, 315–316
identidade System, 315–316
identidades compostas, 295–296
identidades Creator, 315
identidades especiais, 304
identificadores
 I/O, utilização, 95
 processo, 89–90
 produto, 60
IDs de sessão, 90–91, 97
IE ESC (Internet Explorer Enhanced Security Configuration), 60

IIS (Internet Information Services)
 contas de serviço, 339
 Extensão do WinRM, 38
 função IIS (Web Server), 34
imagens, Windows
 comando DISM, 48
 recursos, instalação a partir do PowerShell, 62–63
implantar software por meio de Group Policy, 179–185
importar contas, 370
impressão, 33, 50, 148–149, 472
independência de linguagem, modularização, 4–5
índices, 219
informações de contato, definir para contas de usuário, 345–348
ingresso de computadores a domínios ou grupos de trabalho, 265–268
ingresso em domínio, recurso remoto, 220
ingresso offline no domínio, 266–268
inicialização
 ambiente de pré-inicialização do Windows, 4–5, 445–447
 BCD Editor, 431–433
 caixa de diálogo Startup And Recovery, 82–84
 definir inicialização padrão SO, 82–83
 definir opções, tela Recovery, 541
 mecanismo de servidor DHCP, 569–570
 modo de depuração, 542
 modo de segurança, 541–543
 partições de inicialização, 400–401, 431–433, 441–442
 restaurar opções, 542
 scripts, 176–177
 Startup Recovery Options, 545
 Startup Repair (StR), 540, 542, 545
 Windows Boot Manager, 82–83, 445
 Windows Preboot Environment, 4–5
Ink and Handwriting Services, 35
Instalação
 comandos de linha de comando, tabela, 47–51
 etapas da instalação, 43–47
 log, 106
instalações
 alterar tipo, 54–55
 atualizações, etapas para realizar, 46–47
 chave do produto, 44–46
 espaço em disco requerido, 43–44
 instalação com interface mínima do servidor, 3–4, 39–40, 55
 instalações com interface gráfica do usuário, 3–4. *Consulte também instalações de servidor completo*

- instalações de interface mínima, 3–4, 39–40, 55
 instalações Server Core, 3–4, 39–46, 55–57, 523–524
 layouts de teclado, 43–45
 limpar, etapas, 43–46
 limpar vs. atualizações, 42–43
 partições, gerenciamento durante, 51–54
 requisitos de hardware, 42–44
 requisitos para processador de 64 bits, 42–44
 termos de licenciamento, 44–45
 tipo, escolher, 44–45, 47
 tipos que podem ser alterados após instalação, 3–4
 uso de linha de comando, 47–48
Where Do You Want to Install Windows, 44–45
- instalações de servidor completo
 instalações de interface mínima, converter de e para, 55
 recursos inclusos, 3–4, 39–40
- instalações Server Core
 configurar comandos, 45–46
 converter outros tipos de instalação, 55–56
 DHCP padrão, 45
 funcionalidade limitada, 3–4
 funções suportadas, 39–40
 interface de usuário, 39–41
 opções da ferramenta de backup, 523–524
 prompt de comando, abrir novo, 40–41
 recursos que podem ser instalados, 41–42
 Sconfig, 40–42, 57
 Windows Logon, 39–41
- interface USB, 394–395
 Internet Explorer, 60
 Internet Printing, 3–4, 33, 35
 Internet Storage Naming (iSNS) Server Service, 35
 intranets, 15–16, 18–19
 ipconfig
 endereços de autoconfiguração, 574
 endereços MAC, 602–604
 liberar endereços reservados, 605–607
 parâmetro all , 41–42
 versão Mini Windows PC, 49
- iSCSI
 iSNS Server Service, 35
 novo disco virtual, criar, 434–435
 serviço Target Server, 33
 serviços de função, 434–435
 serviços de função iSCSI Target, 385
- ISTG (Inter-Site Replication Topology Generator), 289–291
- K**
- Kerberos
 autenticação, 294
 configurar políticas, 319–320, 324–325
 controles de acesso baseados em declarações, 493–495
 delegação restrita entre domínios, 220
 opções de segurança da conta, 359
 pré-autenticação, 359
 tiquetes, 325
 with Armoring, 220, 295–296, 493
- Kerberos with Armoring, 220, 295–296, 493
- kernel, SO
 estatísticas de memória, 96
 Kernel Transaction Manager (KTM), 448
 uso, rastreamento, 94
- KTM (Kernel Transaction Manager), 448
- L**
- laptops com Windows Server, 8–9
 Last Known Good Configuration, 542
 latência, rede, 132
 layouts de teclado, 43–45
 LDAP (Lightweight Directory Access Protocol)
 definir Security Configuration Wizard, 207
 Ferramenta administrativa do Active Directory, 250
 importar arquivos com atributos LDAP, 370
 objeto InetOrgPerson, 299–300
 portas utilizadas, 290–291
 uso do Active Directory, 240
- Ldp.exe, 244
- leitura, desempenho de disco para, 131
- letras de unidade
 alterar em sistemas baseados em padrões, 434–435
 atribuir, 405, 406, 423, 441–442
 discos movidos, 403–404
 volumes padrão, atribuir, 440–441
- letras de unidade de volume do sistema, 441–442
- licenciamento, 33, 41–42
 limitação, processador, 8–12
 Linear Tape Open (LTO), 520–521
 Link-Local Multicast Name Resolution (LLMNR), 22–24
 Lixeira, Active Directory, 220, 242–246
 Lixeira otimizada do Active Directory , 245–246
- LLMNR (Link-Local Multicast Name Resolution), 22–24, 36, 613
- Local Users And Groups
 criação de grupo local, 335–336
 senhas, redefinição, 371
- log. Consulte auditoria; logs
 log de eventos encaminhado, 106

