

Официальное учебное пособие для самоподготовки

Учебный курс

Microsoft®

С учетом
версии R2

Администрирование

Windows Server® 2008

2-е издание, дополненное

Орин Томас
Йен Маклин

Экзамен **70-646**

MCITP

Экзамен 70-646: Администрирование Windows Server® 2008 (второе издание)

Тема	Расположение в книге
Планирование развертывания сервера	
Планирование установки и обновления сервера	Глава 1, занятие 1
Планирование автоматического развертывания сервера	Глава 1, занятие 2
Планирование ролей сервера для служб инфраструктуры	Глава 2 Глава 3 Глава 9, занятие 1
Планирование серверов приложений и служб	Глава 6, занятие 1
Планирование ролей файлового сервера и сервера печати	Глава 7
Планирование управления сервером	
Планирование стратегий управления серверами	Глава 5, занятие 1
Планирование делегированного администрирования	Глава 5, занятие 2
Планирование и реализация стратегии групповой политики	Глава 4
Мониторинг и обслуживание серверов	
Реализация стратегии управления обновлениями	Глава 8, занятие 2
Мониторинг серверов для оценки и оптимизации производительности	Глава 12
Мониторинг и поддержка безопасности и политик	Глава 8, занятие 1 Глава 9, занятие 2
Планирование подготовки приложений и данных	
Подготовка приложений	Глава 6, занятие 2
Подготовка данных	Глава 10, занятие 1
Планирование поддержки работоспособности и высокой доступности	
Планирование хранилищ	Глава 10, занятие 2
Планирование высокой доступности	Глава 11
Планирование резервного копирования и восстановления	Глава 13

Перечисленные в таблице темы экзамена актуальны на момент публикации книги. Темы экзамена могут изменяться в любое время без предварительного уведомления, по решению Microsoft. Текущий список тем экзамена можно найти по адресу <http://www.microsoft.com/learning/en/us/Exam.aspx?ID=70-646>.

MCITP
Self-Paced Training Kit

Exam **70-646**

Windows Server[®] 2008 Server Administrator

2nd Edition

Orin Thomas
Jan McLean

Официальное пособие для самоподготовки

Учебный курс *Microsoft®*

Администрирование Windows Server® 2008

2-е издание, дополненное

Орин Томас
Йен Маклин

экзамен **70-646**

MCITP

Москва 2013

УДК 004.45
ББК 32.973.81–018.2
Т56

Томас Орин, Маклин Йен

Т56 Администрирование Windows Server 2008. Учебный курс Microsoft / Пер. с англ. — М. : Издательство «Русская редакция», 2013. — 688 стр. : ил.

ISBN 978-5-7502-0427-4

Подробное руководство по настройке и администрированию операционной системы Windows Server 2008 R2. Детально описывается установка, развертывание и обновление системы, планирование сетевых служб и инфраструктуры Active Directory, подготовка приложений и данных. Рассматриваются вопросы виртуализации серверов, обеспечения высокой надежности, мониторинга и оптимизации производительности. Особое внимание уделяется стратегиям планирования. Авторы не только описывают способы выполнения различных операций, но и объясняют, почему и когда следует предпринимать те или иные действия.

Книга является ценным справочником и позволяет самостоятельно подготовиться к сдаче экзамена 70-646 по программе сертификации MCITP (Microsoft Certified IT Professional). Состоит из 13 глав и приложения, содержит множество иллюстраций и примеров из практики. На прилагаемом компакт-диске находится электронная версия книги (на англ. языке), вопросы пробного экзамена и другие справочные материалы.

Системным администраторам, квалифицированным пользователям и всем, кто хочет получить исчерпывающие знания в области развертывания и обслуживания Windows Server 2008 R2.

УДК 004.45
ББК 32.973.81–018.2

Microsoft, а также содержание списка, расположенного по адресу: <http://www.microsoft.com/about/legal/en/us/IntellectualProperty/Trademarks/EN-US.aspx> являются товарными знаками или охраняемыми товарными знаками корпорации Microsoft в США и/или других странах. Все другие товарные знаки являются собственностью соответствующих фирм.

Все адреса, названия компаний, организаций и продуктов, а также имена лиц, используемые в примерах, вымышлены и не имеют никакого отношения к реальным компаниям, организациям, продуктам и лицам.

© 2013, Translation Russian Edition Publishers.

Authorized Russian translation of the English edition of MCITP Self-Paced Training Kit (Exam 70-646): Windows Server® 2008 Server Administrator (2nd Edition), ISBN 9780735649095 © Orin Thomas, Ian McLean.

This translation is published and sold by permission of O'Reilly Media, Inc., which owns or controls all rights to publish and sell the same.

© 2013, перевод ООО «Издательство «Русская редакция».

Авторизованный перевод с английского на русский язык произведения MCITP Self-Paced Training Kit (Exam 70-646): Windows Server® 2008 Server Administrator (2-е издание), ISBN 9780735649095 © Orin Thomas, Ian McLean.

Этот перевод оригинального издания публикуется и продается с разрешения O'Reilly Media, Inc., которая владеет или распоряжается всеми правами на его публикацию и продажу.

© 2013, оформление и подготовка к изданию, ООО «Издательство «Русская редакция».

ISBN 978-0-7356-4909-5 (англ.)
ISBN 978-5-7502-0427-4

Содержание

Введение	XIV
Глава 1 Установка, обновление и развертывание Windows Server 2008 R2	1
Занятие 1. Планирование установки и обновления	2
Отличия между Windows Server 2008 и Windows Server 2008 R2	3
Выбор подходящей версии	3
Foundation Edition	6
HPC Server	6
Установка в режиме Server Core	6
Физическое и виртуальное развертывание	9
Установка Windows Server 2008 R2	10
Обновление Windows Server 2003	11
Резюме	13
Закрепление материала	13
Занятие 2. Автоматическое развертывание серверов	14
Файлы ответов Windows Server 2008 R2	15
Службы развертывания Windows	17
Многоадресное, запланированное и автоматическое развертывание	19
Подготовка отката	23
Резюме	23
Закрепление материала	24
Практикум. Установка и настройка Windows Server 2008 R2 и роли WDS	25
Упражнение 1. Установка Windows Server 2008 R2 Enterprise Edition	26
Упражнение 2. Подготовка к установке роли сервера WDS	27
Упражнение 3. Установка роли сервера WDS и добавление файлов образов	29
Закрепление материала главы	31
Резюме главы	31
Основные термины	32
Лабораторная работа	32
Задание 1. Переход Contoso на Windows Server 2008	32
Задание 2. Автоматизация развертывания Windows Server 2008 в Tailspin Toys	33
Рекомендуемые упражнения	33
Планирование установки и обновления серверов	33
Планирование автоматического развертывания серверов	33
Пробный экзамен	34
Глава 2 Планирование служб инфраструктуры	35
Занятие 1. Планирование IPv6	37
Анализ структуры адресов IPv6	37
Совместимость IPv4 с IPv6 и переход на IPv6	44
Использование утилит IPv6	51
Настройка клиентов через DHCPv6	57
Планирование сети на основе протокола IPv6	59

Резюме	63
Закрепление материала	64
Занятие 2. Планирование DNS	65
Планирование DNS Windows Server 2008 и 2008 R2	66
Новые и усовершенствованные функции DNS	76
Планирование инфраструктуры DNS	83
Закрепление материала	91
Резюме	92
Практикум. Настройка IPv6	92
Упражнение 1. Настройка IPv6 на компьютере VAN-DC1	92
Упражнение 2. Создание адреса ISATAP	94
Упражнение 3 (дополнительное). Включение маршрутизатора ISATAP	94
Практикум. Настройка DNS	95
Упражнение 1. Настройка записи AAAA	95
Упражнение 2. Настройка зоны обратного просмотра IPv6	96
Закрепление материала главы	98
Резюме главы	98
Основные термины	98
Лабораторная работа	98
Задание 1. Внедрение IPv6	99
Задание 2. Настройка DNS	99
Рекомендуемые упражнения	99
Настройка IPv6	99
Настройка DNS	100
Пробный экзамен	100
Глава 3 Планирование основы инфраструктуры Active Directory	101
Занятие 1. Служба каталогов Active Directory	103
Планирование роли сервера AD DS	104
Планирование и использование RODC	111
Планирование аудита AD DS	123
Планирование функциональности домена и леса	125
Планирование доверия лесов	131
Резюме	135
Закрепление материала	136
Занятие 2. Службы сертификации Active Directory	138
Типы центров сертификации	139
Улучшения в Windows Server 2008 R2	144
Настройка перемещения учетных данных	146
Настройка авторегистрации	147
Настройка поддержки регистрации через Интернет	150
Настройка списков отзыва сертификатов	151
Настройка сетевого ответчика для служб сертификации	153
Служба подачи заявок на сетевые устройства	156
Использование PKI предприятия для мониторинга работоспособности ЦС	157
Резюме	158
Закрепление материала	159
Практикум. Повышение функционального уровня домена и леса,	
включение корзины Active Directory и настройка детальной политики паролей	160
Упражнение 1. Повышение функционального уровня домена	160
Упражнение 2. Повышение функционального уровня леса	161
Упражнение 3. Включение Корзины Active Directory	162

Упражнение 4. Создание PSO	163
Практикум. Развертывание служб сертификации Active Directory и сетевого ответчика...	166
Упражнение 1. Развертывание AD CS.....	166
Упражнение 2. Развертывание сетевого ответчика.....	167
Закрепление материала главы.....	171
Резюме главы.....	171
Основные термины.....	172
Лабораторная работа	172
Задание 1. Планирование обновления с Windows Server 2003 до Windows Server 2008 R2.....	172
Задание 2. Развертывание служб сертификации в Coho Vineyard	173
Рекомендуемые упражнения	173
Настройте PSO	173
Изучите RODC подробнее	174
Настройте аудит	174
Настройте регистрацию через Интернет	174
Пробный экзамен	174
Глава 4 Стратегии групповой политики.....	175
Занятие 1. Планирование объектов групповой политики.....	177
Использование начальных объектов групповой политики	178
Резервное копирование и восстановление начальных GPO	180
Планирование административных шаблонов.....	181
Резюме	186
Закрепление материала	187
Занятие 2. Стратегия объектов групповой политики	189
Планирование стратегии групповой политики.....	189
Решение проблем с групповой политикой.....	197
Резюме	201
Закрепление материала	202
Практикум. Установка консоли GPMC и создание центрального хранилища для файлов групповой политики.....	204
Упражнение 1. Установка консоли GPMC.....	204
Упражнение 2. Создание центрального хранилища для ADMX-файлов	205
Практикум. Создание и настройка GPO и создание отчета	207
Упражнение 1. Создание и настройка GPO.....	207
Упражнение 2. Создание отчета GPO.....	208
Упражнение 3. Проверка параметров политики	209
Закрепление материала главы.....	210
Резюме главы.....	210
Основные термины.....	211
Лабораторная работа	211
Задание 1. Использование начальных GPO.....	211
Задание 2. Планирование и документирование процедур по решению проблем	211
Рекомендуемые упражнения	212
Используйте консоль GPMC и редактор управления групповой политикой	212
Изучайте ADMX-файлы	212
Изучайте отчеты GPO.....	212
Изучите программы из списка RemoteApp.....	212
Пробный экзамен	213

Глава 5 Планирование администрирования серверов	214
Занятие 1. Технологии управления серверами.....	215
Инструменты для администрирования Windows Server 2008 и 2008 R2.....	215
Технологии удаленного администрирования	220
Управление журналами событий	224
Резюме	234
Закрепление материала	235
Занятие 2. Делегирование полномочий	236
Политики делегирования.....	237
Процедуры делегирования	237
Делегирование учетных данных	241
Делегирование управления приложениями.....	243
Резюме	245
Закрепление материала	245
Практикум. Удаленное управление и делегирование	247
Упражнение 1. Удаленное управление с помощью PowerShell 2.0	247
Упражнение 2. Делегирование управления паролями всех учетных записей пользователей из подразделения.....	248
Упражнение 3. Отмена делегирования с помощью команды dscls	249
Закрепление материала главы.....	249
Резюме главы.....	250
Основные термины.....	250
Лабораторная работа	250
Задание 1. Управление событиями	250
Задание 2. Делегирование прав доверенным пользователям.....	251
Рекомендуемые упражнения	251
Планирование стратегий управления серверами	251
Планирование делегированного администрирования.....	251
Пробный экзамен	252
Глава 6 Виртуализация представлений и приложений	253
Занятие 1. Виртуализация представлений.....	254
Планирование инфраструктуры удаленных рабочих столов.....	255
Планирование программного обеспечения на сервере сеансов удаленных рабочих столов.....	256
Лицензирование службы удаленных рабочих столов.....	256
Область обнаружения сервера лицензирования	256
Активация сервера лицензирования.....	257
Клиентские лицензии удаленных рабочих столов.....	258
Резервное копирование и восстановление сервера лицензирования.....	259
Развертывание серверов лицензирования	260
Настройка серверов узлов сеансов удаленных рабочих столов	260
Свойства сервера.....	263
Настройка удаленных рабочих столов с помощью групповой политики.....	264
Веб-доступ к удаленным рабочим столам.....	267
Посредник подключений к удаленному рабочему столу.....	267
Сервер шлюза удаленных рабочих столов	269
Узел виртуализации удаленных рабочих столов	269
Мониторинг служб удаленных рабочих столов.....	269
Резюме	271
Закрепление материала	271
Занятие 2. Развертывание и виртуализация приложений	273

Традиционное развертывание приложений	273
Развертывание веб-приложений	274
WebDAV в Windows Server 2008 R2	275
FTP 7.5 в Windows Server 2008 R2	276
Удаленные приложения RemoteApp	277
App-V	279
Резюме	280
Закрепление материала	280
Практикум. Установка и настройка служб удаленных рабочих столов и RemoteApp	281
Упражнение 1. Подготовка сервера и установка служб удаленных рабочих столов	282
Упражнение 2. Настройка веб-доступа к удаленным рабочим столам	283
Упражнение 3. Настройка RemoteApp и установщика Windows	283
Закрепление материала главы	284
Резюме главы	284
Лабораторная работа	285
Задание 1. Планирование стратегии служб виртуальных рабочих столов для Wingtip Toys	285
Задание 2. App-V в компании Contoso	285
Рекомендуемые упражнения	286
Предоставление приложений	286
Планирование сервера приложений и служб	286
Пробный экзамен	286
Глава 7 Файловые серверы и серверы печати	287
Занятие 1. Планирование управления службами печати	288
Планирование служб печати и документов	289
Улучшения служб печати в Windows Server 2008 R2	292
Управление принтерами с помощью оснастки Управление печатью	295
Резюме	306
Закрепление материала	306
Занятие 2. Планирование файловых серверов	307
Настройка файлового сервера	307
Улучшения в файловых службах Windows Server 2008 R2	319
Управление доступом	332
Настройка квот, политики блокирования файлов и отчетов хранилищ	339
Резюме	344
Закрепление материала	344
Практикум. Добавление роли сервера Службы печати и документов	345
Практикум. Добавление служб ролей для роли сервера Файловые службы и настройка квоты	349
Упражнение 1. Добавление служб ролей для роли сервера Файловые службы	349
Упражнение 2. Настройка квоты	354
Закрепление материала главы	356
Резюме главы	356
Основные термины	356
Лабораторная работа	356
Задание 1. Планирование обновления Windows Server 2008 R2	357
Рекомендуемые упражнения	357
Используйте улучшенную оснастку Управление печатью	357
Используйте диспетчер ресурсов файлового сервера	357
Узнайте подробнее о Windows Storage Server 2008 R2	358
Узнайте подробнее о BranchCache для сетевых файлов	358

Пробный экзамен	358
Глава 8 Планирование политик безопасности	359
Занятие 1. Разработка политик безопасности	361
Планирование системы безопасности сервера	361
Развертывание политик безопасности для реализации решения	369
Мониторинг безопасности сервера	376
Мониторинг журнала безопасности	376
Использование шифрованной файловой системы	378
Резюме	380
Закрепление материала	381
Занятие 2. Управление безопасностью сервера	383
Развертывание обновлений при помощи WSUS	383
Новые возможности WSUS 3.0 SP2	388
Автономный режим и режим реплики	389
Использование групп компьютеров	390
Настройка клиента WSUS	392
Стратегии обновления и синхронизации	395
Управление обновлениями и соответствие условиям	396
Другие средства управления обновлениями	398
Резюме	399
Закрепление материала	400
Практикум. Мониторинг создания учетных записей неопытным администратором	401
Упражнение 1. Настройка аудита создания пользователей и групп безопасности и повышение пользователя до администратора домена	401
Упражнение 2. Вход под учетной записью Don Hall для создания пользователя и группы безопасности	404
Упражнение 3. Аудит создания пользователей и групп	405
Практикум. Установка WSUS 3.0 SP2 (необязательный)	407
Упражнение. Установка WSUS 3.0 SP2	407
Закрепление материала главы	412
Резюме главы	412
Основные термины	412
Лабораторная работа	412
Задание 1. Реализация плана по обеспечению безопасности сети корпорации Adatum ..	413
Задание 2. Развертывание WSUS 3.0 SP2 в компании Fabrikam	413
Рекомендуемые упражнения	414
Мониторинг безопасности сервера	414
Реализация стратегии управления обновлениями	414
Пробный экзамен	414
Глава 9 Удаленный доступ и защита доступа к сети	415
Занятие 1. Управление удаленным доступом	416
Проверка подлинности VPN	420
Протоколы VPN	421
IKEv2	422
DirectAccess	424
Серверы NPS RADIUS	429
Учет удаленного доступа	431
Серверы шлюзов удаленных рабочих столов	434
Резюме	435
Закрепление материала	436
Занятие 2. Брандмауэры и защита доступа к сети	437

Брандмауэр Windows с повышенной безопасностью.....	437
Forefront Threat Management Gateway.....	439
Защита доступа к сети.....	440
Способы применения NAP.....	441
Серверы обновлений.....	445
Режим мониторинга.....	446
Резюме.....	446
Закрепление материала.....	447
Практикум. Установка и настройка NAP для DHCP.....	448
Упражнение 1. Установка сервера сетевых политик и настройка DHCP.....	448
Упражнение 2. Настройка NPS.....	449
Упражнение 3. Настройка SHV.....	450
Закрепление материала главы.....	451
Резюме главы.....	451
Основные термины.....	452
Лабораторная работа.....	452
Задание 1. Удаленный доступ в Wingtip Toys.....	452
Задание 2. NAP в Coho Vineyard.....	453
Рекомендуемые упражнения.....	453
Мониторинг и обслуживание политик безопасности.....	453
Планирование ролей серверов служб инфраструктуры.....	454
Пробный экзамен.....	454
Глава 10 Подготовка данных и планирование хранилищ.....	455
Занятие 1. Подготовка данных.....	456
Планирование доступности данных.....	456
Аппаратная избыточность.....	457
Избыточный массив недорогих дисков.....	458
Распределенная файловая система (DFS).....	459
Настройка автономного доступа к данным.....	467
Настройка индексирования в службе поиска Windows.....	468
SharePoint Foundation 2010.....	470
Резюме.....	473
Закрепление материала.....	473
Занятие 2. Планирование хранилища Windows Server 2008 R2.....	475
Логические номера устройств.....	475
Диспетчер хранилища для сетей SAN.....	477
Многопутевой ввод-вывод.....	479
Проводник хранилищ.....	481
Резюме.....	482
Закрепление материала.....	482
Практикум. Установка и настройка DFS.....	483
Упражнение 1. Установка DFS.....	483
Упражнение 2. Настройка пространства имен DFS и добавление сервера пространств имен.....	483
Упражнение 3. Создание новой папки DFS и группы репликации.....	484
Упражнение 4. Настройка параметров автономных файлов для общих папок.....	486
Закрепление материала главы.....	486
Резюме главы.....	486
Основные термины.....	487
Лабораторная работа.....	487
Задание 1. DFS в Wingtip Toys.....	487

Задание 2. Подготовка данных в Contoso.....	487
Рекомендуемые упражнения	488
Подготовка данных.....	488
Настройка хранилища.....	488
Пробный экзамен	488
Глава 11 Кластеризация и высокая доступность	489
Занятие 1. Циклическое обслуживание DNS и балансировка сетевой нагрузки.....	490
Простые стратегии обеспечения доступности.....	490
Циклическое обслуживание DNS	491
Балансировка сетевой нагрузки	493
Управление NLB-кластерами	495
Правила для портов NLB	496
Сравнение циклического обслуживания DNS с балансировкой сетевой нагрузки	498
Резюме	499
Закрепление материала	499
Занятие 2. Средства кластеризации Windows Server 2008 R2	500
Принципы работы кластеров.....	502
Установка средства отказоустойчивости кластеров	505
Проверка конфигурации отказоустойчивости кластера.....	505
Создание отказоустойчивого кластера.....	506
Настройка служб для обеспечения высокой доступности	507
Управление отказоустойчивым кластером	508
Резюме	510
Закрепление материала	510
Практикум. Установка и настройка кластера NLB в Windows Server 2008 R2	511
Упражнение 1. Подготовка DNS и рядовых серверов для создания кластера NLB	511
Упражнение 2. Настройка и тестирование NLB-кластера.....	512
Упражнение 3. Удаление кластера NLB и компонента NLB	513
Закрепление материала главы.....	514
Резюме главы.....	514
Основные термины.....	515
Лабораторная работа	515
Задание 1. Выбор подходящей стратегии доступности.....	515
Рекомендуемые упражнения	516
Планирование высокой доступности.....	516
Пробный экзамен	516
Глава 12 Оценка и оптимизация производительности.....	517
Занятие 1. Данные мониторинга.....	519
Мониторинг производительности и создание отчетов.....	520
Слежение за надежностью, стабильностью и общей производительностью системы ...	530
Использование центра поддержки	534
Использование системных инструментов для изучения процессов и служб.....	535
Запись и пересылка событий и подписки на события	546
Практикум. Оценка производительности диска.....	556
Упражнение 1. Добавление и мониторинг счетчиков диска.....	556
Упражнение 2. Настройка свойств системного монитора и мониторинг производительности диска	559
Резюме	561
Закрепление материала	562
Закрепление материала главы.....	563
Резюме главы.....	563

Основные термины.....	564
Лабораторная работа	564
Задание 1. Использование групп сборщиков данных и пересылка событий.....	564
Задание 2. Планирование мониторинга на серверах.....	565
Рекомендуемые упражнения	565
Использование инструментов мониторинга производительности	566
Управление ведением журналов событий.....	566
Изучение Process Explorer	566
Пробный экзамен	566
Глава 13 Архивация и восстановление.....	567
Занятие 1. Архивация данных	568
Использование теневых копий общих папок.....	569
Система архивации данных Windows Server	571
Утилита командной строки Wbadmin	578
Архивация ролей серверов и приложений.....	581
Удаленная архивация компьютеров.....	582
Дальнейшие соображения по планированию архивации	583
System Center Data Protection Manager	584
Резюме	585
Закрепление материала	585
Занятие 2. Аварийное восстановление.....	587
Режимы восстановления системы архивации данных Windows Server	588
Восстановление Active Directory и ролей сервера.....	592
Hyper-V и аварийное восстановление	599
Резюме	599
Закрепление материала	600
Практикум. Архивация Windows Server 2008 R2.....	601
Упражнение 1. Архивация вручную при помощи системы архивации данных Windows Server	602
Упражнение 2. Архивация тома и состояния системы при помощи Wbadmin.exe.....	605
Практикум. Восстановление Windows Server 2008 R2.....	605
Упражнение 1. Восстановление файлов и папок	606
Упражнение 2. Выполнение принудительного восстановления	608
Упражнение 3. Восстановление каталога архивов	610
Закрепление материала главы.....	611
Резюме главы.....	612
Основные термины.....	612
Лабораторная работа	612
Задание 1. Инфраструктура архивации в компании Wingtip Toys	612
Задание 2. Аварийное восстановление в компании Fabrikam.....	613
Рекомендуемые упражнения	613
Удаленная архивация	614
Восстановление сервера	614
Пробный экзамен	614
Приложение. Настройка компьютеров для выполнения упражнений и практикумов.....	615
Ответы	619
Об авторах	669

Введение

Данный учебный курс предназначен для администраторов серверов и доменов, имеющих двух- или трехлетний опыт управления серверами Windows и инфраструктурой в среде с 250–5000 (и даже более) пользователями, находящимися в трех или более физических местоположениях, и тремя и более контроллерами доменов. В задачи администратора входит поддержка сетевых служб и ресурсов: серверов передачи сообщений, серверов баз данных, служб файлов и печати, прокси-серверов, брандмауэров, ресурсов Интернета и интрасети, удаленного доступа и клиентов. Также администратор отвечает за сетевую связь, в том числе подключение удаленных филиалов и отдельных пользователей к корпоративной сети и подключение корпоративных сетей к Интернету.

Данный учебный курс, как и сертификационный экзамен 70-646, посвящен сетевым технологиям Windows Server 2008 и 2008 R2, поддерживающим распределенный доступ к веб-содержимому, мультимедиа, операционным системам и приложениям. Темы учебного курса соответствуют темам экзамена, описанным на странице экзамена на вкладке **Skills Measured** (<http://www.microsoft.com/learning/en/us/exam.aspx?ID=70-647&locale=en-us>). Изучив излагаемый здесь материал, вы научитесь:

- планировать и выполнять развертывание серверов под управлением Windows Server 2008 и Windows Server 2008 R2;
- планировать и выполнять управление серверами Windows Server 2008 и Windows Server 2008 R2;
- выполнять мониторинг, обслуживание и оптимизацию серверов;
- планировать развертывание приложений и подготовку данных;
- планировать и внедрять стратегии обеспечения высокой готовности и бесперебойной работы инфраструктуры.

В начале книги вы найдете таблицу сопоставления тем экзамена с главами книги.

Системные требования

Ниже приведены минимальные системные требования, которым должен соответствовать ваш компьютер для выполнения практических упражнений и запуска компакт-диска, прилагаемого к книге. Чтобы свести к минимуму время и стоимость настройки физических компьютеров для данного учебного курса, рекомендуем использовать Hyper-V — функцию Windows Server 2008 и 2008 R2. Можно использовать средства виртуализации сторонних производителей, однако в приведенных инструкциях по установке предполагается использова-

ние Hyper-V.

Требования к аппаратному обеспечению

Почти все упражнения данной книги можно выполнять, используя виртуальные машины вместо физического серверного оборудования. Системные требования для Windows Server 2008 R2 можно найти по адресу <http://technet.microsoft.com/ru-ru/windowsserver/bb414778>.

Если вы собираетесь использовать несколько виртуальных машин на одном компьютере (рекомендуется), то лучше использовать более мощную систему. Компьютер с 8 ГБ оперативной памяти и свободным дисковым пространством в 150 ГБ позволит работать со всеми виртуальными машинами, необходимыми для выполнения упражнений книги.

Требования к программному обеспечению

Для выполнения упражнений книги необходимо следующее ПО:

- Windows Server 2008 R2 Enterprise Edition;
- Windows 7 Enterprise или Ultimate Edition.

Можно скачать пробные версии Windows Server 2008 R2 Enterprise Edition и Windows 7 Enterprise edition из центра загрузки Microsoft по адресу <http://www.microsoft.com/Downloads/Search.aspx>.

Подготовка компьютеров к работе с Windows Server 2008 R2 Enterprise Edition

Подробные инструкции по установке Windows Server 2008 R2, а также установке и настройке контроллера домена и рядового сервера под управлением Windows Server 2008 R2 Enterprise Edition содержатся в Приложении. Необходимые роли сервера будут добавлены при выполнении упражнений из последующих глав.

Инструкции по установке

Для выполнения предлагаемых упражнений необходимо минимум два компьютера или две виртуальных машины, а именно:

- один сервер под управлением Windows Server 2008 R2 Enterprise, настроенный в качестве контроллера домена;
- один сервер под управлением Windows Server 2008 R2 Enterprise, настроенный в качестве рядового сервера.

Для выполнения упражнений главы 4 потребуется дополнительный клиент под управлением Windows 7 Enterprise или Ultimate Edition. Все компьютеры могут быть виртуальными машинами. Для выполнения упражнений главы 13 потребуется второй жесткий диск (встроенный или внешний), подключенный к контроллеру домена. Если используется виртуальная машина, жесткий диск может быть виртуальным.

Все компьютеры должны быть физически подключены к одной сети. Для

выполнения упражнений рекомендуем использовать изолированную сеть, не являющуюся частью рабочей сети. Чтобы свести к минимуму время и стоимость настройки физических компьютеров, рекомендуем использовать виртуальные машины. Для запуска компьютеров как виртуальных машин на сервере под управлением Windows Server 2008 или 2008 R2, требуется установить роль сервера Hyper-V. Как вариант, можно использовать поддерживаемые виртуальные машины сторонних производителей.

Использование компакт-диска

Компакт-диск, прилагаемый к книге, имеет следующее содержимое:

- **Пробный экзамен.** Для закрепления знаний по настройке Windows Server 2008 R2 используйте электронные пробные тесты, которые можно составлять на основе перечня вопросов из разделов «Обзор урока» данной книги согласно вашим потребностям. Чтобы проверить уровень подготовки, можно попрактиковаться в сдаче сертификационного экзамена 70-646 с помощью тестов, составляемых из 200 реалистичных экзаменационных вопросов.
- **Электронная книга.** Для удобства на диск добавлена электронная версия данной книги в формате Portable Document Format (PDF), которую можно читать с помощью программ Adobe Acrobat и Adobe Reader.

Установка пробных тестов

Чтобы установить с компакт-диска программу для прохождения пробных тестов, выполните следующее:

1. Вставьте компакт-диск в дисковод и примите условия лицензионного соглашения. Откроется меню компакт-диска.

ПРИМЕЧАНИЕ Если не открывается меню

Если меню компакт-диска или лицензионное соглашение не открывается, возможно, на компьютере отключена функция автозапуска. Альтернативные способы установки описаны в файле Readme.txt на компакт-диске.

2. Щелкните **Practice Tests** и следуйте инструкциям на экране.

Использование пробных тестов

Чтобы запустить программу для прохождения пробных тестов, выполните следующее:

1. Щелкните **Пуск | Все программы | Microsoft Press Training Kit Exam Prep**. Откроется окно, в котором будут показаны все модули программы Microsoft Press Training Kit Exam Prep, установленные на компьютере.
2. Дважды щелкните обзор урока или пробный тест, который хотите использовать.

ПРИМЕЧАНИЕ Обзоры уроков и пробные тесты

Если хотите попробовать ответить на вопросы из разделов «Обзор урока», выберите Lesson review\ (70-646) Windows Server 2008 R2 Server Administrator. Чтобы ответить на любой из 300 вопросов, аналогичных используемым на сертификационном экзамене 70-646, выберите Practice test\ (70-646) Windows Server 2008 R2 Server Administrator.

Обзоры уроков

При запуске обзора урока откроется диалоговое окно **Custom Mode**, в котором можно настроить тест. Можно щелкнуть **OK**, чтобы принять параметры по умолчанию, или настроить желаемое количество вопросов, параметры работы программы пробных тестов, темы экзамена, по которым будут задаваться вопросы, а также таймер пробного теста. Если хотите повторно пройти тест, можно выбрать отображение всех вопросов или только тех, которые вы пропустили или на которые не ответили.

Чтобы запустить обзор урока, щелкните **OK**.

- Отвечая на вопросы теста, используйте кнопки **Next**, **Previous** и **Go To** для перехода от одного вопроса к другому.
- Если хотите узнать, правильно ли ответили на вопрос, и получить объяснение правильного ответа, щелкните **Explanation**.
- Если предпочитаете узнать результаты после окончания теста, ответьте на все вопросы и щелкните **Score Test**. Вы увидите краткий перечень выбранных тем экзамена и процент правильных ответов на вопросы, общий и по каждой теме. После этого можно распечатать копию теста, просмотреть ответы или заново пройти тест.

Параметры пробных тестов

Начав пробный тест, можно выбрать режим сертификации (**Certification Mode**), учебный режим (**Study Mode**) или пользовательский режим (**Custom Mode**).

- **Certification Mode.** Этот режим очень похож на сертификационный экзамен. Тест содержит определенное количество вопросов, время выполнения ограничено таймером, который нельзя поставить на паузу или перезапустить.
- **Study Mode.** В этом режиме тестирование проводится без таймера, а для каждого вопроса можно посмотреть правильный ответ и пояснения к каждому из вариантов ответов.
- **Custom Mode.** В этом режиме вы полностью контролируете параметры теста и можете настраивать их по своему усмотрению.

Во всех режимах пользовательский интерфейс практически одинаковый, но включаются и отключаются разные параметры. Основные параметры описаны в предыдущем разделе.

Просматривая ответ на конкретный вопрос теста, вы увидите раздел **References** с указанием разделов учебного курса, где можно найти информацию по данному вопросу, и ссылки на другие источники информации. Щелкнув **Test Results** для просмотра результатов всего теста, вы можете перейти на вкладку **Learning Plan**, чтобы просмотреть перечень ссылок по каждой теме.

Удаление пробных тестов

Чтобы удалить программу для выполнения пробных тестов, используйте апплет Панели управления **Программы и компоненты** (Program And Features).

ПРИМЕЧАНИЕ Дополнительные материалы для электронной книги

Если вы приобрели цифровую версию книги, вы можете выборочно загружать материалы компакт-диска, прилагаемого к печатному изданию. Для загрузки материалов перейдите по адресу: <http://go.microsoft.com/FWLink/?Linkid=219765>.

Поддержка и обратная связь

Ниже приводится информация об опечатках, поддержке книги и обратной связи, а также контактные данные.

Ошибки и поддержка книги

Мы сделали все возможное, чтобы исключить ошибки в нашей книге и дополнительных материалах. Все ошибки, обнаруженные после издания книги, указаны на сайте Microsoft Press:

<http://go.microsoft.com/FWLink/?Linkid=219763>

Если вы обнаружите ошибку, отсутствующую в списке, вы можете сообщить об этом на этой же странице.

Если вам нужна дополнительная поддержка, присылайте письма в службу поддержки Microsoft Press по адресу msspinput@microsoft.com.

Пожалуйста, обратите внимание: техническая поддержка программ Microsoft по вышеуказанным адресам не предоставляется.

Подготовка к экзамену

Сертификационные экзамены Microsoft — отличный способ укрепить резюме и сообщить всему миру о вашем уровне компетенции. Сертификационные экзамены подтверждают ваш опыт и знания. Опыт работы ничем нельзя заменить, однако обучение и практика помогут вам подготовиться к экзамену. Советуем вам составить план подготовки к экзамену, используя доступные учебные материалы и курсы. Например, можно воспользоваться данным учебным курсом и другими учебными пособиями для самоподготовки, а также пройти учебный курс Microsoft Official Curriculum. Выберите для себя наиболее подходящий вариант.

Г Л А В А 1

Установка, обновление и развертывание Windows Server 2008 R2

Занятие 1. Планирование установки и обновления	2
Занятие 2. Автоматическое развертывание серверов	14

Эта глава — о планировании развертывания Windows Server 2008 и 2008 R2. Далее в книге мы будем использовать название Windows Server 2008 R2, но вся информация относится также и к Windows Server 2008, если не указано обратное. На первом занятии вы узнаете, какие версии Windows Server 2008 R2 лучше всего подходят для разных наборов ролей, каковы различия в условиях лицензирования этих версий, как выбрать между физическим и виртуальным развертыванием, и что требуется для обновления Windows Server 2003. На втором занятии рассказывается о возможностях автоматического развертывания, от создания и применения файлов несопровождаемой установки до развертывания множества систем Windows Server 2008 R2 при помощи служб Windows Deployment Services и System Center Configuration Manager 2007 R3.

ВНИМАНИЕ! Прочитайте Введение

Там рассказывается, какие знания необходимы для успешной сдачи экзамена.

Темы экзамена

- Планирование установки и обновления серверов.
- Планирование автоматического развертывания серверов.

Прежде всего

Для выполнения упражнений этой главы потребуется:

- Компьютер со следующими минимальными характеристиками: 32 ГБ нераспределенного дискового пространства, 512 МБ ОЗУ, процессор x64 1,3 ГГц. В упражнениях предполагается, что используемый компьютер не имеет прямого или косвенного доступа к Интернету, но подключен к сети с частным IP-адресом.

- Пробная версия Windows Server 2008 R2 Enterprise Edition, загруженная с сайта Microsoft (<http://www.microsoft.com/Downloads>).

Для изучения этой главы дополнительной настройки не требуется.