- log de File Replication Service, 107
log de segurança, auditoria, 495–501
log do Directory Service, 107
log Microsoft Windows, 107
log System, 106, 141–142
logon único, 294–295
logons
autenticação de protocolos, 294–295
desconectar usuários forçosamente no término do horário de logon, 355
direitos, 310–311
falhas, registro em log, 377–378
horários permitidos, gerenciamento, 353–355, 375
identidade de logon anônimo, 315
mensagens de erro, 377–379
nomes. *Consulte* nomes de logon
opções de controle, 376
permitir por estação de trabalho, 355–356, 376, 378–379
políticas de bloqueio, 323–324
problemas no perfil do usuário, 359.
Consulte também perfis de usuário
scripts. *Consulte* scripts de logon
senhas. *Consulte* senhas
Server Core, 39–41
solução de problemas, 376–379
tokens de segurança gerados, 303
validação. *Consulte* autenticação
- logs
arquivos, 114–116
auditoria. *Consulte* auditoria
caixa de diálogo Log Properties, 113–114
conjuntos de coletores de dados, 122–128
Event Viewer, 109–113
limpar, 114
lista de disponíveis, 106–107
log de erro de parada, 82–83
log Hardware Events, 107
logs de DHCP, 581–582
modos de substituição, 114
níveis de eventos, 109–110
propriedades, colunas, 108, 110
Server Manager para visualização, 107–113
serviço Windows Event Log, 106–107
tamanho, definir máximo, 113
- logs de aplicativos e serviços, 106–107
logs de evento. *Consulte também* logs
arquivos, 114–116
caixa de diálogo Log Properties, 113–114
categorias de tarefas, 110
coluna Data, 110
conjuntos de coletores de dados, 122–128
Event Viewer, 109–113
exibições personalizadas, criar, 110–112
filtrar, 110–113
gerenciamento remoto, 66
- limpar, 114
lista de disponíveis, 106–107
log de eventos encaminhado, 106
modelos de segurança, 191–193
modos de substituição, 114
nível de eventos, 109–110
opções de configuração, 113–114
propriedades, colunas, 108, 110
Server Manager para visualização, 107–113
serviço Windows Event Log, 106–107
servidores DNS, 643–644
tamanho, definir máximo, 113
visualizar arquivos, 116
- logs do Windows, 106
Lpd.exe, 250
LPR Port Monitor, 35
LTO (Linear Tape Open), 520–521
LUNs. *Consulte* discos virtuais
- M**
- mapeamento de unidades de rede, 472–474, 481–482
máscaras de sub-rede, 562–563, 569–570
MBR (master boot record)
conversões de disco básico para dinâmico, 401–402
GPT, comparação, 390
número de partíciones permitidas, 404–405
selecionar durante instalação, 397
medição de linha de base, estabelecer, 117–118
memória
ajuste de desempenho, 128–130
alocação entre SO e aplicativos, 128
arquivos de despejo, 82–84
cached, estatística, 96
contadores, tabela, 129–130
Data Execution Prevention, 79–80
diagnósticos internos, 540
disponível, diretrizes, 129
estatísticas de uso do Resource Monitor, 118
falhas de página, 89–90, 129–130
Guia Performance, Task Manager para
estatísticas, 95–96
Peak Working Set, processo, 89–90
privilegio Lock Pages In Memory, 310
processos, reservados, 87–88
reserva de memória não paginável, 89–90
Windows Memory Diagnostic Tools, 545
- memória virtual
configurar, 76–79
contador Committed Bytes, 129
estatística Committed, 95
Resource Exhaustion Detection And Recovery, 539

- Message Queuing, 35
 mestre de infraestrutura
 catálogos globais, relação, 236–237
 execução, 274–278
 tarefas, 241
 transferência, 274
 visualizar, 271–272
 mestres de chave, 628–630
 mestres de operações
 atribuição, 241
 definição, 229
 execução de funções, 274–278
 função de emulador PDC, 241–242
 função de mestre de esquema, 240, 242
 função de mestre de ID relativo, 240, 242
 função de mestre de infraestrutura.
 Consulte mestres de infraestrutura
 função de mestre de nomeação de domínios, 240, 242
 funções requeridas pelo Active Directory, 240–241
 mestres de operações de reserva, 241
 situação com controlador de domínio único, 241
 transferir funções, 272–274
 visualizar, 271–272
 método user publishing para implantação de software, 180
 MFT (master file table), 391
 Microsoft Exchange Server
 contas de serviço, 339
 Windows Server Backup, 524
 Microsoft Management Console, 3–4
 Microsoft Online Backup Service, 522–524
 Microsoft Online Crash Analysis, 540–541
 Microsoft Update, 34
 migração, 46
 migrações de serviço de diretório X.500, 299–300
 Mini Windows PC, comandos, 47–51
 Modeling Wizard, Group Policy, 159–161
 modelo de replicação multimestre, 14–15
 modelos administrativos, 148–150
 modelos de segurança
 aplicabilidade, 189
 configurações de caminho de arquivo, 196–199
 configurações de políticas, 191–193
 configurações de políticas para serviços do sistema, 194–195
 configurações de registros, 196–198
 configurações de Restricted Groups, 193–194
 configurar, 199–202
 criar, 190, 191
 etapas para utilizar, geral, 190
 implantação de múltiplos computadores, 202–203
 modelos de reversão, 201–202
 pastas, 191
 políticas de segurança, incorporar, 204, 208
 Security Configuration And Analysis, 190–191, 199–202
 modo de inicialização, habilitar, 542
 modo de resfriamento ativo, 8–10
 modo de resfriamento passivo, 8–10
 modo de segurança, 541–543
 modo Windows Error Recovery, 541
 modos de resfriamento, 8–10
 modularização, 4–5
 módulo ServerManager para PowerShell, 62–63
 monitorar servidores, 116–118. *Consulte* também desempenho
 monitores, 6–7, 75–76
 móveis
 certificados de criptografia em perfis, 412, 549
 perfis móveis, 360–362, 366, 549
 MPIO (Multipath I/O), 35, 384
 MS-DOS, RAID não conformidade, 425–426
 MSI (Microsoft Installer), 42–43, 180–181
 Multipath I/O (MPIO), 35, 384
- N**
- NAP (Network Access Protection), 584–587
 NDF (Network Diagnostic Framework), 560
 .NET Framework, 36
 Net-DMA (network direct memory access), 13–14
 NetBIOS, 20–22, 49, 613
 Netmon, 560
 Network Access Protection (NAP), 584–587
 Network And Sharing Center
 Advanced Sharing Settings, 457–459
 conexões de rede, 567–568
 configuração, básica, 12–13
 configurações de múltiplos gateways, 565–566
 configurações do DNS, 615–616
 endereçamento IP, 563–565
 endereçamento IP alternativo, 564–565
 indicadores de status, 557–558
 opções de solução de problemas, 558
 página Network Connections, 558
 Network Awareness, 556
 Network Device Enrollment Service, 32
 Network Diagnostic Framework (NDF), 560
 Network Diagnostics, 555, 560
 Network Discovery, 12–13, 556–558
 Network Explorer, 555–557

Network File System. *Consulte NFS (Network File System)*
Network Load Balancing (NLB), 36, 62
Network Location Awareness, 141–142
Network Monitoring, 560
Network Policy and Access Services (NPAS), 33, 584–587
Network Policy Server, 584–587
Network Unlock, 389–390
Next Generation TCP/IP stack, 14–15
NFS (Network File System)
 Client for NFS, 35
 compartilhamento de arquivos, 460–461, 476–479
 opções de perfis de compartilhamento, 463–464
 serviço de função, 33
 serviço de função Server for NFS, 385
níveis funcionais
 Adprep para atualização, 230–233
 aumentar, 233–235
 listas e descrições, 223–225, 229–230
 modo 2003, 229–234
 modo 2008, 229, 231–232
 modo 2008 R2, 229–233
 modo 2012, 229–230, 232–233
 requisito de nível mínimo, 230]
nível 0, RAID, 424–427, 432–433
nível 1, RAID, 424–433
nível 5, RAID, 424–426, 429, 432–434
NLB (Network Load Balancing), 36, 62
nomes de computadores, 45–46, 74–75
nomes de exibição, 316–317, 329, 331–332
nomes de logon
 atribuição de códigos numéricos, 318
 criar para uma conta, 329, 331–332
 nomeação de esquemas, 318
 partes, 299–300
 pré-Windows 2000, problemas, 329, 331
 regras, 316–317
nomes de usuário
 alterar, função de SIDs, 300
 nomes de logon, construção, 299–300
 políticas de nomeação, 316–318
 variável de ambiente, 350
Notepad, 40–41
novos recursos do Windows Server 2012, 5–7
NPAS (Network Policy and Access Services), 33
NPS (Network Policy Server), 356
NTFS Transacional, 447–448
núcleos, múltiplos, 5–6, 10–12
números de telefone, contato do usuário, 346–348

O
objeto InetOrgPerson, 299–300
objetos
 editar permissões, 484
 ferramentas de gerenciamento e gerenciadores, 482–485
 grupo. *Consulte GPOs (Group Policy Objects)*
 herança, 484–485
 posse, 483–484
 tipos, 482–483
objetos de diretivas. *Consulte GPOs (Group Policy Objects)*
objetos de usuário, 299–300
objetos filhos, 484
objetos pais, 484
Ocsetup.exe, 41–42
OCSP (Online Certificate Status Protocol), 559
Online Certificate Status Protocol (OCSP), 559
Online Responder, 32
opções de energia, 4–12
opções de Visual Effects, 75–76
Optimize Drives, 451–453
OUs (unidades organizacionais)
 definição, 135–136
 gerenciamento, 226, 279–280
 permissões para gerenciar a Group Policy, 153
políticas de domínio padrão, 144–145
vantagens em criar, 224–226

P
p-states, 10–12
pacotes para implantação de software com Group Policy, 180
página da Web, definir para usuários, 346, 348
paginação, 76–79, 400–401
painel Organization, 347
parâmetros de retorno de chamada, 357
partições
 ativas, 400–401, 443
 compactação, habilitar, 408–411
 conversões de disco básico para dinâmico, 400–401
 crash dump, 400–401
 criar, 53, 405–408
 de diretório de aplicativos, 235–236
 do sistema, 400–401
 estendidas, 54, 405
 estrutura, 404–405
 excluir, 51–54, 443
 formatações rápidas, 408–409
 formatar, 53, 405, 407–409, 423
 formato de sistema de arquivos, selecionar, 407, 409

- GPT (GUID partition table), 390, 397, 401–402, 405
 inicialização, 400–401, 431–433, 441–442
 instalação, alterar durante, 52–54
 instalações limpas, opções, 43–44
 MBR (master boot record), 390, 397, 401–402, 404–405
 montar em pastas NTFS vazias, 406
 número permitido por unidade, 405
 preparação, 390–392
 primária, 405
 redimensionar, 445–447
 rotular, 407, 423
 unidades lógicas, 390, 399–400, 402–403, 405
 utilitário DiskPart, 48, 51–52
- pasta Public, 454–458
 pastas
 compartilhamento. *Consulte*
 compartilhamento de arquivos; pastas
 compartilhadas
 configurar permissões para, 488–492
 criptografar, 413–414
 modelos de segurança, 198–199
 opções de herança, 492
 permissões especiais, 488–489
 permissões NTFS, visualizar, 485
 redirecionamento, 171–175
 relações pai-filho, 484
 restaurar pastas que não são do sistema, 547–548
 pastas base, contas de usuário, 349, 351–353, 369, 371, 375
 pastas compartilhadas
 compartilhamento de pasta pública, 454–455
 discos removíveis, 396
 permisões baseadas em declarações, 495
 políticas do modelo administrativo, 148–149
 pastas especiais, redirecionar, 171–175
 pastas redirecionadas, 171–175, 361
 payloads, 24–25, 56, 62–64, 71–72, 216
 Peer Name Resolution Protocol, 36
 perfil de usuário obrigatório, 360, 362, 377–379
 perfis de usuário
 armazenamento em cache, 360
 caminhos, definir, 349
 certificados de criptografia, 412
 computadores primários, 361
 EFS com perfis móveis, 360
 gerenciar, 359, 361–366, 371
 múltiplas contas, definir, 374–375
 nomes, 363
 perfis móveis, 360–362
 perfis obrigatórios, 360, 362, 377–379
 problemas de implantação de aplicativos, 361
 perfis locais
 alterar tipos, 366
 criar, 361, 364
 finalidade, 360
 gerenciar, 364–366
 nomes, 363
 Performance Monitor
 abrir, 119
 alertas, 127–128
 contadores, 119–122
 credenciais requeridas, 121
 exibição do gráfico, 119
 finalidade, 117–118
 instâncias, 120–121
 modos de exibição, 120
 nó Data Collector Sets, 122–128
 objetos, desempenho, 121
 Reports, coletor de dados, 126–127
 permissão de compartilhamento Change, 467–468
 permissão de compartilhamento Full Control, 467–468
 permissão de compartilhamento No Access, 466–467
 permissão de compartilhamento Read, 467–468
 permissão especial Change Permissions, 487–489
 permissão especial Create Files/Write Data, 487–489
 permissão especial Create Folders/Append Data, 487–489
 permissão especial Delete, 487–489
 permissão especial Delete Subfolders And Files, 487–489
 permissão especial List Folder/Read Data, 487–489
 permissão especial Read Attributes, 487–489
 permissão especial Read Permissions, 487–489
 permissão especial Take Ownership, 487–489
 permissão especial Traverse Folder/Execute File, 487–489
 permissão especial Write Attributes, 487–489
 permissão especial Write Extended Attributes, 487–489
 permissão Full Control, 486
 permissão List Folder Contents, 486
 permissão Modify, 486
 permissão Read, 486
 permissão Write, 486
 permissões
 Active Directory, definir, 378–379
 backups, 525

- básicas, 485–491
compartilhamento de arquivos. *Consulte* permissões de compartilhamento
controles de acesso baseados em declarações, definir, 493–495
definir para arquivos e pastas, 488–492
direitos de logon, concedidos, 310–311
editar para objetos, 484
especiais, 486–492
herança, 484–485, 492
NFS, 476–479
pasta, modelos de segurança, 198–199
permissões de arquivo e pasta, tabela, 486
permissões para o gerenciamento de Group Policy, 151–153
privilegios, relação, 308
serviços do sistema, definir, 195
tokens de segurança, 303
unidades de rede, 481–482
permissões de compartilhamento
configurar no Computer Management, 467–469
configurar no Server Manager, 469–471
função de compartilhamento de arquivos, 454–455
lista, 466–468
opções, 462–466
permutação automática, 396
pesquisar
 Active Directory para usuários e grupos, 348–349
 aplicativos, instalados, 6–7
 caixa Search, focada, 134–135
 contas, listagem, 366–367
 para objetos do Active Directory, 252–254
 Windows TIFF Filter, 38
pesquisas diretas, 619
pesquisas inversas, 619, 623–624
planejamento com Modeling Wizard, 159–161
plano de energia Balanced, 8–9
Pnputil.exe, 41–42
PNRP (Peer Name Resolution Protocol), 36
política de declarações (claims), 219
Política refinada de senha aprimorada, 220
política Support Dynamic Access Control And Kerberos Armoring, 493–494
políticas de bloqueio, 323–324
políticas de conta
 bloqueio, 192–193, 319–320, 323–324
 configurações, 319–320
 Default Domain Policy GPO, 144–145
 modelos de segurança, 191–193
políticas de redes de celular, 166
políticas de segurança
 aplicar, 209
 comando Scwcmd, 204, 210
 computadores múltiplos, implantação, 210
configuração da política de auditoria, 208
configuração de funções de servidor, 206
configuração de rede, 207
criação, 205
definir configurações de registro, 207–208
editar, 209
finalidade, 204
modelos de segurança, adicionar, 208
opções de Save Security Policy, 208
pastas, padrão, 208
reversão, 209–211
serviços e recursos, configuração, 206–207
visualizar bancos de dados de configurações de segurança, 205–206
pools de armazenamento
armazenamento baseado em padrões,
 função, 433–434
criação de disco virtual, 438–440
criar, 436–439
discos físicos, controlados por, 437
pools primordiais, 437
portas utilizadas pelo Active Directory,
 290–292
posse de objetos, 483–484
PowerShell. *Consulte* Windows PowerShell 3.0
Previous Versions, 479–481
privilegio Act As Part Of The Operating System, 308
privilegio Add Workstations To Domain, 308
privilegio Adjust Memory Quotas For A Process, 308
privilegio Bypass Traverse Checking, 308
privilegio Debug Programs, 309
privilegio Force Shutdown From A Remote System, 309
privilegio Generate Security Audits, 309
privilegio Impersonate A Client, 309
privilegio Increase A Process Working Set, 309
privilegio Manage Auditing And Security Log, 310
privilegio Modify Firmware Environment, 310
privilegio Remove Computer From Docking Station, 310
privilegio Replace A Process Level Token, 310
privilegio Take Ownership Of Files Or Other Objects, 310
privilegios
 contas de usuário, conceder, 307–308
 processos, visualizar, 89–90
 tabela, para usuários e grupos, 308–310
privilegios Change Time, 308
privilegios Create, 308–309
privilegios Increase, 309
problemas, visualizar atuais, 539
processadores
 ajuste de desempenho, 130–131
 c-states, 10–12