Реальный мир

Орин Томас

Организациям требуется время для перехода на новую операционную систему. В отличие от пользовательских ОС, которые люди во множестве покупают и устанавливают в день выпуска, развертывание серверных систем требует подготовки. На серверах обычно работают важные службы, к запуску которых следует подходить серьезно и без спешки.

Приступая к развертыванию сервера, необходимо все тщательно продумать. Корректное развертывание очень важно. Десять лет назад, когда объемы дисков были намного меньше, легко было попасть в затруднительную ситуацию, не рассчитав место на томе с системными файлами. Могло оказаться, что невозможно установить на сервер новые программы, несмотря на то, что на другом томе достаточно свободного пространства. Причина этого была в том, что установщик развертываемой программы требовал размещения файлов на уже заполненном системном томе.

Сегодня один из самых главных вопросов развертывания — выбор между физической и виртуальной машиной. Развертывание на физическом компьютере обычно более дорогое, поскольку необходимо приобрести новую лицензию и аппаратное обеспечение. Развертывание на виртуальной машине позволяет использовать существующую виртуальную лицензию и сэкономить на оборудовании, но может привести к проблемам с производительностью других систем на том же сервере Hyper-V. Следует учитывать, что можно переходить с физической машины на виртуальную и обратно, и теперь это делать легче, чем во времена Windows NT 4.0 Server.

Занятие 1. Планирование установки и обновления

На этом занятии рассматриваются разные версии Windows Server 2008 R2 и роли, для которых они предназначены. Вы узнаете о режиме Server Core, в котором сервер управляется только с помощью командной строки. Также мы расскажем о процессе установки и обновления Windows Server 2008, различиях в условиях лицензирования разных версий и о выборе между физическим и виртуальным развертыванием.

Изучив материал этого занятия, вы сможете:

- ✓ Планировать установку и обновление Windows Server 2008 и Windows Server 2008 R2.
- ✓ Определять, какая версия Windows Server подходит для разных условий.
- ✓ Понимать условия лицензирования.
- ✓ Определять наиболее подходящий вариант развертывания: физический или виртуальный.

Продолжительность занятия — примерно 60 мин.

Отличия между Windows Server 2008 и Windows Server 2008 R2

Обновленный экзамен 70-646 охватывает и Windows Server 2008, и Windows Server 2008 R2. Если между этими продуктами есть разница, например, в поддержке динамического распределения памяти в Hyper-V или поддержке RemoteFX протоколом RDP, то в вопросах экзамена явно указывается, что используется операционная система Windows Server 2008 R2. Если есть разница в терминологии (например, Службы терминалов в 2008 и Службы удаленных рабочих столов в 2008 R2), то в книге и вопросах экзамена используется терминология Windows Server 2008 R2, но упоминается и терминология Windows Server 2008. Например, вопрос по Службам удаленных рабочих столов может выглядеть так:

Вы планируете развертывание Служб удаленных рабочих столов (Службы терминалов в Windows Server 2008) на нескольких узлах, расположенных в разных доменах леса Active Directory вашей организации. Вы хотите настроить сервер лицензирования так, чтобы все серверы Служб удаленных рабочих столов могли централизованно получать лицензии. Какие из перечисленных параметров сервера лицензирования Служб удаленных рабочих столов следует настроить?

Перечислим ключевые различия между версиями операционных систем:

- Windows Server 2008 R2 поддерживает процессоры x64 и IA 64, но не поддерживает процессоры x86. Windows Server 2008 поддерживает процессоры всех трех типов;
- Windows Server 2008 R2 имеет версию Foundation Edition, которой нет у Windows Server 2008;
- Службы терминалов в Windows Server 2008 R2 переименованы в Службы удаленных рабочих столов;
- Windows Server 2008 R2 включает новые функции, такие как Корзина Active Directory, динамическая память Hyper-V, управляемые учетные записи служб, AppLocker, DirectAccess, BranchCache, IIS 7.5 и поддержка служб сертификатов в режиме Server Core.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Различия между Windows Server 2008 и Windows Server 2008 R2

Полный список различий см. по адресу <http://www.microsoft.com/windows-server2008/en/us/whats-new.aspx>.

Выбор подходящей версии

Windows Server 2008 R2 поставляется в нескольких версиях, каждая из которых оптимизирована для выполнения определенной роли. Одна версия и конфигурация может подходить для офисного файлового сервера, другая — для почтового сервера Exchange Server 2010, поддерживающего группы доступности баз данных. Кроме того, большинство версий имеет вариации для разных архитектур процессоров, и у каждой версии есть возможность установки ограниченного варианта, работающего в режиме Server Core. Далее рассказывается, как все эти варианты вписываются в различные планы развертывания, и как опреде-

лить, какая версия Windows Server 2008 R2 лучше всего подходит для конкретных ситуаций.

Windows Server 2008 R2 Standard Edition

Windows Server 2008 R2 Standard Edition — версия, предназначенная для небольших и средних компаний. Эта версия подходит для поддержки большинства ролей. Следующие характеристики Windows Server 2008 R2 отличаются от других версий ОС:

- поддерживает до 4 физических процессоров (сокетов) и 32 ГБ ОЗУ максимум;
- лицензия на один хост и одну виртуальную машину;
- не поддерживает отказоустойчивые кластеры;
- не поддерживает службы федерации Active Directory;
- ограничение на 250 входящих подключений к службе маршрутизации и удаленного доступа или шлюзу удаленного рабочего стола;
- поддерживает не все функции роли службы сертификатов Active Directory.

В большинстве случаев Standard Edition подходит для ролей контроллера домена, сервера приложений, DNS-сервера, DHCP-сервера, файлового сервера и сервера печати. Хотя все эти службы жизненно важны для сетевой инфраструктуры, они не требуют дополнительных возможностей, представленных в версиях Enterprise и Datacenter. Если вам не нужны функции версии Enterprise, такие как отказоустойчивые кластеры или службы федерации Active Directory, следует использовать Windows Server 2008 R2 Standard Edition.

Windows Server 2008 R2 Enterprise Edition

Эта версия предназначена для крупных компаний. Планируйте ее развертывание на серверах, предназначенных для запуска таких приложений, как Exchange Server 2010, если хотите использовать группы доступности баз данных или отказоустойчивые кластеры Microsoft SQL Server. Эти продукты требуют дополнительной вычислительной мощности, оперативной памяти и таких функций, как обеспечение отказоустойчивости кластеров, поддерживаемых версией Enterprise. Windows Server 2008 R2 Enterprise Edition подходит для ситуаций, требующих использования возможностей, недоступных в Windows Server 2008 R2 Standard Edition:

- поддержка до 2 терабайт (ТБ) ОЗУ и 8 сокетов;
- лицензия на хост и 4 виртуальных машины;
- поддержка отказоустойчивых кластеров;
- поддержка служб федерации Active Directory;
- поддержка всех функций службы сертификатов Active Directory.

Версия Enterprise при развертывании, скорее всего, будет использоваться совместно с версией Standard. Последняя позволяет удовлетворить большинство требований организации, тогда как первую следует использовать только в том случае, если к серверу предъявляются повышенные требования, такие как включение в отказоустойчивый кластер и необходимость в повышенной мощности или объеме памяти.

Windows Server 2008 R2 Datacenter Edition

Версия Datacenter предназначена для очень крупных организаций. Основная причина для развертывания Windows Server 2008 R2 Datacenter Edition вместо Enterprise Edition — версия Datacenter поддерживает неограниченное число виртуальных машин. Эта версия будет наилучшим выбором для организаций, использующих виртуализацию для консолидации существующих серверов или просто требующих значительных аппаратных мощностей для серверов приложений. Windows Server 2008 R2 Datacenter Edition обладает следующими характеристиками:

- поддержка до 2 ТБ оперативной памяти и 64 сокетов;
- лицензия на хост и неограниченное число виртуальных машин;
- поддержка всех ролей и функций.

Windows Web Server 2008 R2

Эта версия предназначена специально для функционирования в качестве сервера веб-приложений. Другие роли, такие как сервер развертывания Windows и службы домена Active Directory, не поддерживаются. Эта роль сервера развертывается либо в экранированной подсети для поддержки веб-сайта, просматриваемого внешними хостами, либо в качестве сервера интрасети. Эта ограниченная роль не поддерживает мощные аппаратные конфигурации, поддерживаемые другими версиями Windows Server 2008 R2. Windows Web Server 2008 R2 обладает следующими характеристиками:

- поддержка до 32 ГБ оперативной памяти и 4 сокетов в симметричной многопроцессорной (SMP) конфигурации.

Windows Web Server 2008 R2 следует развертывать в режиме Server Core, чтобы минимизировать поверхность атаки, что очень важно для сервера, взаимодействующего с внешними хостами. Полную версию следует развертывать только в том случае, если веб-приложениям организации требуются функции, недоступные в режиме Server Core. В отличие от режима Server Core Windows Web Server 2008, Windows Web Server 2008 R2 поддерживает больше функций служб IIS.

Windows Server 2008 R2 для Itanium

Эта версия предназначена для систем с 64-разрядными процессорами с архитектурой Itanium, отличающейся от архитектуры x64, на которой основаны такие процессоры, как Intel Core i7 и AMD Turion. Это единственная версия Windows Server 2008 R2, которую можно установить на систему с архитектурой Itanium, и для ее установки требуется процессор Itanium 2. В этой версии доступна функциональность сервера приложений и веб-сервера. Другие роли сервера, такие как виртуализация и службы развертывания Windows (WDS), недоступны. Поддерживается до 64 процессоров в конфигурации SMP и 2 ТБ оперативной памяти. Это последняя версия линейки продуктов Windows Server, поддерживающая архитектуру Itanium.

Foundation Edition

Эта версия предназначена для организаций, имеющих 15 и менее пользователей. Сервер можно настроить в качестве контроллера домена, но если в доменных службах Active Directory больше 15 пользователей, он переключится в ограниченный режим. Foundation Edition поддерживает AD RMS, IIS 7.5, NAP, удаленный рабочий стол и WDS, но не поддерживает Hyper-V, отказоустойчивые кластеры и возможность функционировать в качестве сервера BranchCache. Эта версия не рассматривается в экзамене 70-646; описание приводится здесь для полноты сведений.

HPC Server

Windows HPC Server 2008 R2 — версия, предназначенная для организаций, требующих высокопроизводительного распределенного выполнения вычислений. Например, финансовые компании, выполняющие анализ больших объемов данных, хранящихся в таблицах Excel, могут использовать HPC Server в качестве распределенной платформы для вычислений. На экзамене 70-646 эта версия не рассматривается; описание приводится здесь для полноты сведений.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Windows HPC Server 2008 R2

Реальный пример использования HPC Server 2008 R2 в исследовательской лаборатории для выполнения научных вычислений можно найти в статье из журнала TechNet по адресу <http://technet.microsoft.com/en-us/magazine/2009.04.hpc.aspx> (на англ. языке).

Установка в режиме Server Core

Server Core — ограниченный режим установки Windows Server 2008 R2. Полный рабочий стол не предоставляется, а управление Windows Server 2008 R2 выполняется из командной строки (рис. 1-1). Системой, работающей в режиме Server Core, можно управлять удаленно, подключившись через консоль MMC. Можно также подключаться по протоколу удаленного рабочего стола (RDP), хотя для выполнения административных задач после подключения придется использовать оболочку командной строки. Систему в режиме Server Core можно удаленно администрировать при помощи управляющих консолей и команд PowerShell, при условии корректной настройки клиентской оболочки WinRM (Windows Remote Management).

Установка Windows Server 2008 R2 в режиме Server Core имеет следующие преимущества:

- **Сниженные требования к обновлению.** Компьютер, имеющий небольшой набор компонентов для выполнения одной специализированной роли, требует меньшего числа обновлений. Например, обновления безопасности, связанные с Internet Explorer, не нужны для систем Windows Server 2008 R2, установленных в режиме Server Core. Необходимость в меньшем числе обновлений означает, что требуется реже перезагружать сервер.
- **Уменьшенная поверхность атаки.** Устанавливается меньше двоичных файлов, что уменьшает число компонентов, которые могут быть атакованы в попытках скомпрометировать компьютер.

- **Сниженные требования к оборудованию.** В режиме Server Core из операционной системы убрано так много всего, что ее можно использовать на компьютере, мощности которого недостаточно для работы полной установки Windows Server 2008 R2. Это позволяет использовать старые компьютеры, например, приобретенные для Windows 2000 Server.

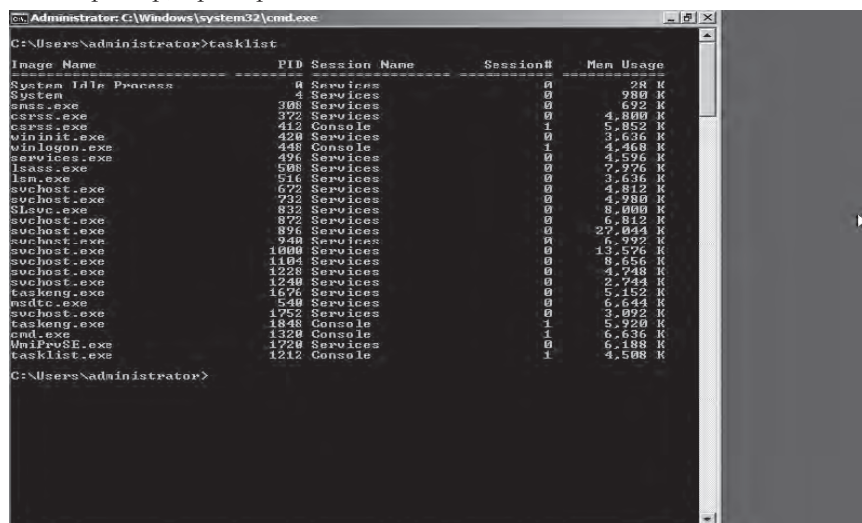


Рис. 1-1. Рабочий стол системы в режиме Server Core

Приобретая лицензию на какую-либо версию Windows Server 2008 R2, вы получаете возможность полной установки или установки в режиме Server Core. Стоимость лицензии одинакова в любом случае. Имея лицензию, можно выполнить полную установку или установку в режиме Server Core (рис. 1-2). Windows Server 2008 R2 Foundation Edition не поддерживает режим Server Core.

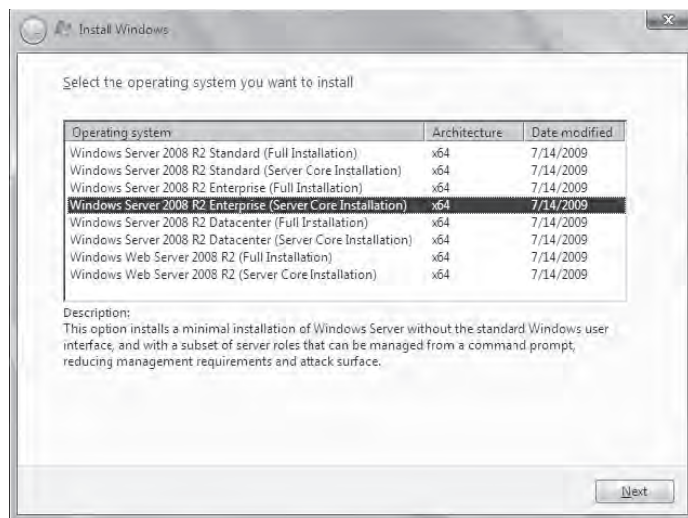


Рис. 1-2. Варианты установки

ПРИМЕЧАНИЕ Различия между режимами Server Core в Windows Server 2008 и Windows Server 2008 R2

Режимы Server Core в Windows Server 2008 и Windows Server 2008 R2 отличаются одним очень важным аспектом: в Windows Server 2008 этот режим не имеет прямой поддержки PowerShell, хотя некоторые команды PowerShell можно запускать удаленно.

Windows Server 2008 R2 в режиме Server Core поддерживает PowerShell V2 и возможность удаленного выполнения команд PowerShell V2. Кроме того, в режиме Server Core можно выполнять сценарии Windows Script Host так же, как в полных установках Windows Server 2008 R2.

Как показано на рис. 1-3, в режиме Server Core можно запустить несколько важных утилит с графическим интерфейсом, включая редактор реестра и Блокнот. Можно также открывать апплеты Панели управления Дата и время (Time and Date) и Язык и региональные стандарты (International Settings) командами `control timedate.cpl` и `control intl.cpl`.

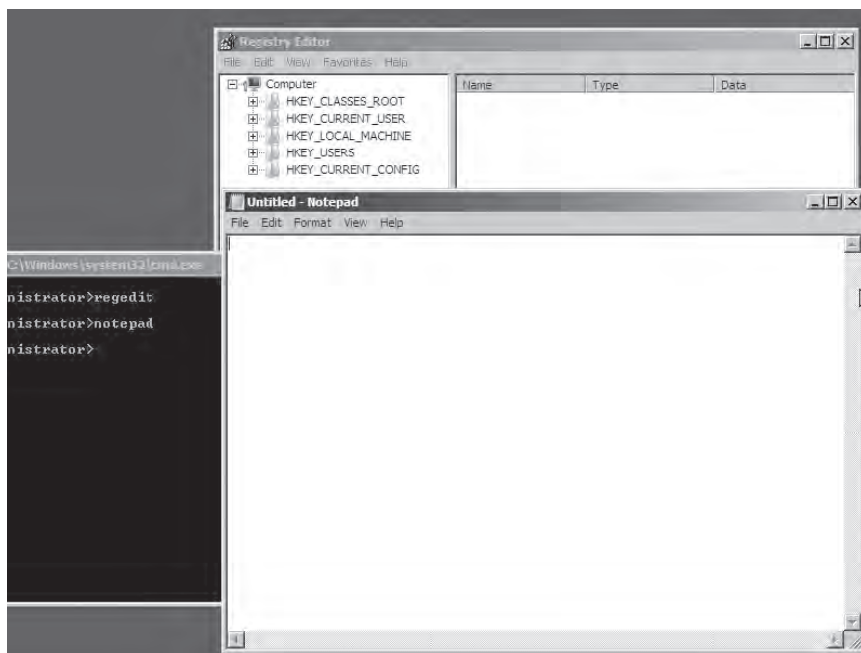


Рис. 1-3. Редактор реестра и Блокнот доступны в режиме Server Core

Две более важные команды — `oclist.exe` и `ocsetup.exe`. Первая показывает список всех ролей сервера, установленных на сервере в текущий момент, и ролей, доступных для установки. На рис. 1-4 показан список функций, установленных по умолчанию в Windows Server 2008 R2 Enterprise Edition в режиме Server Core. Добавлять и удалять эти функции можно при помощи команды `ocsetup.exe`. Например, для установки роли веб-служб (IIS) выполните команду `ocsetup.exe IIS-WebServerRole`. Важно заметить, что название роли чувствительно к регистру. Для удаления роли веб-служб используется команда `ocsetup.exe /uninstall IIS-WebServerRole`, перед выполнением которой необходимо убедиться, что работа всех служб этой роли завершена.

Рассматривая Server Core в качестве варианта развертывания, учитывайте следующее:

- невозможно обновить установку Server Core до полной установки;
- невозможно обновить Windows Server 2003 до Windows Server 2008 R2 в режиме Server Core;
- в режиме Server Core недоступны некоторые роли, включая службы федерации Active Directory, WDS и службы политики сети и доступа.

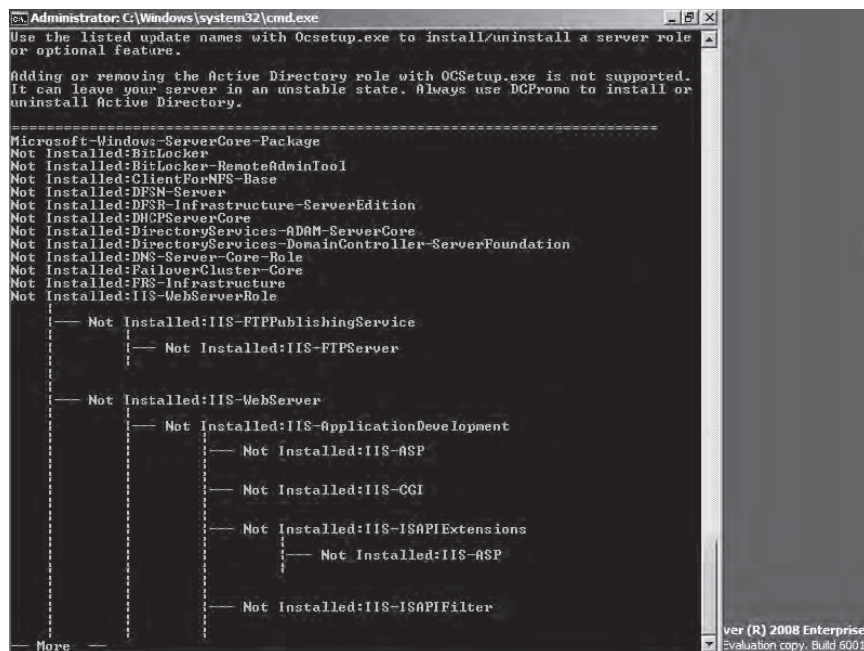


Рис. 1-4. Просмотр ролей и функций, доступных в режиме Server Core

Проверьте себя

- Сколько лицензий на виртуальные машины имеет Windows Server Enterprise Edition?

Ответ

- Windows Server 2008 R2 Enterprise Edition имеет лицензии на четыре виртуальных машины.

Физическое и виртуальное развертывание

Важный вопрос при планировании: как будет развертываться Windows Server 2008 R2 — виртуально или физически? Традиционно администраторы использовали для развертывания серверов физическое оборудование в головных офисах и филиалах. Например, если филиалу требовался сервер DNS, сервер DHCP, контроллер домена, сервер IIS и файловый сервер, для этих ролей обычно развертывалось несколько физических серверов. В некоторых случаях роли можно

объединять на одном сервере, как, например, DHCP, DNS и контроллер домена. Если требуется обеспечить доступность и избыточность, может понадобиться развертывание большего числа серверов.

Можно выбрать более простой альтернативный способ: создать отказоустойчивый кластер Hyper-V, используя два физических сервера с виртуальными машинами, расположенными в сети хранения данных (SAN). Используя преимущества включенных лицензий на виртуальные машины, можно снизить расходы на серверные лицензии и оборудование, развернув два компьютера с Windows Server 2008 R2, служащими узлами кластера Hyper-V. Если один узел выйдет из строя, виртуальные машины из второго узла будут принимать нагрузку до тех пор, пока первый узел не будет возвращен к работе.

Нет строгих правил, предписывающих, какой тип развертывания следует использовать в тех или иных случаях. Выбирая между физическим и виртуальным развертыванием, учитывайте следующее:

- В Enterprise Edition включено четыре лицензии на виртуальные машины, что позволяет разместить на одном физическом компьютере хост и четыре виртуальные машины.
- Datacenter Edition имеет лицензии на неограниченное число виртуальных машин. Это значит, что на одном физическом компьютере можно иметь хост и неограниченное число виртуальных машин. Единственное ограничение — ресурсы физической платформы.
- Для систем с большой нагрузкой виртуальные машины могут быть не лучшим вариантом, поскольку другие виртуальные машины будут использовать те же ресурсы хоста. Если виртуальная машина потребляет слишком большую долю ресурсов процессора, сети или диска, это отрицательно скажется на ресурсах, доступных другим виртуальным машинам, размещенным на той же платформе.
- Виртуальное развертывание может упростить процесс назначения административных разрешений. Чтобы не беспокоиться о том, что пользователи, обслуживающие сервер, будут выполнять задачи, выходящие за рамки их полномочий, можно изолировать роль сервера в одной виртуальной машине; например, если требуется развернуть IIS 7.5 и SQL Server 2008 R2, но администраторы одной службы не должны иметь прав на управление другой. Хотя можно разделить два набора пользователей, назначив им разные разрешения, может быть проще установить IIS 7.5 на одной виртуальной машине, а SQL Server на другой, размещенной на той же платформе.

Установка Windows Server 2008 R2

Традиционный способ установки Windows Server 2008 R2 весьма прост. Главное — помнить, что компьютер должен удовлетворять минимальным требованиям к оборудованию, и что при установке любой версии Windows Server 2008 R2, кроме Itanium Edition, оборудование или платформа виртуализации должна иметь процессор, поддерживающий архитектуру x64. Для установки выполните следующее:

1. Выполните загрузку с установочного носителя.

2. Выберите язык.
3. Выберите версию ОС и вариант установки (полная или Server Core).
4. Примите условия лицензионного соглашения.
5. Выберите обновление или установку нового экземпляра ОС.
6. Выберите, куда будет установлена ОС. После этого начинается сама установка.
7. Укажите пароль для локальной учетной записи администратора.

В отличие от предыдущих версий операционных систем Windows Server, во время установки не требуется вводить ключ продукта. Ключ продукта вводится перед активацией. Об активации рассказывается далее в этой главе.

ПРИМЕЧАНИЕ Не выполняйте активацию сразу

Ознакомительный период перед активацией можно использовать для проверки работы сервера, чтобы убедиться, что не требуется никаких серьезных изменений, таких как замена процессора и добавление оперативной памяти (что обычно требует повторной активации). Можно также до трех раз сбрасывать таймер активации при помощи команды `slmgr.vbs -rearm`. Подождите, убедитесь, что сервер не требует обновления оборудования, а затем выполните активацию.

Если компьютер, на который будет устанавливаться Windows Server 2008 R2, не имеет привода DVD-ROM, доступны другие способы установки:

- Можно загрузить компьютер с USB-носителя, на котором размещены установочные файлы Windows Server. Так как у таких устройств скорость передачи данных обычно выше, чем у приводов оптических дисков, этот способ развертывания может быть самым быстрым.
- Если компьютер имеет сетевую карту, поддерживающую загрузку PXE, можно настроить WDS (см. занятие 2) в качестве метода развертывания Windows Server 2008 R2 по сети. В крупных сетях имеет смысл использовать методы автоматического развертывания вместо традиционных способов установки с носителей.
- Можно загрузить компьютер, используя USB-устройство со средой предустановки Windows (Windows PE). После этого можно подключиться к сетевому диску с файлами операционной системы и выполнить установку по сети. Хотя такой способ установки возможен, проще использовать USB-устройство с установочными файлами Windows Server.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Windows PE

Подробнее о Windows PE можно прочитать по адресу [http://technet.microsoft.com/ru-ru/library/dd799308\(WS.10\).aspx](http://technet.microsoft.com/ru-ru/library/dd799308(WS.10).aspx).

Обновление Windows Server 2003

Некоторым организациям требуется обновить имеющиеся системы Windows Server 2003 до Windows Server 2008 или Windows Server 2008 R2. Обновление выполняется при помощи того же носителя, использующегося для выполнения обычной установки. Выполнить обновление проще, чем переносить приложения и данные на новую платформу. Планируя обновление, учитывайте следующее:

- нельзя обновить версию x86 до версии x64;
- Windows Server 2003 версии x86 можно обновить только до Windows Server 2008 версии x86;
- можно выполнить обновление до эквивалентной версии, если архитектура процессора та же;
- Standard Edition можно обновить до Enterprise Edition, если архитектура процессора та же;
- до Datacenter Edition можно обновить только версию Datacenter предыдущей операционной системы, если архитектура процессора та же;
- нельзя обновить Windows Server 2003 до любой версии Windows Server 2008 или 2008 R2 в режиме Server Core;
- Windows Server 2008 в режиме Server Core можно обновить до Windows Server 2008 R2 в режиме Server Core, если архитектура процессора — x64;
- Windows Server 2003 можно обновить до Windows Server 2008, только если установлен пакет обновлений SP1 или выше.

При планировании не всегда понятно, как следует поступить: обновить существующий сервер или выполнить резервное копирование, отформатировать жесткий диск, установить Windows Server 2008 R2, а затем восстановить данные и переустановить приложения. Виртуализация затрудняет принятие этого решения, так как добавляется возможность преобразовать физическую систему в виртуальную, удалить исходный хост, выполнить чистую установку Windows Server 2008 R2, установить Hyper-V и разместить исходный сервер на виртуальной машине в новой установке Windows Server.

Обновления хорошо подходят для простых переходов, таких как обновление контроллера домена Windows Server 2003 до контроллера домена Windows Server 2008 R2. Когда сервер имеет более сложную роль, например, содержит экземпляр SQL Server 2008, следует тщательно обдумать все варианты. Если после установки придется выполнять много действий по настройке конфигурации для ролей сервера, то обновление может быть гораздо более быстрым вариантом. В любом случае, перед обновлением или переносом всегда следует выполнять полное резервное копирование, поэтому попробуйте сначала произвести обновление, а затем рассмотреть другие варианты, включая возврат к исходной конфигурации (откат), если обновление пройдет неудачно. Сценарии отката подробнее рассматриваются на занятии 2.

ПРИМЕЧАНИЕ Itanium

Хотя Itanium — 64-разрядная архитектура, она отличается от архитектуры x64. Windows Server 2003 Itanium Edition можно обновить только до Windows Server 2008 Itanium Edition. И наоборот, до Windows Server 2008 Itanium Edition можно обновить только Windows Server 2003 Itanium Edition.

Прежде чем начать процесс обновления, программа установки Windows Server 2008 R2 выполнит проверку совместимости и предоставит отчет о результатах.

Отчет о совместимости включает рекомендации по предотвращению проблем, которые могут возникнуть при обновлении. Важно заметить, что в этом отчете сообщается только о тех проблемах, о которых известно Microsoft. Если

обновляемый компьютер имеет необычную аппаратную или программную конфигурацию, при проверке совместимости проблема может не быть обнаружена, и вы не будете знать о ней, пока непосредственно не столкнетесь. Если вы работаете со специализированным ПО, рекомендуем протестировать его в среде разработки, прежде чем пытаться обновлять рабочий сервер.

Чтобы результаты проверки совместимости были максимально точными, обеспечьте Windows Server доступ к наиболее свежим установочным файлам, когда программа установки спросит о получении обновленных файлов. Важно также заметить, что для обновления требуется гораздо больше дискового пространства, чем для новой установки. Перед обновлением необходимо убедиться, что системный том имеет минимум 30 ГБ свободного пространства. Планы на случай непредвиденных обстоятельств рассматриваются на занятии 2.

Резюме

- Windows Server 2008 и Windows Server 2008 R2 имеют версии Standard, Enterprise, Datacenter, Web Server и Itanium. Версии Enterprise и Datacenter поддерживают отказоустойчивые кластеры, службы федерации Active Directory и более мощные аппаратные конфигурации. Windows Server 2008 R2 имеет также версии HPC и Foundation.
- Standard Edition имеет одну лицензию на виртуальную машину, Enterprise Edition — четыре лицензии, Datacenter Edition — неограниченное число лицензий.
- Windows Server 2008 R2 можно устанавливать только на 64-разрядные процессоры.
- Server Core — режим установки, позволяющий развертывать Windows Server 2008 R2 с меньшей поверхностью атаки и меньшими требованиями к оборудованию, чем у полной установки.
- Нельзя обновить 32-разрядную версию Windows Server 2003 до 64-разрядной версии Windows Server 2008 или Windows Server 2008 R2. Нельзя обновить 32-разрядную версию Windows Server 2008 до Windows Server 2008 R2.

Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных на занятии 1. Эти вопросы предоставлены также в электронном виде на прилагаемом к книге компакт-диске.

ПРИМЕЧАНИЕ Ответы

Ответы на вопросы и пояснения к их вариантам размещены в разделе «Ответы» в конце книги.

1. Ваша организация имеет компьютер с Windows Server 2003 R2 x64 Standard Edition, функционирующий в качестве сервера интрасети. Какие варианты обновления доступны для этого компьютера?
 - a. Windows Server 2008 R2 Datacenter Edition.
 - b. Windows Web Server 2008 R2.

- c. Windows Server 2008 R2 Enterprise Edition.
 - d. Windows Server 2008 x86 Standard Edition.
 - e. Windows Server 2008 x64 Standard Edition (Server Core).
2. Ваша организация имеет компьютер с архитектурой процессора x64, на который установлена ОС Windows Server 2003 R2 (x86) Standard Edition. До какой из версий Windows Server 2008 или Windows Server 2008 R2 можно обновить этот компьютер?
- a. Windows Server 2008 (x86) Standard Edition.
 - b. Windows Server 2008 R2 Standard Edition.
 - c. Windows Server 2008 (x86) Datacenter Edition.
 - d. Windows Server 2008 R2 Enterprise Edition.
3. Какая из следующих служб и ролей поддерживается на компьютере с Windows Server 2008 R2 Enterprise Edition в режиме Server Core?
- a. Доменные службы Active Directory.
 - b. Службы управления правами Active Directory.
 - c. Службы федерации Active Directory.
 - d. Службы развертывания Windows.
4. Сколько лицензий на виртуальные машины включено в лицензию на Windows Server 2008 R2 Enterprise Edition?
- a. Одна.
 - b. Две.
 - c. Четыре.
 - d. Неограниченное число.
5. Какую версию Windows Server 2008 R2 следует выбрать для развертывания почтового сервера Exchange Server 2010 с группами доступности баз данных? Группы доступности баз данных требуют использования отказоустойчивых кластеров.
- a. Windows Web Server 2008 R2.
 - b. Windows Server 2008 R2 Standard Edition.
 - c. Windows Server 2008 R2 Enterprise Edition.
 - d. Windows Server 2008 R2 Foundation Edition.

Занятие 2. Автоматическое развертывание серверов

Опытные системные администраторы доводят развертывание серверов до уровня искусства. Возможно, вы так часто выполняли этот процесс, что можете делать это с закрытыми глазами. На этом занятии вы узнаете, какие инструменты можно использовать для создания файлов XML с ответами для процесса установки Windows Server 2008 R2 и как устанавливать и настраивать WDS, службу, позволяющую отправлять образы операционной системы на совместимые клиенты по сети.

Изучив материал этого занятия, вы сможете:

- ✓ Создавать и использовать файлы XML для несопровождаемой установки Windows Server 2008 R2.
- ✓ Планировать развертывание Windows Server 2008 R2 с использованием образов операционной системы и служб развертывания Windows.

Продолжительность занятия – примерно 60 мин.

Файлы ответов Windows Server 2008 R2

Файл ответов позволяет выбирать различные параметры установки, такие как способ разбиения жестких дисков на разделы, расположение устанавливаемого образа Windows Server 2008 R2 и ключ продукта. Файл ответов для Windows Server 2008 R2 обычно называется Autounattend.xml. Программа установки автоматически ищет файл с таким именем на локальных и подключенных носителях, пытаясь инициировать несопровождаемую установку.

Файл ответов имеет формат XML. Администраторы почти всегда создают такие файлы при помощи Диспетчера системных образов Windows (Windows SIM). Эта утилита входит в пакет автоматической установки Windows (Windows AIK или WAIK), который можно найти в Центре загрузок Microsoft или в пакете Microsoft Deployment Toolkit (MDT) Deployment Workbench. Хотя файл ответов можно создать и в текстовом редакторе, из-за сложности синтаксиса XML несопровождаемой установки эффективнее использовать утилиты Windows AIK. Кроме того, диспетчер системных образов позволяет проверить, дает ли файл ответов желаемый результат.

Чтобы создать файл ответов, используя Windows SIM, выполните следующее:

Запустите Windows SIM. Это приложение можно загрузить в качестве обновления для MDT с сайта Microsoft (<http://technet.microsoft.com/en-us/solutionaccelerators/dd407791.aspx>).

1. Скопируйте файл \Sources\Install.wim из дистрибутива Windows Server 2008 R2 во временную папку на компьютере с Windows Server 2008 R2, на который установлен компонент Windows AIK пакета MDT 2010.
2. В меню **Файл** (File) выберите команду **Выбрать образ Windows** (Select Windows Image). Перейдите во временную папку, в которую скопировали Install.wim, и выберите этот файл. Этот файл содержит все версии Windows Server 2008 R2, которые можно установить с установочных носителей.
3. Будет предложено выбрать образ из файла образов Windows. Выберите Server Enterprise или другой образ, для которого хотите создать файл ответов, и щелкните **ОК**.
4. Когда будет предложено создать файл каталога, щелкните **Да** (Yes). В диалоговом окне контроля учетных записей пользователей щелкните **Продолжить** (Continue). Будет создан файл каталога.
5. В меню **Файл** (File) выберите **Создать файл ответов** (New Answer File).

6. Выбрав компонент образа Windows, можно настроить свойства этого компонента. На рис. 1-5 показаны параметры конфигурации, позволяющие устанавливаемой системе автоматически войти в домен contoso.internal, используя указанные учетные данные.