- configurações de afinidade, 10–11
 contadores, 130–131
 estados de energia, 8–12
 estatísticas de uso da CPU, 94–95
 limitação, 8–12
 lógicos, visualizar quantidade de, 94
 opções de agendamento, 76
 p-states, 10–12
 problema de enfileiramento de threads, 130
 recurso de processador NX (no-execute), 79
 suporte a múltiplos núcleos em um processador, 5–6
 suspensão de processador lógico, 10–11
 uso, monitoramento, 131
 variável de ambiente de arquitetura de processador, 351
- processadores físicos, 5–6
 processadores lógicos, 5–6, 10–12
 processamento de loopback, Group Policy, 165
- processos
 aguardar recursos bloqueados, 90–91
 árvores, 92–93
 comando End Task, 87–88, 92–93
 contagem de threads, 90–91
 dependências, 90–93
 executáveis, encontrar relacionados, 87–88
 fornecedores, 87–88
 IDs de sessão, 90–91
 memória reservada, 87–89
 PIDs, 87–88, 90–93
 primeiro plano vs. segundo plano, 85
 propriedades, colunas, 88–91
 status, determinar, 87–89
 tipos, 87–88
- processos de 32 bits, 89–91
 processos em primeiro plano, 85
 processos em segundo plano, 85
 programas
 abertura, opções, 6–7
 aplicativos, 6–7, 134–135, 361
 exceções DEP, 79–80
 implantação, 179–185
 privilégio Debug Programs, 309
 repositórios de dados de diretório específicos, 15–16
 prompts de segurança, 4–6, 90–91
 prompts elevados, 4–6, 90–91
 propriedades
 recurso, 296–298
 servidor, visualizar no Server Manager, 58–61
 proteção de nome, 582
 protocolo TCP/IP
 arquitetura de camada dupla, 12–15
 configuração dinâmica. *Consulte DHCP (Dynamic Host Configuration Protocol)*
- configurações de Group Policy, 555
 endereços. *Consulte endereços IP*
 instalação, 561–562
 resolução de nomes. *Consulte DNS (Domain Name System)*
 Serviços TCP/IP Simples, 36
 PSOs (objetos de configuração de senha), 220
 publicar
 compartilhamentos, 466–467
 fornecedores de processo, 87–88
 lista de fornecedores confiáveis, 560
 repositórios de dados, 235–236
 software, 180
- Q**
Quality Windows Audio Video Experience, 36
- R**
RACTask, 120
RAID
 contador de duração de fila, 131
Diskraid.exe, 41–42
 espelhamento de disco, 424–433
 excluir volumes, 424
 faixa de disco, 424–427, 429, 432–434
 fazer backup de sistemas usando, 520–522
 níveis suportados, 418
 nível 0, 424–427, 432–433
 nível 1, 424–432
 nível 5, 424–426, 429, 432–434
 reparar, 430–434
 verificar paridade, 424
RAS Connection Manager, 36
 rastrear dados, coletar, 123–126
recovery point objective (RPO), 516–518
recovery time objective (RTO), 516–518
 recuperação. *Consulte também restaurar*
 Active Directory, 243–246, 544
 baseada em EFS, 412–413, 415
 caixa de diálogo Startup And Recovery, 82–84
 certificados de criptografia, 548–550
 comando RECOVER, 50
 comandos Wbadmin de recuperação e backup, 530
 ferramentas, instalação, 523–524
 inicializações em modo de segurança, 541–543
 melhorias no Windows Server 2012, 538–539
 opções da tela Recovery, 541
 políticas, configurar, 415
 recuperação de imagem de sistema, 43–44, 541
 serviços, configurar, 104–105

- sistema. *Consulte* recuperação de sistema volumes que não são do sistema com Windows Server Backup, 547–548
- recuperação do sistema ferramentas, 544–546 problemas na recuperação completa do sistema, 545 recuperação do Server Core, 553 restaurar estado do sistema, 543 recurso de processador NX (no-execute), 79 recurso Media Foundation, 35 recurso System Image Recovery, 43–44 recursos Add Roles And Features Wizard, 57, 69–72 adicionar com ServerManager, 62 associações com tipos de instalações, 54–55 comando add-windowsfeature, 62 comando get-windowsfeature, 62 configurar, ferramenta, 31 propriedades, 296–298 Remove Roles And Features Wizard, 70–73 sessões, visualizar, 473–475 subordinados, adicionar todos, 62 tabela de, 34–38 rede ajuste de desempenho, 132 apoio DNS64, 13–14 apoio NAT64/DNS64, 13–14 atribuição dinâmica de endereço. *Consulte* DHCP (Dynamic Host Configuration Protocol) comando Netsh, 41–42, 45, 50, 560, 587 comando ping, 563 configuração da política de segurança, 207 configuração das propriedades de Ethernet, Server Manager, 58–60 configurações de compartilhamento, 12–13 descoberta, 12–13, 556–558 DirectAccess, 13–14 endereços, rede, 13–15. *Consulte também* endereços IP estatísticas de uso do Resource Monitor, 118 estatísticas de utilização, 96 ferramentas, lista, 555–556 gerenciamento de perfil, 558 Hyper-V, 566–567 identidade Network, 315–316 IPv4. *Consulte* endereços IPv4 IPv6. *Consulte* endereços IPv6 nomes de domínio. *Consulte* DNS (Domain Name System) pacote de ferramentas, 11–13 políticas de dispositivo móvel, 166 políticas de modelo administrativo, 148–149 problemas de latência, 132 recursos de segurança, lista, 559 redes pagas, 166 redes privadas, 12–13, 621–622 redes públicas, 12–13, 621–622 servidores de nome, sem, 22–24 TCP Chimney Offload, 13–14 TCP/IP. *Consulte* protocolo TCP/IP Teredo, 560 tipo de rede Home, 12–13 tipo de rede Work, 12–13 tipos de redes, 12–13, 556 rede de dispositivos móveis, 166 redes de domínio, 556 redes ponto a ponto com LLNMR, 22–24 redes sem fio políticas, 166, 558–559 Wireless LAN Service, 38, 133 reexaminar todas as unidades, 402–403 ReFS (Resilient File System), 391, 447, 456–457, 501 Regedit, 40–41 registrar utilização de cache, 94–95 registro auditoria, 499–500 coletores de dados, 125–126 comandos REG, lista, 50 configuração da política de segurança, 207–208 modelos administrativos, 148–150 modelos de segurança, 196–198 registro automático, 184–186 registros CNAME (canonical name), 631, 633 registros de SOA (start of authority), 632, 636–637 regras de acesso central, 296–299 Regsvr32, 38 reiniciar servidores, 6–9 relatórios, coletor de dados, 126–127 Reliability Monitor, 117–120 Remote Desktop assinatura de arquivo RDP, 560 clientes, visualizar, 98–99 desconectar, 98–99 estatísticas de utilização, 98–99 gerenciamento remoto, independência, 66 gerenciar, 134 identidade Remote Desktop Services User, 315–316 Services, 33, 60 Session Host, 3–4 Task Manager para gerenciamento, 97–99 Remote Differential Compression, 36 Remote Server Administration Tools (RSAT), 36, 64, 133, 254 Remote Service Management, 66 Remove Roles And Features Wizard, 70–73, 270–271

- Repadmin.exe, 250, 275, 291–292
Repair Your Computer, 522–523
 replicação
 cmdlets para visualização, 276–277
 configuração de DNS, 620–621
 de dados de diretório por controladores de domínio, 228–229
 de GPOs utilizando DFS, 140
 dependências de serviços, 290–291
 ferramenta Replication Diagnostics, 250
 links de site, 283–284
 listagem de dados, 291–292
 log de File Replication Service, 107
 modelo multimestre de controlador de domínio, 14–15
 partições de diretório de aplicativos, 235–236
 recuperação após falhas, 289–290
 Repadmin.exe, 275–276, 291–292
 serviço de função DFS Replication, 385
 servidores bridgehead, 289–292
 solução de problemas, 290–292
 tipos de dados replicados, 235–240
 topologia de replicação intersite, 289–291
 USNs (update sequence numbers), 275, 291–292
 repositórios de dados, 14–15, 235–237
 reserva de memória não paginável, 89–90, 96
 reserva de memória paginável, 89–90, 96, 130
 resolução de nomes
 aumentar sufixos automaticamente, 615
 configurações de computador cliente, 615–616
 DNS. *Consulte DNS (Domain Name System)*
 DNSSEC (DNS Security Extensions), 19–21, 627–630
 guia Computer Name, 73–75
 LLMNR, 22–24
 pesquisas diretas, 619
 pesquisas inversas, 619, 623–624
 resolução de nomes de rótulo único, 614
 serviços suportados, 17–18
 WINS, 20–22
 resolução de nomes de rótulo único, 614
 Resource Manager, Windows System, 10–11, 37
 Resource Monitor, 117–118
 Restart Manager, 539
 Restartable Active Directory Domain Services, 16–18
 restaurar. *Consulte também recuperação*
 Active Directory, 242–246, 544
 certificados de criptografia, 551–552
 configuração do DHCP, 587–588
 configurações de segurança com modelos de reversão, 202
 configurações de segurança de GPOs, 211
 conjuntos espelhados de unidades, 430–432
 cópias de sombra, 479–481
 estado do sistema, 543
 GPOs (Group Policy Objects), 163–164
 Group Policy Objects padrão, 170–172
 privilégio Restore Files And Directories, 310
 volumes que não são do sistema, 547–548
 Resultant Set of Policy (RSOP), 151–152, 164
 retomada funcionalidade, ausência, 4–5
 RID (ID relativo)
 função de mestre. *Consulte função de mestre de ID relativo*
 limite de software e avisos, 221
 RODCs (controladores de domínio somente leitura), 16–17, 19–20, 217, 614
 RPCs (Remote Procedure Calls)
 RPC sobre IP, links de site, 284
 RPC sobre Proxy HTTP, 36
 Windows Firewall, 66
 RPO (recovery point objective), 516–518
 RSAT (Remote Server Administration Tools), 36, 64, 133, 254
 RSOP (Resultant Set of Policy), 151–152, 164, 169–171
 RSS (receive-side scaling), 13–14
 RTO (recovery time objective), 516–518
- ## S
- SATA (Serial ATA), 388, 395
 Sconfig (Server Configuration), 40–41, 45, 57
 scripts, 176–177
 scripts de logoff, 178–179
 scripts de logon
 atribuir, 178–179
 caminho, configuração, 349
 especificar, 351–352
 renomear, 369
 variável de ambiente para caminho, 350
 %UserName%, 374–375
 scripts em lote, 48, 176–177, 315
 scrubbers de dados, 391
 SCSI (Small Computer System Interface), 388
 Secure Socket Tunneling Protocol (SSTP), 559
 Secure Sockets Layer (SSL), 559
 Secured Boot, 389–390
 Security Configuration And Analysis, 190–191, 199–202
 Security Configuration Wizard
 capacidades, 204
 configuração de rede, 207
 definir configurações de registro, 207–208
 funções de servidor, serviços e recursos, 206–207
 modelos, adicionar, 208
 políticas de segurança, gerenciar, 205, 208–211