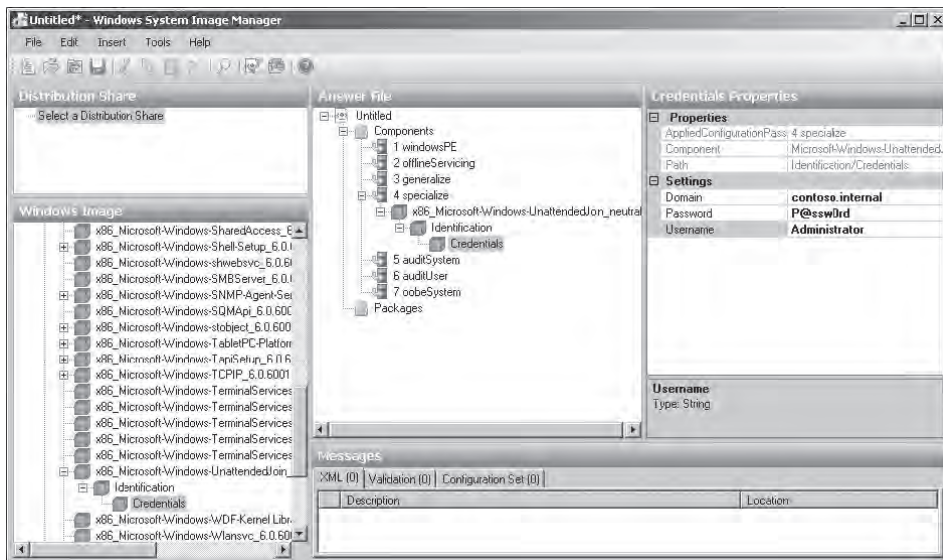


Рис. 1-5. Создание файла Autounattend.xml в Windows SIM

7. После сохранения файл ответов автоматически проверяется на соответствие загруженному образу операционной системы.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Файлы несопровождаемой установки

Подробнее о создании и настройке файлов несопровождаемой установки см. в руководстве по несопровождаемой установке Windows, доступном в меню **Справка (Help)** Windows SIM.

Выполнение несопровождаемой установки

Традиционно для выполнения несопровождаемой установки использовались дискеты с текстовым файлом с параметрами установки. Современное серверное оборудование не имеет дисководов для чтения дискет, поэтому, как говорилось ранее, программа установки Windows Server 2008 R2 автоматически ищет файл Autounattend.xml на всех локальных томах сервера и всех подключенных носителях USB.

Если для установки будут использоваться файлы, расположенные на сетевом диске, необходимо выполнить загрузку в среду Windows PE, подключиться к сетевому диску, а затем выполнить команду `setup.exe /unattend:x:\autounattend.xml` (где `x:\` — путь к файлу Autounattend.xml). В разделе «Службы развертывания Windows» ниже рассказывается, как использовать файлы несопровождаемой установки с WDS.

Проверьте себя

- Какая утилита используется для создания файла XML для несопро-
вождаемой установки?

Ответ

- Windows SIM.

Службы развертывания Windows

Службы развертывания Windows (WDS) — роль Windows Server 2008 R2, позволяющая выполнять удаленное развертывание Windows Server 2008 R2, Windows Server 2008, Windows 7 и Windows Vista.

Службы WDS требуют, чтобы клиент имел PXE-совместимую сетевую карту. Если клиент не имеет такой карты, придется использовать другой способ установки, например, создание загрузочного образа, который сможет определить сервер WDS. Чтобы такой способ работал, компьютер с сетевой картой PXE должен запуститься и найти сервер WDS. Если настроена групповая передача, а клиент прошел авторизацию, процесс установки начнется автоматически. Одноадресная передача, менее эффективная при наличии нескольких клиентов, становится доступной после установки образа операционной системы. Если на сервере WDS нет файла ответов Autounattend.xml, установка продолжится в обычном режиме, требуя участия администратора. Единственное отличие установки с использованием WDS от обычной установки состоит в том, что сервер загружается при помощи установочных файлов Windows Server 2008 R2 по сети, а не с локального компакт-диска.

WDS можно установить на компьютер с Windows Server 2008 R2 только при выполнении следующих условий:

- компьютер, на котором развертываются службы WDS, является членом домена AD DS. Требуется сервер DNS, хотя это подразумевается существованием домена;
- в сети имеется авторизованный сервер DHCP;
- для хранения образов операционной системы доступен раздел NTFS.

Нельзя развернуть WDS на компьютере с Windows Server 2008 R2 в режиме Server Core. После установки служб WDS необходимо настроить их, прежде чем их можно будет активировать. Это можно сделать при помощи Мастера настройки служб развертывания Windows, рассматриваемого в конце этого занятия, или утилиты командной строки Wdsutil.exe.

Если сервер WDS размещен совместно с сервером DHCP, необходимо настроить службы WDS так, чтобы они не прослушивали порт 67. Если не сделать этого, WDS и DHCP будут конфликтовать. Важно также настроить сервер WDS, добавив тег 60 DHCP-параметра, как показано на рис. 1-6, чтобы клиенты PXE могли найти сервер WDS.

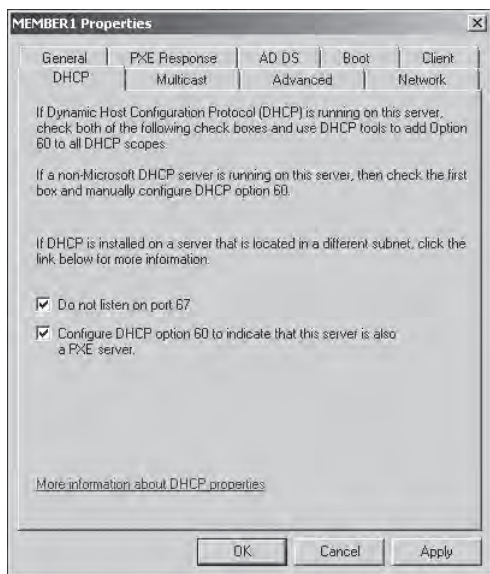


Рис. 1-6. Вкладка DHCP диалогового окна параметров сервера WDS

На вкладке **Клиент** (Client) диалогового окна свойств сервера WDS (рис. 1-7) можно указать файл несопровождаемой установки для каждой архитектуры процессора. Если файл Autounattend.xml не указан для устанавливаемой архитектуры, установка будет проходить в обычном режиме с ручным вводом.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Несопровождаемая установка

Подробнее о настройке WDS для несопровождаемой установки см. по адресу [http://technet.microsoft.com/ru-ru/library/cc771508\(WS.10\).aspx](http://technet.microsoft.com/ru-ru/library/cc771508(WS.10).aspx).

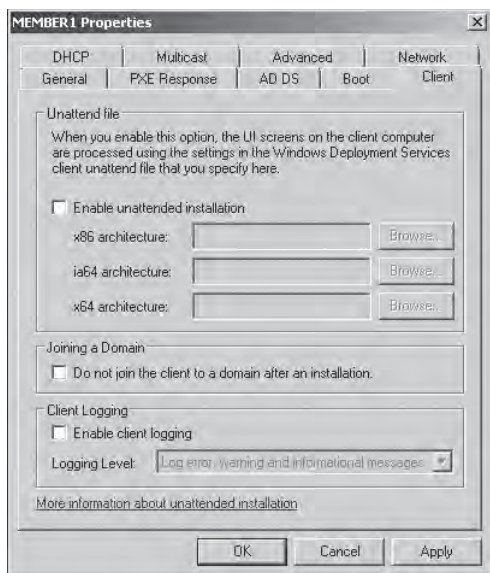


Рис. 1-7. На сервере WDS можно указать файлы несопровождаемой установки, используемые по умолчанию

В некоторых сетях используются службы для организации телеконференций и передачи видео, использующие IP-адреса из диапазона многоадресной передачи. На вкладке **Многоадресная передача (Multicast)** (рис. 1-8) можно настроить диапазон IP-адресов для многоадресной передачи WDS и порты UDP, которые будут использоваться сервером многоадресной передачи. Здесь же можно настроить параметры передачи, чтобы клиенты с разной скоростью сетевого подключения работали в разных сеансах многоадресной передачи. Возможность разделять клиентов по различным параметрам позволяет не задерживать всю передачу развертывания из-за одного компьютера с медленной сетевой картой.

Можно также настроить политику отклика PXE, настроив параметры сервера WDS. Первый параметр — задержка отклика PXE. Этот параметр позволяет указать порядок, в котором серверы WDS отвечают на запросы PXE. Доступно три варианта отклика PXE:

- **Не отвечать никаким клиентским компьютерам (Do Not Respond To Any Client Computer)** — сервер WDS не отвечает на запросы PXE;
- **Отвечать только известным клиентским компьютерам (Respond Only To Known Client Computers)** — используется, если клиенты предварительно настроены в доменных службах Active Directory;
- **Отвечать всем клиентским компьютерам (известным и неизвестным) [Respond To All (Known And Unknown) Client Computers]** — с этим параметром связан дополнительный флажок, позволяющий администраторам вручную утверждать неизвестных клиентов.

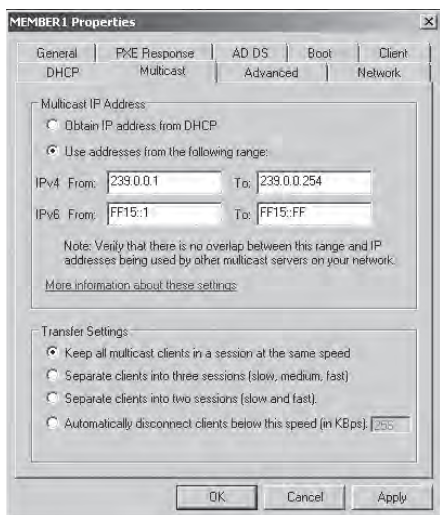


Рис. 1-8. Настройка IP-адресов для многоадресной передачи

Многоадресное, запланированное и автоматическое развертывание

Многоадресная передача повышает эффективность использования сетевого трафика, позволяя единожды передавать образ ОС по сети для нескольких

клиентов. Например, если вы развертываете 20 компьютеров с Windows Server 2008 R2, разница между передачей по сети одного образа (примерно 1,5 ГБ данных) и двадцати (примерно 60 ГБ данных) значительна. Многоадресное развертывание поддерживается только в сетях с маршрутизаторами, поддерживающими многоадресную передачу.

Развертывание можно также выполнять по расписанию и передавать установочные образы в заранее указанное время. Например, можно выполнять развертывание в часы наименьшей загруженности, когда передача значительного объема данных не особо повлияет на обычную работу сети. Можно также настроить запланированную многоадресную передачу так, чтобы она выполнялась, когда определенное число клиентов будет готово принять образ. Кроме того, эти параметры можно комбинировать. Например, на рис. 1-9 показана настройка многоадресной передачи, выполняющейся в 03:00, если 10 клиентов будут готовы принять образ. При использовании WDS и файла несопровождаемой установки можно включить группу компьютеров перед тем как уйти вечером из офиса, а наутро иметь автоматически установленные и настроенные во время ночного простоя системы. Автоматическая передача (auto-cast) означает, что многоадресная передача начнется сразу, как только клиент запросит установочный образ. Автоматическая передача чаще всего используется для разового развертывания. Для крупномасштабного развертывания больше подходит запланированная передача.

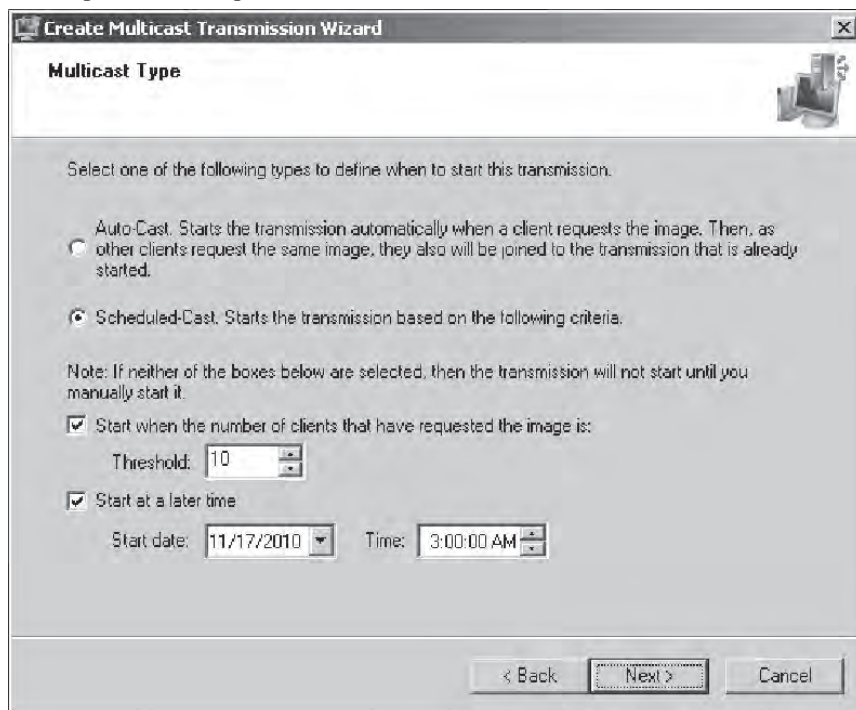


Рис. 1-9. Настройка многоадресной передачи

СОВЕТ Подготовка к экзамену

Помните, что для развертывания, запланированного на ночь, требуется файл ответов. В противном случае процесс остановится, требуя ввода данных.

Образы WDS

Службы WDS используют два типа образов: установочные и загрузочные. Установочные образы — образы операционной системы для развертывания на компьютерах с Windows Server 2008 R2, Windows Server 2008, Windows 7 или Windows Vista. Стандартный установочный образ с именем Install.wim расположен в папке \Sources установочного DVD. При использовании WDS для развертывания Windows 7 на компьютерах с разной архитектурой процессоров необходимо добавить на сервер WDS отдельный установочный образ для каждой архитектуры. Образы для разной архитектуры можно найти на установочных носителях для этой архитектуры; например, образ для Itanium расположен на установочном носителе для Itanium, а стандартный установочный образ для архитектуры x64 расположен на установочном носителе для x64. Хотя можно создавать собственные образы, для каждой архитектуры процессора должен быть только один образ. Например, для развертывания Windows Server 2008 R2 Enterprise Edition x64 на компьютере с двумя процессорами x64 и компьютере с восемью процессорами x64 в конфигурации SMP требуется доступ только к установочному образу для x64, используемому по умолчанию.

Загрузочные образы используются для запуска клиентского компьютера перед установкой образа операционной системы. Когда компьютер запускается при помощи загрузочного образа по сети, появляется меню с доступными образами, которые можно развернуть с сервера WDS. Файл Windows Server 2008 R2 Boot.wim предоставляет дополнительные возможности развертывания, и его следует использовать вместо файла Boot.wim, доступного из других источников.

Кроме базового загрузочного образа, есть два типа дополнительных загрузочных образов, которые можно настроить для использования с WDS. Образ захвата — загрузочный образ, запускающий утилиту захвата WDS. Эта утилита копирует образ компьютера, подготовленного при помощи утилиты Sysprep, и использует его для развертывания через WDS. Второй тип — образы обнаружения. Эти образы используются для развертывания на компьютерах, не поддерживающих PXE, или в сетях, где не разрешено использование PXE. Такие образы записываются на CD, DVD или USB-носители; компьютер загружается с этих носителей, а не через сетевую карту PXE, как обычно при использовании WDS.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Управление образами

Подробнее об управлении образами WDS см. в статье TechNet по адресу <http://technet.microsoft.com/ru-ru/library/cc770460.aspx>.

WDS и активация продукта

Хотя активацию продукта не обязательно выполнять в процессе установки, администраторы, использующие WDS для автоматизации развертывания, могут автоматизировать и эту задачу, используя многопользовательскую активацию. Многопользовательская активация предоставляет системным администраторам простой централизованный способ активации большого числа развернутых

серверов. При этом можно использовать два типа ключей и три способа активации. Используются ключи многократной активации (Multiple Activation Key, MAK) и ключи службы управления ключами (Key Management Services, KMS).

Ключ MAK позволяет активировать определенное число компьютеров, которое уменьшается с каждой успешной активацией. Например, ключ на 100 активаций позволяет активировать 100 компьютеров. С ключом MAK можно использовать прокси-активацию MAK и независимую активацию MAK. Для прокси-активации используется одно подключение к серверам активации Microsoft, по которому отправляется централизованный запрос на активацию нескольких продуктов. Прокси-активация выполняется при помощи средства управления активацией корпоративных лицензий (Volume Activation Management Tool, VAMT). Независимая активация MAK требует индивидуального подключения каждого компьютера к серверам активации Microsoft.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ VAMT

Подробнее о средстве управления активацией корпоративных лицензий см. по адресу <http://technet.microsoft.com/en-us/library/ff686876.aspx> (на англ. языке).

Ключи службы управления ключами (KMS) позволяют активировать компьютеры в управляемой среде, не требуя индивидуальных подключений к серверам Microsoft. Компьютеры активируются на сервере KMS, а не серверах активации Microsoft. Служба KMS имеет следующие особенности:

- для использования KMS необходимо минимум пять компьютеров с Windows Server 2008 R2 или Windows Server 2008 или 25 компьютеров с клиентской ОС, такой как Windows 7 или Windows Vista;
- чтобы установить KMS, получите у Microsoft ключ KMS и установите его в Windows Server 2008 R2. Когда система будет активирована (напрямую или по телефону), она начнет функционировать как сервер KMS. Хотя KMS можно установить на компьютер с Windows 7, этот компьютер нельзя будет использовать для активации компьютеров с Windows Server 2008 R2;
- один ключ KMS можно установить на шесть компьютеров; каждый из этих шести компьютеров можно повторно активировать до девяти раз;
- все компьютеры, активированные серверами KMS, должны иметь возможность подключения к серверу KMS каждые 180 дней. Если это условие не выполняется, компьютеры переходят в режим ограниченной функциональности;
- сервер KMS требуется активировать только один раз. Повторная активация требуется только при значительном изменении аппаратной конфигурации сервера.

Ключи KMS и MAK можно использовать совместно. Число компьютеров, частота подключения к сети и наличие связи с Интернетом определяет, какое решение лучше использовать. Если есть много компьютеров, не подключающихся к сети дольше 180 дней, следует использовать MAK. Если нет подключения к Интернету, а серверов больше 5 или клиентов больше 25, следует развертывать KMS. Если нет подключения к Интернету, а серверов меньше 5 или клиентов меньше 25, придется использовать MAK и VAMT для прокси-активации. Прокси-активация позволяет собрать данные об активации с компью-

теров сети, не подключенной к Интернету, экспортировать эти данные на клиент с выходом в Интернет, выполнить активацию и экспортировать сведения об активации на исходные компьютеры.

Подготовка отката

В идеале каждое обновление должно проходить гладко, повышая функциональность, стабильность и производительность обновляемого компьютера. На практике системному администратору лучше всего принять за аксиому один из законов Мерфи: если что-то может пойти не так, оно с большой вероятностью пойдет не так. Прежде чем обновлять Windows Server 2003 до Windows Server 2008 R2, следует подготовить план отката на случай возникновения проблем.

Откат часто необходим, когда обновление компрометирует функциональность сервера. Например, в Windows Server 2003 могут быть установлены приложения, переставшие работать после обновления до Windows Server 2008 R2. Если эти приложения важны для работы организации, придется возвращаться к Windows Server 2003, чтобы продолжать их использовать.

В процессе обновления можно выполнить откат до существующей установки Windows Server 2003. Однако после успешного входа в систему возможность отката исчезает. Недостаток такого подхода в том, что проблемы с обновлением часто можно обнаружить только после входа в систему. Единственный способ выполнить откат — отформатировать жесткий диск и восстановить Windows Server 2003 из резервной копии, созданной перед обновлением. Альтернативный вариант — развернуть Windows Server 2003 при помощи средств виртуализации Windows Server 2008 R2.

Перед обновлением Windows Server 2003 до Windows Server 2008 R2 примите следующие меры предосторожности:

- в Windows Server 2003 создайте запись для автоматического восстановления системы (Automated System Recovery, ASR);
- выполните полное резервное копирование данных, включая данные состояния системы;
- спланируйте откат обновления на случай возникновения проблем.

Если необходимо удалить Windows Server 2008 R2 после обновления Windows Server 2003, самый быстрый способ — восстановить резервную копию ASR, восстановить данные состояния системы и пользовательские данные, а затем переустановить все дополнительные приложения.

Резюме

- Файл ответов для Windows Server 2008 R2 позволяет автоматизировать некоторые или все этапы установки, предоставляя программе установки информацию об устанавливаемых компонентах и параметрах конфигурации.
- Файл ответов обычно называется Autounattend.xml и создается при помощи Windows SIM, компонента Windows AIK.
- Файлы ответов можно хранить на съемном USB-носителе, где они будут автоматически обнаруживаться программой установки Windows Server 2008 R2. Можно также хранить их на сетевом диске, если выполняется сетевая установка из Windows PE.

- Службы WDS можно использовать для развертывания образов Windows Server 2008 R2 на клиентах PXE, используя многоадресную передачу. Преимущество многоадресной передачи в том, что данные образа передаются по сети только один раз, минимизируя трафик.
- Можно запланировать многоадресную передачу, чтобы она выполнялась в указанное время или при подключении к серверу WDS определенного числа клиентов, а можно объединить оба условия. Можно также настроить автоматический запуск передачи.
- Если сервер WDS объединен с сервером DHCP, необходимо настроить WDS на прослушивание отдельного порта и включить тег 60 DHCP-параметра для всех диапазонов.
- Многопользовательская активация позволяет использовать два типа ключей активации. МАК — одиночный ключ, которым можно активировать несколько компьютеров. Активацию можно выполнять на каждом компьютере в отдельности или при помощи прокси. Служба управления ключами (KMS) требует наличия минимум 5 серверов или 25 клиентов, подключающихся к серверу KMS каждые 180 дней.

Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных на занятии 2. Эти вопросы предоставлены также в электронном виде на прилагаемом к книге компакт-диске.

ПРИМЕЧАНИЕ Ответы

Ответы на вопросы и пояснения к их вариантам размещены в разделе «Ответы» в конце книги.

1. Вы только что установили Windows Server 2008 R2 на компьютер, на котором собираетесь развернуть роль сервера WDS. Какие из указанных требований должны выполняться перед установкой роли сервера WDS? (Каждый ответ представляет часть решения. Выберите три.)
 - a. Компьютер должен входить в домен AD DS.
 - b. В сети должен иметься авторизованный сервер DHCP.
 - c. В сети должен иметься сервер DNS.
 - d. На компьютере с Windows Server 2008 должна быть установлена роль сервера приложений.
2. Какое из указанных окружений позволяет инициировать несопровождаемую установку?
 - a. Windows PE.
 - b. Загрузочный диск Windows NT.
 - c. Загрузочный диск MS DOS.
 - d. Установочный носитель Windows Server 2008.
3. Вы только что развернули роль сервера WDS на компьютере, функционирующем как контроллер домена, сервер DHCP и сервер DNS. Попытавшись запустить сервер при помощи сетевой карты PXE, вы не смогли подключить-

- ся к серверу PXE в WDS. Что следует предпринять для решения этой проблемы?
- Настроить параметры DHCP в свойствах сервера WDS.
 - Настроить параметры DHCP в консоли сервера DHCP.
 - Настроить параметры DNS в консоли сервера DNS.
 - Настроить параметры клиента в свойствах сервера WDS.
4. Вы настроили в WDS многоадресную передачу, которая должна начинаться в 19:00 в пятницу, после подключения 10 клиентов, готовых принять образ. Сервер WDS расположен в серверной на нижнем этаже, а 10 компьютеров, на которые вы собираетесь установить Windows Server 2008 R2, — на четвертом этаже рядом с вашим кабинетом. Серверная и остальная часть здания относятся к разным подсетям. Службы DNS и DHCP установлены на отдельном от WDS сервере. На сервер WDS вы скопировали необходимый файл несопровождаемой установки. Вы остались в офисе, чтобы убедиться, что развертывание началось нормально, но оно не началось. Какие изменения необходимо внести, чтобы описанный способ развертывания работал?
- Обновить зоны DNS, чтобы они были интегрированы в AD DS.
 - Настроить специальный диапазон DHCP IPv6 для клиентов PXE.
 - Настроить специальный диапазон DHCP IPv4 для клиентов PXE.
 - Заменить маршрутизатор на поддерживающий многоадресную передачу.
5. У вас есть 15 образов Windows Server 2008 для развертывания на клиентах через WDS. Все серверы должны быть настроены почти идентично. Ни один из серверов не имеет приводов для чтения дискет или оптических дисков. Как настроить WDS, чтобы минимизировать объем ручной работы по установке этих серверов?
- Поместить файл XML для несопровождаемой установки в сетевую папку.
 - Настроить многоадресную передачу в WDS.
 - Настроить файл XML для несопровождаемой установки в свойствах сервера WDS.
 - Поместить файл XML для несопровождаемой установки на съемный USB-носитель и подключать этот носитель к каждому серверу.

Практикум. Установка и настройка Windows Server 2008 R2 и роли WDS

На этом практикуме вы установите Windows Server 2008 R2, настроите этот компьютер как контроллер домена, настроите роль WDS, импортируете образы операционной системы с установочного носителя Windows Server 2008 R2 и настроите многоадресную передачу для развертывания этих образов на клиентах PXE, настроенных соответствующим образом.

Упражнение 1. Установка Windows Server 2008 R2 Enterprise Edition

Это упражнение посвящено установке и первоначальной настройке Windows Server 2008 R2. Вы установите операционную систему на чистый компьютер, а затем настроите сервер как контроллер нового домена. Вся настройка будет выполняться под учетной записью администратора. Последующие упражнения будут выполняться под учетной записью Kim_Akers.

Запустите компьютер или виртуальную машину, куда будете устанавливать операционную систему с установочного носителя Windows Server 2008 R2 Enterprise Edition, который можно загрузить с сайта Microsoft (<http://www.microsoft.com/Downloads/Search.aspx>).

1. На странице **Установка Windows** (Install Windows) выберите язык, формат времени и денежных единиц, раскладку клавиатуры или метод ввода и щелкните **Далее** (Next).
2. Щелкните **Установить** (Install Now). В списке версий операционной системы выберите полную установку Windows Server 2008 R2 Enterprise и щелкните **Далее** (Next).
3. На странице **Ознакомьтесь с условиями лицензии** (Please Read The License Terms) прочитайте лицензионное соглашение, установите флажок **Я принимаю условия лицензии** (I Accept The License Terms). Щелкните **Далее** (Next).
4. На странице **Выберите тип установки** (Which Type Of Installation Do You Want?) выберите **Полная установка (дополнительные параметры)** [Custom (Advanced)].
5. На странице **Выберите раздел для установки Windows** (Where Do You Want To Install Windows?) щелкните **Далее** (Next).
6. Начнется процесс установки. Он может длиться до 20 минут, в зависимости от скорости оборудования, на которое устанавливается ОС. За это время компьютер дважды перезагрузится.
7. Будет запрошена смена пароля перед первым входом в систему. Здесь задается пароль для локальной учетной записи администратора. Щелкните **ОК**, дважды введите пароль **Pa\$\$w0rd** и нажмите Enter. В окне с уведомлением о смене пароля щелкните **ОК**, после чего будет произведен вход в систему.
8. Откройте командную строку с повышенными привилегиями и выполните следующие команды:

```
Netsh interface ipv4 set address «Подключение по локальной сети» static 10.10.0.10
Netdom renamecomputer %computername% /newname:VAN-DC1
```

ПРИМЕЧАНИЕ

В английской версии первая команда должна иметь следующий синтаксис:
Netsh interface ipv4 set address "Local Area Connection" static 10.10.0.10

9. Перезагрузите компьютер и войдите в систему под учетной записью администратора.
10. Щелкните **Пуск**. В поле **Найти программы и файлы** (Search Programs and Files) введите Dcprgmo и нажмите Enter.
11. Когда запустится мастер установки доменных служб Active Directory, щелкните **Далее** (Next) два раза.
12. На странице **Выберите конфигурацию развертывания** (Choose A Deployment Configuration) выберите **Создать новый домен в новом лесу** (Create A New Domain In A New Forest) и щелкните **Далее** (Next).
13. На странице **Укажите имя корневого домена леса** (Name The Forest Root Domain) введите **Adatum.com** и щелкните **Далее** (Next).
14. На странице **Задайте режим работы леса** (Set Forest Functional Level) выберите режим **Windows Server 2008 R2** и щелкните **Далее** (Next).
15. Убедитесь, что на странице **Дополнительные параметры контроллера домена** (Additional Domain Controller Options) установлен флажок **DNS-сервер** (DNS Server), и щелкните **Далее** (Next). В окне с предупреждением о невозможности DNS-делегирования щелкните **Да** (Yes), чтобы продолжить.
16. Примите предложенные по умолчанию расположения папок Database, Log Files и SYSVOL и щелкните **Далее** (Next).
17. В диалоговом окне **Пароль администратора для восстановления служб каталогов** (Directory Services Restore Mode Administrator Password) дважды введите пароль **Pa\$\$w0rd** и щелкните **Далее** (Next).
18. На странице сводных данных щелкните **Далее** (Next), чтобы начать установку доменных служб Active Directory на компьютер VAN-DC1. Когда мастер завершит работу, щелкните **Готово** (Finish). Когда будет предложено, щелкните **Перезагрузка** (Restart Now), чтобы перезагрузить сервер.

Упражнение 2. Подготовка к установке роли сервера WDS

В этом коротком упражнении вы выполните несколько организационных задач, чтобы подготовить сервер к установке роли сервера WDS. Сюда входит установка службы сервера DHCP и создание учетной записи с ограниченными административными правами. Примерно такие учетные записи имеют ИТ-специалисты, работа которых соответствует темам экзамена 70-646. Эта учетная запись имеет административные права, но не входит в группы Schema Admins (Администраторы схемы) и Enterprise Admins (Администраторы предприятия).

1. Зайдите на контроллер домена VAN-DC1 под учетной записью администратора.
2. Откройте апплет **Active Directory — пользователи и компьютеры** (Active Directory Users And Computers) из меню **Администрирование** (Administrative Tools).
3. В контейнере **Пользователи** (Users) создайте новую учетную запись с именем **Kim_Akers**. Назначьте этой учетной записи пароль **Pa\$\$w0rd** с неограниченным сроком действия.

ПРИМЕЧАНИЕ Только для удобства выполнения упражнений

На практике для учетных записей администраторов должна действовать та же политика истечения срока действия паролей, что и для всех остальных учетных записей.

4. Добавьте созданную учетную запись в группу безопасности **Администраторы домена** (Domain Admins), но не добавляйте в любые другие административные группы.
5. Выйдите из системы и войдите под учетной записью Kim_Akers.
6. Если консоль **Диспетчер сервера** (Server Manager) не открылась автоматически, откройте ее при помощи ярлыка, прикрепленного к панели задач, или меню **Пуск | Администрирование** (Start | Administrative Tools).
7. Щелкните правой кнопкой мыши узел **Роли** (Roles) и выберите команду **Добавить роли** (Add Roles). Будет запущен мастер добавления ролей.
8. На странице **Перед началом работы** (Before You Begin) щелкните **Далее** (Next).
9. На странице **Выбор ролей сервера** (Select Server Roles) выберите **DHCP-сервер** (DHCP Server) и щелкните **Далее** (Next).
10. На странице **Знакомство с DHCP-сервером** (Introduction To DHCP Server) щелкните **Далее** (Next).
11. На странице **Привязки сетевых подключений** (Network Connection Bindings) выберите интерфейс 10.10.0.10 как интерфейс для получения запросов DHCP и щелкните **Далее** (Next).
12. Убедитесь, что данные на странице **Параметры IPv4 DNS-сервера** (IPv4 DNS Settings) соответствуют данным на рис. 1-10. Щелкните **Проверить подлинность** (Validate), затем щелкните **Далее** (Next).

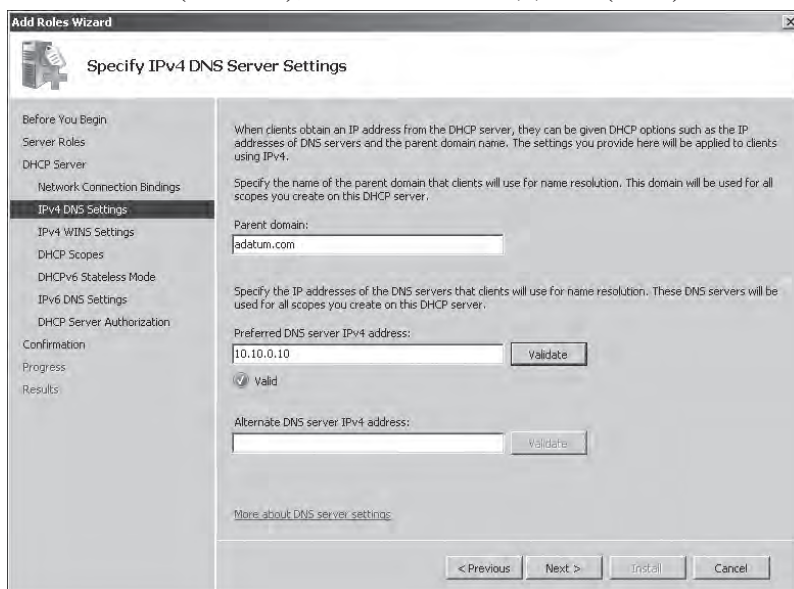


Рис. 1-10. Параметры DNS для сервера DHCP

13. На странице **Параметры IPv4 WINS-сервера** (IPv4 WINS Settings) оставьте параметры по умолчанию и щелкните **Далее** (Next).
14. На странице **Области DHCP** (DHCP Scopes) щелкните **Добавить** (Add).
15. В диалоговом окне **Добавление области** (Add Scope) добавьте элементы в соответствии с рис. 1-11. Два раза щелкните **ОК**, затем щелкните **Далее** (Next).

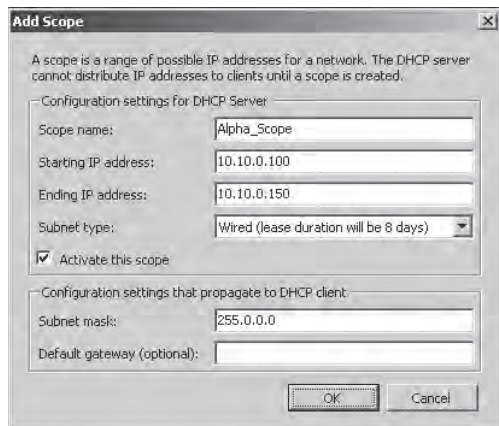


Рис. 1-11. Параметры области DHCP

16. Просмотрите стандартные параметры режима DHCPv6 без отслеживания состояния и щелкните **Далее** (Next).
17. Просмотрите стандартные параметры DHCP IPv6 DNS-сервера и щелкните **Далее** (Next).
18. Убедитесь, что установлен переключатель **Использовать текущие учетные данные** (Use Current Credentials), а в поле **Имя пользователя** (User Name) указано ADATUM\kim_akers. Щелкните **Далее** (Next). На странице подтверждения щелкните **Установить** (Install). Начнется установка роли сервера DHCP.
19. Когда роль сервера DHCP будет установлена, закройте окно мастера добавления ролей.

Упражнение 3. Установка роли сервера WDS и добавление файлов образов

В этом упражнении вы установите роль сервера WDS и добавите файлы образов с установочного носителя Windows Server 2008 R2. Убедитесь, что установочный носитель находится в приводе DVD-ROM.

1. Если консоль **Роли сервера** (Server Roles) закрыта, откройте ее при помощи ярлыка на панели задач или из меню **Администрирование** (Administrative Tools).
2. Щелкните правой кнопкой мыши узел **Роли** (Roles) и выберите **Добавить роли** (Add Roles).