- seções de configuração, 204–205
visualizar bancos de dados de configurações de segurança, 205–206
- segurança
atualizar Group Policy, 156–160, 164, 166–167
Configuration Wizard. Consulte Security Configuration Wizard
contas Administrator, etapas para proteger, 305–306
contas de serviço, considerações, 103
Data Execution Prevention, 79–80
Default Domain Policy GPO, 144–145
efeitos da detecção de links lentos, 166–167
identificadores. Consulte SIDs
(identificadores de segurança)
log Security, 106
modelos. Consulte modelos de segurança
opções de conta, 358–359
permissões. Consulte permissões políticas. Consulte políticas de segurança
problemas do DNS, 621–622, 627–630
recursos de rede, 559
serviços, desabilitar desnecessários, 105
snap-in Security Configuration And Analysis, 190–191, 199–202
tokens, 303
verificação de usuário. Consulte autenticação
segurança biométrica, 37
senhas
conta Administrator, 306
contas de computador, 262–264
contas de serviço gerenciado, 341–343
contas de usuários, relação, 300
estratégias para senhas seguras, 318–319
logon único, 294–295
modelos de segurança, 191–193
nova, criar para contas, 330–331
opções, definir ao criar, 330–331
opções de segurança de conta, 358–359
opções para controlar, 376
política Account Lockout, 323–324
políticas regendo, 319–321
PSOs (objetos de configuração de senha), 220
redefinir, 371
senha de canal seguro, 262–264
- Server Graphical Shell, 3–4, 55
- Server Manager
abrir, 60–61
Add Other Servers To Manage, 57
Add Roles And Features Wizard, 24–25, 57, 69–72, 216
adicionar servidores, 66–67
agrupar servidores, 57
Analizador de Melhores Práticas, 58–59
- assistente administrativo, acesso pelo, 23–24
capacidades, 31, 56–57
capacidades de tarefas, 30
compartilhamentos de arquivos, visualizar, 459–461
configuração de permissão de compartilhamento, 469–471
configuração inicial, 57–61
console DHCP, 577–578
Create Server Group, 57
credenciais alternativas para servidores, 57
credenciais alternativas para servidores, inserir, 57
criar pool de armazenamento, 436–439
dependências, notificações, 31
ferramenta Group Policy. Consulte GPMC (Group Policy Management Console)
gerenciamento de grupo baseado em funções, 69–73
gerenciamento de pastas compartilhadas, 460–467
integração com o Active Directory, 221
interromper compartilhamento de pastas, 475–476
modo de exibição All Servers, 67
modo de exibição padrão, 57–58
nó Disks, 435–436
nó File And Storage Services, 434–437
nó Volumes, 434–436
opções de árvore de console, 58
opções de inicialização, 57
painei Events, 58–59, 107–113
painei Performance, 58–59
painei Properties, 58–61
painei Roles And Features, 58–59
painei Services, 58–59, 98–99. Consulte também serviços
permissões, configuração, 490–492
propriedades do Local Server, 58
rebaixar controladores de domínio, 270–271
Remove Roles And Features Wizard, 70–73
requisitos para o gerenciamento remoto, 64–65
versão de linha de comando, 62–63
- serviço Data Deduplication, 33, 384
- serviço de função File Server, 33, 385
- serviço de função Transport Server, 34
- serviço Identity Federation Support, 32
- serviço Remote Access, 33, 356–358
- serviço Windows Event Log, 106–107
- serviços. Consulte também serviços específicos Computer Management, configuração, 100–105
configuração da política de segurança, 206–207
configuração de inicialização, 101–102

- configuração de logon, 102–103
configuração de recuperação, 104–105
considerações de segurança, 103
contas gerenciadas, 339–342
cotas de disco com contas, 501
do tipo inicialização, visualizar, 99
gerenciamento, 105
guia Task Manager Services, 92–93
interromper, 93, 101
logon de contas, visualizar, 100
nomes, 99–100
organização de grupo, 99
Remote Service Management, 66
restrições, em execução sob, 92–93
Server Manager Services, 58–59, 98–99
sistema, 92–93, 194–195
status, visualizar, 99–100
serviços de diretório. *Consulte* Active Directory
serviços de federação, 15–16, 32, 295
serviços de função
 adicionar com módulo ServerManager, 62
 funções de servidor, relação, 31
 Ocsetup.exe para configuração, 41–42
serviços do sistema, 92–93, 194–195
Serviços Web, Active Directory, 219
servidor DHCP
 arquivos de banco de dados, 606–607
 arquivos de origem, 576
 associações, configurar, 580
 ativar/desativar escopos, 597
 auditoria, 581–582
 autorizar no Active Directory, 579
 conexões remotas, 578–579
 configuração das estatísticas, 580
 conflitos de endereços IP, evitar, 587
 console DHCP, 577–578
 descrição da função, 32
 escopos de failover, 598–601
 escopos de multicast, 594
 escopos normais, 589–594
 especificação de credenciais, 576–577
 excluir concessões e reservas, 606–607
 excluir escopos, 598
 fazer backup do banco de dados, 606–608
 filtrar endereço MAC, 602–604
 forçar regeneração do banco de dados, 608–609
 grupos delegados para administração, 576
 indicadores de escopo, 578
 indicadores de status, 578
 iniciar e interromper, 579
 instalação, 575–577
 integração de DNS, 582–583
 intervalos de exclusão, configuração, 603–605
 modificar propriedades de reservas, 605
 mover banco de dados, 607–609
 Network Policy Server, configurar como, 584–587
 opções de escopo, 595–597
 reconciliação, 608–609
 reservar endereços, 604–607
 restaurar banco de dados, 607–609
 salvar configurações, 587–588
 serviço, 579
 superescopos, 575, 587–590
 vários escopos, 598
 visualizar estatísticas do escopo, 601
servidores autônomos, 14–15
servidores bridgehead, 289–292
servidores de arquivo, 383–387, 485
servidores de nome, adicionar, 634–635
servidores DNS
 configuração da zona GlobalNames, 614, 624–625
 configuração de nova zona, 620–621
 configurar servidores primários, 619–622, 636–637
 configurar servidores secundários, 622, 637–639
 console Manager. *Consulte* console DNS Manager
 definir durante configuração, 618–619
 dicas de raiz, 619
 endereços do servidor, ordem de uso, 615
 endereços IP, desabilitar, 641–642
 endereços site-local conhecidos para servidores, 612
 função, servidor DNS, 32
 horários de reinicialização, 612
 iniciar ou interromper por meio do console Manager, 627
 instalar serviços, 617–619
 log de eventos, 643–644
 opções de atualização dinâmica, 621, 640
 opções de encaminhamento, 641–644
 pesquisas inversas, 619, 623–624
 serviço, 610–612, 617–618, 627
 servidores primários, 616, 619–622, 636–637
 servidores primários integrados ao Active Directory, 616
 servidores secundários, 617–618, 622, 637–639
 servidores somente encaminhamento, 617–618
 solução de problemas, 250, 644–645
 tarefas de inicialização, 612
servidores membros, relação com domínios, 14–15
servidores Web
 controlador de domínio, incapaz de executar, 5–6
 função Web Server (IIS), 34