3. Если откроется страница **Перед началом работы** (Before You Begin), щелкните **Далее** (Next). Если нет, переходите к шагу 4.
4. На странице **Выбор ролей сервера** (Select Server Roles) выберите **Службы развертывания Windows** (Windows Deployment Services) и щелкните **Далее** (Next).
5. На странице **Обзор служб развертывания Windows** (Overview of Windows Deployment Services) просмотрите раздел **На что обратить внимание** (Things to Note) и щелкните **Далее** (Next).
6. Убедитесь, что на странице **Выбор ролей сервера** (Select Server Roles) выбраны роли **Сервер развертывания** (Deployment Server) и **Транспортный сервер** (Transport Server). Щелкните **Далее** (Next), а затем **Установить** (Install). Установка завершится, щелкните **Закрыть** (Close).
7. В меню **Администрирование** (Administrative Tools) выберите **Службы развертывания Windows** (Windows Deployment Services).
8. В консоли **Службы развертывания Windows** (Windows Deployment Services) раскройте узел **Серверы** (Servers), щелкните правой кнопкой мыши сервер VAN-DC1.adatum.com, а затем щелкните **Настроить сервер** (Configure Server). Будет запущен мастер настройки служб развертывания Windows. Щелкните **Далее** (Next).
9. Примите расположение папки удаленной установки (C:\RemoteInstall) и щелкните **Далее** (Next).
10. На странице **Предупреждение о системном томе** (System Volume Warning) прочитайте рекомендации о размещении папки удаленной установки на томе, отличном от системного, и щелкните **Да** (Yes).
11. Убедитесь, что установлены флажки **Не прослушивать порт 67** (Do not listen on port 67) и **Настроить тег 60 DHCP-параметра для значения «PXEClient»** (Configure DHCP Option 60 To «PXEClient»), и щелкните **Далее** (Next).
12. На странице **Исходные параметры PXE-сервера** (PXE Server Initial Settings) выберите **Отвечать только известным клиентским компьютерам** (Respond Only to Known Client Computers) и щелкните **Готово** (Finish).
13. Убедитесь, что на странице **Настройка завершена** (Configuration Complete) установлен флажок **Добавить образы на сервер развертывания Windows сейчас** (Add Images to the Windows Deployment Server Now) и щелкните **Готово** (Finish).

ПРИМЕЧАНИЕ Требуется установочный носитель

Прежде чем выполнять шаг 17, убедитесь, что в привод DVD вставлен установочный носитель Windows Server 2008 R2. Для образов потребуется около 3 ГБ дискового пространства.

14. В диалоговом окне **Расположение файлов образов Windows** (Windows Image Files Location) щелкните **Обзор** (Browse) и перейдите в папку Sources на DVD. Щелкните **ОК**, а затем **Далее** (Next).
15. Убедитесь, что на странице **Группа образов** (Image Group) установлен переключатель **Создание новой группы образов** (Create A New Image Group), а имя новой группы — ImageGroup1. Щелкните **Далее**.

16. В диалоговом окне **Просмотр параметров** (Review Settings) убедитесь, что на сервер будет передан 1 загрузочный образ и 8 установочных, после чего щелкните **Далее** (Next). Образы будут переданы с установочного носителя Windows Server 2008 R2 в папку C:\RemoteInstall.
17. Когда передача образов закончится, щелкните **Готово** (Finish).
18. В консоли **Службы развертывания Windows** (Windows Deployment Services) щелкните правой кнопкой мыши узел **Многоадресные передачи** (Multicast Transmissions) и выберите **Создать многоадресную передачу** (Create Multicast Transmission).
19. На странице **Имя передачи** (Transmission Name) введите **TestAlpha** и щелкните **Далее** (Next).
20. Убедитесь, что на странице **Выбор образа** (Select Image) выбрана группа ImageGroup1, и щелкните **Далее** (Next).
21. Убедитесь, что на странице **Тип многоадресной передачи** (Multicast Type) установлен переключатель **По расписанию** (Scheduled-Cast). Установите флажок **Запускать автоматически, когда число клиентов, готовых принять образ, составляет** (Start automatically when the number of clients ready to receive this image is) и введите значение 10. Щелкните **Далее** (Next), а затем **Готово** (Finish).
22. Закройте консоль и выключите компьютер.

Закрепление материала главы

Чтобы закрепить знания, полученные при изучении этой главы, выполните следующее:

- прочитайте резюме главы;
- просмотрите список основных терминов, представленных в этой главе;
- выполните задания лабораторной работы, моделирующей реальные ситуации, требующие применения полученных знаний;
- выполните рекомендуемые упражнения;
- пройдите пробный тест.

Резюме главы

- Выбор подходящей версии Windows Server 2008 R2 определяется требованиями к оборудованию, кластеризации и необходимым ролям сервера.
- Windows Server 2008 R2 традиционно развертывается при помощи установочного DVD. Можно также использовать Windows PE для загрузки в среду с сетевой папкой, содержащей установочные файлы операционной системы, хотя такая возможность обычно используется, только когда нет сетевой карты PXE и нельзя использовать WDS.
- Файл ответов для Windows Server 2008 обычно называется Autounattend.xml и создается при помощи утилиты Windows SIM, входящей в Windows AIK.

WDS можно настроить для использования файла Autounattend.xml, чтобы автоматизировать процесс установки.

- Службы WDS позволяют развертывать образы операционной системы на компьютерах с сетевыми картами PXE, используя запланированные многоадресные передачи. Многоадресные передачи минимизируют трафик, а запуск по расписанию позволяет передавать образы во время низкой загрузки сети.

Основные термины

Проверьте, знаете ли вы, что означают перечисленные ниже термины из этой главы:

- загрузочный раздел;
- DHCP;
- многоадресная передача;
- PXE;
- системный раздел;
- среда предустановки Windows (Windows PE).

Лабораторная работа

Для выполнения заданий лабораторной работы используйте знания о планировании установки и обновления серверов, полученные из этой главы. Ответы можно найти в разделе «Ответы» в конце книги.

Задание 1. Переход Contoso на Windows Server 2008

Компания Contoso переводит инфраструктуру сети с Windows Server 2003 на Windows Server 2008 R2. По некоторым вопросам планирования перехода требуются ваши советы. Ниже описаны ситуации, по которым требуются ваши рекомендации.

1. Пять серверов из филиалов компании должны работать под управлением Windows Server 2008 R2 Standard Edition в режиме Server Core. Сейчас эти серверы работают под управлением Windows Server 2003 x64 Standard Edition. Каждый сервер имеет процессор Core 2 Duo 2 ГГц, 4 ГБ ОЗУ и 1 ТБ свободного дискового пространства. Как спланировать переход?
2. Какая версия Windows Server 2008 R2 лучше всего подойдет для развертывания в экранированной подсети Contoso, если серверу используется только для размещения корпоративного веб-сайта?
3. Вы собираетесь разместить большое число виртуальных машин с Windows Server 2008 R2 на мощном сервере. Какую версию Windows Server 2008 R2 следует выбрать, чтобы минимизировать расходы на приобретение дополнительных лицензий?

Задание 2. Автоматизация развертывания Windows Server 2008 в Tailspin Toys

Tailspin Toys — компания по производству игрушек, планирующая модернизацию устаревшей сетевой инфраструктуры, в том числе развертывание значительного числа систем Windows Server 2008 R2. Вас пригласили в качестве консультанта для помощи в развертывании новых серверов.

1. Физическая инфраструктура сети компании создавалась почти десять лет назад. Какие компоненты инфраструктуры должны быть обновлены или заменены перед развертыванием Windows Server 2008 R2 при помощи многоадресной передачи?
2. Что следует предпринять, если сервер будет совмещать роль WDS и роль сервера DHCP?
3. У вас есть 10 серверов, установку которых вы хотите провести с помощью WDS. Вы беспокоитесь, что многоадресная передача начнется раньше, чем все 10 серверов будут готовы, и не хотите выполнять несколько передач. Что следует предпринять в этом случае?

Рекомендуемые упражнения

Чтобы успешно справиться с экзаменационными заданиями по темам этой главы, выполните следующие упражнения.

Планирование установки и обновления серверов

Если у вас есть доступное оборудование или возможность использовать виртуальные машины, выполните следующие упражнения, используя полученные из этой главы знания:

- **Упражнение 1.** На отдельном компьютере установите Windows Server 2008 R2 в режиме Server Core.
- **Упражнение 2.** Добавьте установку Server Core в домен, созданный при выполнении упражнений этой главы. Добавьте этому компьютеру роль сервера IIS.

Планирование автоматического развертывания серверов

Если у вас есть доступное оборудование или возможность использовать виртуальные машины, и вы хотите подробнее изучить автоматизацию развертывания серверов, выполните следующие упражнения, используя полученные из этой главы знания:

- **Упражнение 1.** Загрузите и установите Windows AIK с веб-сайта Microsoft.
- **Упражнение 2.** Используйте Windows SIM, компонент Windows AIK, для создания собственного образа на основе одного из установочных образов Windows Server 2008 R2.
- **Упражнение 3.** Используйте Windows SIM для создания файла ответов для установки Windows Server 2008 R2.

Пробный экзамен

Тренировочные тесты на прилагаемом к книге компакт-диске позволяют проверить знания только по одной или сразу по всем темам сертификационного экзамена 70-646. Тестирование можно организовать так, чтобы оно проводилось как настоящий экзамен, а можно проходить в режиме обучения, просматривая правильные ответы и объяснения после каждого ответа.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Пробный экзамен

Подробнее о пробном экзамене рассказано во Введении.

Г Л А В А 2

Планирование служб инфраструктуры

Занятие 1. Планирование IPv6	37
Занятие 2. Планирование DNS	65

Администратор, отвечающий за сеть с большим числом узлов, обычно отвечает и за всю архитектуру ИТ-среды компании. Администратор должен уметь планировать инфраструктуру и выполнять глобальные изменения конфигурации. Для этого необходимо иметь опыт администрирования Windows Server 2008/2008 R2 или других серверных ОС Windows.

Как опытный специалист, вы наверняка знакомы с разрешением имен и адресацией IPv4. Возможно, вы знакомы также с форматом адресов IPv6, но не полностью понимаете различные типы адресов IPv6 и стратегии перехода с IPv4 на IPv6. Вы должны быть знакомы с разрешением имен, в частности, с системой доменных имен (DNS), но, возможно, никогда не настраивали зоны обратного просмотра DNS для IPv6. Изучив эту главу, вы расширите свои знания и навыки по планированию и настройке сетей с несколькими сайтами.

Темы экзамена

- Планирование ролей сервера для служб инфраструктуры.

Прежде всего

Для выполнения упражнений этой главы потребуется:

- Сервер с именем VAN-DC1, работающий под управлением Windows Server 2008 R2 Enterprise Edition, настроенный как контроллер домена Adatum.com, как описано в Приложении А.
- Компьютер с именем VAN-SRV1, работающий под управлением Windows Server 2008 R2 Enterprise Edition, настроенный как рядовой сервер домена Adatum.com, как описано в Приложении А. Этот сервер может действовать как клиент контроллера домена, и в этой главе мы будем называть его клиентом.
- Учетная запись пользователя Kim Akers с паролем Pa\$\$w0rd в домене Adatum.com, включенная в группы администраторов домена, администрато-

ров предприятия и администраторов схемы. Если вы не знаете, как добавить учетную запись в группу безопасности, откройте оснастку **Active Directory — Пользователи и компьютеры** (Active Directory Users And Computers) и обратитесь к справочной системе.

- Для выполнения практических упражнений рекомендуем использовать изолированную сеть, не входящую в рабочую сеть. Доступ к Интернету не требуется, как и настройка шлюза по умолчанию. Для экономии времени и затрат на настройку физических компьютеров используйте виртуальные машины, например, созданные с использованием роли сервера Hyper-V.

Реальный мир

Йен Маклин

Помните ошибку двухтысячного года?

В 1999 г. компьютерный мир был в панике (во всяком случае, если верить прессе). Предполагалось, что в полночь, когда закончится 1999 год, компьютеры взорвутся, самолеты полетят задом наперед, и произойдет еще много катаклизмов из-за ошибок в старых программах, не способных перевести дату на двухтысячный год.

Специалисты знали о возможных проблемах, особенно, со старыми 4-разрядными микропроцессорами. Но у нас было много времени, чтобы исправить ситуацию, и много умных людей работало над этим. Многие специалисты предсказывали (и правильно), что ничего особенного не случится. К сожалению, была и другая проблема, угрожающая миру компьютерных сетей.

Предсказывалось, что к апрелю 2000 г. кончатся свободные адреса IPv4. Уже существовала система адресации IPv6 и глобальная сеть IPv6 (которую потом назвали 6Bone). Однако эта технология не имела широкого распространения. Некоторые сетевые инженеры вели себя совсем не профессионально и выказывали признаки паники. Один старый циник, которого звали Ян Маклин, собирался написать книгу о IPv6.

Эта книга не была написана, и это хорошо, потому что она бы не продавалась. Внезапно популярность приобрела трансляция сетевых адресов (NAT) и частные сети. Организации, требующие сотен открытых адресов, обнаружили, что им вполне достаточно двух. Использование бесклассовой междоменной маршрутизации (CIDR) позволило Центру по присвоению параметров протоколов Интернета (IANA) забрать у организаций неиспользуемые IP-адреса. Проблема была решена.

Однако, это было лишь временное решение, и проблема до сих пор существует. Пространство адресов IPv4 остается под угрозой исчерпания, а структура заголовка IPv4 все еще вызывает проблемы с Интернет-маршрутизаторами. Автоматическое назначение частных IP-адресов (APIPA) позволяет выдавать только немаршрутизируемые внутренние адреса, и приходится во многом полагаться на протокол динамического конфигурирования узла (DHCP). Мы лишь выиграли немного времени для перехода, который происходит сейчас. Раньше под «протоколом Интернета» всегда подразумевался протокол IPv4, теперь это IPv6. Сове-

менные серверные и клиентские операционные системы используют IPv6.

- Папа, что такое IPv4?
- Когда-то, давным-давно...

Занятие 1. Планирование IPv6

Опытный специалист должен знать, что диапазоны частных IP-адресов — 10.0.0.0/8, 172.16.0.0/12 и 192.168.0.0/16, а диапазон автоматически назначаемых частных IP-адресов (APIPA) — 169.254.0.0/16. Также следует знать, что NAT обычно позволяет использовать относительно небольшое число открытых IP-адресов для предоставления доступа к Интернету многим внутренним клиентам, имеющим частные IP-адреса. Вы должны уметь отличать сети классов A, B и C и помнить, что большинство современных сетей использует CIDR. Помните также, что адреса класса D (224.0.0.0/4) используются для многоадресной передачи.

Вы должны знать, что DHCP может назначать адреса IPv4, маски подсетей, шлюзы по умолчанию, адреса серверов DNS и WINS и многие другие параметры, и что с помощью APIPA можно автоматически настраивать адреса IPv4 для использования в изолированной частной сети. Существует три модели инфраструктуры DHCP: централизованная, децентрализованная и комбинированная. Вы должны знать, что DHCP работает совместно с DNS, и при выделении IP-адресов сервером DHCP в зоны DNS добавляются записи хоста (Host) и указателя (PTR).

О настройке DHCP и IPv4 написано много книг, и мы не будем повторять эту информацию. Возможно, вы не так хорошо знакомы с инфраструктурой IPv6, типами адресов IPv6, функционированием DHCP версии 6 (DHCPv6) и настройкой областей DHCPv6. Также вам необходимо понимать стратегию перехода с IPv4 на IPv6 и взаимодействие IPv4 с IPv6, в частности, использование адресов Teredo. На этом занятии мы рассмотрим IPv6, DHCPv6, стратегию перехода и взаимодействие двух стеков.

Изучив материал этого занятия, вы сможете:

- ✓ Различать типы адресов IPv6 и понимать их предназначение.
- ✓ Определять адреса IPv6, которые могут маршрутизироваться в Интернете IPv4.
- ✓ Подбирать подходящую стратегию перехода с IPv4 на IPv6.
- ✓ Использовать утилиты IPv6.
- ✓ Настраивать области DHCPv6.

Продолжительность занятия — примерно 35 мин.

Анализ структуры адресов IPv6

Очень большое (2^{128}) пространство адресов IPv6 делает возможным создание нескольких уровней подсетей и распределение адресов между магистральным

маршрутизатором и отдельными подсетями организации. Это позволяет выделять сетевой сущности не один, а несколько уникальных адресов IPv6, каждый из которых будет использоваться для разных целей.

IPv6 предоставляет адреса, эквивалентные типам адресов IPv4, и другие, присущие только IPv6. Узел может иметь несколько адресов IPv6, каждый из которых имеет собственное предназначение. В этом разделе описывается синтаксис адреса IPv6 и разные классы адресов IPv6.

Синтаксис адреса IPv6

128-разрядный адрес IPv6 разделен на 16-разрядные блоки, каждый из которых преобразован в 4-разрядное шестнадцатеричное число. В качестве разделителей используются двоеточия. Такое представление называется шестнадцатеричным с двоеточиями.

Глобальные адреса одноадресной рассылки эквивалентны открытым адресам IPv4 одноадресной рассылки. Для демонстрации синтаксиса адреса IPv6 рассмотрим следующий адрес IPv6 глобальной одноадресной рассылки:

```
21cd:0053:0000:0000:03ad:003f:af37:8d62
```

Представление IPv6 можно упростить, удалив начальные нули из каждого 16-разрядного блока. Однако каждый блок должен иметь минимум одну цифру. В упрощенном представлении адрес выглядит следующим образом:

```
21cd:53:0:0:3ad:3f:af37:8d62
```

Непрерывную последовательность нулевых блоков можно сжать до двух двоеточий (::). Таким образом, адрес из нашего примера можно записать так:

```
21cd:53::3ad:3f:af37:8d62
```

Некоторые типы адресов содержат длинные последовательности нулей, и для их записи удобно использовать такую нотацию. Например, адрес многоадресной рассылки ff05:0:0:0:0:0:0:2 можно сжать до ff05::2.

Префиксы адресов IPv6

Префикс — часть адреса, указывающая биты, имеющие фиксированные значения, или биты идентификатора сети. Префиксы IPv6 выражаются так же, как в нотации IPv4 CIDR или нотации с косой чертой. Например, 21cd:53::/64 — подсеть, в которой находится адрес 21cd:53::23ad:3f:af37:8d62. В этом случае первые 64 бита адреса являются префиксом сети. Префикс подсети IPv6 (или идентификатор подсети) назначается отдельному каналу связи. Одному каналу связи может быть назначено несколько идентификаторов подсети. Это называется многосетевой конфигурацией (multinetting).

ПРИМЕЧАНИЕ Маски подсетей

В IPv6 для описания подсетей не используется точечно-десятичная нотация. Поддерживается только нотация длины префикса. Точечно-десятичное представление адресов подсетей, используемое в IPv4 (например, 255.255.255.0), не имеет прямого эквивалента.

Типы адресов IPv6

Адреса IPv6 бывают трех типов: одноадресные, многоадресные и произвольной рассылки.

- **Адрес одноадресной рассылки (Unicast).** Определяет один интерфейс в пределах области адресов одноадресной рассылки. Пакеты, отправляемые на адрес одноадресной рассылки, доставляются на один интерфейс. Документ RFC 2373 допускает использование одного адреса несколькими интерфейсами, если протокол IPv6 на хосте рассматривает эти интерфейсы как один интерфейс. Это используется системами балансировки нагрузки.
- **Адрес многоадресной рассылки (Multicast).** Определяет несколько интерфейсов. Пакеты, отправляемые на такой адрес, доставляются на все интерфейсы этого адреса.
- **Адрес произвольной рассылки (Anycast).** Определяет несколько интерфейсов. Пакеты, отправляемые на такой адрес, доставляются на ближайший интерфейс, определенный адресом. Близость интерфейса определяется по расстоянию маршрутизации, по числу прыжков. Адреса произвольной рассылки используются для взаимодействия один-к-одному-из-многих, доставка выполняется на один интерфейс.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Архитектура адресации IPv6

Подробнее о структуре и архитектуре адресов IPv6 см. в RFC 2373 по адресу <http://www.ietf.org/rfc/rfc2373.txt>.

ПРИМЕЧАНИЕ Интерфейсы и узлы

Адреса IPv6 определяют интерфейсы, а не узлы. Узел идентифицируется любым адресом одноадресной рассылки, назначенным одному из интерфейсов узла.

Адреса одноадресной рассылки IPv6

IPv6 поддерживает следующие типы адресов многоадресной рассылки:

- глобальной рассылки;
- локальной связи;
- локального сайта;
- специальные;
- сопоставленные адреса NSAP и IPX.

Адреса глобальной одноадресной рассылки

Адреса глобальной одноадресной рассылки IPv6 (глобальные адреса) эквивалентны открытым адресам IPv4. Они глобально маршрутизируемы и доступны в Интернете IPv6. Такие адреса могут комбинироваться для создания эффективной инфраструктуры маршрутизации, и их иногда называют комбинируемыми глобальными адресами. Комбинируемый адрес уникален во всем Интернете IPv6. (Часть сети, в которой IP-адрес уникален, называется *областью* адреса.)

Префикс формата (Format Prefix, FP) глобального адреса указывается в трех старших битах, которые всегда равны 001. Следующие 13 бит, называемые идентификатором составляющей верхнего уровня (Top Level Aggregator, TLA), выделяются IANA. IANA выдает поля TLA локальным реестрам Интернета, которые, в свою очередь, выделяют индивидуальные TLA крупным поставщикам услуг Интернета. Следующие 8 бит адреса зарезервированы для расширения в будущем.

Следующие 24 бита адреса содержат идентификатор составляющей следующего уровня (Next Level Aggregator, NLA). Такой идентификатор указывает сайт конкретного потребителя. Поле NLA позволяет поставщикам услуг Интернета создавать в сети многоуровневую иерархию адресации. Следующие 16 бит содержат идентификатор составляющей уровня сайта (Site Level Aggregator, SLA), используемый для организации адресации и маршрутизации нижестоящими поставщиками услуг Интернета, а также для идентификации сайтов и подсетей в пределах сайта.

Следующие 64 бита идентифицируют интерфейс в подсети. Это 64-разрядный расширенный уникальный идентификатор (EUI-64), определенный IEEE. Адреса EUI-64 назначаются либо напрямую сетевым адаптерам, либо производятся на основе 48-разрядного MAC-адреса сетевого адаптера в соответствии со стандартом IEEE 802. Проще говоря, идентификатор интерфейса предоставляется оборудованием — сетевым адаптером.

Подведем итог: FP, TLA, зарезервированные биты и NLA идентифицируют открытую топологию, SLA идентифицирует топологию сайта, а идентификатор интерфейса указывает интерфейс. Структура комбинированного адреса глобальной одноадресной рассылки показана на рис. 2-1.

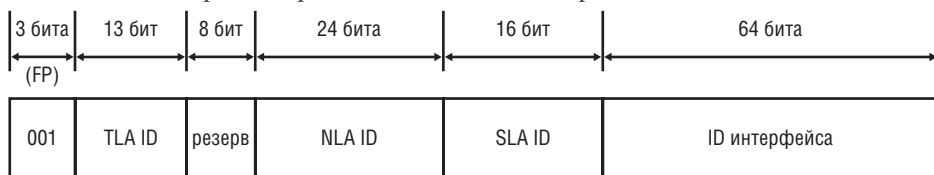


Рис. 2-1. Структура адреса глобальной одноадресной рассылки

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Формат адреса глобальной одноадресной рассылки

Подробнее о комбинируемых адресах глобальной одноадресной рассылки см. в RFC 2374 по адресу <http://www.ietf.org/rfc/rfc2374.txt>.

СОВЕТ Подготовка к экзамену

На экзамене необходимо знать, что комбинируемые адреса глобальной одноадресной рассылки в IPv6 эквивалентны открытым адресам одноадресной рассылки в IPv4. Вы должны уметь идентифицировать глобальные адреса одноадресной рассылки по значению трех старших бит. Знание составляющих адреса поможет понять, как работает адресация IPv6, но на экзамене это вряд ли будет проверяться с такой же точностью, как описано в документах RFC.

Адреса локальной связи

Адреса локальной связи IPv6 эквивалентны адресам IPv4, автоматически настраиваемым через APIPA и использующим префикс 169.254.0.0/16. Идентифицировать адрес локальной связи можно по префиксу формата 1111 1110 10, за которым следует 54 нуля (адреса локальной связи всегда начинаются с *fe8*). Узлы используют адреса локальной связи при взаимодействии с соседними узлами, подключенными к тому же каналу связи. Область адресов локальной связи — соответствующая локальная связь. Адрес локальной связи требуется

процессам изучения окружения и всегда настраивается автоматически, даже при отсутствии всех прочих адресов одноадресной рассылки.

На рис. 2-2 показан адрес локальной связи, настроенный на интерфейсе контроллера домена VAN-DC1. В конфигурации нет глобальных адресов, поскольку контроллеры домена никогда не подключаются к Интернету напрямую. Адреса IPv6 на вашем тестовом компьютере будут другими.

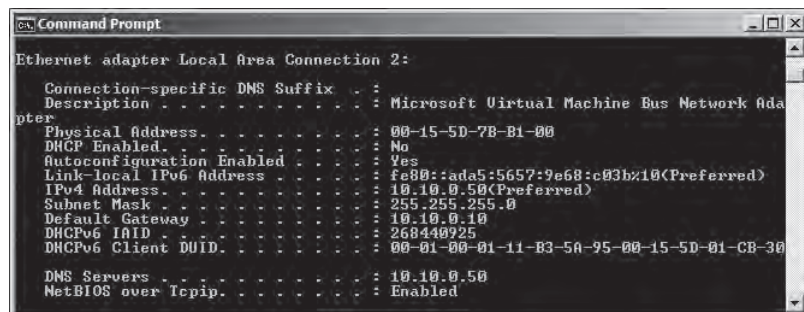


Рис. 2-2. Адреса IPv6 на интерфейсах компьютера

Адреса локального сайта

В настоящий момент адреса локального сайта не рекомендуется использовать, но общепринятой замены для них пока нет, и они продолжают широко использоваться в корпоративных сетях, так что вам необходимо знать о них. Такие адреса эквивалентны частному пространству адресов IPv4 (10.0.0.0/8, 172.16.0.0/12 и 192.168.0.0/16). Частные интрасети, не имеющие прямого маршрутизируемого подключения к Интернету IPv6, могут использовать адреса локального сайта без конфликтов с комбинируемыми адресами глобальной одноадресной рассылки. Областью адреса локального сайта является сайт (или объединенная сеть организации).

Адреса локального сайта могут выделяться при помощи процесса настройки с ведением базы данных, например, из области DHCPv6. Хост использует настройку с ведением базы данных, когда получает объявления маршрутизатора, не включающие префиксы адресов. Хост будет использовать протокол настройки адреса с ведением базы данных, когда в локальном канале связи нет маршрутизаторов.

Адреса локального сайта могут настраиваться также без ведения базы данных. Этот процесс основан на объявлениях маршрутизатора, включающих префиксы адресов, не входящих в базу данных, и требует, чтобы хост не использовал протокол настройки с использованием базы данных.

Кроме того, настройка адреса может выполняться со смешением процессов с ведением и без ведения базы данных. Это происходит, когда объявления маршрутизатора включают префиксы адресов, не входящих в базу данных, но требуют, чтобы хосты использовали протокол настройки с ведением базы данных.

ПРИМЕЧАНИЯ Небольшие сети

В небольших сетях, включающих лишь несколько компьютеров и имеющих медленные или ненадежные каналы связи, использование DHCP и DHCPv6 может быть неподходящим вариантом, и разумнее выполнять ручную настройку.

Адреса локального сайта начинаются со значения *fec0*, за которым идет 32 нуля и 16-разрядный идентификатор подсети, который можно использовать для создания подсетей внутри организации. 64-разрядное поле идентификатора интерфейса указывает определенный интерфейс в подсети.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Замена для адресов локального сайта

О предлагаемых вариантах замены адресов локального сайта можно почитать по адресу <http://www.ietf.org/rfc/rfc4291.txt>.

Адреса локальной связи и локального сайта

Подключение по протоколу IPv6 между хостами изолированной подсети можно организовать при помощи адресов локальной связи. Однако такие адреса нельзя назначать интерфейсам маршрутизаторов (шлюзов по умолчанию), и нельзя выполнять маршрутизацию между подсетями, если используются только адреса локальной связи. DNS-серверы не могут использовать одни только адреса локальной связи. Если используется адрес локальной связи, необходимо указать его идентификатор интерфейса, т.е. номер после символа % в конце адреса (см. рис. 2-2). Адреса локальной связи не регистрируются динамически в DNS в Windows Server 2008 и 2008 R2.

По этим причинам в подсетях частных сетей для реализации связи IPv6 используются адреса локального сайта (пока таким адресам не найдена общепринятая замена). Если каждое устройство в сети будет иметь собственный глобальный адрес (заявленная цель внедрения IPv6), можно будет маршрутизировать глобальные адреса между внутренними подсетями, в периферийных зонах и в Интернете.

Специальные адреса

Существует два специальных адреса IPv6: неуказанный адрес и адрес замыкания на себя. Неуказанный адрес 0:0:0:0:0:0 (или ::) используется для обозначения отсутствия адреса и эквивалентен неуказанному адресу IPv4 0.0.0.0. Он обычно используется как адрес источника пакетов, отправляемых для проверки уникальности пробного адреса. Неуказанный адрес никогда не назначается интерфейсу и не используется в качестве адреса назначения. Адрес замыкания на себя 0:0:0:0:0:1 (или ::1) используется для идентификации интерфейса замыкания на себя. Он эквивалентен адресу замыкания на себя IPv4 127.0.0.1.

Адреса NSAP и IPX

Адреса NSAP являются идентифицирующими метками для конечных точек сети, используемых в сетях OSI (Open System Interconnection). Они используются для определения оборудования, подключенного к сети ATM (Asynchronous Transfer Mode). Протокол IPX вышел из широкого использования, так как современные сети Novell Netware поддерживают TCP/IP. Адреса IPv6 с форматом префикса 0000001 сопоставляются с адресами NSAP. Адреса IPv6 с форматом префикса 0000010 сопоставляются с адресами IPX.

СОВЕТ Подготовка к экзамену

На экзамене 70-646 вам вряд ли встретятся вопросы о сопоставлении NSAP и IPX.

Адреса многоадресной рассылки IPv6

Адреса многоадресной рассылки IPv6 позволяют отправлять пакеты IPv6 на несколько хостов, все из которых имеют одинаковый адрес многоадресной рассылки. Такие адреса имеют формат префикса 11111111 (всегда начинаются с *ff*). Последующие поля указывают флаги, область и идентификатор группы (рис. 2-3).

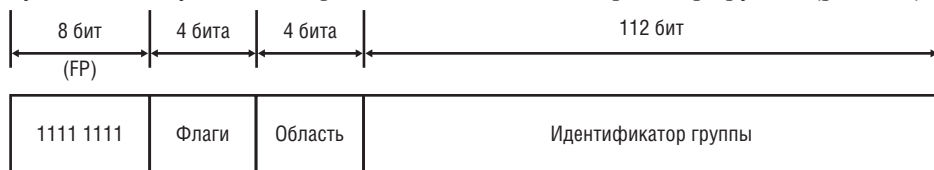


Рис. 2-3. Структура адреса многоадресной рассылки

Поле *флаги* содержит параметры флагов. В настоящий момент определен только флаг Transient (Т), использующий бит поля низшего разряда. Если этот флаг имеет значение 0, адрес многоадресной рассылки известен; другими словами, он назначен перманентно и выделен IANA. Если флаг имеет значение 1, адрес временный.

Проверьте себя

Определите тип адреса fec0:0:0:eadf::1ff.

Ответ

Адрес локального сайта для одноадресной рассылки.

Поле *область* указывает область сети IPv6, для которой предназначен трафик многоадресной рассылки. Маршрутизаторы используют эту информацию совместно с информацией, предоставленной протоколами маршрутизации многоадресной передачи, чтобы определить, можно ли перенаправить трафик. Например, область трафика с адресом многоадресной рассылки ff02::2 — локальная связь, и этот трафик никогда не будет перенаправляться за пределы локального канала связи. В табл. 2-1 перечислены значения поля области.

Табл. 2-1

Значение	Область
0	Зарезервирована
1	Область локального узла
2	Область локальной связи
5	Область локального сайта
8	Область локальной организации
e	Глобальная область
f	Зарезервирована

Идентификатор группы, уникальный в пределах области, представляет группу многоадресной рассылки. Перманентно назначенные идентификаторы групп независимы от области. Временные идентификаторы групп относятся только к определенной области. Адреса многоадресной рассылки от ff01:: до ff0f:: — зарезервированные известные адреса.

Теоретически доступно 2^{112} идентификаторов групп. На практике, из-за особенностей способа сопоставления адресов многоадресной рассылки IPv6 с MAC-адресами Ethernet, в документе RFC 2373 рекомендуется назначать идентификаторы групп из младших 32 бит адреса многоадресной рассылки IPv6 и задавать оставшимся битам идентификатора нулевые значения. Это позволяет сопоставить каждый идентификатор группы с уникальным MAC-адресом Ethernet для многоадресной рассылки.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Назначение идентификаторов групп

Подробнее о назначении идентификаторов групп см. по адресу <http://www.ietf.org/rfc/rfc2373.txt>.

Совместимость IPv4 с IPv6 и переход на IPv6

В этом разделе обсуждается переход с IPv4 на IPv6 и его преимущества. Однако во многих организациях IPv4 и IPv6 сосуществуют, и переход с IPv4 на IPv6 обычно происходит постепенно. Поэтому мы рассмотрим также совместимость IPv4 с IPv6.

Протокол IPv6 создавался для преодоления ограничений IPv4 и имеет следующие преимущества над своим предшественником:

- **Увеличенное адресное пространство.** 32-разрядной структуры, используемой IPv4, не было достаточно для структуры адресации. IPv6 имеет 128-разрядную структуру. Это дает достаточно адресов для каждого устройства, требующего уникального открытого адреса. Кроме того, 64-разрядная часть адреса IPv6, описывающая хост (идентификатор интерфейса), может генерироваться автоматически на основе данных сетевого адаптера.
- **Автоматическая настройка адресов.** Обычно адреса IPv4 настраиваются либо вручную, либо при помощи DHCP. Автоматическая настройка через APIPA доступна для изолированных подсетей, адреса которых не маршрутизируются в другие сети. IPv6 удовлетворяет потребность в более простой и более автоматизированной настройке адресов, поддерживая оба типа настройки — с ведением базы данных (stateful) и без ведения базы данных (stateless). Для настройки с ведением базы данных используется DHCPv6. Если используется настройка без ведения базы данных, хосты, подключенные к каналу связи, автоматически выполняют настройку адресов IPv6 для этого канала связи и (если требуется) адресов, произведенных на основе префиксов, переданных локальными маршрутизаторами. Можно также использовать настройку при помощи DHCPv6 без ведения базы данных, при которой адреса хостам не назначаются, но, например, могут назначаться параметры серверам DNS, чьи доменные имена не включены в объявления маршрутизаторов.
- **Безопасность на уровне сети.** Частные каналы связи через Интернет требуют шифрования для защиты передаваемых данных от просмотра или изме-

нения. Такую возможность предоставляет протокол IPSec, но его использование в IPv4 не является обязательным. В IPv6 протокол IPSec стал обязательным. Это предоставляет стандартизированное решение для обеспечения безопасности сети и повышает совместимость между разными реализациями IPv6.

- **Доставка данных в реальном времени.** В IPv4 реализованы стандарты качества обслуживания (QoS), и для передачи данных (таких как видео и аудио) в реальном времени можно гарантированно предоставить определенную полосу пропускания. Однако в IPv4 для передачи данных в реальном времени используется поле ToS (тип службы) и определение полезных данных, обычно при помощи порта UDP или TCP. Поле ToS IPv4 имеет ограниченную функциональность, и определение полезных данных, пересылаемых через порты TCP или UDP невозможно при шифровании полезных данных пакетов IPv4. Определение полезных данных включено в поле Flow Label заголовка IPv6, так что шифрование не влияет на функционирование QoS.
- **Размер таблиц маршрутизации.** Структура глобальных адресов IPv6, используемых в Интернете IPv6, позволяет создавать эффективную объединяемую иерархическую инфраструктуру маршрутизации на основе общих данных нескольких уровней поставщиков услуг Интернета. В Интернете IPv6 магистральные маршрутизации имеют значительно уменьшенные таблицы маршрутизации, использующие агрегирование маршрутов и соответствующие инфраструктуре маршрутизации агрегаторов верхнего уровня.
- **Размер заголовка и заголовки расширения.** Заголовки IPv4 и IPv6 не совместимы, так что хосты или маршрутизаторы должны использовать обе реализации — IPv4 и IPv6 — для распознавания и обработки заголовков разного формата. Поэтому для заголовка IPv6 выбрана такая структура, которая обеспечивает минимальную длину без ущерба для работы. Несущественные и необязательные поля перемещены в заголовки расширения, идущие за заголовком IPv6. В результате этого заголовок IPv6 только в два раза больше заголовка IPv4, а размер заголовков расширения ограничен только размером пакета IPv6.
- **Устранение широковещательного трафика.** В протоколе IPv4 разрешение IP-адресов в MAC-адреса сетевых адаптеров выполняется при помощи широковещательной рассылки по протоколу ARP. Широковещательные рассылки увеличивают сетевой трафик и не являются эффективными, так как их обрабатывает каждый хост. Протокол представления с соседним узлом (Neighbor Discovery, ND) для IPv6 использует серии сообщений ICMPv6 (Internet Control Message Protocol for IPv6), управляющие взаимодействием узлов, подключенных к одному каналу связи (соседних узлов). ND заменяет широковещательные рассылки ARP, сообщения ICMPv4 Router Discovery (обнаружение маршрутизатора) и ICMPv4 Redirect (перенаправление) эффективными сообщениями одноадресной и многоадресной рассылки ND.