- sessões
gerenciar, 473–475
tipo, exibir, 97
- Sidebar, Windows, 4–5
- Sidebar do Windows, 4–5
- SIDs (security identifiers)
contas de computador, 302–303
cotas de disco NTFS, usar com, 503
estrutura, 300
renomear contas de usuários, 367–369
- ícone de compartilhamento especial (\$), 471–472
- Simple Network Management Protocol (SNMP), 37
- sistema de arquivos NTFS
autocorreção do NTFS, 448–449
compactação, habilitar, 408
compartilhamento de arquivos, vantagens, 460–461
converter volumes, 443–445
cotas. *Consulte* cotas de disco NTFS
criptografia, 411–412, 414
estrutura de volumes, 391
NTFS Transacional, 447–448
permissões, 454–455, 485
- sistemas com múltiplos processadores, 94, 120
- sistemas de 64 bits, 5–6, 42–44
- sistemas de arquivos
alterar em sistemas baseados em padrões, 434–435
determinar tipo, 419
FAT, 390–391, 443–445, 449–450, 454–455
lista de suportados, 390–391
MFT (master file table), 391
NTFS. *Consulte* sistema de arquivos NTFS
organização, 383
partições, relação, 390
ReFS (Resilient File System), 391, 447, 456–457, 501
reparação de erros, 435–436
selecionar para partições, 407, 409
tamanho de unidades de alocação, definir, 407, 409
volumes padrão, formatar, 440–441
- sistemas de arquivos FAT, 390–391, 443–445, 449–450, 454–455
- sistemas de fita autoloader, 520–521
- sistemas de inicialização dupla, 419
- sistemas operacionais múltiplos, 82–83
- sites, Active Directory
Active Directory Sites And Services para gerenciamento, 227–228
bem conectados, 227
controladores de domínio, associação, 283
criar, 280–281
links entre, configurar, 283–288
nó GPMC Sites, 146–147
- permissões para gerenciar a Group Policy, 153
- relações estruturais, 135–136, 227
- servidores bridgehead, 289–292
- sub-redes, associar, 282
- topologia de replicação intersite, 289–291
- SMB (server message block)
cmdlet get-smbshare, 458–459
configuração de política de segurança, 207
criptografia das opções de compartilhamento, 465–466
melhorias na versão 3.0, 454
opções de perfis de compartilhamento, 463–464
porta utilizada, 291–292
vantagens para o compartilhamento de arquivos, 456–457
- SMTP (Simple Mail Transfer Protocol), 36, 284
- snap-in Domains And Trusts, 224–225
- Snipping Tool, 4–6
- SNMP (Simple Network Management Protocol), 37
- software antimalware, 543
- solução de problemas
Active Directory, 290–292
melhorias nos mecanismos de recuperação, 538–539
modo de segurança, 541–543
problemas, visualizar atuais, 539
problemas de logon, 376–379
servidores DNS, 644–645
Startup Repair Wizard, 545
- Sound Recorder, 4–6
- SQL Server, 339
- SSL (Secure Sockets Layer), 559
- SSTP (Secure Socket Tunneling Protocol), 559
- Storage Services, 33
- STR (Startup Repair), 540, 542, 545
- SUA (Subsystem for UNIX-Based Applications), 37
- sub-redes
criar e associar com sites, 282
excluir de servidores DNS, 147–148, 631
localização na estrutura geral de domínio, 221–222
resolução de nomes com LLMNR, 22–24
sites, relação, 135–136
zonas de pesquisa inversa, 623–624
- subdomínios, 18–19
- subordinados diretos, definir para usuários, 348
- Subsystem for UNIX-Based Applications, 37
- superescopos, 575, 587–590
- suporte a múltiplos núcleos em um processador, 5–6

Svhost.exe, 93
 Sync Center, 4–5
 System Idle Process, 90–91

T

tarefas agendadas, 66
 Task Manager
 coluna Status, processos, 87–89
 comando End Task, 87–88, 92–93
 guia Details, 88–93
 guia Performance, 93–97
 guia Processes, 86–93
 guia Services, 92–93
 guia Users, 97–99
 opções, 86–88
 Remote Desktop, gerenciamento, 97–99
 Task Scheduler, 134, 536–537
 TCP Chimney Offload, 13–14, 560
 tecla Windows, 6–7
 tela Iniciar, 6–7, 148–149
 telnet, 37
 temas, área de trabalho, 4–5
 Teredo, 560
 teste do ARP, 569–570
 threads, 90–91, 95, 130
 tipo de rede Home, 12–13
 tipo de rede Work, 12–13
 tipos de instalação
 alterar, 54–57
 escolher, 44–45, 47
 lista dos, 3–4
 tíquetes, Kerberos, 325
 TLDs (top-level domains), 216
 tokens, 303
 tolerância a falhas, RAID, 424–426
 topologia da replicação entre sites, 289–291

U

UAC (User Account Control), 4–6, 90–91
 unidades
 básicas, 393, 399–403, 419
 dinâmicas. *Consulte* unidades dinâmicas
 disco rígido. *Consulte* unidades de disco rígido
 particionamento. *Consulte* partições
 unidades de fita, 520–523
 unidades de rede, 481–482
 volumes. *Consulte* volumes
 unidades, dispositivo, 41–42, 52, 74–76, 309, 542
 unidades DAT (digital audio tape), 520–521
 unidades de alocação, 407, 409, 423, 440–441
 unidades de disco. *Consulte* unidades de disco rígido

unidades de disco rígido. *Consulte também* unidades
 analisar, 451–452
 arquiteturas de interface de unidade suportadas, 388
 autocorreção do NTFS, 448–449
 backups. *Consulte* backups básicos, 393, 399–403, 419
 caminhos de unidade, 405
 características de temperatura, 389
 Check Disk, 448–451
 comando FORMAT, 48
 compactação, habilitar, 48, 408–411, 423
 considerações de planejamento, 387
 controladores de disco, duplicar, 427
 criptografia de hardware, 389
 desfragmentar, 451–453
 desinstalar, 403–404
 dinâmicas. *Consulte* unidades dinâmicas
 discos removíveis, 393
 discos virtuais, adicionar/remover funções, 70–72
 Disk Management para configurar, 392–394
 dispositivos de armazenamento removíveis, 394–396
 estatísticas de uso de disco Resource Monitor, 118
 expandir unidades compactadas, 410–412
 formatos de unidade física, 387–390
 Free Space, 392
 gerenciador. *Consulte* Disk Management GPT (GUID partition table), 390, 397, 401–402, 405
 inicialização, 396–397
 instalação, 396–397
 listagem para um computador, 403–404
 MBR (master boot record), 390, 397, 401–402, 404–405
 mean time to failure (MTTF), 389
 mover para novos sistemas, 402–404
 NTFS Transacional, 447–448
 opções do nó Disks, Server Manager, 435–436
 otimizar, 451–453
 paginação, configurar, 76–79
 partições. *Consulte* partições
 partições ativas, 400–401
 partições crash dump, 400–401
 partições de inicialização, 400–401
 permutação automática, 396
 preparação para uso, 390–392
 problemas de status de volumes, tabela de, 420–421
 propriedade, Capacidade de, 419
 propriedades, visualizar, 393–394
 reativar, 402–403
 redefinir, 435–436

- reexaminar todas as unidades, 402–403
remover, 403–404
selecionar para incluir em volumes, 422–423
sistemas de arquivos. *Consulte* sistemas de arquivos
status Foreign, 398
status No Media, 398
status Not Initialized, 398
status Offline, 397, 402–403
status Online, 397, 402–403
status Unreadable, 398, 402–403
status Unrecognized, 398
tamanho de unidades de alocação, configurar, 407, 409, 423, 440–441
tamanhos de setor físico, 387
taxa de transferência máxima sustentada, 389
tempo médio de busca, 388–389
tipos de configuração de disco, 393
tipos de seção de unidade, 400–401
tolerância a falhas, 424–426
unidades, carregamento durante instalações, 52
unidades Advanced Format, 387
unidades de fita, 520–523
unidades de rede, 481–482
unidades desmontadas, 441–442
unidades lógicas, 390, 399–400, 402–403, 405
unidades Standard Format, 387
valores de status, tabela de, 397–398
velocidade de rotação, 388–389
VHD (virtual hard disk), 393
virtual. *Consulte* armazenamento baseado em padrões; discos virtuais
volumes de sistema, 400–401
volumes padrão, criar, 439–442
unidades dinâmicas
capacidades, 399–400
capacidades do RAID, 418
comparadas a outros tipos, 393, 419
compatibilidade do UNIX, 400–401
converter para e a partir de discos básicos, 400–403
mover para novos sistemas, 402–404
reativar, 402–403
tipos de seção de unidade, 400–401
unidades físicas. *Consulte* unidades de disco rígido
unidades organizacionais. *Consulte* OUs (unidades organizacionais)
UNIX, 37, 460–461, 476–479
Up Time, propriedade do sistema, 95
User Account Control (UAC), 4–6
User Interfaces And Infrastructure, 37–38
USNs (update sequence numbers), 275, 291–292
usuários de conexão discada, 315, 356–358
utilitário Convert, 443–445
utilitário System
capacidades de tarefas, 30
console, 72–84
gerenciamento de perfil local, 363–366
UUIDs (universally unique identifiers), 260