Агрегация маршрутов

Агрегация маршрутов позволяет выполнять маршрутизацию трафика из сетей с меньшими префиксами в сети с большими префиксами. Другими словами, она позволяет объединить несколько непрерывных блоков адреса в более крупный блок адреса. Агрегация маршрутов снижает число объявляемых маршрутов в крупных сетях. Когда провайдер услуг Интернета разбивает свою сеть на небольшие подсети для предоставления услуг нижестоящим провайдерам, требуется объявить только маршрут к основной суперсети, чтобы можно было отправлять трафик в подсети нижестоящих провайдеров.

Агрегация маршрутов используется, когда крупный провайдер имеет непрерывный диапазон IP-адресов. IP-адреса (IPv4 или IPv6), которые можно объединять, называются *комбинируемыми адресами*.

Реализация совместимости IPv4 с IPv6

Кроме описанных выше типов адресов, IPv6 предоставляет адреса совместимости, облегчающие переход с IPv4 на IPv6 и реализацию технологий перехода.

IPv4-совместимые адреса

IPv4-совместимый адрес 0:0:0:0:0:w.x.y.z (или ::w.x.y.z) используется узлами с двумя стеками, взаимодействующими по протоколу IPv6 поверх инфраструктуры IPv4. Последние 4 октета (w.x.y.z) соответствуют точечно-десятичному представлению адреса IPv4. Узлы с двумя стеками — это узлы, использующие оба протокола — IPv4 и IPv6. Когда IPv4-совместимый адрес используется в качестве назначения IPv6, трафик IPv6 инкапсулируется в заголовок IPv4 и автоматически отправляется по назначению с использованием инфраструктуры IPv4.

ПРИМЕЧАНИЕ IPv4-совместимые адреса выходят из употребления

Текущие механизмы перехода на IPv6 больше не используют IPv4-совместимые адреса. Новые и обновленные реализации не требуют поддержки адресов такого типа. Об этих адресах необходимо знать, так как они могут встретиться на практике в схемах обеспечения совместимости, но их не следует использовать при создании новых схем.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ IPv4-совместимые адреса

Подробнее о выходе из употребления IPv4-совместимых адресов см. по адресу <http://www.ietf.org/rfc/rfc4291.txt>.

IPv4-сопоставленные адреса

IPv4-сопоставленный адрес 0:0:0:0:ffff:w.x.y.z (или ::ffff:w.x.y.z) используется для представления узла, работающего только по протоколу IPv4, узлу IPv6, а значит, проецирует устройства, не совместимые с IPv6, в адресное пространство IPv6. IPv4-сопоставленные адреса никогда не используются в качестве адреса источника или назначения пакета IPv6.

Адреса Teredo

Адрес Teredo состоит из 32-разрядного префикса Teredo. В Windows Server 2008 и Windows Server 2008 R2 (а также в Windows Vista и Windows 7) это 2001::/32. За префиксом идет 32-разрядный открытый адрес IPv4 сервера Teredo, участвующего в настройке адреса. Следующие 16 бит зарезервированы для флагов Teredo. В настоящий момент определен только старший бит флагов. Это флаг конуса (Cone), устанавливаемый, когда система NAT, подключенная к Интернету, является конусной системой NAT.

ПРИМЕЧАНИЕ Teredo в Windows XP и Windows Server 2003

В Windows XP и Windows Server 2003 изначально использовался префикс Teredo 3ffe:831f::/32. После установки обновления безопасности MS06-064 эти системы используют префикс 2001::/32.

Следующие 16 бит хранят скрытую версию внешнего UDP-порта, по которому передается весь трафик Teredo для клиентского интерфейса Teredo. Когда клиент Teredo отправляет первый пакет на сервер Teredo, NAT сопоставляет UDP-порт источника пакета с другим, внешним UDP-портом. Весь трафик Teredo для интерфейса хоста использует этот внешний сопоставленный UDP-порт. Значение, представляющее этот внешний порт, маскировано или скрыто выполнением операции исключающего ИЛИ (XOR) со значением 0xffff. Скрытие внешнего порта предотвращает его трансляцию вместе с полезными данными перенаправляемого пакета.

Последние 32 бита хранят скрытую версию внешнего адреса IPv4, по которому передается весь трафик Teredo для клиентского интерфейса Teredo. Этот внешний адрес скрывается операцией XOR со значением 0xffffffff. Как и в случае с UDP-портом, это предотвращает трансляцию NAT внешнего адреса с полезными данными перенаправляемого пакета.

Например, в компании Northwind Traders реализованы следующие частные сети IPv4:

- главный офис: 10.0.100.0 /24;
- филиал 1: 10.0.0.0 /24;
- филиал 2: 10.0.10.0 /24;
- филиал 3: 10.0.20.0 /24.

Компания хочет организовать взаимодействие по протоколу IPv6 между несколькими клиентами Teredo, а также между клиентами Teredo и хостами, работающими только по протоколу IPv6. Наличие серверов Teredo в Интернете IPv4 делает возможным такое взаимодействие. Сервер Teredo — это узел IPv6/IPv4, подключенный к Интернету IPv4 и Интернету IPv6 и поддерживающий интерфейс туннелирования Teredo. Адреса Teredo сетей Northwind Traders зависят от нескольких факторов, таких как порт и тип используемых NAT-серверов, но они, например, могут быть следующими:

- главный офис: 2001::ce49:7601:e866:efff:f5ff:9bfe — 2001::0a0a:64fe:e866:efff:f5ff:9b01;
- офис 1: 2001::ce49:7601:e866:efff:f5ff:fffe — 2001::0a0a:0afe:e866:efff:f5ff:ff01;
- офис 2: 2001::ce49:7601:e866:efff:f5ff:f5fe — 2001::0a0a:14fe:e866:efff:f5ff:f501;
- офис 3: 2001::ce49:7601:e866:efff:f5ff:ebfe — 2001::0a0a:1efe:e866:efff:f5ff:ebfe.

Заметьте, что, например, адрес 10.0.100.1 эквивалентен адресу 0a00:6401, а после выполнения операции XOR со значением ffff:ffff получается f5ff:9bfe.

СОВЕТ Подготовка к экзамену

Microsoft поддерживает адреса Teredo, но на экзамене 70-646 вряд ли будут вопросы относительно генерации таких адресов. Однако могут встретиться вопросы, в которых требуется идентифицировать такой адрес и включенный в него адрес IPv4. К счастью, на экзамене можно пользоваться научным калькулятором.

Конусные системы сетевой трансляции

Конусные NAT бывают следующих типов: полный конус, ограниченный конус и конус с ограниченными портами. В полном конусе NAT все запросы с одного внутреннего IP-адреса и порта сопоставляются с одним внешним IP-адресом и портом, и любой внешний хост может отправить пакет внутреннему хосту по сопоставленному внешнему адресу.

В ограниченном конусе NAT все запросы с одного внутреннего IP-адреса и порта сопоставляются с одним внешним IP-адресом и портом, но внешний хост может отправлять пакеты внутреннему хосту, только если внутренний хост ранее отправлял пакет внешнему хосту.

В конусе с ограниченными портами ограничение включает номера портов. Внешний хост с определенным IP-адресом и портом источника может отправить пакет внутреннему хосту, только если внутренний хост ранее отправлял пакет на этот IP-адрес и порт.

Адреса ISATAP

Протокол IPv6 может использовать адрес ISATAP для организации взаимодействия между двумя узлами в интрасети IPv4. Адрес ISATAP начинается с 64-разрядного адреса локальной связи, адреса локального сайта, глобального адреса или глобального префикса 6to4. Следующие 32 разряда представляют идентификатор ISATAP 0:5efe. Последние 32 разряда содержат адрес IPv4 в десятично-точечной или шестнадцатеричной нотации. Адрес ISATAP может включать открытый или частный адрес IPv4.

Например, адрес ISATAP fe80::5efe:w.x.y.z имеет префикс локальной связи, адрес fec0::1111:0:5efe:w.x.y.z — префикс локального сайта, адрес 3ffe:1a05:510:1111:0:5efe:w.x.y.z — глобальный префикс, а адрес 2002:9d36:1:2:0:5efe:w.x.y.z — глобальный префикс 6to4. Во всех случаях w.x.y.z представляет адрес IPv4.

По умолчанию в Windows Server 2008 и 2008 R2 для каждого адреса IPv4, назначенного узлу, автоматически настраивается адрес ISATAP fe80::5efe:w.x.y.z. Это адрес ISATAP локальной связи, позволяющий двум хостам взаимодействовать по сети IPv4, используя адреса ISATAP друг друга.

Сопоставление IPv6-IPv4 можно настроить при помощи утилит IPv6 netsh interface ipv6 6to4, netsh interface ipv6 isatap и netsh interface ipv6 add v6v4tunnel. Например, чтобы создать туннель IPv6 в IPv4 между локальным адресом 10.0.0.11 и удаленным адресом 192.168.123.116 с интерфейсом *Remote*, выполните такую команду:

```
netsh interface ipv6 add v6v4tunnel «Remote» 10.0.0.11 192.168.123.116
```

Можно также настроить соответствующие адреса совместимости вручную, используя команду `netsh interface ipv6 set address` или средства настройки TCP/IPv6 с графическим интерфейсом (описаны далее на этом занятии).

ПРИМЕЧАНИЕ 6to4cfg

Windows Server 2008 и Windows Server 2008 R2 не поддерживают утилиту 6to4cfg.

Планирование стратегии перехода с IPv4 на IPv6

Для перехода с IPv4 на IPv6 нет обязательных сроков. Администраторы сами решают, быть ли им в числе первых и сразу пользоваться преимуществами IPv6, такими как расширенная адресация и повышенная безопасность, или же ждать и учиться на чужом опыте. Обе стратегии допустимы.

Однако необходимо выяснить, обеспечивают ли поддержку IPv6 вышестоящие поставщики услуг Интернета и сетевое оборудование организации (или всех организаций предприятия). Самый простой способ перехода — использование двух стеков: IPv4 и IPv6. Заметим, что не следует слишком долго задерживать переход на IPv6. Если дотянуть до того, что адресное пространство IPv4 будет полностью исчерпано, использование двух стеков будет невозможно, и переход будет гораздо более резким.

В настоящее время отправной точкой при планировании перехода является доступность существующей инфраструктуры IPv4, а первостепенная задача — организация передачи пакетов IPv6 по существующим сетям IPv4, позволяющей избежать возникновения изолированных островков сетей IPv6. Когда большинство сетей выполнит переход, задача поменяется: потребуется передавать пакеты IPv4 по инфраструктурам IPv6 для поддержки старых приложений, работающих по протоколу IPv4, и избегать появления изолированных островков IPv4.

Так как нет единой стратегии, подходящей для всех ситуаций, существует несколько стратегий и технологий перехода. В RFC 4213 описаны ключевые элементы технологий перехода, таких как использование двух стеков и настройка туннелирования. В этом документе также определены типы узлов по поддержке разных протоколов, включая старые системы, поддерживающие только IPv4, будущие системы, поддерживающие только IPv6, и двойные узлы с поддержкой IPv6 и IPv4.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Переход с IPv4 на IPv6

Подробнее о базовых механизмах перехода см. в RFC 4213 (<http://www.ietf.org/rfc/rfc4213.txt>) и в документе «IPv6 Transition Technologies», который можно скачать по адресу <http://technet.microsoft.com/en-us/library/bb726951.aspx>.

Переход с использованием двух стеков

Использование двух стеков (или *двойного IP-уровня*) — наверно, самый простой способ перехода. Предполагается, что хосты и маршрутизаторы поддерживают оба протокола и могут отправлять и принимать пакеты IPv4 и IPv6. Таким образом, узел с двумя стеками может взаимодействовать с устройствами, работающими по протоколу IPv4, используя пакеты IPv4, и с устройствами, работающими по протоколу IPv6, используя пакеты IPv6. Такой узел может функционировать в одном из трех режимов:

- с включением только стека IPv4;
- с включением только стека IPv6;
- с включением обоих стеков — IPv4 и IPv6.

Так как узлы с двумя стеками поддерживают оба протокола, им можно назначать и 32-разрядные адреса IPv4, и 128-разрядные адреса IPv6. Например, можно использовать DHCP для назначения адресов IPv4 и автоматическую настройку без ведения базы данных или DHCPv6 для назначения адресов IPv6. Текущие реализации IPv6 обычно используют два стека. Продукт, поддерживающий только IPv6, найдет очень мало партнеров по взаимодействию.

Переход с настройкой туннелирования

При таком переходе существующая инфраструктура маршрутизации IPv4 продолжает функционировать и используется для передачи трафика IPv6, пока разрабатывается инфраструктура маршрутизации IPv6. *Туннель* — это двусторонний канал связи типа «точка-точка» между двумя конечными точками сети. Данные передаются по туннелю с использованием инкапсуляции, при которой пакет IPv6 заключается в пакет IPv4. Инкапсулированный заголовок IPv4 создается на входе в туннель и удаляется на выходе. Адреса конечных точек туннеля определяются на основе сведений о конфигурации, хранящихся в точке инкапсуляции.

Такие туннели также называют *явными*. Их можно настраивать между маршрутизаторами, между хостом и маршрутизатором, между хостами и между маршрутизатором и хостом. Чаще всего используются туннели между двумя маршрутизаторами. Для управления настроенным туннелем может использоваться *брокер туннелей*. Это выделенный сервер, управляющий запросами на создание туннелей, полученных от пользователей (RFC 3053).

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Брокер туннелей

Подробнее о брокере туннелей см. в RFC 3053 по адресу <http://www.ietf.org/rfc/rfc3053.txt>.

Автоматическое туннелирование

В RFC 2893 (впоследствии замененном на RFC 4213) описывается автоматическое туннелирование, позволяющее узлам IPv4/IPv6 взаимодействовать через инфраструктуру маршрутизации IPv4, не используя предварительно настроенные туннели. Узлом, выполняющим автоматическое туннелирование, назначаются адреса специального типа, называемые IPv4-совместимыми адресами (см. далее), содержащие 32-разрядный адрес IPv4 в формате 128-разрядного адреса IPv6. Адрес IPv4 может автоматически извлекаться из адреса IPv6.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Автоматическое туннелирование

Подробнее об автоматическом туннелировании см. в RFC 2893 по адресу <http://www.ietf.org/rfc/rfc2893.txt>. Однако учитывайте, что этот документ устарел, и текущим стандартом является RFC 4213.

6to4

В RFC 3056 описывается схема туннелирования 6to4, позволяющая сайтам IPv6 взаимодействовать друг с другом по сети IPv4, не используя явных туннелей, и с доменами в основном режиме IPv6 через ретранслирующие маршрутизаторы. В этой стратегии Интернет IPv4 рассматривается как единый канал данных.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Туннелирование 6to4

Подробнее о туннелировании 6to4 см. в RFC 3056 по адресу <http://www.ietf.org/rfc/rfc3056.txt>.

Teredo

В RFC 4380 описывается технология Teredo, являющаяся усовершенствованием метода 6to4 и поддерживаемая Windows Server 2008 и 2008 R2. Teredo позволяет узлам, расположенным за устройством NAT IPv4, взаимодействовать по протоколу IPv6, используя пакеты туннелей UDP. Teredo требует использования сервера и элементов ретрансляции для обеспечения связи. Структура адресов Teredo обсуждалась ранее на этом занятии.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Teredo

Подробнее о Teredo см. в RFC 4380 по адресам <http://www.ietf.org/rfc/rfc4380.txt> и <http://www.microsoft.com/technet/network/ipv6/teredo.msp>.

Протокол ISATAP

В RFC 4214 определен протокол адресации автоматического межсайтового туннелирования (ISATAP), соединяющий хосты и маршрутизаторы IPv6 по сети IPv4 при помощи процесса, рассматривающего сеть IPv4 как канальный уровень сети IPv6, а другие узлы — как потенциальные хосты или маршрутизаторы IPv6. Таким образом автоматически создается туннель между хостами, между хостом и маршрутизатором или между маршрутизатором и хостом.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ ISATAP

Подробнее о протоколе ISATAP см. в RFC 4214 по адресу <http://www.ietf.org/rfc/rfc4214.txt> и в документе «Manageable Transition to IPv6 using ISATAP», который можно скачать по адресу <http://www.microsoft.com/downloads/details.aspx?FamilyId=B8F50E07-17BF-4B5C-A1F9-5A09E2AF698B&displaylang=en>.

Использование утилит IPv6

В Windows Server 2008 и 2008 R2 имеются утилиты, позволяющие настраивать интерфейсы IPv6 и проверять работоспособность подключения и маршрутизации. Есть также утилиты для обеспечения и проверки совместимости IPv4 с IPv6.

Стандартные утилиты Windows Server 2008 и 2008 R2, такие как ping, ipconfig, pathping, tracert, netstat и route, имеют полную функциональность в сетях IPv6. Например, на рис. 2-4 показан результат выполнения команды ping, использованной для проверки подключения по адресу локальной связи в тестовой сети IPv6. Адреса IPv6 в вашей тестовой сети будут другими. Если выполнять эту команду с одного хоста для проверки другого хоста, потребуется также указать идентификатор интерфейса, например, ping fe80::ada5:5657:9e68:c03b%10. Идентификаторы интерфейсов обсуждаются далее в этом занятии.

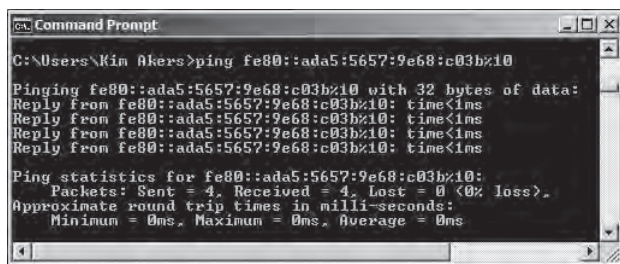


Рис. 2-4. Проверка подключения по адресу IPv6 командой ping

ПРИМЕЧАНИЕ Ping6

Утилита командной строки ping6 не поддерживается в Windows Server 2008 и 2008 R2.

Утилиты, специфичные для IPv6, представлены в структуре команды netsh. Например, команда netsh interface ipv6 show neighbors показывает интерфейсы IPv6 всех хостов в локальной подсети. Далее на этом занятии вы используете эту команду на практике, после того как настроите связь IPv6 в подсети.

Проверка конфигурации и подключения IPv6

Когда требуется решить проблемы с подключением или просто проверить конфигурацию, наверно, самым полезным и, определенно, наиболее часто используемым, инструментом является ipconfig. Команда ipconfig /all показывает конфигурацию IPv4 и IPv6.

Если хотите просмотреть только конфигурацию интерфейсов IPv6 локального компьютера, используйте команду netsh interface ipv6 show address. На рис. 2-5 показан результат выполнения этой команды на компьютере VAN-DC1. Обратите внимание на символ % с номером после каждого адреса IPv6. Это идентификатор интерфейса, имеющего адрес IPv6.

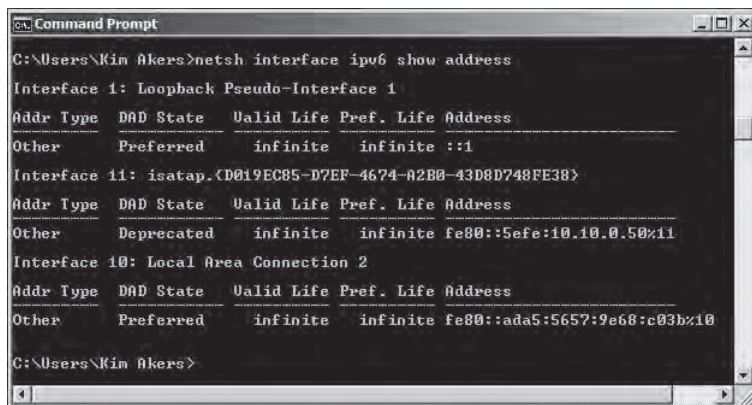


Рис. 2-5. Просмотр адресов IPv6 и идентификаторов интерфейсов

Если вы администрируете сеть предприятия с несколькими сайтами, вам необходимо знать также идентификаторы сайтов (или идентификаторы областей). Получить эти идентификаторы можно командой netsh interface ipv6 show address level=verbose (см. рис. 2-6).

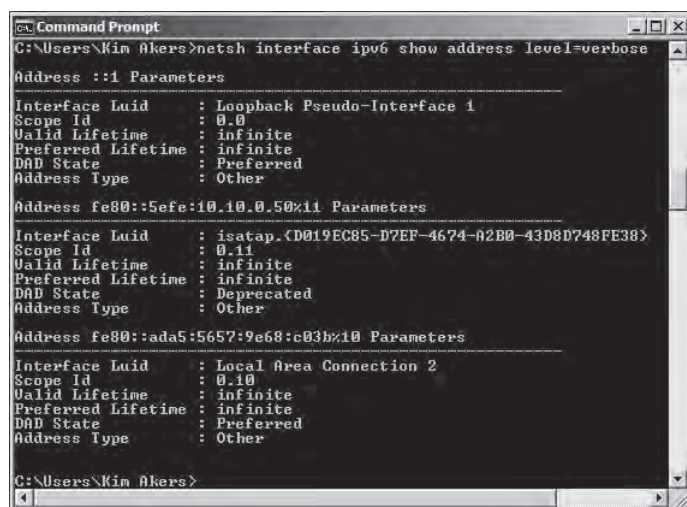


Рис. 2-6. Просмотр адресов IPv6 и идентификаторов сайтов

Настройка интерфейсов IPv6

Обычно большинство адресов IPv6 назначается при помощи автоматической настройки или DHCPv6. Однако если требуется настроить адрес IPv6 вручную, можно использовать команду `netsh interface ipv6 set address`, как показано ниже:

```
netsh interface ipv6 set address «local area connection 2» fec0:0:0:fffe::2
```

Для использования этой команды необходимо запустить оболочку командной строки от имени администратора. Кроме того, в Windows Server 2008 и 2008 R2 (а также в Windows Vista и Windows 7) адреса IPv6 можно настраивать вручную в окне свойств TCP/IPv6 (рис. 2-7).

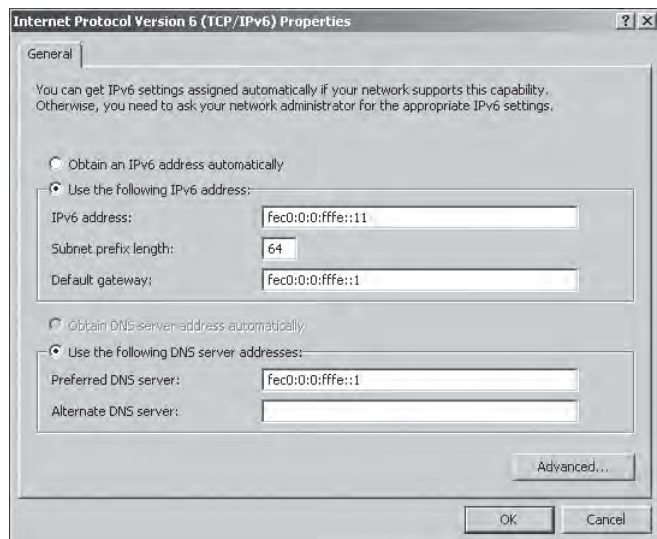


Рис. 2-7. Настройка адреса IPv6 при помощи графического интерфейса

Преимущество графического интерфейса в том, что кроме адреса интерфейса можно указать адреса IPv6 одного или нескольких DNS-серверов. Если вы все же решите использовать интерфейс командной строки (CLI), команда для добавления адресов IPv6 DNS-серверов — `netsh interface ipv6 add dnsserver`. Пример:

```
netsh interface ipv6 add dnsserver «local area connection 2» fec0:0:0:fffe::1
```

Для изменения свойств интерфейсов IPv6 (но не их конфигурации) используется команда `netsh interface ipv6 set interface`. Пример:

```
netsh interface ipv6 set interface «local area connection 2» forwarding=enabled
```

Для использования команд `netsh interface ipv6 add` и `netsh interface ipv6 set` необходимо запустить командную строку от имени администратора.

Проверьте себя

- Какая команда `netsh` позволяет просмотреть идентификаторы сайта?

Ответ

- `netsh interface ipv6 show address level=verbose`.

Проверка подключения IPv6

Первый этап проверки подключения к локальной сети — очистка кэша соседей, хранящего недавно разрешенные адреса уровня канала связи. Неочищенный кэш может привести к неверным результатам при проверке изменений, связанных с разрешением адресов. Содержимое кэша соседей проверяется командой `netsh interface ipv6 show neighbors`. Команда `netsh interface ipv6 delete neighbors` очищает кэш. На рис. 2-8 показаны результаты выполнения этих двух команд. Для использования утилиты `netsh` необходимо запустить командную строку от имени администратора.

```

Administrator: Command Prompt
C:\Windows\system32>netsh interface ipv6 show neighbors

Interface 1: Loopback Pseudo-Interface 1

Internet Address      Physical Address      Type
-----
ff02::2               Permanent
ff02::c               Permanent
ff02::16              Permanent
ff02::1:2             Permanent
ff02::1:ffcc:78c5     Permanent

Interface 10: Local Area Connection 2

Internet Address      Physical Address      Type
-----
ff02::2               33-33-00-00-00-02    Permanent
ff02::16              33-33-00-00-00-16    Permanent
ff02::1:2             33-33-00-01-00-02    Permanent
ff02::1:3             33-33-00-01-00-03    Permanent
ff02::1:ff68:c03b     33-33-ff-68-c0-3b    Permanent

C:\Windows\system32>netsh interface ipv6 delete neighbors
Ok.

C:\Windows\system32>
  
```

Рис. 2-8. Просмотр и очистка кэша соседей

Подключение к локальному хосту в текущей подсети и к шлюзу по умолчанию можно проверить при помощи команды `ping`. В адрес IPv6 интерфейса

можно добавить идентификатор интерфейса, чтобы убедиться, что адрес настроен на нужном интерфейсе. На рис. 2-4 выше показаны результаты выполнения команды `ping` для адреса IPv6.

При проверке подключения к хосту в удаленной сети в первую очередь следует проверить и очистить конечный кэш, хранящий адреса IPv6 следующего прыжка для назначений. Просмотреть текущее содержимое конечного кэша можно командой `netsh interface ipv6 show destinationcache`. Очистка конечного кэша выполняется командой `netsh interface ipv6 delete destinationcache`. Для использования этой команды необходимо запустить командную строку от имени администратора.

Следующий этап — проверка подключения к интерфейсу маршрутизатора, используемого по умолчанию в локальной подсети. Это шлюз по умолчанию. Определить адрес IPv6 интерфейса маршрутизатора по умолчанию можно командами `ipconfig`, `netsh interface ipv6 show routes` и `route print`. Можно также указать код зоны, являющийся идентификатором интерфейса для шлюза по умолчанию в том интерфейсе, на который нужно отправлять сообщения эхо-запроса ICMPv6. Убедившись, что шлюз по умолчанию доступен, проверьте командой `ping` возможность подключения к удаленному хосту по его адресу IPv6. Заметьте, что командой `ping` нельзя обращаться к удаленному хосту (или интерфейсу маршрутизатора) по адресу IPv6 локальной связи, так как такие адреса не маршрутизируются.

Если удастся подключиться к шлюзу по умолчанию, но не к конечному удаленному адресу, отследите маршрут до этого удаленного адреса, используя команду `tracert -d` с указанием конечного адреса IPv6. Параметр `-d` запрещает выполнять обратный запрос DNS по интерфейсам маршрутизаторов в пути маршрутизации. Это ускоряет отображение пути маршрутизации. Если хотите получить больше информации о маршрутизаторах из этого пути, в частности, если хотите проверить надежность маршрутизаторов, используйте команду `pathping -d`, указав конечный адрес IPv6.

Проверьте себя

- Какая команда `netsh` используется для определения адреса IPv6 интерфейса маршрутизатора по умолчанию?

Ответ

- `netsh interface ipv6 show route.`

Решение проблем с подключением

Опытные администраторы знают, что если не удастся подключиться к удаленному хосту, сначала следует проверить аппаратные каналы связи (проводные и беспроводные) и убедиться, что все устройства работают нормально. Если при этом причина проблемы не обнаружена, она может быть в неправильной настройке параметров IPSec или брандмауэра (например, в неверной настройке фильтров пакетов).

Для проверки и настройки политик IPSec можно использовать оснастку MMC **Управление политикой IP-безопасности** (IP Security Policies Manage-

ment), а для проверки и настройки фильтров пакетов IPv6 — оснастку **Брандмауэр Windows в режиме повышенной безопасности** (Windows Firewall With Advanced Security). Заметьте, что первая оснастка (рис. 2-9) позволяет создавать политики IPSec, действующие для компьютеров с Windows Vista и Windows Server 2008, но она не позволяет использовать новые алгоритмы безопасности и другие новые функции, доступные в Windows 7 и Windows Server 2008 R2. Для создания политик IPSec для этих компьютеров используйте вторую оснастку (рис. 2-10), которая, однако, не позволяет создавать политики, применяющиеся к ранним версиям Windows.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Использование оснасток Управление политикой IP-безопасности и Брандмауэр Windows в режиме повышенной безопасности

Подробнее о том, какую из этих оснасток использовать в разных ситуациях, см. по адресу [http://technet.microsoft.com/ru-ru/library/cc730656\(Ws.10\).aspx](http://technet.microsoft.com/ru-ru/library/cc730656(Ws.10).aspx).

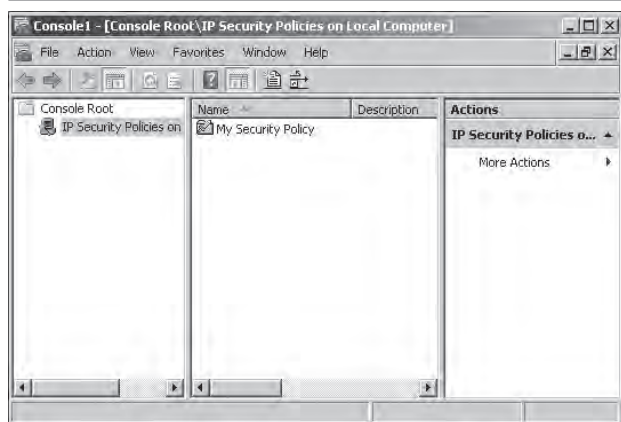


Рис. 2-9. Оснастка политики IP-безопасности

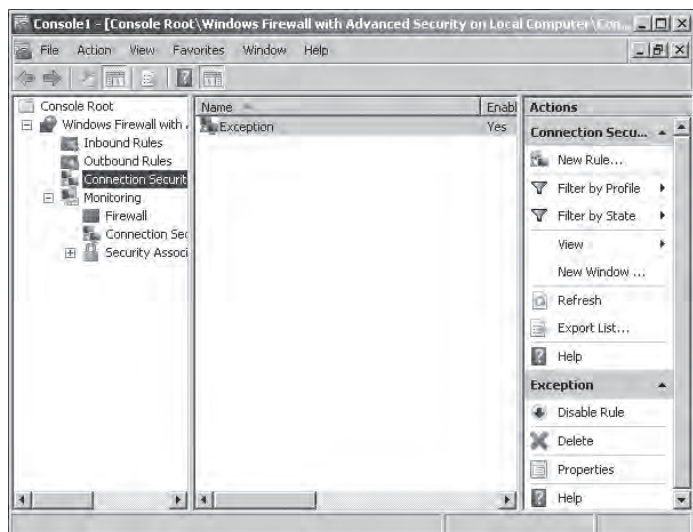


Рис. 2-10. Оснастка Брандмауэр Windows в режиме повышенной безопасности

ПРИМЕЧАНИЕ IPsec6

Утилита IPsec6 в Windows Server 2008 и 2008 R2 не реализована.

Локальный или удаленный конечный адрес может быть недоступен из-за неверных или отсутствующих маршрутов в локальной таблице маршрутизации IPv6. Чтобы просмотреть локальную таблицу маршрутизации IPv6 и убедиться, что в ней есть маршрут, соответствующий локальной подсети и шлюзу по умолчанию, используйте команду `netstat -r` или `netsh interface ipv6 show route`. Запомните, что команда `netstat -r` показывает таблицы маршрутизации IPv4 и IPv6.

Если есть несколько маршрутов по умолчанию с одинаковой метрикой, может потребоваться изменение конфигурации маршрутизатора IPv6, чтобы маршрут по умолчанию с наименьшей метрикой использовал интерфейс, подключающийся к сети с наибольшим числом подсетей. Изменить существующий маршрут можно командой `netsh interface ipv6 set route`. Для добавления маршрута в таблицу маршрутизации IPv6 используется команда `netsh interface ipv6 add route`. Команда `netsh interface ipv6 delete route` удаляет существующий маршрут. Для использования этих команд необходимо запустить командную строку от имени администратора.

Если локальный или удаленный хост доступен по адресу IPv4, но не по имени хоста, это может указывать на проблемы с DNS. Инструменты для настройки, проверки и отладки DNS, включая `dnscmd`, `ipconfig`, `netsh interface ipv6 show dnsservers`, `netsh interface ipv6 add dnsserver`, `nslookup` и средства с графическим интерфейсом, рассматриваются на занятии 2 этой главы.

Проверка подключений IPv6 на основе протокола TCP

Если установлен клиент `telnet`, можно проверить возможность TCP-подключения к порту TCP, выполнив команду `telnet` с конечным адресом IPv6 и номером порта TCP; например: `telnet fec0:0:0:fff::1 80`. Если TCP-подключение успешно установлено, появляется приглашение `telnet>`, после которого можно вводить команды `telnet`. Если подключение не удастся установить, появится сообщение об ошибке.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Установка клиента telnet

Подробнее о `telnet`, включая установку клиента `telnet`, можно узнать, выполнив поиск в справочной системе Windows Server 2008 или 2008 R2 по запросу «Telnet: часто задаваемые вопросы».

Настройка клиентов через DHCPv6

Настраивая hosts при помощи DHCPv6, можно выбрать настройку с ведением или без ведения базы данных. При настройке без ведения базы данных (`stateless`) адрес хоста не генерируется, а настраивается автоматически, но можно, например, указать адрес DNS-сервера. При настройке с ведением базы данных (`stateful`) указываются адреса хостов.

Независимо от выбора способа настройки, можно назначать адреса IPv6 DNS-серверов через параметр DHCPv6 для рекурсивных запросов DNS (параметр 0023). Если выбрать настройку с ведением базы данных, адреса IPv6 DNS-

серверов можно настраивать как параметры областей, так что разные области могут иметь разные DNS-серверы. Параметры областей переопределяют параметры сервера для соответствующей области. Это предпочитаемый способ настройки адресов IPv6 DNS-серверов, не настроенных через параметры представления маршрутизатора.

При использовании DHCPv6 хост IPv6 может получать префиксы подсетей и другие параметры конфигурации. В сетях Windows, работающих по протоколу IPv6, DHCPv6 обычно используется для автоматической настройки адресов IPv6 DNS-серверов.

В настоящее время при настройке области IPv6 указывается 64-разрядный префикс. По умолчанию DHCPv6 может выделять адреса хостов из 64-разрядного диапазона, соответствующего этому префиксу. Это делает возможным настройку адресов IPv6 на основе данных сетевого адаптера. Также можно настраивать диапазоны исключений. Так, если требуется выделять хостам адреса только из диапазона `fec0::0:0:0:1-fec0::0:0:0:fffe`, следует исключить адреса `fec0::0:0:1:1-fec0::ffff:ffff:ffff:fffe`.

Существует несколько параметров DHCPv6. Наверно, самый полезный параметр — указывающий DNS-сервер. Другие параметры связаны с совместимостью с другими системами, поддерживающими IPv6, такими как служба сетевой интеграции UNIX (NIS).

Служба DHCPv6 во многом аналогична DHCP. Например, параметры областей переопределяют параметры сервера, а запросы и подтверждения DHCPv6 могут проходить через маршрутизаторы с поддержкой BOOTP коммутаторы третьего уровня (почти все современные маршрутизаторы и коммутаторы действуют как агенты ретрансляции DHCP), так что сервер DHCPv6 может настраивать параметры клиентов из удаленной подсети.

СОВЕТ Подготовка к экзамену

Чтобы настроить сервер под управлением Windows Server 2008 или 2008 R2 в качестве агента ретрансляции DHCP, необходимо установить службу роли RRAS (службы маршрутизации и удаленного доступа).

Как и в случае с DHCP, можно реализовать правило 80/20 и создать для подсети, в которой находится сервер DHCPv6, область, содержащую 80% доступных для этой подсети адресов, а для удаленной подсети другую область, содержащую 20% доступных адресов. Аналогично настроенный сервер DHCPv6 в удаленной подсети обеспечит отказоустойчивость. Если любой из этих серверов выйдет из строя, хосты в обеих подсетях все равно будут получать параметры конфигурации.

Например, офис компании Tailspin Toys в Мельбурне имеет две частные виртуальные локальные сети (VLAN), имеющие следующие диапазоны адресов локального сайта:

- VLAN1: `fec0:0:0:aaaa::1-fec0:0:0:aaaa:fffe`;
- VLAN2: `fec0:0:0:aaab::1-fec0:0:0:aaab:fffe`.

Определены исключения, позволяющие назначать серверам статические адреса IPv6. В данном случае можно применить правило 80/20, настроив на DHCP-сервере в первой VLAN следующие области DHCPv6:

- fec0:0:0:aaaa::1-fec0:0:0:aaaa::cccb;
- fec0:0:0:aaab::cccc-fec0:0:0:aaab::fffe.

Затем следует настроить на DHCP-сервере во второй VLAN следующие области DHCPv6:

- fec0:0:0:aaab::1-fec0:0:0:aaab::cccb;
- fec0:0:0:aaaa::cccc-fec0:0:0:aaaa::fffe.

DHCP-серверы (особенно серверы с областями с 20% адресов) отлично подходят для виртуализации, так как выполняют ограниченные операции ввода-вывода. Кроме того, эту роль можно развертывать в режиме Server Core. Это особенно удобно в более сложных сетях.

ПРИМЕЧАНИЕ Виртуальные DNS-серверы

Как и DHCP-серверы, DNS-серверы, особенно дополнительные, — отличные кандидаты для виртуализации.

Например, компания Trey Research имеет один сайт, включающий пять зданий, подключенных оптоволокном к коммутатору третьего уровня, создающему виртуальную сеть для каждого здания. Сеть главного офиса, VLAN1, включает большинство компьютеров компании. Большинство оставшихся компьютеров входит в VLAN3. Сети VLAN2, VLAN4 и VLAN5 включают лишь небольшое число компьютеров.

В этом случае DHCP-сервер в VLAN1 может отвечать за 80% диапазона адресов VLAN1. В этой же VLAN можно создать виртуальный DHCP-сервер, отвечающий за 20% адресов сетей VLAN2-VLAN5. В VLAN3 можно настроить DHCP-сервер, отвечающий за 80% адресов VLAN2-VLAN5, и виртуальный сервер с 20% адресов VLAN1. Если любой из этих серверов выйдет из строя, хосты во всех VLAN продолжают получать параметры конфигурации через DHCP.

ПРИМЕЧАНИЕ Правило 80/20

Правило 80/20 обычно применяется в пределах сайта, поскольку каналы связи с глобальными сетями (WAN), проходящие через маршрутизаторы сторонних организаций, могут не пропускать трафик DHCP. Для обеспечения отказоустойчивости DHCP при помощи правила 80/20 потребуется минимум два DHCP-сервера для каждого сайта.

Планирование сети на основе протокола IPv6

Настройка и реализация IPv6 относительно проста, чего нельзя сказать о планировании сети на основе IPv6. Каждый конкретный случай имеет свои особенности, но можно рассматривать несколько общих ситуаций. Может потребоваться развернуть сеть IPv6 совместно с существующей сетью IPv4. Могут иметься приложения, требующие IPv6, хотя сеть работает на основе IPv4. Можно спроектировать новую сеть или перепланировать существующую, чтобы она работала преимущественно на основе протокола IPv6. Сеть может проектироваться для крупной многонациональной организации с множеством сайтов и тысячами пользователей или для небольшой компании с двумя офисами.

Независимо от ситуации, потребуется сохранить старую функциональность и возможность использования IPv4. Даже в новой сети IPv6 вряд ли можно будет совершенно избавиться от IPv4, по крайней мере, в настоящее время.

Анализ требований к оборудованию

В начале проектирования следует определить и проанализировать необходимые компоненты сетевой инфраструктуры. Аппаратные компоненты могут быть следующими:

- маршрутизаторы;
- коммутаторы третьего уровня;
- принтеры;
- факсы;
- брандмауэры;
- оборудование для защиты от вторжения;
- аппаратные балансировщики нагрузки;
- кластеры серверов для балансировки нагрузки;
- точки входа и выхода виртуальных частных сетей (VPN);
- серверы и службы;
- оборудование для соединения сетей;
- интеллектуальные сетевые адаптеры.

Это не строго определенный список, и в зависимости от конкретной ситуации могут потребоваться другие устройства. Какие устройства будут хранить, отображать и позволять вводить IP-адреса? Можно ли обновить все необходимое оборудование, чтобы оно поддерживало IPv6? Если нет, как можно решить эту проблему? Если требуется заменить оборудование, есть ли деньги и время для этого?

Анализ требований к программному обеспечению

С точки зрения программного обеспечения, на управление сетью больше всего влияет версия используемых IP-адресов, хотя это может повлиять и на некоторые бизнес-приложения (LOB). Часто требуется учитывать требования и совместимость следующих компонентов сети IPv6:

- средства управления сетевой инфраструктурой, такие как WINS;
- системы управления сетью, например, системы на основе протокола SNMP;
- системы управления производительностью;
- высокоуровневые приложения управления сетью (обычно ПО сторонних производителей);
- средства управления конфигурацией, такие как DHCP и DHCPv6;
- средства управления и внедрения политики безопасности;
- бизнес-приложения;
- средства перехода.

Использование средств перехода предполагает необходимость определения стратегии перехода (не требуется только в новых сетях IPv6). Стратегии перехода (см. далее на этом занятии) во многом зависят от планируемого сценария и доступности стеков IPv4 и IPv6. Если в сети есть старые компоненты, не поддерживающие IPv6, необходимо продумать, как будет обеспечиваться их поддержка во время перехода, и потребуется ли поддержка двух стеков после за-

вершения перехода. Администратор должен обеспечить взаимодействие компонентов IPv4 и IPv6.

Первым этапом управления конфигурацией может быть выбор между настройкой с ведением базы данных и без нее. При использовании IPv6 каждый компонент сети может иметь собственный глобальный адрес одноадресной рассылки. Безопасность обеспечивается брандмауэрами, фильтрами вирусов, фильтрами спама, IP-фильтрацией и всеми остальными обычными средствами. Протокол IPSec обеспечивает сквозное шифрование. В сетях IPv6, как и в сетях IPv4, можно настраивать периферийные зоны. DHCPv6 в режиме без ведения базы данных позволяет настраивать параметры (например, DNS-серверов), не настраиваемые посредством представления маршрутизатора. В любом случае, необходимо убедиться, что провайдер услуг Интернета поддерживает IPv6 и имеет диапазон адресов IPv6.

Интеграция DHCP с NAP

Можно повысить безопасность сети, интегрировав DHCP и DHCPv6 с платформой NAP (защита доступа к сети). NAP предоставляет компоненты применения политики, помогающие обеспечить соответствие компьютеров, взаимодействующих по сети или подключающихся к ней, требованиям, определенным администратором. Если компьютеры не соответствуют этим требованиям, им предоставляется ограниченный доступ к ресурсам, необходимым для обновления компьютеров в соответствии с предъявляемыми требованиями. При интеграции DHCP с NAP компьютер должен соответствовать предъявляемым требованиям, чтобы получить от DHCP-сервера конфигурацию IP-адреса с неограниченным доступом. Компьютеры, не соответствующие требованиям, получают конфигурацию IP-адреса, разрешающую доступ только к ограниченной сети. Использование DHCP гарантирует проверку требований политики каждый раз, когда клиент DHCP пытается получить или обновить конфигурацию IP-адреса. Кроме того, при этом выполняется активный мониторинг работоспособности клиентов NAP, и если клиент перестает удовлетворять требованиям, то при обновлении конфигурации IP-адреса разрешается только доступ к ограниченной сети.

При планировании интеграции DHCP с NAP необходимо решить, будет ли применение политики выполняться во всех областях DHCP, выбранных областях DHCP или не будет выполняться совсем. Кроме того, необходимо выбрать, какой профиль NAP будет использоваться для применения политики. Наконец, необходимо определить, каким будет поведение DHCP-сервера, если сервер сетевой политики (NPS) недоступен. В зависимости от настройки, DHCP-сервер может предоставлять полный доступ, предоставлять ограниченный доступ или уничтожать пакеты, если сервер NPS недоступен.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ NAP

Подробнее о NAP см. по адресу <http://technet.microsoft.com/en-us/network/bb545879.aspx> (на англ. языке).

Администратор может решить, что предоставление глобальных адресов односторонней рассылки всем компонентам сети IPv6 рискованно с точки зрения безопасности. Этот вопрос активно обсуждается в сетевом сообществе и выходит за рамки нашей книги. Приняв такое решение, вы можете использовать во внутренних подсетях адреса IPv6 локального сайта, если ваши серверы NAT поддерживают IPv6. Можно использовать настройку при помощи DHCP с ведением базы данных. Если маршрутизаторы или коммутаторы третьего уровня могут передавать трафик DHCP, можно применять в подсетях или виртуальных сетях правило 80/20, чтобы настройка выполнялась даже после выхода из строя одного сервера DHCP.

Приняв основные решения насчет сетевой инфраструктуры и стратегии перехода и выяснив, может ли существующая (или предполагаемая новая) сеть поддерживать IPv6, можно переходить к решению других вопросов. Например, необходимо обеспечить работоспособность имеющейся инфраструктуры IPv4 во время перехода, если только не создается новая сеть IPv6. С учетом этого требования может быть невозможным развертывание IPv6 во всех сегментах сети одновременно.

С другой стороны, если единственным требованием является развертывание определенных приложений IPv6 (например, обеспечивающих прямое взаимодействие узлов), развертывание IPv6 может быть ограничено до минимума, необходимого для их функционирования.

Документирование требований

Дальнейшие действия — определить и документировать, что именно требуется. Например, список вопросов может быть следующим:

- Требуется ли внешняя связь (например, с Интернетом IPv6)?
- Сколько сайтов имеет организация — один или несколько? Если несколько, то каково их географическое положение, и как обеспечивается безопасность передачи данных между ними?
- Какова текущая структура межсетевого взаимодействия по протоколу IPv4?
- Какой план назначения адресов IPv6 поддерживается провайдером?
- Какие службы IPv6 предоставляются провайдером?
- Как должно выполняться делегирование выделения префиксов в сети предприятия?
- Требуются ли протоколы маршрутизации IPv6 для внешних и внутренних сайтов? Если требуются, то какие?
- Использует ли предприятие внешние серверы (например, серверы, расположенные у провайдера)?
- Можно ли использовать IPv6 по тем же каналам связи, что и IPv4?
- Какие приложения требуют поддержки IPv6, и можно ли их обновить для обеспечения такой поддержки? Должны ли эти приложения поддерживать и IPv6, и IPv4?
- Поддерживают ли платформы предприятия оба протокола — IPv6 и IPv4? Установлен ли протокол IPv6 по умолчанию на серверах и клиентах?
- Доступна ли система NAT v4-v6, и имеют ли приложения какие-либо проблемы с ее использованием?

- Требуются ли приложения глобально маршрутизируемые IP-адреса?
- Будут ли использоваться адреса многоадресной и одноадресной передачи?
Также нужно проанализировать и документировать рабочие процедуры и структуру поддержки. Для этого потребуется следующая информация:
- Кто владеет сетью? Например, поддерживается ли сеть собственными сотрудниками или сторонними организациями?
- Существует ли подробная база данных ресурсов?
- Поддерживает ли организация работу из дома? Если да, то как?
- Используются ли в сети IPv6 мобильные устройства? Если нет, то требуется ли их поддержка?
- Какова политика предприятия относительно географической нумерации?
- Имеют ли разные сайты предприятия разных провайдеров?
- Какова текущая политика QoS IPv4 (если не проектируются новая сеть, поддерживающая только IPv6)? Будет ли она изменена после внедрения IPv6?
- Каковы планы по обучению технического персонала использованию IPv6?

Сбор и анализ этой информации займет много времени. Однако без этого не будут известны точные требования к внедрению IPv6, реализация проекта продлится гораздо дольше, а результат будет хуже. Собрав эту информацию, можно планировать задачи, которые необходимо выполнить, и прогнозировать результат. Это даст более точное представление о длительности и стоимости проекта, а также о необходимости его разбиения на этапы.

Следующий шаг — составить и реализовать план проекта. Планирование проектов выходит за рамки этой книги. Однако учтите, что нельзя игнорировать задачи, которые могут показаться несущественными или несрочными. Одна из таких задач — обучение техперсонала. Каждая часть итогового плана важна, и результат будет далеко не оптимальным, если не реализовать каждый аспект. В худшем случае проект будет полностью провален из-за неучтенного компонента.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Сети IPv6

Подробные сведения о планировании сетей IPv6 с примерами можно найти в RFC 4057 по адресу <http://www.ietf.org/rfc/rfc4057>.

Резюме

- Протокол IPv6 поддерживает адреса многоадресной, одноадресной и произвольной рассылки. Адреса одноадресной рассылки могут быть глобальными, локального сайта, локальной связи или особыми. Поддерживаются также сопоставленные адреса IPX и NSAP.
- IPv6 полностью поддерживается в Windows Server 2008 и 2008 R2. Этот протокол позволяет решить проблемы, присущие IPv4, такие как недостаток адресного пространства.
- Структура адресов IPv6 обеспечивает обратную совместимость с адресами IPv4. Стратегии перехода включают использование двух стеков, настройку туннелирования, автоматическое туннелирование, 6to4, Teredo и ISATAP.

- Адреса IPv6 можно настраивать с ведением базы данных (DHCPv6) и без ведения базы данных (автонастройка). DHCPv6 можно использовать в режиме без ведения базы данных для настройки DNS-серверов совместно с автоматической настройкой хостов.
- Для настройки и решения проблем с IPv6 используются утилиты `ping`, `ipconfig`, `tracert`, `pathping` и `netsh`. Настраивать параметры IPv6 можно также при помощи графического интерфейса — окна свойств TCP/IPv6.

Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных на занятии 1. Эти вопросы предоставлены также в электронном виде на прилагаемом к книге компакт-диске.

ПРИМЕЧАНИЕ Ответы

Ответы на вопросы и пояснения к их вариантам размещены в разделе «Ответы» в конце книги.

1. Какой тип адресов IPv6 эквивалентен открытым адресам IPv4 для одноадресной рассылки?
 - a. Локального сайта.
 - b. Глобальные.
 - c. Локальной связи.
 - d. Специальные.
2. Узел имеет адрес локальной связи IPv6 `fe80::6b:28c:16a7:d43a`. Какой адрес запроса узла соответствует ему?
 - a. `ff02::1:ffa7:d43a`.
 - b. `ff02::1:ff00:0:16a7:d43a`.
 - c. `fec0::1:ffa7:d43a`.
 - d. `fec0::1:ff00:0:16a7:d43a`.
3. Какой протокол использует сообщения ICMPv6 для управления взаимодействием соседних узлов?
 - a. ARP.
 - b. EUI-64.
 - c. DHCPv6.
 - d. ND.
4. В какой стратегии перехода с IPv4 на IPv6 используются предварительно настроенные туннели и выполняется инкапсуляция пакетов IPv6 в пакеты IPv4?
 - a. Использование настроенного туннелирования.
 - b. Использование двух стеков.
 - c. ISATAP.
 - d. Teredo.
5. Какая команда позволяет вручную настраивать адреса IPv6 на указанном интерфейсе?

- a. netsh interface ipv6 show address.
 - b. netsh interface ipv6 add address.
 - c. netsh interface ipv6 set interface.
 - d. netsh interface ipv6 set address.
6. Trey Research — новаторская исследовательская организация, гордящаяся тем, что идет в ногу с развитием технологий. У компании есть 82 клиентских ПК, работающих под управлением Windows 7 Enterprise Edition. Все серверы, включая контроллер домена, недавно обновлены до Windows Server 2008 R2 Enterprise Edition. Сайт компании включает два здания, соединенных оптоволоконным кабелем. Каждое здание имеет собственную VLAN, а периферийная зона компании находится в отдельной VLAN. Все клиенты компании получают конфигурацию IPv4 через DHCP. Для обеспечения отказоустойчивости DHCP применяется правило 80/20. Все интерфейсы маршрутизаторов, серверы, сетевые принтеры и сетевые проекторы настроены вручную. Компания имеет открытые адреса IPv4 класса C и не видит необходимости в реализации NAT. Используется система управления сетью на основе SNMP. Используется несколько высокоуровневых графических приложений, а также бизнес-приложения и пакет Microsoft Office 2010. Компания хочет внедрить конфигурацию IPv6 и иметь доступ к Интернету IPv6. Провайдер компании, как и все сетевое оборудование, полностью поддерживает IPv6. Какие из перечисленных пунктов следует включить в план внедрения IPv6 в компании Trey Research? (Каждый ответ является частью решения. Выберите четыре.)
- a. Использовать стратегию перехода с двумя стеками.
 - b. Использовать стратегию перехода с настроенным туннелированием.
 - c. Настроить для хостов внутренней сети адреса локального сайта для одноадресной рассылки.
 - d. Настроить для хостов внутренней сети глобальные адреса одноадресной рассылки.
 - e. Убедиться, что серверы и клиенты поддерживают IPv6.
 - f. Убедиться, что сетевые проекторы и сетевые принтеры поддерживают IPv6.
 - g. Убедиться, что система управления сетью совместима с IPv6.
 - h. Убедиться, что графические приложения совместимы с IPv6.

Занятие 2. Планирование DNS

Как опытный администратор, вы должны иметь опыт работы с DNS и динамической DNS (DDNS) и быть знакомы с именами NetBIOS, расширенным пользовательским интерфейсом NetBIOS (NetBEUI) и WINS. Если у вас нет такого опыта, то на этом занятии вы познакомитесь с этими технологиями. Мы рассмотрим усовершенствования, появившиеся в этих технологиях (особенно в DNS) в Windows Server 2008 и 2008 R2 и обсудим планирование инфраструктуры разрешения имен для сети предприятия.

Один из первых вопросов при планировании — будет ли использоваться WINS для разрешения имен NetBIOS. Когда Microsoft представила DDNS, предполагалось, что эта система заменит WINS, но WINS все еще используется во многих сетях и поддерживается в Windows Server 2008 и 2008 R2. Однако IPv6 не поддерживает WINS. Microsoft описывает WINS как устаревающую технологию и представляет зону DNS глобальных имен GlobalNames для разрешения однокомпонентных имен в крупных сетях, где служба WINS не развернута. Если вы не используете WINS, можете отключить в своей сети протокол NetBIOS поверх TCP/IP (NetBT).

При планировании инфраструктуры DNS необходимо решить, в каких случаях будут использоваться различные зоны DNS — интегрированные с доменными службами Active Directory (AD DS), стандартные основные, дополнительные, зоны-заглушки, зоны обратного просмотра и зоны GlobalNames. Необходимо спланировать пересылку DNS и определить, когда будет использоваться условная пересылка, особо важная для окружений с несколькими лесами AD DS в одной интрасети. Сети предприятий часто включают DNS-серверы, произведенными не Microsoft, или требуют интеграции с ними, и вы должны знать, как DNS Microsoft взаимодействует, например, с серверами BIND (Berkeley Internet Daemon). Windows Server 2008 и 2008 R2 (а также Windows Vista и Windows 7) по умолчанию поддерживают протокол IPv6, и вам необходимо понимать и уметь использовать записи IPv6 в DNS. Настройка зоны обратного просмотра IPv6 — сложная процедура, которую мы рассмотрим в одном из практических упражнений этой главы.

Изучив материал этого занятия, вы сможете:

- ✓ Учитывать функции DNS Windows Server 2008 и 2008 R2 при планировании инфраструктуры разрешения имен.
- ✓ Использовать усовершенствованные функции DNS Windows Server 2008 и 2008 R2 в процессе планирования.
- ✓ Настраивать статические записи DNS IPv6.
- ✓ Настраивать зону обратного просмотра IPv6.
- ✓ Администрировать DNS при помощи оснастки MMC и утилит командной строки.

Продолжительность занятия — примерно 45 мин.

Планирование DNS Windows Server 2008 и 2008 R2

Система доменных имен (DNS) разрешает имена хостов в IP-адреса и может разрешать IP-адреса в имена хостов, если настроены зоны обратного просмотра DNS. Разрешение имен важно для IPv4, поскольку адреса IPv4 сложно запоминать, и мы чаще всего используем имена хостов или полные доменные имена (fully qualified domain name, FQDN), такие как Интернет-адреса *www.litware.com*. Запомнить адреса IPv6 почти невозможно, поэтому в сегменте IPv6 всемирной сети (в Интернете IPv6) разрешение имен имеет еще большее значение. В этом разделе рассматриваются улучшения в системе DNS, появившиеся в Windows Server 2008 и 2008 R2, и рассказывается, как DNS работает с адресами IPv6.

В Windows Server 2008 и 2008 R2 роли DNS-сервера сохранили функции, имевшиеся в Windows Server 2003, включая динамическую настройку и добавочные передачи зон, и приобрели несколько новых функций и значительных улучшений.

Служба DNS Windows Server 2008/2008 R2 в сети Windows поддерживает AD DS. Если вы устанавливаете на сервер роль AD DS или выполняете команду `dcpromo`, а DNS-сервер, удовлетворяющий требованиям AD DS, не обнаружен, вы можете установить и настроить DNS-сервер и (по умолчанию) автоматически создать зону DNS, интегрированную в AD DS. Обычно это выполняется при установке первого контроллера домена в лесу.

Раздел — это контейнер данных в AD DS, хранящий данные для репликации. Данные зон DNS можно хранить в разделе каталога домена или разделе каталога приложений. Администратор может указать, в каком разделе будет храниться зона. Этот выбор определяет набор контроллеров домена, на которые будут реплицироваться данные этой зоны. Репликация DNS выполняется между всеми контроллерами домена, указанными в области репликации в разделе каталога приложений DNS.

Microsoft рекомендует использовать службу DNS-сервера Windows Server 2008, хотя при развертывании AD DS можно использовать и другие типы DNS-серверов. Разделы позволяют реплицировать на другие DNS-серверы только обновления зон DNS. Добавочные передачи зон рассматриваются далее на этом занятии.

СОВЕТ Подготовка к экзамену

Как опытный специалист по сетям, вы должны быть знакомы с главными и подчиненными, основными и дополнительными, а также полномочными серверами именования. Вопросы экзамена 70-646 относятся к планированию инфраструктуры, а не к настройке одиночного сайта. Например, если DNS-серверы, используемые клиентами, указываются при помощи DHCP, следует ли настроить DNS-сервер в офисе филиала как основной, а DNS-сервер в главном офисе как дополнительный? Помните, что локальный сервер DNS обычно является основным и полномочным.

ПРИМЕЧАНИЕ DNS-серверы с файловой поддержкой

DNS-сервер с файловой поддержкой — DNS-сервер, не интегрированный с AD DS. Такой сервер можно установить на любом автономном компьютере. Обычно такие серверы используются в периферийных зонах, где использование рядовых серверов (и, особенно, контроллеров домена) может представлять риск для безопасности. Серверы с файловой поддержкой обычно содержат стандартные основные или дополнительные зоны, хотя могут содержать и зоны-заглушки или быть только кэширующими серверами, не содержащими каких-либо зон DNS.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Определение требуемого числа серверов и их расположения

Подробнее о том, как определить требуемое число DNS-серверов и как спланировать их расположение, см. по адресу <http://technet.microsoft.com/ru-ru/library/cc732715.aspx>.

Соответствие стандартам

Роль DNS-сервера в Windows Server 2008 и 2008 R2 соответствует всем RFC, определяющим и стандартизирующим протокол DNS. Эта роль использует стандартный файл данных DNS и стандартные форматы записей ресурсов и может успешно работать с большинством других реализаций DNS-серверов, например, серверами BIND. Windows Server 2008/2008 R2 полностью поддерживает протокол динамического обновления, определенный в RFC 2136.

Настройка DNS Windows Server 2008 и 2008 R2

Благодаря тесной интеграции с другими службами Windows, включая AD DS, WINS (если включена), DHCP и DHCPv6, служба DDNS Windows Server 2008 почти не требует ручной настройки, а иногда не требует совсем. Компьютеры, на которых запущена служба DNS-клиента, регистрируют свои имена хоста, адреса IPv4 и IPv6 (но не адреса локальной связи IPv6) динамически. Службы DNS-сервера и DNS-клиента можно настроить для выполнения безопасного динамического обновления. Это гарантирует, что только аутентифицированные пользователи, обладающие соответствующими правами, могут обновлять записи ресурсов на DNS-сервере. На рис. 2-11 показано, как настроить зону, чтобы разрешить только безопасные динамические обновления.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Протокол динамического обновления

Подробнее о протоколе динамического обновления см. по адресам <http://www.ietf.org/rfc/rfc2136.txt> и <http://www.ietf.org/rfc/rfc3007>.

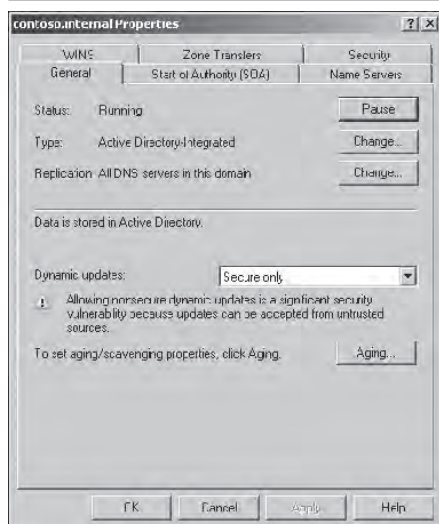


Рис. 2-11. Разрешение только безопасных динамических обновлений

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Развертывание безопасных DNS-серверов

О развертывании безопасных DNS-серверов см. по адресу [http://technet.microsoft.com/en-us/library/cc772661\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc772661(WS.10).aspx).

ПРИМЕЧАНИЕ Безопасные динамические обновления

Безопасные динамические обновления доступны только для зон, интегрированных с AD DS.

Использование зон-заглушек

Зона-заглушка — копия зоны, содержащая только записи ресурсов, необходимые для определения полномочных DNS-серверов для этой зоны. Зоны-заглушки позволяют DNS-серверам, содержащим родительские зоны, определять полномочные DNS-серверы для дочерних зон, помогая обеспечивать эффективное разрешение имен. Зону-заглушку можно создать при помощи мастера создания зон (рис. 2-12).

Зоны-заглушки можно использовать, когда серверы именования в целевой зоне находятся в процессе перехода, например, если часть сети или вся сеть компании переходит на новые IP-адреса, и разрешение имен проблематично. Рассмотрим пример. Компания Contoso недавно приобрела торговую компанию Litware. Contoso имеет домен Windows Server 2008 R2. Litware имеет домен Windows 2000 Server, работающий в смешанном режиме, а также автономные DNS-серверы Windows NT 4.0 и серверы BIND для разрешения имен. В Contoso решили, что имя Litware больше не будет использоваться, а компания Litware станет подразделением Contoso, отвечающим за продажи, и получит поддомен sales.contoso.com. Вы планируете создать новый поддомен sales.contoso.com с новой системой разрешения имен и структуру IP-адресации, соответствующую политике Contoso.

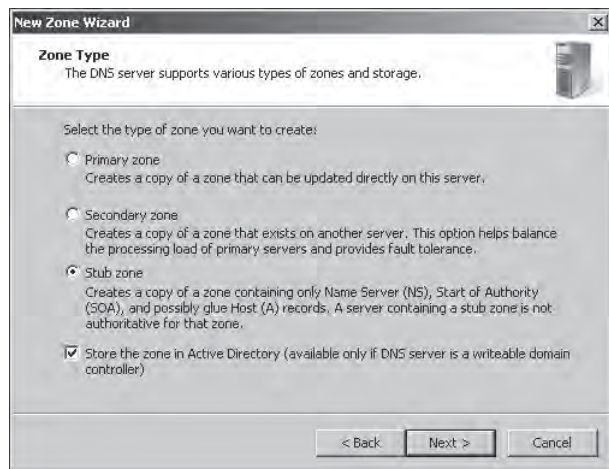


Рис. 2-12. Создание зоны-заглушки

В этом случае следует включить в домен contoso.com зону-заглушку, содержащую записи ресурсов, которые указывают полномочные DNS-серверы для поддомена sales.contoso.com. Когда домен sales.contoso.com будет создан, а имена и IP-адреса его DNS-серверов изменятся, зону-заглушку в домене contoso.com можно будет легко изменить.

Зоны-заглушки обычно используются для хранения записей DNS-серверов в делегированных зонах. В этом случае запись сервера имен (NS) в родитель-

ской зоне указывает сервер имен, полномочный для делегированной зоны. Например, сервер имен для зоны contoso.com может делегировать полномочия на зону sales.contoso.com DNS-серверу, расположенному в этой делегированной зоне. Зоны-заглушки можно использовать для поддержания актуальности информации в делегированной зоне, повышения эффективности разрешения имен и упрощения администрирования DNS.

ПРИМЕЧАНИЕ Записи делегирования и связывающие записи в Windows Server 2008 и 2008 R2

Роль DNS-сервера в Windows Server 2008 и 2008 R2 автоматически добавляет записи делегирования и связывающие записи, когда выполняется делегирование поддомена. Делегированные серверы имен перечисляются по имени, а не IP-адресу. Таким образом, серверу разрешения имен требуется выяснить IP-адрес сервера, с которым связано имя, и выполнить для этого еще один DNS-запрос. Это может привести к круговой зависимости, в которой сервер имен обращается к записи NS, ссылающейся на сам этот сервер. Чтобы этого не происходило, сервер имен, выполняющий делегирование, может предоставить IP-адрес следующего сервера именования. Такая запись называется *связывающей записью*.

Пересылка DNS

DNS-серверы, которым другие DNS-серверы пересылают запросы, называются *серверами пересылки*. Если DNS-сервер не имеет в своей базе данных записи для удаленного хоста, указанного в запросе клиента, он может вернуть клиенту адрес DNS-сервера, который может иметь эту информацию, или же самостоятельно отправить запрос другому DNS-серверу. Этот процесс выполняется рекурсивно, пока клиент не получит IP-адрес, или пока DNS-сервер не определит, что запрашиваемое имя не может быть разрешено.

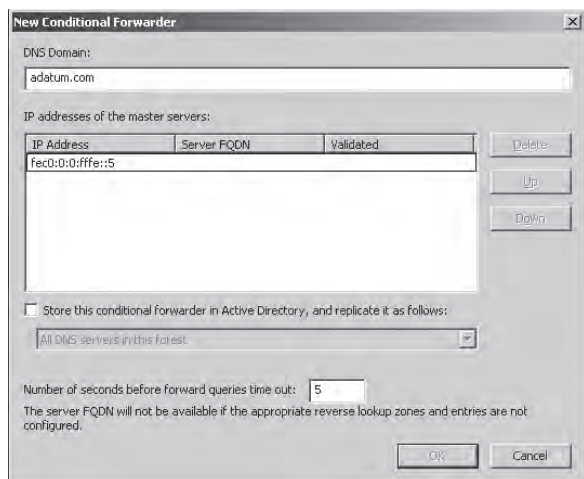


Рис. 2-13. Назначение сервера условной пересылки

В Windows Server 2008 служба DNS-сервера использует *серверы условной пересылки* для расширения стандартной конфигурации пересылки. Сервер условной пересылки — это DNS-сервер, пересылающий DNS-запросы в соответствии с именем домена DNS в запросе. Например, можно настроить DNS-

сервер так, чтобы при получении любых запросов на разрешение имен, оканчивающихся на *adatum.com*, он пересылал их на IP-адрес одного или нескольких DNS-серверов, являющихся полномочными для домена *adatum.com*. Эта функция особенно полезна во внешних сетях предприятия, в которых несколько организаций и доменов обращаются к общей частной объединенной сети.

СОВЕТ Подготовка к экзамену

В Windows Server 2008 и 2008 R2 записи условной пересылки можно хранить в AD DS и реплицировать на все DNS-серверы леса, все DNS-серверы домена или все контроллеры домена.

На рис. 2-13 показано диалоговое окно, используемое для создания сервера условной пересылки. Создать такой сервер в тестовой сети не получится, если в ней только один DNS-сервер.

Репликация зон

В Windows Server 2008 и 2008 R2 зоны DNS можно реплицировать между DNS-серверами для обеспечения отказоустойчивости и повышения эффективности разрешения имен. Передача зон обеспечивает репликацию и синхронизацию зон. Если добавить в сеть новый DNS-сервер и настроить его как дополнительный DNS-сервер для существующей зоны, он выполнит полную передачу зоны, чтобы получить доступную только для чтения копию записей ресурсов этой зоны. Любые изменения, внесенные в полномочную зону после этого, реплицируются в дополнительную зону. В Windows Server 2003 появилась добавочная репликация зон, при которой реплицируются только изменения, произошедшие в полномочной зоне. В Windows Server 2008 и 2008 R2 такая возможность тоже поддерживается. До выхода Windows Server 2003 для репликации на дополнительный DNS-сервер любых изменений, произошедших в полномочной зоне DNS, приходилось выполнять полную репликацию этой зоны. Добавочная передача позволяет дополнительному серверу получать только те изменения, которые необходимы для синхронизации его копии зоны с исходной зоной, которая может быть основной или дополнительной копией зоны, поддерживаемой другим DNS-сервером.

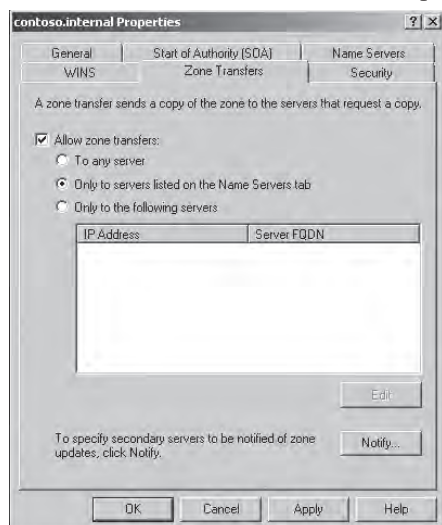


Рис. 2-14. Настройка передачи зон

Администратор может разрешить передачу зон на любой DNS-сервер, только на указанные DNS-серверы и на DNS-серверы, перечисленные на странице серверов имен (любые серверы, зарегистрировавшие запись NS). На рис. 2-14 показана настройка зоны DNS для разрешения передачи зон на DNS-серверы, перечисленные на странице серверов имен.

Записи DNS

Как опытный специалист по сетям, вы должны быть знакомы со стандартными типами записей DNS: хост IPv4 (A), SOA, PTR, CNAME, NS, MX, SRV и т.д. Если вы обеспечивали совместимость с системами DNS, работающими не на основе Windows, вы могли использовать записи DNS другого типа, такие как записи файловой системы AFSDB (Andrew File System Database) и адреса асинхронного режима передачи (ATM). На рис. 2-15 показаны некоторые типы записей, доступные в DNS Windows Server 2008 и 2008 R2. Если требуется создать запись IPv6 для клиента, который не может зарегистрировать себя в AD DS, нужно создать запись AAAA (четыре A) вручную.