V

- variáveis de ambiente
comandos SET, 51
configurar, 80–82
%UserName%, 350–351, 353, 361–362, 374–375
variáveis de ambiente do sistema
comuns, lista, 350–351
configurar, 80–82
variáveis de ambientes do usuário, 80–82
variável %UserName%, 350–351, 353, 361–362, 374–375
velocidades do ventilador, 8–9
verificar paridade, 424
VHD (disco rígido virtual), 393, 403–404, 523–524
vídeo
Quality Windows Audio Video Experience, 36
Vídeo para Windows, 4–5
Volume Activation Services, 33
Volume Shadow Copy Service (VSS), 522–523
volumes
ativos, 400–401
atribuição de letra de unidade, 406, 423
baseados em padrões. *Consulte* armazenamento baseado em padrões
caminhos de unidade, 405
capacidades, 419
comando CHKNTFS, 48
comando MOUNTVOL, 49
comando VOL, 51
compactação, habilitar, 408–411
converter em NTFS, 443–445
criar, 405–408, 422–423, 435–436
de disco NTFS, habilitar, 505–507
de inicialização, 400–401, 431–433, 441–442
distribuídos, 422–427, 429, 432–434
espelhados, 424–433
excluir, 424, 434–435
expandir, 434–435, 445–447
gerenciamento remoto, 66
nó Volumes, Server Manager, 434–436
número de ativos, limite, 405
padrão, criar, 439–442
paginação, configurar, 76–79, 441–442
privilegio Perform Volume Maintenance Tasks, 310

- problemas de status, 419–421
 propriedade File System, 419
 propriedade Free Space, 419
 propriedade Layout, 418
 propriedade Type, 418
 redimensionar, 445–447
 restaurar os que não são do sistema, 547–548
 reverter inteiros em cópias de sombra, 480–481
 rotular, 407, 409, 423, 442–443
 simples, 418
 status Failed, 420
 status Healthy, 421
 tamanho, especificar, 406
 tamanho de unidades de alocação, definir, 423
 unidades lógicas, 405–406
 volumes do sistema, 400–401, 441–442
- volumes estendidos
 gerenciar, 422–424, 445–447
 problemas de status, tabela, 420–421
 vs. volumes simples, 418
- VPNs (Virtual Private Networks), 33, 356–358, 559
- VSS (Volume Shadow Copy Service), 522–523, 531–532
- W**
- WANs (wide area networks), 222, 561
- WDS (Windows Deployment Services), 3–4, 34, 260–261
- WER (Windows Error Reporting), 41–42, 60–61
- Wi-Fi. *Consulte* redes sem fio
- WIM (Windows Imaging Format), 4–5, 56, 63–64
- Windows 8, 3–5, 64, 66
- Windows Aero, 4–5
- Windows Biometric Framework, 37
- Windows Boot Manager
 configurar, 82–83
 redimensionamento possível, 445
- Windows Defender, 4–5
- Windows Deployment Services, 3–4, 34, 260–261
- Windows Domain Manager, 250
- Windows Error Reporting (WER), 41–42, 60–61
- Windows File Protection, 38
- Windows Firewall
 acessar, 134–135
 exceções, 65–66
 painel Properties, 60–61
 problemas do Active Directory, 248
 requisitos do Graphical Shell, 3–4
- Windows Imaging Format (WIM), 4–5
- Windows Internal Database, 37
- Windows Internet Name Service (WINS), 20–22
- Windows Logon, 39–42
- Windows Management Instrumentation (WMI), 65
- Windows Media Foundation, 35
- Windows Media Player, 4–5
- Windows Memory Diagnostics, 540
- Windows PE (Preinstallation Environment) 4.0, 4–5
- Windows PowerShell 3.0
 aliases, 25–26
 cmdlets, 24–26
 compatibilidade com versões anteriores, 24–25
 desabilitar gerenciamento remoto para servidor local, 65
 execução de comando de caixa Search, 134–135
 função Server Manager, 62–63
 gerenciamento remoto, 25–29, 64–65, 69–70
 iniciar, 24–25
 listagem de cmdlets, 25–26
 log de evento, 107
 módulo do Active Directory, 25–26
 problemas de ordem de execução, 25–26
 recursos, 24–25
 suporte de script, 176
- Windows Preboot Environment, 4–5
- Windows Process Activation Service, 37
- Windows Remote Management (WinRM). *Consulte* WinRM (Windows Remote Management)
- Windows Server Backup
 agendar backup automático, 531–535
 backups manuais, 537–538
 comparação com outros utilitários de backup, 522–523
 configurar, 524–526
 dados de aplicativos, 525, 530–531
 dados do estado do sistema, 525, 530–531
 especificação do local de armazenamento, 530–532
 excluir localizações ou tipos de arquivo selecionados, 531–532
 iniciar, 524
 instalação, 384, 522–524
 interromper backups agendados, 535
 Microsoft Exchange Server, 524
 modificar backups agendados, 535
 opção de linha de comando. *Consulte* comando Wbadmin de backup
 opção somente volumes críticos, 530–531
 opções de tipos de destino, 534
 opções de volume, 530–531

- pastas compartilhadas remotas, 530–531, 536, 538
permissões, 525
problemas na recuperação completa do sistema, 545
recuperação de volumes que não são do sistema, 547–548
vantagens, 522–524
VSS Settings, 531–532
- Windows Server Update Services (WSUS), 187–188
- Windows Standards-Based Storage Management, 37, 434–435
- Windows System Resource Manager, 10–11, 37
- Windows TIFF IFilter, 38
- Windows Time, 134–135
- Windows Token-Based Agent, 32
- Windows Update
gerenciar com Group Policy, 185–188
painel Properties, 60–61
payloads, Group Policy, 63–64
restaurar payloads, 216
- WinRM (Windows Remote Management)
configurar, 26–29
desabilitar para servidor local, 65
efeitos da Group Policy, 29
exceções do Windows Firewall, padrão, 65
gateway da web, 26–27
- IIS Extension, 38
ouvintes, 28–29
problemas de autenticação, 26–29
requisitos, 25–27
- Windows 8, habilitar gerenciamento remoto, 66
- WINS (Windows Internet Name Service), 20–22
- Wow64, 38
- WS-Management, 42–43
- WSH (Windows Script Host), 176
- WSRM (Windows System Resource Manager), 10–11, 37
- WSUS (Windows Server Update Services), 187–188
- WSUS (Windows Server Update Services), 34, 187–188
- X**
- XPS Viewer, 38
- Z**
- zona GlobalNames, 614
- zonas, DNS
adicionar registros, 631–635
configuração DNSSEC, 20–21, 627–630
configurar nova, 620–623
domínios filhos, criar, 629–631
integração do Active Directory, 610–612
modos de integração, definir, 640
propriedades, definir, 636–640
registros de SOA (start of authority), 632, 636–637
restrições de transferência, 637–639
servidores secundários, notificações, 639
tipos, definir, 640
- zonas de segurança, 60