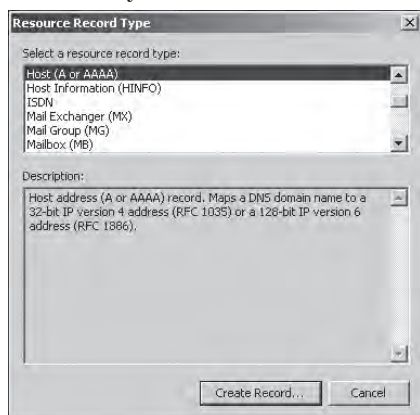


Рис. 2-15. Типы записей DNS

Администрирование DNS

Для управления и настройки службы DNS-сервера можно использовать оснастку MMC **Диспетчер DNS** (DNS Manager). В Windows Server 2008 и 2008 R2 доступны также мастера настройки, позволяющие выполнять распространенные задачи администрирования серверов. На рис. 2-16 показано окно Диспетчера DNS с записями хостов IPv4 и IPv6, динамически зарегистрированными в DNS.

В Windows Server 2008 и 2008 R2 имеются утилиты командной строки, облегчающие управление и поддержку DNS-серверов и клиентов. Утилита `dnscmd` используется для настройки и администрирования записей IPv4 и IPv6 и создания зон обратного просмотра. На рис. 2-17 показаны параметры командной строки для этой утилиты. Обычно для использования `dnscmd` требуется запустить командную строку от имени администратора.

Команда `ipconfig` позволяет просматривать конфигурации интерфейсов адаптера. Конфигурации IPv4 и IPv6 можно освобождать командами `ipconfig /release` и `ipconfig /release6`, соответственно. Обновлять конфигурации можно командами `ipconfig /renew` и `ipconfig /renew6`. Хотя обычный пользователь может ис-

пользовать команды `ipconfig` и `ipconfig /all` для просмотра конфигурации, для использования других команд утилиты `ipconfig` обычно требуются права администратора.

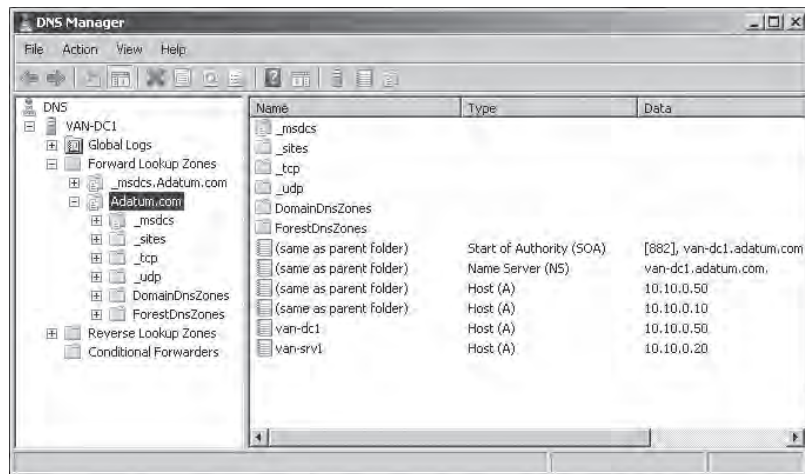


Рис. 2-16. Диспетчер DNS

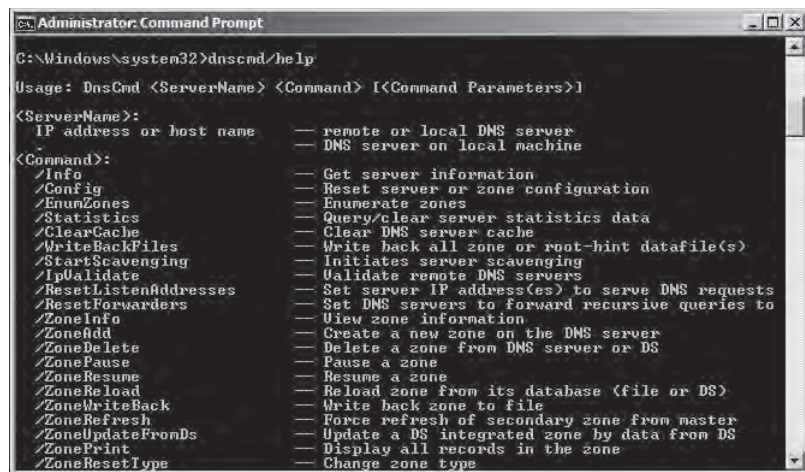


Рис. 2-17. Утилита dnscmd

Если клиент отправляет запрос на DNS-сервер, который не может разрешить имя удаленного хоста, в кэш DNS на клиенте сохраняется информация о том, что разрешение не выполнено. Эта функция называется кэшированием отрицательных ответов (negative caching). Она предотвращает непрерывное обращение клиентов к DNS-серверам в попытках разрешить неразрешимые имена хостов. Однако есть и недостаток: если имя не удастся разрешить из-за проблемы с сервером, которая затем устраняется, клиент по-прежнему не может получить разрешенное имя хоста, если не удалить соответствующие данные из кэша. В такой ситуации можно использовать на клиенте команду `ipconfig /flushdns` для немедленной очистки кэша. Обычно кэш обновляется каждые 15 минут, так что эта проблема решится сама собой, даже если администратор не выполнит очистку.

Новому клиенту в сети требуется некоторое время для регистрации в динамической DNS. Этот процесс можно ускорить, выполнив команду `ipconfig /registerdns`. Просмотреть информацию о DNS можно командой `ipconfig /displaydns`. Команды `ipconfig`, отображающие информацию, можно выполнять без повышенных привилегий. Команды для настройки интерфейсов, освобождения конфигурации, очистки кэша и регистрации клиента должны выполняться от имени администратора. На рис. 2-18 показаны параметры команды `ipconfig`.

```

C:\Windows\system32>ipconfig /?

USAGE:
    ipconfig [/allcompartments] [/? | /all |
        /renew [adapter1] /release [adapter1] |
        /renew6 [adapter1] /release6 [adapter1] |
        /flushdns | /displaydns | /registerdns |
        /showclassid adapter |
        /setclassid adapter [classid1] |
        /showclassid6 adapter |
        /setclassid6 adapter [classid1] ]

where
    adapter      Connection name
                  (wildcard characters * and ? allowed, see examples)

Options:
    /?           Display this help message.
    /all         Display full configuration information.
    /release     Release the IPv4 address for the specified adapter.
    /release6    Release the IPv6 address for the specified adapter.
    /renew       Renew the IPv4 address for the specified adapter.
    /renew6      Renew the IPv6 address for the specified adapter.
    /flushdns    Purges the DNS Resolver cache.
    /registerdns Refreshes all DHCP leases and re-registers DNS names.
    /displaydns  Display the contents of the DNS Resolver Cache.
    /showclassid Displays all the dhcp class IDs allowed for adapter.
    /setclassid  Modifies the dhcp class id.
    /showclassid6 Displays all the IPv6 DHCP class IDs allowed for adapter.
    /setclassid6 Modifies the IPv6 DHCP class id.
  
```

Рис. 2-18. Параметры утилиты `ipconfig`

Проверьте себя

1. Какая утилита командной строки позволяет создавать зоны обратного просмотра?
2. Какие команды освобождают и обновляют нестатическую конфигурацию IPv6?

Ответ

1. `dnscmd`.
2. `ipconfig /release6` и `ipconfig /renew6`.

Если клиент не может получить разрешенное имя от DNS-сервера, а команда `ping` показала, что связь между сервером и хостом есть, можно использовать команду `nslookup`, чтобы выяснить, есть ли на сервере служба DNS. Если, например, выполнить на клиенте VAN-SRV1 в тестовой сети команду `nslookup VAN-DC1`, будет проверена связь с сервером VAN-DC1.adatum.com. На том же клиенте можно выполнить команду `nslookup adatum.com`, чтобы получить адреса IPv4 DNS-серверов домена `adatum.com`.

Если на VAN-SRV1 выполнить команду `nslookup`, а затем после приглашения `nslookup>` ввести `ls -d adatum.com`, будет показан список всех записей DNS из домена `adatum.com` (рис. 2-19).

ПРИМЕЧАНИЕ nslookup ls id <домен>

Команда `nslookup ls id <домен>` не работает, если не включить передачу зон (см. рис. 2-14), даже если выполнить ее на DNS-сервере, содержащем зону домена. Если эта команда не работает, попробуйте установить на вкладке **Передачи зон** (Zone Transfers) переключатель **На любой сервер** (To Any Server), но учтите, что это компрометирует безопасность.

```

C:\Command Prompt - nslookup
> ls -d adatum.com
[Unknown]
adatum.com. SOA van-dc1.adatum.com hostmaster.adatum.com.
(882 700 600 86400 3600)
adatum.com. A 10.10.0.50
adatum.com. A 10.10.0.10
adatum.com. NS van-dc1.adatum.com
adatum.com. NS van-dc1.adatum.com
_gc_tcp.Default-First-Site-Name._sites SRV priority=0, weight=100, port=326
0, van-dc1.adatum.com
_kerberos_tcp.Default-First-Site-Name._sites SRV priority=0, weight=100, po
rt=88, van-dc1.adatum.com
_ldap_tcp.Default-First-Site-Name._sites SRV priority=0, weight=100, port=3
89, van-dc1.adatum.com
_gc_tcp SRV priority=0, weight=100, port=3260, van-dc
1.adatum.com
_kerberos_tcp SRV priority=0, weight=100, port=88, van-dc1.
adatum.com
_kpasswd_tcp SRV priority=0, weight=100, port=464, van-dc1
.adatum.com
_ldap_tcp SRV priority=0, weight=100, port=389, van-dc1
.adatum.com
_kerberos_udp SRV priority=0, weight=100, port=88, van-dc1.
adatum.com
_kpasswd_udp SRV priority=0, weight=100, port=464, van-dc1
.adatum.com
DomainDnsZones A 10.10.0.50
DomainDnsZones A 10.10.0.10
_ldap_tcp.Default-First-Site-Name._sites.DomainDnsZones SRV priority=0, wei
ght=100, port=389, van-dc1.adatum.com
_ldap_tcp.DomainDnsZones SRV priority=0, weight=100, port=389, van-dc1
.adatum.com
ForestDnsZones A 10.10.0.50
ForestDnsZones A 10.10.0.10
_ldap_tcp.Default-First-Site-Name._sites.ForestDnsZones SRV priority=0, wei
ght=100, port=389, van-dc1.adatum.com
_ldap_tcp.ForestDnsZones SRV priority=0, weight=100, port=389, van-dc1
.adatum.com
van-dc1 A 10.10.0.50

```

Рис. 2-19. Записи DNS для домена adatum.com

Список команд `nslookup` показан на рис. 2-20.

```

C:\Command Prompt - nslookup
Commands: <identifiers are shown in uppercase, [I] means optional>
NAME - print info about the host/domain NAME using default server
NAME1 NAME2 - as above, but use NAME2 as server
help or ? - print info on common commands
set OPTION - set an option
all - print options, current server and host
InoIdbug - print debugging information
InoId2 - print exhaustive debugging information
InoIdname - append domain name to each query
InoIdrecurse - ask for recursive answer to query
InoIdsearch - use domain search list
InoIdvc - always use a virtual circuit
domain-NAME - set default domain name to NAME
searchlist=N1/N2/.../N6 - set domain to N1 and search list to N1,N2, etc.
root=NAME - set root server to NAME
retry=X - set number of retries to X
timeout=X - set initial time-out interval to X seconds
type=X - set query type (ex. A,AAAA,A*AAAA,ANY,CNAME,MX,NS,PTR,
SOA,SRV)
querytype=X - same as type
class=X - set query class (ex. IN (Internet), ANY)
InoIdmxfr - use MS fast zone transfer
ixfrver=X - current version to use in IXFR transfer request
server NAME - set default server to NAME, using current default server
lserver NAME - set default server to NAME, using initial server
root - set current default server to the root
ls [opt] DOMAIN [I] FILE - list addresses in DOMAIN (optional: output to FILE)
-a - list canonical names and aliases
-d - list all records
-t TYPE - list records of the given RFC record type (ex. A,CNAME,MX,NS,
PTR etc.)
view FILE - sort an 'ls' output file and view it with pg
exit - exit the program

```

Рис. 2-20. Команды nslookup

Команда `netsh interface ipv6 show dnsservers` отображает конфигурации DNS IPv6 и показывает, какие адреса DNS-серверов являются статическими.

Новые и усовершенствованные функции DNS

Роль DNS-сервера Windows Server 2008 предоставляет следующие новые и улучшенные функции:

- **Поддержка контроллеров домена только для чтения (read-only domain controllers, RODC).** Роль DNS-сервера Windows Sever 2008 предоставляет таким контроллерам домена зоны, доступные только для чтения. Зона DNS на контроллере домена только для чтения является полномочной, но не обновляется динамически каждый раз, когда в домен добавляется новая сетевая сущность (клиент, сервер, сетевой принтер или сетевой проектор). Если сетевая сущность добавляется в тот же сайт, где находится контроллер домена только для чтения, этот контроллер домена может получить соответствующие записи DNS от контроллера домена, доступного для записи, если тот разрешает это. Это позволяет выполнять разрешение имен локально в пределах сайта, а не по глобальной сети.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Контроллеры домена только для чтения

Подробнее о контроллерах домена только для чтения см. по адресу [http://technet.microsoft.com/ru-ru/library/cc772234\(Ws.10\).aspx](http://technet.microsoft.com/ru-ru/library/cc772234(Ws.10).aspx).

- **Фоновая загрузка зон.** В Windows Server 2008 и 2008 R2 загрузка данных зон DNS выполняется как фоновая операция. Если необходимо перезагрузить DNS-сервер, содержащий одну или несколько крупных зон DNS, хранящихся в AD DS, сервер может начать отвечать на клиентские запросы быстрее, так как ему не требуется ждать полной загрузки данных зоны.
- **Глобальные однокомпонентные имена.** DNS-зона GlobalNames обеспечивает разрешение однокомпонентных имен в крупных сетях, в которых не возвращена служба WINS. Эта зона используется, когда непрактично использовать суффиксы имен DNS для выполнения разрешения однокомпонентных имен.
- **Поддержка IPv6.** Роль службы DNS-сервера в Windows Server 2008 полностью поддерживает адреса IPv6. Она позволяет использовать записи AAAA и IP6 и поддерживает зоны обратного просмотра IPv6.

Поддержка контроллеров домена только для чтения

Контроллер домена только для чтения содержит теньную копию контроллера домена и не может настраиваться напрямую. Это делает его менее подверженным атакам. Microsoft советует использовать контроллеры домена только для чтения в местах, где нельзя гарантировать физическую безопасность контроллера домена. Настройку контроллера домена только для чтения можно делегировать неадминистративным учетным записям, и наличие администраторов домена или администраторов предприятия в филиалах не требуется.

Операционные системы Windows Server 2008 и 2008 R2 поддерживают основные полномочные зоны, доступные только для чтения (иногда их называют *зонами филиалов*). Контроллер домена только для чтения реплицирует доступную только для чтения копию всех разделов AD DS, используемых DNS, включая раздел каталога домена, ForestDNSZones и DomainDNSZones. Пользо-

ватель, имеющий соответствующие разрешения, может просматривать содержимое основной зоны, доступной только для чтения, но не может изменять его. Содержимое зоны, доступной только для чтения, расположенной на контроллере домена только для чтения, изменяется, только когда изменяется зона DNS на главном контроллере домена, а главный контроллер домена разрешает контроллеру домену только для чтения получать эти изменения.

Фоновая загрузка зон

В крупных сетях, имеющих крупные зоны Windows Server 2003 (и более ранние), хранящие данные DNS в службе каталогов Active Directory, перезагрузка DNS-сервера может занимать значительное время. DNS-серверу требуется извлекать данные зон из AD DS, и он недоступен для клиентских запросов, пока это происходит.

В Windows Server 2008 и 2008 R2 служба DNS решает эту проблему при помощи фоновой загрузки зон. DNS-сервер загружает данные зон из AD DS в фоновом режиме и может отвечать на клиентские запросы почти немедленно после перезагрузки, а не ждет, пока зоны загрузятся полностью. Кроме того, данные зон хранятся в службе каталогов, а не в файле, поэтому к данным можно обращаться асинхронно и незамедлительно после получения запроса. Данные зон, хранящиеся в файлах, можно извлекать только посредством последовательных операций чтения, и это занимает больше времени, чем извлечение данных из AD DS.

После запуска DNS-сервер определяет все зоны, которые необходимо загрузить, загружает из файлов или хранилища AD DS корневые ссылки, загружает имеющиеся зоны с файловой поддержкой и начинает отвечать на запросы и удаленные вызовы процедур (RPC), в то же время используя фоновые процессы (дополнительные потоки процессора) для загрузки зон, хранящихся в AD DS.

Если клиент DNS запрашивает данные о хосте из уже загруженной зоны, DNS-сервер отвечает, как требуется. Если запрашивается еще не загруженная в память информация, DNS-сервер считывает из AD DS данные, необходимые для выполнения запроса.

В планируемую инфраструктуру разрешения имен следует включать более одного DNS-сервера для обслуживания запросов на разрешение имен. Обычно все контроллеры домена AD DS (для записи и только для чтения) содержат зоны DNS, интегрированные с AD DS. И интегрированные, и стандартные основные зоны могут использовать дополнительные зоны для разделения нагрузки и обеспечения отказоустойчивости. Дополнительные DNS-серверы хорошо подходят для виртуализации. Когда основной сервер перезагружается, запросы DNS нормально обрабатываются другими интегрированными или дополнительными DNS-серверами. Эффект фоновой загрузки в данной ситуации в том, что перезагруженный DNS-сервер быстрее возвращается к работе и разделяет нагрузку по удовлетворению клиентских запросов.

Проверьте себя

- Какая запись DNS позволяет разрешать имя хоста в адрес IPv6?

Ответ

- AAAA.

Использование зоны GlobalNames для разрешения однокомпонентных имен

Служба WINS использует протокол NetBT, который Microsoft характеризует как устаревающий, и который не поддерживается в IPv6. Тем не менее, протокол NetBT, предоставляющий статические глобальные записи с однокомпонентными именами, все еще широко используется. В DNS Windows Server 2008 появилась зона GlobalNames, содержащая однокомпонентные имена и обеспечивающая поддержку старых сетей, ранее использовавших WINS для разрешения имен NetBIOS. В Windows Server 2008 R2 зона GlobalNames используется для той же цели.

Обычно областью репликации этой зоны является весь лес, что обеспечивает уникальность предоставляемых однокомпонентных имен в пределах леса. Зона GlobalNames может также поддерживать разрешение однокомпонентных имен в организациях, имеющих несколько лесов, если для публикации расположения зоны GlobalNames используются записи ресурсов обнаружения службы (SRV). Это позволяет отключить службу WINS и протокол NetBT, которые, возможно, не будут поддерживаться в будущих версиях Windows Server. Помните об этом при планировании изменений в структуре разрешения имен и принятии решения о сохранении или отключении WINS. Если отключение NetBT допустимо, это уменьшит поверхность атаки серверов и сделает их менее уязвимыми.

Зона GlobalNames обеспечивает разрешение однокомпонентных имен для ограниченного набора имен хостов, которые обычно являются централизованно управляемыми корпоративными серверами и веб-сайтами, и не используются для однорангового разрешения имен. Разрешение имен клиентских рабочих станций и динамические обновления не поддерживаются. Вместо этого зона GlobalNames содержит записи ресурсов CNAME для сопоставления однокомпонентного имени с полным доменным именем (FQDN). В сетях, использующих WINS, зона GlobalNames обычно содержит записи ресурсов для централизованно управляемых имен, которые уже статически настроены на сервере WINS.

Microsoft рекомендует интегрировать зону GlobalNames с доменными службами Active Directory и добавлять на каждый полномочный DNS-сервер локальную копию зоны GlobalNames. Это обеспечивает максимальную производительность и масштабируемость. Интеграция зоны GlobalNames с AD DS требуется для поддержки развертывания этой зоны в нескольких лесах.

ПРИМЕЧАНИЕ Настройка DNS-серверов для поддержки зон GlobalNames

Параметр /config утилиты командной строки dnscmd включает поддержку зон GlobalNames DNS-сервером.

СОВЕТ Подготовка к экзамену

В отличие от WINS, зона GlobalNames не поддерживает динамическую регистрацию записей с именами хостов. Все записи имен хостов в зоне GlobalNames необходимо создавать вручную.

Планирование репликации WINS для старых сетей

В некоторых случаях требуется поддержка старых сетей, например, доменов Windows NT 4.0. Поэтому вы должны знать, как поддерживать WINS, и учитывать эту службу при планировании и проектировании. Основное решение, которое необходимо принять при планировании служб WINS, связано с топологией репликации. Возможно, вы давно не использовали WINS, поэтому мы приведем базовую информацию для обзора.

Репликация базы данных WINS происходит каждый раз, когда эта база данных изменяется на любом сервере WINS, например, когда освобождается имя NetBIOS. Репликация позволяет серверу WINS разрешать NetBIOS-имена хостов, зарегистрированные другими серверами WINS. Для репликации записей базы данных каждый сервер WINS должен быть настроен как извещающий (push) или опрашивающий (pull) партнер минимум для одного другого сервера WINS.

Извещающий партнер отправляет сообщения опрашивающим партнерам, уведомляя их об изменениях своей базы данных WINS. Когда опрашивающие партнеры отвечают на это сообщение запросом на репликацию, сервер передает им копию новых записей базы данных. *Опрашивающий партнер* — сервер WINS, запрашивающий у своих извещающих партнеров записи базы данных с более высоким номером версии, чем при последней репликации.

Извещающая репликация выполняется, когда в базе данных WINS происходит определенное число изменений. Такую репликацию лучше использовать, если серверы WINS соединены быстрыми каналами связи, обеспечивающими высокую пропускную способность. Опрашивающая репликация может выполняться через определенные промежутки времени, а ее трафик можно контролировать, изменяя пропускную способность. Опрашивающая репликация используется между сайтами, соединенными медленными каналами связи, проходящими через глобальные сети. Для репликации базы данных в обоих направлениях каждый сервер должен быть настроен и как опрашивающий, и как извещающий партнер. Чтобы репликация была полной, каждый сервер WINS должен быть и опрашивающим, и извещающим партнером (но не обязательно для каждого другого сервера).

Совет Подготовка к экзамену

Извещающая репликация выполняется после выполнения определенного числа обновлений записей базы данных WINS. Опрашивающая репликация может выполняться через определенные промежутки времени.

Планирование топологии репликации зависит в первую очередь от топологии сети и требований к восстановлению, предъявляемых организацией. Доступны следующие топологии репликации WINS:

- **Централизованная топология.** Используется один централизованный WINS-сервер или кластер WINS-серверов с высокой доступностью. Эта топология упрощает развертывание и обслуживание. Затраты ресурсов на репликацию между серверами отсутствуют, и все клиенты получают один адрес WINS-сервера. Отказоустойчивость можно обеспечить кластеризацией. Однако если совместно используемая база данных кластера будет повреждена, ее придется восстанавливать из резервной копии. Репликация WINS в этой

топологии не выполняется. Централизованная топология не обеспечивает отказоустойчивости базы данных WINS.

- **Топология полного сцепления.** Имеет распределенную структуру с несколькими WINS-серверами или кластерами, развернутыми в сети предприятия. Репликацию WINS необходимо планировать так, чтобы обеспечить синхронизацию базы данных WINS между всеми WINS-серверами. Каждый WINS-сервер выполняет репликацию с каждым остальным WINS-сервером. Репликацию можно настроить вручную или при помощи автоматического обнаружения WINS (автоматической настройки партнеров). Топологию полного сцепления можно настроить так, чтобы некоторые клиенты использовали один WINS-сервер как основной, а другой WINS-сервер будет использоваться остальными клиентами. Это позволяет организовать балансировку нагрузки. Такая топология обычно используется в сетях, включающих много центров данных и удаленных офисов. Каждый WINS-сервер выполняет репликацию с каждым другим WINS-сервером, что приводит к значительному повышению трафика. Эта топология может скомпрометировать систему безопасности и требует больше работы по управлению и поддержке по сравнению с другими технологиями. Топология полного сцепления показана на рис. 2-21.

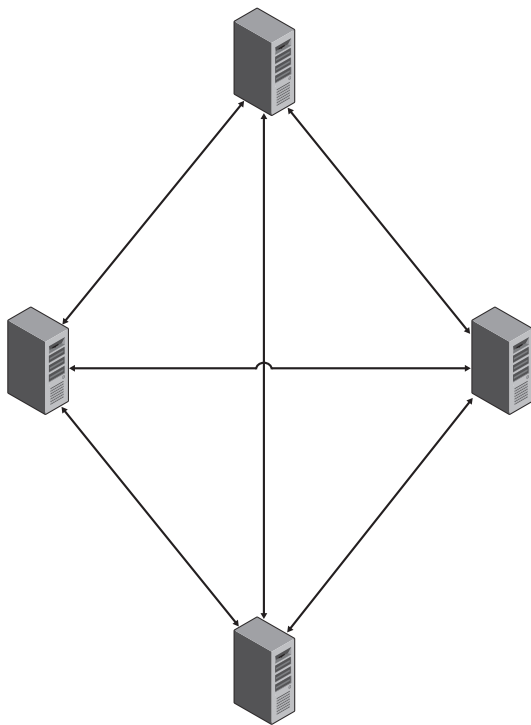


Рис. 2-21. Топология полного сцепления WINS

- **Кольцевая топология.** Имеет распределенную структуру, в которой каждый WINS-сервер имеет одного партнера по репликации, создавая круг. Такая топология создается вручную, так как связи между серверами определяются

и настраиваются администратором WINS. Кольцевую топологию проще обслуживать, чем топологию полного сцепления. Балансировку нагрузки можно организовать, распределив клиентов по WINS-серверам. Однако в кольцевой топологии сложнее решать проблемы, а период конвергенции (время, необходимое для репликации изменения в базе данных на все WINS-серверы) больше, так как обновления последовательно передаются от сервера к серверу. Кольцевая топология показана на рис. 2-22.

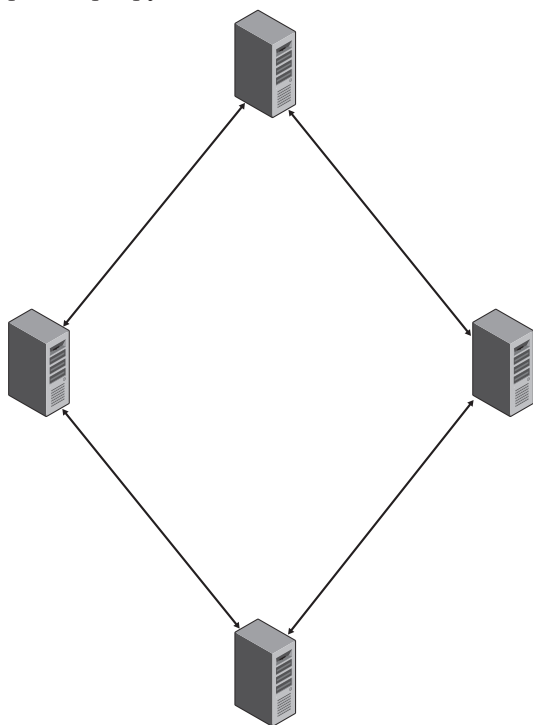


Рис. 2-22. Кольцевая топология WINS

- **Центрально-лучевая топология.** Имеет распределенную структуру, в которой один WINS-сервер назначается центральным, а дополнительные WINS-серверы выполняют репликацию только с центральным сервером из того сайта, в котором расположены. Центрально-лучевая топология обеспечивает эффективную конвергенцию и простое управление, а также дает возможность организовать балансировку нагрузки. Такая топология обычно используется в сетях, имеющих один главный центр данных и несколько филиалов или удаленных офисов. Обычно главный центр данных обеспечивает разрешение имен для большинства компьютеров в сети, а в филиалах выполняется разрешение имен локальных компьютеров. Центрально-лучевая топология показана на рис. 2-23.

Спланировав топологию репликации WINS, можно определить необходимое число WINS-серверов. Оно зависит от числа клиентов, которым требуется разрешение имен WINS, и от пропускной способности, доступной для клиентских запросов и межсайтовой репликации. Рекомендуется иметь один WINS-сервер

на каждые 10000 клиентов и минимум два сервера для обеспечения отказоустойчивости в сайтах, требующих высокой доступности служб WINS.

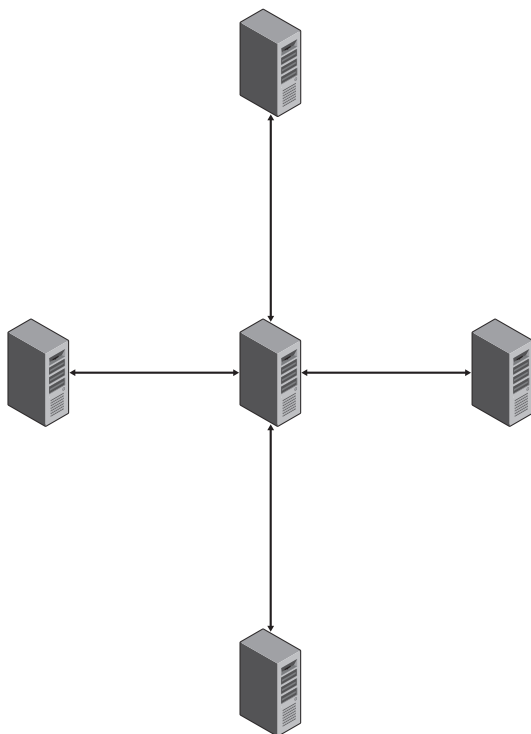


Рис. 2-23. Центральнo-лучевая топология WINS

Поддержка адресов IPv6

В Windows Server 2008 и 2008 R2 служба DNS полностью поддерживает адреса IPv6, как и адреса IPv4. Адреса IPv6 регистрируются динамически, и можно вручную создать запись AAAA для каждого компьютера, не поддерживающего динамическую регистрацию. Также можно создавать зоны обратного просмотра IPv6. На практическом занятии далее в этой главе вы настроите запись AAAA и создадите зону обратного просмотра IPv6.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Зоны обратного просмотра IPv6

Подробнее о зонах обратного просмотра и других вопросах, связанных с протоколом IPv6, см. по адресу <http://www.microsoft.com/technet/network/ipv6/ipv6faq.mspx>.

Утилита командной строки `dnscmd` принимает адреса в обоих форматах: IPv4 и IPv6. DNS-серверы Windows Server 2008 и 2008 R2 могут отправлять рекурсивные запросы к серверам, поддерживающим только IPv6, а список пересылки DNS-сервера может включать адреса IPv4 и IPv6. Клиенты DHCP могут регистрировать адреса IPv6 в дополнение к адресам IPv4 или вместо них. DNS-серверы Windows Server 2008 и 2008 R2 поддерживают пространство имен `ip6.агра` для обратного сопоставления.

Проверьте себя

- Какой компонент DNS Windows Server 2008 и 2008 R2 помогает отказать от WINS и NetBT?

Ответ

- Зона GlobalNames.

Планирование инфраструктуры DNS

В динамической системе DNS большинство хостов и серверов регистрируют свои записи хоста (A) автоматически, и можно настроить DHCP-сервер, чтобы он создавал записи DNS при назначении конфигураций. По сравнению со старой статической системой DNS, где записи приходилось добавлять вручную (если не было интеграции DNS с WINS), динамическая DNS требует очень мало ручной настройки. Возможно, вы имеете опыт создания зон обратного просмотра IPv4. На практическом занятии далее в этой главе вы создадите зону обратного просмотра IPv6.

Планирование инфраструктуры DNS может занимать очень много времени. Рассмотрим этот процесс подробнее.

Планирование пространства имен DNS

Планированием и определением пространства имен DNS обычно занимается главный администратор. Вы должны знать, какие возможности доступны, чтобы наиболее эффективно планировать и реализовывать решения на уровне предприятия.

Если пространство имен DNS используется только для внутренних задач, имена могут не соответствовать стандартам, определенным в RFC 1123 (требования к интернет-хостам) и RFC 2181 (уточнения к спецификации DNS), и набору символов, определенному в RFC 2044. Например, для внутренних задач можно использовать пространство имен contoso.internal.

Однако если определяется корпоративное пространство имен для использования в Интернете, необходимо зарегистрировать его в соответствующей организации и обеспечить его соответствие стандартам RFC. Примеры корпоративных имен: treyresearch.com, tailspintoys.co.uk. Большинство организаций имеет и частную, и открытую сеть. Инфраструктуру DNS можно организовать по одной из следующих схем:

- использовать отдельные пространства имен для внешних и внутренних ресурсов, например, tailspintoys.com и tailspintoys.private. Это повышает безопасность за счет изоляции двух пространств имен друг от друга и предотвращения прямого доступа к ресурсам из Интернета. Передачи зон между двумя пространствами имен не требуются, и существующее пространство имен DNS остается без изменений;
- использовать корпоративное пространство имен для внутренней и внешней (Интернет) части сети. Такая конфигурация проста в исполнении и предоставляет доступ как к внутренним, так и к внешним ресурсам. Однако необходимо организовать хранение соответствующих записей на внутреннем и внешнем DNS-серверах и обеспечить безопасность внутренней сети;

ПРИМЕЧАНИЕ Внутренним пользователям требуется доступ к внешним ресурсам

Использование одного корпоративного пространства имен может создать проблему, когда внутренним пользователям требуется разрешение имен открыто доступных ресурсов, так как внешняя зона DNS не настроена для разрешения внутренних имен. Эту проблему можно решить, скопировав внешнюю зону на внутренние DNS-серверы, чтобы клиенты могли разрешать имена ресурсов. Можно также настроить разделенную конфигурацию DNS (см. далее).

СОВЕТ Подготовка к экзамену

Использование одного пространства имен для внутренних и внешних ресурсов требует дублирования внешней зоны на внутренние DNS-серверы, чтобы клиенты могли разрешать имена внешних ресурсов.

- использовать делегированные пространства имен для определения внутренней сети организации. Например, компания Trey Research может иметь открытое пространство имен `treyresearch.com` и частное пространство имен `intranet.treyresearch.com`. Это полностью соответствует структуре AD DS и легко реализуется, если используются зоны DNS, интегрированные с AD DS. Необходимо убедиться, что внутренние клиенты могут разрешать адреса из внешнего пространства имен, но внешние клиенты не могут разрешать адреса из внутреннего пространства имен. Все данные внутреннего домена изолированы в дереве доменов и требуют собственной инфраструктуры DNS-серверов. Внутренний DNS-сервер будет пересылать запросы к адресам из внешнего пространства имен внешнему DNS-серверу. Недостаток делегирования пространств имен в том, что полные доменные имена могут становиться весьма длинными. Максимальная длина полного доменного имени контроллера домена — 155 байт.

Интеграция DNS с AD DS предоставляет несколько преимуществ, и ее всегда следует рассматривать как вариант при планировании структуры DNS. Одно из важных преимуществ в том, что информация о зонах DNS автоматически реплицируется вместе с другой информацией доменных служб во время репликации распределенной файловой системы (DFS). Можно использовать контроллеры домена только для чтения, содержащие полномочные зоны DNS, доступные только для чтения, и обеспечивающие безопасное разрешение локальных имен в сетях филиалов, где нельзя гарантировать физическую безопасность серверов. Дополнительные зоны DNS можно размещать на DNS-серверах Windows или BIND, не являющихся частью структуры AD DS. Например, DNS-серверы в периферийных зонах часто являются автономными серверами.

Способ реализации AD DS в сети имеет решающее значение в определении способа создания доменов и их вложения. Структура зон обычно повторяет структуру домена AD DS, хотя это не обязательно. Можно легко создавать делегированные зоны. Например, можно использовать пространство имен `engineering.tailspintoys.com`, а не `tailspintoys.com/engineering`.

Пространство имен DNS можно разделить по географическому положению, по подразделениям или по обоим принципам. Например, если Tailspin Toys имеет несколько офисов, а отдел кадров есть только в центральном офисе, можно использовать для этого отдела пространство имен `hr.tailspintoys.com`.

Если Contoso имеет главный офис в Денвере и производственные помещения в Бостоне и Далласе, можно создать пространства имен `denver.contoso.com`, `boston.contoso.com` и `dallas.contoso.com`. Можно объединять эти системы именования, создавая такие пространства имен, как `maintenance.dallas.contoso.com`. Если в структуре получается слишком много иерархических уровней, можно использовать организационные единицы AD DS, например, `dallas.contoso.com/maintenance`.

Разделенная DNS

В разделенной инфраструктуре DNS для одного домена создается две зоны на двух разных серверах имен. Эти зоны имеют одинаковые имена, например, `contoso.com`. Клиенты внутренней сети используют одну зону, а клиенты внешней сети — другую. Требуется как минимум два сервера имен, так как один сервер не может содержать две разные зоны с одним именем.

Зона, используемая внешними клиентами, используется для разрешения имен хостов в открытые IP-адреса. Например, база данных во внешней зоне домена `contoso.com` может содержать записи DNS, приведенные в табл. 2-2.

Табл. 2-2. Записи DNS для внешней зоны `contoso.com`

Имя хоста	Тип записи	Разрешается в адрес
www	A	207.46.232.182
ftp	A	207.46.232.184
mail	A	207.46.232.186
-	MX	mail.corp.net

Зона, используемая внутренними клиентами, используется для разрешения имен хостов в частные IP-адреса и предоставляет псевдонимы для имен внешних хостов. База данных внутренней зоны домена `contoso.com` может содержать записи DNS, показанные в табл. 2-3.

Табл. 2-3. Записи DNS для внутренней зоны `contoso.com`

Имя хоста	Тип записи	Разрешается в адрес
www	CNAME	webserver.corp.net
ftp	CNAME	ftpserver.corp.net
mail	CNAME	exchange.corp.net
exchange	A	10.0.0.25
webserver	A	10.0.0.27
ftpserver	A	10.0.0.29

Когда клиенты внешней сети разрешают имя `www.contoso.com`, они получают внешний IP-адрес веб-сервера 207.46.232.182, что и требуется. Клиенты внешней сети не должны получать частный IP-адрес сервера из внутренней сети.

Когда клиенты внутренней сети обращаются по адресу `www.contoso.com`, они подключаются к серверу `webserver`, используя внутренний частный IP-адрес 10.0.0.27. Запись CNAME для имени `www` разрешается в запись хоста (A) с

именем `webserver.contoso.com`, и запросы перенаправляются по адресу `10.0.0.27`. Для поддержки разделенной DNS необходимо также настроить в сети сервер ISA (Internet Security and Acceleration), но рассмотрение настройки серверов ISA выходит за рамки этой книги.

Планирование пересылки DNS

Сервер пересылки DNS получает от другого DNS-сервера пересылаемые рекурсивные запросы на просмотр и выполняет для него разрешение запроса. Например, локальный DNS-сервер может пересылать запросы DNS центральному DNS-серверу, являющемуся полномочным для внутренней зоны DNS. Если пересылающий сервер не получает требуемого разрешения от сервера, которому пересылает запрос, он пытается разрешить запрос самостоятельно, если не является подчиненным сервером. Подчиненные серверы не пытаются разрешить запрос, если не получают требуемого ответа на пересылаемый запрос DNS. Обычно для подчиненных серверов устанавливаются безопасные Интернет-подключения.

В Windows Server 2003 появилась условная пересылка (см. выше), которую можно использовать в Windows Server 2008 и 2008 R2. Серверы условной пересылки следует использовать, если, например, запросы на разрешение внутренних имен требуется перенаправлять главному DNS-серверу, хранящему внутренние зоны DNS, а запросы на разрешение имен доменов Интернета должны пересылаться в Интернет, где будут удовлетворяться через рекурсию. Условную пересылку можно использовать также во внешних сетях, где запросы, относящиеся к доменам во внешней сети, могут отправляться на DNS-сервер, полномочный для зоны DNS, соответствующей нужному домену, а запросы на разрешение внешних имен могут отправляться в Интернет для рекурсивного разрешения.

СОВЕТ Подготовка к экзамену

Пересылка запросов DNS требует, чтобы DNS-сервер мог отправлять рекурсивные запросы. На экзамене ответы, предполагающие настройку пересылки и отключение рекурсии, можно отбрасывать как неправильные.

В типичной ситуации сервер пересылки может указывать DNS-сервер, которому разрешено пересылать запросы DNS-серверам, расположенным за корпоративным брандмауэром. Это позволяет настроить брандмауэр так, чтобы трафик DNS был разрешен только от одного DNS-сервера, а DNS-серверу в защищенной сети возвращались только действительные ответы. При таком подходе весь остальной трафик DNS, входящий и исходящий, не проходит через брандмауэр. Это повышает безопасность службы DNS и общую безопасность сети.

Планирование типов зон

В сетях AD DS для разрешения внутренних имен обычно используются зоны, интегрированные с AD DS. При этом информация о зонах DNS содержится на контроллерах домена, доступных для записи (обычно на всех таких контроллерах домена). Это позволяет использовать преимущества репликации распределенной файловой системы, обеспечивает отказоустойчивость при выходе одного контроллера домена из строя и повышает доступность. Если требуется DNS-сервер с возможностью записи, но доступ к базе данных AD DS представляет риск для безопасности (например, в периферийных зонах), можно использовать стандартные основные зоны на автономных серверах Windows. Контрол-

леры домена только для чтения можно использовать там, где требуются преимущества интегрированных зон, но нельзя гарантировать физическую безопасность серверов (например, в офисах филиалов).

И интегрированные, и стандартные основные зоны могут предоставлять информацию стандартным дополнительным зонам DNS. В сетях Windows Server 2008 и 2008 R2 дополнительные зоны DNS можно размещать на рядовых серверах, автономных серверах и контроллерах домена только для чтения. Размещение дополнительного DNS-сервера в удаленном расположении может значительно повысить там скорость разрешения имен. Серверы дополнительной зоны повышают отказоустойчивость, предоставляя услуги по разрешению имен даже после выхода из строя сервера основной зоны, и снижают нагрузку на основные серверы, повышая число серверов, между которыми распределяются запросы на разрешение имен. Серверы дополнительной зоны могут не входить в домен AD DS (кроме контроллеров домена только для чтения). Дополнительные зоны можно размещать на серверах с другими операционными системами (не Windows). Серверы дополнительных зон можно создавать на виртуальных машинах.

Возможно, вы уже имеете опыт настройки параметров устаревания и очистки для записей DNS, динамического обновления, областей репликации и передачи зон. Однако, одно дело — знать, как настраиваются эти параметры, и совсем другое — планировать зоны и определять оптимальные параметры для конкретной структуры разрешения имен. Это задача главного администратора.

Проверьте себя

- Какая запись в зоне-заглушке предотвращает возникновение круговой зависимости, позволяя серверу имен, обеспечивающему делегирование, возвращать IP-адрес следующего сервера имен?

Ответ

- Связывающая запись.

Если в зонах остается много устаревших записей ресурсов, они занимают дисковое пространство и увеличивают трафик передачи зон. DNS-серверы, загружающие зоны с устаревшими записями, могут возвращать в ответ на клиентские запросы устаревшую информацию, что может привести к проблемам с разрешением имен. DNS-серверы и зоны можно настроить так, чтобы устаревшие записи ресурсов удалялись через определенное время. В окружениях, где записи могут устаревать, необходимо включать очистку таких записей.

Параметры устаревания и очистки зависят от трафика, связанного с разрешением имен, и от частоты изменений сети. Для относительно стабильной сети с небольшим числом добавляемых и удаляемых компьютеров можно задать более длительный период старения и менее частую очистку, чем для более динамичного окружения. Частая очистка и короткий период старения могут увеличить сетевой трафик.

Кроме этого, зоны DNS могут разрешать или запрещать динамические обновления, хотя для современных сетей необычно иметь отключенные динамические обновления. Интегрированные зоны можно настроить так, чтобы разрешались только безопасные динамические обновления. Настоятельно рекомен-

дуются использовать безопасные динамические обновления (обсуждались ранее на этом занятии), так как они гарантируют, что в данных DNS будут происходить только авторизованные изменения.

СОВЕТ Подготовка к экзамену

Безопасные динамические обновления поддерживаются только зонами, интегрированными с AD DS.

При планировании области репликации интегрированных зон необходимо решить, должна ли зона реплицироваться на все DNS-серверы леса, все DNS-серверы домена (по умолчанию) или все контроллеры текущего домена. Если требуется расширить область репликации, можно настроить репликацию зоны на все DNS-серверы леса. Репликация на все контроллеры домена рекомендуется, только если в сети есть контроллеры домена Windows 2000 Server.

В начальной записи зоны (Start of Authority, SOA) можно указать основной сервер имен, интервал обновления и минимальное время жизни (TTL) записей ресурсов. Значение TTL определяет минимальный период времени, в течение которого клиенты, включая другие DNS-серверы, кэшируют записи ресурсов зоны. Если в сети часто меняются IP-адреса, следует устанавливать низкое значение минимального времени жизни, например, один день.

При планировании зон DNS необходимо указать, разрешены ли передачи зоны, и если разрешены, то на какие серверы. Можно настроить передачи зон на любой сервер, на серверы имен, указанные на вкладке **Серверы имен** (Name Servers), или на серверы, указанные в списке.

Планирование корневых ссылок

Если устанавливаемый DNS-сервер Windows Server 2008 или 2008 R2 имеет доступ к Интернету, он автоматически настраивает список корневых серверов. Когда DNS-сервер получает запрос к зоне DNS, для которой не является полномочным, он отправляет запрос одному из корневых серверов, который иницирует серию запросов для разрешения имени. Для подготовки серверов, являющихся полномочными для некорневых зон, можно использовать корневые ссылки, позволяющие находить полномочные серверы, управляющие доменами более высокого уровня или другими поддеревьями пространства имен DNS.

Корневые ссылки необходимы серверам, полномочным для более низких уровней пространства имен, для обнаружения других серверов. По умолчанию служба DNS-сервера использует корневые ссылки из файла `cache.dns`, который обычно содержит записи NS и A для корневых серверов Интернета. На DNS-сервере в частной сети этот файл следует изменить или заменить на файл с аналогичными записями, указывающими внутренние корневые DNS-серверы.

Планирование интеграции AD DS с существующей инфраструктурой DNS

Многие крупные организации, имеющие несколько сайтов, уже используют один или несколько серверов BIND, обеспечивающих разрешение имен для систем UNIX или имен Интернета для внутренних пользователей. В таких случаях служба DNS Windows, интегрированная с AD DS, должна взаимодействовать со структурой DNS BIND.

Инфраструктура DNS Windows Server 2008 и 2008 R2 предоставляет два варианта:

- Можно использовать существующую инфраструктуру DNS для размещения зоны DNS для AD DS. Это снизит требования к оборудованию и объем административной работы. Однако это может означать, что инфраструктура DNS и доменные службы будут поддерживаться разными людьми. Руководство может не принять такой вариант, так как одна из задач администратора предприятия — рационализировать поддержку инфраструктуры.
- Можно развернуть DNS Windows Server 2008 или 2008 R2 и использовать серверы пересылки для интегрирования обеих инфраструктур. Это дает больше гибкости при проектировании инфраструктуры и пространства имен DNS и моделировании администрирования DNS. Для интегрированных зон требуется служба DNS Windows, а для обеспечения взаимодействия инфраструктуры DNS Windows Server 2008/2008 R2 с существующей инфраструктурой DNS можно использовать серверы пересылки. DNS-серверы Windows Server 2008 и 2008 R2 могут пересылать на существующие DNS-серверы любые DNS-запросы к записям из существующей инфраструктуры DNS.

На рис. 2-24 показана схема пересылки запросов DNS между инфраструктурой DNS Windows Server 2008 и инфраструктурой DNS BIND.

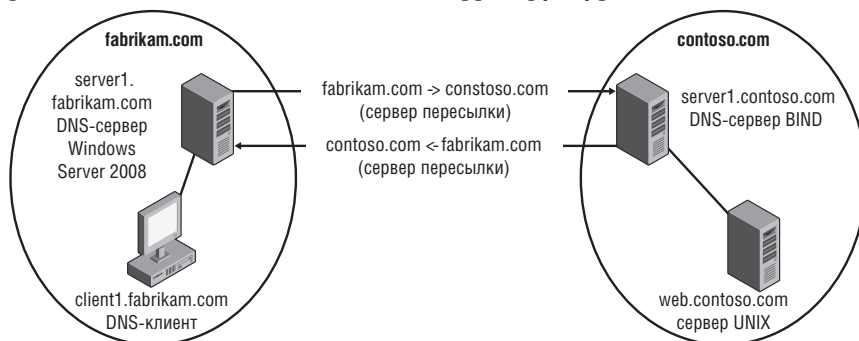


Рис. 2-24. Пересылка запросов DNS

Например, компания Contoso имеет существующую инфраструктуру DNS BIND с доменным именем contoso.com. Компания планирует развертывание новой инфраструктуры DNS Windows Server 2008 R2 для AD DS с доменным именем sales.contoso.com. На DNS-сервере Windows Server 2008 R2 в домене sales.contoso.com добавлена запись для условной пересылки. В домене contoso.com на DNS-сервере BIND создана запись для условной пересылки для домена sales.contoso.com.

Когда клиенту из домена sales.contoso.com требуется доступ к веб-серверу UNIX из домена contoso.com, клиент сначала запрашивает основной DNS-сервер домена sales.contoso.com. Этот сервер не является полномочным для зоны contoso.com, но имеет запись для условной пересылки для зоны contoso.com. Через запись для условной пересылки на DNS-сервере в домене sales.contoso.com клиент связывается с DNS-сервером BIND из домена contoso.com для разрешения имени web.contoso.com.

Планирование зоны GlobalNames

Чтобы уметь планировать структуру зоны GlobalNames, необходимо понимать ситуации, в которых можно настраивать зону GlobalNames. Зону GlobalNames можно развертывать в окружении с одним или несколькими лесами. Развертывание в одном лесу позволяет выполнять разрешение однокомпонентных имен через службу DNS, используя одну зону GlobalNames, интегрированную в AD DS. Развертывание в нескольких лесах позволяет выполнять разрешение однокомпонентных имен через службу DNS, используя одну зону GlobalNames, интегрированную в AD DS, для каждого леса в окружении.

Развертывание зоны GlobalNames в одном лесу можно адаптировать для удовлетворения разных требований к разрешению однокомпонентных имен.

- **Все домены и клиенты в одном лесу.** Этот вариант рекомендуется для организаций, имеющих один лес и небольшое число доменов. Услуги по разрешению однокомпонентных имен предоставляются всем клиентам, входящим в домены леса. В этом случае необходимо убедиться, что все полномочные DNS-серверы в лесу являются контроллерами домена Windows Server 2008 или 2008 R2. Затем администратор должен создать на одном DNS-сервере леса зону GlobalNames, интегрированную с AD DS, и реплицировать ее на все контроллеры домена, являющиеся DNS-серверами. После этого следует добавить записи CNAME для однокомпонентных имен, указывающие полные доменные имена серверов ресурсов.
- **Зона GlobalNames с несколькими лесами.** Этот вариант развертывания рекомендуется компаниям, имеющим много доменов и лесов. DNS-сервер в окружении с несколькими лесами может удовлетворять требования всех доменов и клиентов из всех лесов, если все полномочные DNS-серверы леса являются серверами Windows Server 2008 и 2008 R2, установленными на контроллеры домена. Также необходимо убедиться, что функциональность зоны GlobalNames включена на каждом DNS-сервере леса. На одном DNS-сервере леса создается зона GlobalNames, интегрированная с AD DS, и реплицируется на все контроллеры домена леса, являющиеся DNS-серверами. Затем добавляются записи CNAME для однокомпонентных имен, указывающих полные доменные имена серверов ресурсов. В каждом из других лесов следует добавить в общую для леса зону __msdcs записи ресурсов SRV, указывающие все удаленные контроллеры домена со службой DNS-сервера, содержащие локальную копию зоны GlobalNames.
- **Выбранный набор DNS-серверов содержит зону GlobalNames.** Этот вариант рекомендуется компаниям, имеющим много доменов и лесов, но желающим использовать зону GlobalNames на ограниченном наборе DNS-серверов. Этот вариант обеспечивает разрешение однокомпонентных имен для всех клиентских компьютеров в лесу.
- **Выбранные домены из нескольких лесов.** Этот вариант рекомендуется, когда в окружении с несколькими лесами требуется развернуть зону GlobalNames на нескольких доменах в качестве пилотной программы.

Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных на занятии 2. Эти вопросы предоставлены также в электронном виде на прилагаемом к книге компакт-диске.

ПРИМЕЧАНИЕ Ответы

Ответы на вопросы и пояснения к их вариантам размещены в разделе «Ответы» в конце книги.

1. Требуется создать зону обратного просмотра IPv6, содержащую записи PTR для хостов с адресами IPv6 из подсети fec0::eefd/64. DNS-сервер называется DEN-DC1 и является контроллером домена. Служба DNS интегрирована с AD DS. Вы используете удаленный рабочий стол для подключения к DEN-DC1 и запускаете командную строку от имени администратора. Какой командой вы создадите зону обратного просмотра?
 - a. `dnscmd den-dc1 /ZoneAdd d.f.e.e.0.0.0.0.0.0.0.0.c.e.f.ip6.arpa /Primary.`
 - b. `dnscmd den-dc1 /ZoneAdd d.f.e.e.0.0.0.0.0.0.0.0.c.e.f.ip6.arpa /DsPrimary.`
 - c. `dnscmd den-dc1 /ZoneAdd d.f.e.e.0.0.0.0.0.0.0.0.c.e.f.in-addr.arpa /Primary.`
 - d. `dnscmd den-dc1 /ZoneAdd fec0::eefd/64.ip6.arpa /DsPrimary.`
2. Требуется получить список всех записей DNS из домена adatum.internal. Вы подключаетесь через удаленный рабочий стол к DNS-серверу edinburgh.adatum.internal в Эдинбурге, открываете командную строку и вводите `nslookup`. В приглашении `nslookup>` вы вводите команду `ls -d adatum.internal`. В сообщении об ошибке говорится, что данные зоны не могут быть загружены на этот компьютер. Вы знаете, что в эдинбургском домене есть все записи DNS. Почему они не отображаются?
 - a. Вы не настроили зону прямого просмотра adatum.internal, чтобы разрешить передачи зон.
 - b. Для использования команды `nslookup` необходимо запустить командную строку от имени администратора.
 - c. Необходимо ввести команду `nslookup ls -d adatum.internal` непосредственно из командной строки. Нельзя использовать функцию `ls` из приглашения `nslookup>`.
 - d. Для использования команды `nslookup` необходимо зайти на DNS-сервер интерактивно. Нельзя использовать ее, подключившись через удаленный рабочий стол.
3. Пользователь пытается обратиться к внутреннему веб-сайту компании с клиентского компьютера, но не может из-за проблемы с сетью. Вы исправили проблему, но пользователь все равно не может обратиться к этому веб-сайту, хотя все остальные сайты доступны. Пользователи на других компьютерах не имеют проблем с доступом к этому внутреннему веб-сайту. Как быстро решить проблему?
 - a. Создать в DNS статическую запись хоста для локального веб-сервера.
 - b. Выполнить на основном DNS-сервере команду `ipconfig /flushdns`.

- c. Выполнить на компьютере пользователя команду `ipconfig /registerdns`.
 - d. Выполнить на компьютере пользователя команду `ipconfig /flushdns`.
4. Какая топология WINS использует распределенную структуру с несколькими WINS-серверами или кластерами, развернутыми в сети предприятия, и при этом каждый сервер или кластер выполняет репликацию с каждым другим сервером или кластером?
- a. Централизованная.
 - b. С полным сцеплением.
 - c. Кольцевая.
 - d. Центральнo-лучевая.

Резюме

- Роль DNS-сервера в Windows Server 2008 и 2008 R2 соответствует всем текущим стандартам и может успешно взаимодействовать с большинством других версий DNS-серверов.
- DNS Windows Server 2008 и 2008 R2 — динамическая служба, требующая очень мало статической настройки. Для настройки и управления DNS можно использовать Диспетчер DNS с графическим интерфейсом или утилиты командной строки, такие как `dnscmd`, `nslookup`, `ipconfig` и `netsh`.
- В Windows Server 2008 и 2008 R2 служба DNS поддерживает фоновую загрузку зон, контроллеры домена только для чтения и зоны GlobalNames. Также обеспечивается полная поддержка зон прямого и обратного просмотра IPv6.
- Служба WINS разрешает имена NetBIOS в IP-адреса. Операционные системы Windows Server 2008 и 2008 R2 поддерживают WINS для работы в старых сетях. Зона DNS GlobalNames обеспечивает разрешение однокомпонентных имен для крупных сетей, не имеющих службы WINS.

Практикум. Настройка IPv6

На этом практикуме вы настроите статическую конфигурацию IPv6 на контроллере домена VAN-DC1. Затем вы создадите адрес ISATAP и включите маршрутизатор ISATAP.

Упражнение 1. Настройка IPv6 на компьютере VAN-DC1

В этом упражнении вы настроите протокол IPv6 на контроллере домена VAN-DC1. Обычно главный администратор не занимается настройкой протоколов на отдельном компьютере, так как это задача не его уровня. Однако вам требуется сделать это, чтобы иметь возможность создать зону обратного просмотра IPv6 и запись PTR для VAN-DC1 в следующих упражнениях. В этом упражнении вам потребуется интерактивно зайти на контроллер домена. Если хотите сделать задание более реалистичным, можете вместо этого зайти на клиентский компьютер VAN-SRV1 и с него подключиться к контроллеру домена через удаленный рабочий стол.

1. Зайдите на контроллер домена VAN-DC1 под учетной записью Kim Akers.
2. В Панели управления щелкните **Сеть и Интернет** (Network and Internet). В разделе **Центр управления сетями и общим доступом** (Network and Sharing Center) щелкните **Просмотр состояния сети и задач** (View Network Status And Tasks).
3. В левой части открывшегося диалогового окна щелкните **Изменение параметров адаптера** (Change Adapter Settings).
4. Правой кнопкой мыши щелкните сетевое подключение к частной сети и выберите команду **Свойства** (Properties).
5. Выберите **Протокол Интернета версии 6 (TCP/IPv6)** [Internet Protocol Version 6 (TCP/IPv6)] и щелкните **Свойства** (Properties).
6. Установите переключатель **Использовать следующий IPv6-адрес** (Use The Following IPv6 Address) и введите в поле **IPv6-адрес** (IPv6 Address) статический адрес IPv6 локального сайта **fec0:0:0:ffe::a**.
7. Щелкните в поле **Длина префикса подсети** (Subnet Prefix Length). Значение 64 должно появиться автоматически.
8. Убедитесь, что установлен переключатель **Использовать следующие адреса DNS-серверов** (Use The Following DNS Addresses) и введите адрес **fec0:0:0:ffe::a** в поле **Предпочитаемый DNS-сервер** (Preferred DNS Server). Запомните, что шлюз по умолчанию не указывается, так как ваша изолированная тестовая сеть не настроена для доступа к другим сетям.
9. Если контроллер домена работает под управлением Windows Server 2008 R2, установите флажок **Проверять параметры при выходе** (Validate settings upon exit). Диалоговое окно свойств должно выглядеть аналогично рис. 2-25.

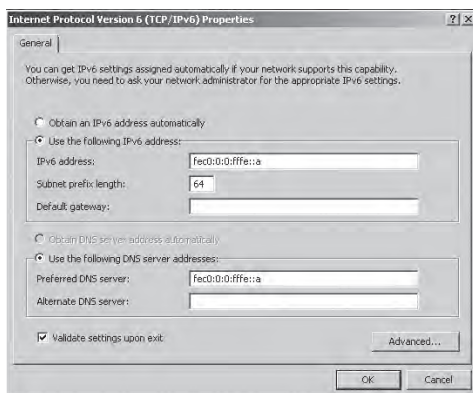


Рис. 2-25. Настройка IPv6 на контроллере домена

10. Щелкните **ОК**. Закройте диалоговое окно свойств.
11. Закройте диалоговое окно **Сетевые подключения** (Network Connections).
12. Закройте окно **Центр управления сетями и общим доступом** (Network and Sharing Center).

Упражнение 2. Создание адреса ISATAP

Протокол IPv6 использует адрес ISATAP для обеспечения взаимодействия двух узлов по сети IPv4. В этом упражнении вы создадите адрес ISATAP, начинающийся с 64-разрядного префикса адреса локального сайта для одноадресной рассылки *fec0:0:0:fffe*. Следующие 32 разряда являются идентификатором ISATAP *0:5efe*. Последние 32 разряда содержат адрес IPv4 10.10.0.50 в точно-десятичной нотации. Прежде чем выполнять это упражнение, выполните упражнение 1.

1. Если требуется, зайдите на контроллер домена VAN-DC1 под учетной записью Kim Akers.
2. Щелкните **Пуск** (Start). Правой кнопкой мыши щелкните командную строку и выберите команду **Запуск от имени администратора** (Run As Administrator).
3. Щелкните **Да** (Yes), чтобы закрыть диалоговое окно службы контроля учетных записей пользователей.
4. Введите команду `netsh`.
5. В приглашении `Netsh>` введите команду `interface`.
6. В приглашении `Netsh interface>` введите команду `ipv6`.
7. В приглашении `Netsh interface ipv6>` введите команду `add address "isatap" fec0: 0:0:fffe:0:5efe:10.10.0.50`.
8. В приглашении `Netsh interface ipv6>` введите команду `exit`.
9. Введите команду `ipconfig /all`.

На экране будут показаны параметры адаптеров (рис. 2-26). Заметьте, что адрес адаптера ISATAP не показан, так как пока не существует подключений ISATAP.

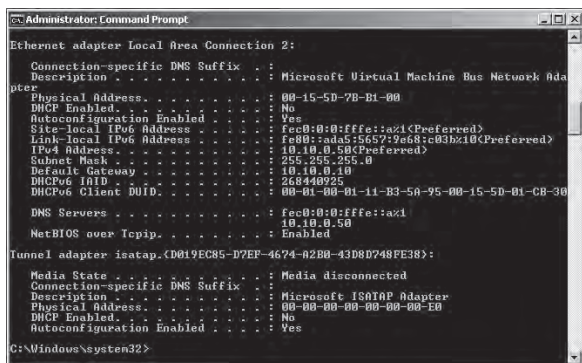


Рис. 2-26. Просмотр конфигураций IPv4 и IPv6 сетевого подключения

Упражнение 3 (дополнительное). Включение маршрутизатора ISATAP

При настройке подключений ISATAP в производственной сети необходимо включить маршрутизацию ISATAP. Это дополнительное упражнение, не влияющее на вашу текущую тестовую сеть. Выполнив его, вы научитесь включать маршрутизацию ISATAP в крупных сетях.

1. Если требуется, зайдите на контроллер домена VAN-DC1 под учетной записью Kim Akers.
2. Если консоль командной строки еще не запущена от имени администратора, щелкните **Пуск** (Start), щелкните командную строку правой кнопкой мыши и щелкните **Да** (Yes), чтобы закрыть диалоговое окно службы контроля учетных записей пользователей.
3. Введите следующую команду:

```
netsh interface ipv6 isatap set router isatap enabled
```

Если команда выполнена успешно, появится сообщение «Ok». В команде можно указать имя маршрутизатора и интервал разрешения в минутах.

Практикум. Настройка DNS

На этом практикуме вы настроите статическую запись AAAA и зону обратного просмотра IPv6. В этой зоне вы создадите запись PTR для компьютера VAN-DC1.

Упражнение 1. Настройка записи AAAA

Автономный сервер DEN-SRV1 имеет операционную систему, которая не может зарегистрироваться в DNS Windows Server 2008 R2. Вы должны вручную создать запись AAAA для этого сервера. Адрес сервера — fec0:0:0::aa. Заметьте, что запись AAAA для этого сервера можно создать даже в том случае, если его пока нет в сети.

1. Если требуется, зайдите на контроллер домена VAN-DC1 под учетной записью Kim Akers.
2. Запустите **Диспетчер DNS** (DNS Manager) из меню **Администрирование** (Administrative Tools).
3. Если появится диалоговое окно службы контроля учетных записей пользователей, щелкните **Да** (Yes).
4. В Диспетчере DNS раскройте узел **Зоны прямого просмотра** (Forward Lookup Zones). Щелкните правой кнопкой мыши узел Adatum.com и выберите команду **Создать узел (A или AAAA)** [New Host (A or AAAA)].
5. Введите имя сервера и адрес IPv6, как показано на рис. 2-27. Убедитесь, что флажок **Создать соответствующую PTR-запись** [Create associated pointer (PTR) record] не установлен.
6. Щелкните **Добавить узел** (Add Host). Щелкните ОК, чтобы закрыть окно сообщения DNS.
7. Щелкните **Готово** (Done). Убедитесь, что новая запись появилась в Диспетчере DNS.
8. Закройте Диспетчер DNS.

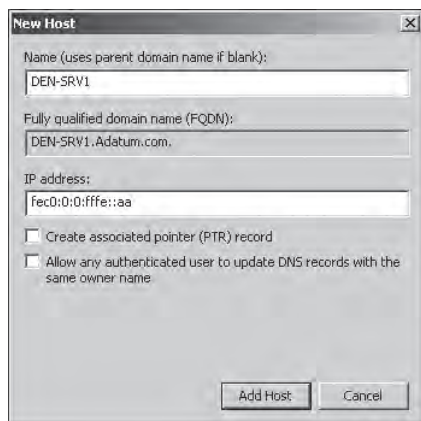


Рис. 2-27. Создание записи узла DNS

Упражнение 2. Настройка зоны обратного просмотра IPv6

В этом упражнении вы создадите зону обратного просмотра IPv6 для всех адресов IPv6 локального сайта, т.е. адресов, начинающихся с *fec0*. Затем вы создадите в этой зоне запись PTR. Заметьте, что в зоне обратного просмотра IPv6 адреса вводятся 4-битными фрагментами в обратном порядке, так что *fec0* превращается в *0.c.e.f*. Перед выполнением этого упражнения необходимо выполнить упражнение 1.

1. Если требуется, зайдите на контролер домена под учетной записью Kim Akers.
2. Щелкните **Пуск** (Start). Щелкните командную строку правой кнопкой мыши и выберите **Запуск от имени администратора** (Run As Administrator).
3. Если появится сообщение службы контроля учетных записей пользователя, щелкните **Да** (Yes).
4. Введите следующую команду:

```
dnscmd VAN-DC1 /ZoneAdd 0.c.e.f.ip6.arpa /DsPrimary
```

На рис. 2-28 показано сообщение об успешном создании зоны. Закройте командную строку.

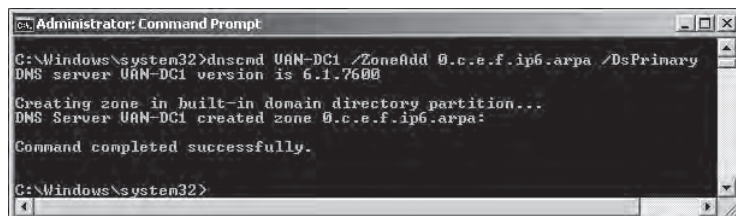


Рис. 2-28. Создание зоны обратного просмотра IPv6

1. Откройте Диспетчер DNS, щелкнув **DNS** в меню **Администрирование** (Administrative Tools). Если откроется окно службы контроля учетных записей, щелкните **Да** (Yes).

2. Раскройте узел **Зоны прямого просмотра** (Forward Lookup Zones). Щелкните `adatum.com`.
3. Правой кнопкой мыши щелкните запись `AAAA` для компьютера `VAN-DC1` и выберите **Свойства** (Properties).
4. Установите флажок **Обновить соответствующую PTR-запись** [Update Associated Pointer (PTR) Record] и щелкните **ОК** (см. рис. 2-29).

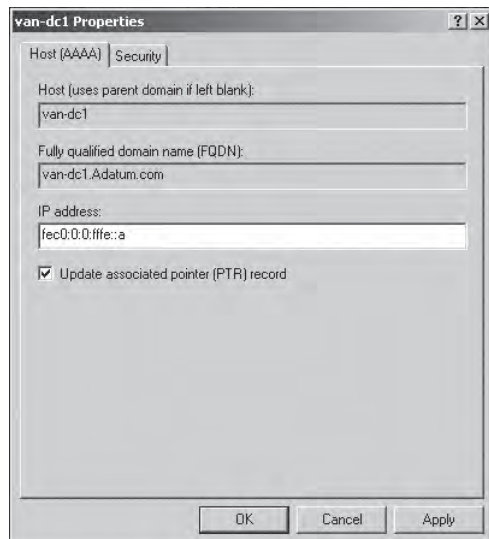


Рис. 2-29. Создание записи PTR

5. Раскройте узел **Зоны обратного просмотра** (Reverse Lookup Zones) и выберите `0.c.e.f.ip6.arpa`. Убедитесь, что запись PTR для `VAN-DC1` существует (рис. 2-30). Если не видите эту запись, выберите в Диспетчере DNS команду **Обновить** (Refresh) из меню **Действия** (Action).

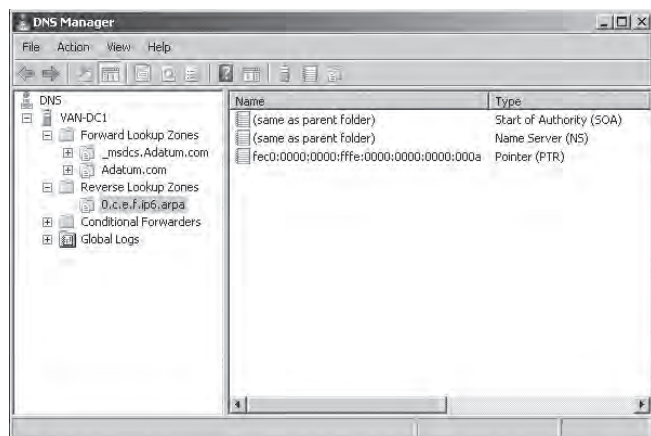


Рис. 2-30. Запись PTR для VAN-DC1

6. Выйдите из системы на контроллере домена.

Закрепление материала главы

Чтобы попрактиковаться и закрепить знания, полученные при изучении этой главы, выполните следующее:

- прочитайте резюме главы;
- просмотрите список основных терминов, представленных в этой главе;
- выполните задания лабораторной работы, моделирующей реальные ситуации, требующие применения полученных знаний;
- выполните рекомендуемые упражнения;
- пройдите пробный тест.

Резюме главы

- Протокол IPv6 полностью поддерживается в Windows Server 2008 и 2008 R2 и устанавливается по умолчанию. Он поддерживает адреса одноадресной, многоадресной и произвольной рассылки. Он обратно совместим с IPv4 и предоставляет разные стратегии перехода.
- Адреса IPv6 можно настраивать с ведением базы данных или без ведения. Для настройки адресов и проверки подключения можно использовать средства с графическим интерфейсом и утилиты командной строки.
- Служба DNS в Windows Server 2008 и 2008 R2 полностью поддерживает IPv6 и имеет несколько новых и улучшенных функций. Она соответствует всем текущим стандартам. Настраивать и проверять функциональность DNS можно при помощи средств с графическим интерфейсом и утилит командной строки.

Основные термины

Проверьте, знаете ли вы, что означают перечисленные ниже термины из этой главы:

- адресное пространство;
- адрес произвольной рассылки;
- поддержка BootP;
- зона прямого просмотра;
- адрес многоадресной рассылки;
- зона обратного просмотра;
- агрегирование маршрутов;
- область;
- адрес одноадресной рассылки;

Лабораторная работа

Для выполнения заданий лабораторной работы используйте знания, полученные из этой главы. Ответы можно найти в разделе «Ответы» в конце книги.

Задание 1. Внедрение IPv6

Вы — главный администратор компании Wingtip Toys. Внутренняя сеть компании состоит из двух подсетей с частными сетями IPv4, настроенными как виртуальные сети, подключенные к коммутатору третьего уровня. Связь с поставщиком услуг Интернета и Интернетом выполняется через ISA-сервер с двойной привязкой, предоставляющий услуги NAT и брандмауэра и подключающийся через периферийную зону к аппаратному брандмауэру и провайдеру услуг Интернета. Компания хочет внедрить IPv6. Все сетевое оборудование поддерживает IPv6, как и провайдер услуг Интернета. Ответьте на следующие вопросы:

1. Какие типы адресов одноадресной рассылки можно использовать в подсетях?
2. Учитывая, что сеть компании может поддерживать и IPv4, и IPv6, какая стратегия перехода будет самой простой?
3. Вы решили использовать настройку с ведением базы данных для выделения конфигураций IPv6 в двух подсетях. Как следует настроить серверы DHCPv6, чтобы обеспечить отказоустойчивость?

Задание 2. Настройка DNS

Вы администрируете сеть Windows Server 2008 R2 AD DS авиакомпании Blue Yonder Airlines. После перехода на Windows Server 2008 R2 используется служба DNS, интегрированная с AD DS, хотя остались два сервера BIND, используемые как дополнительные DNS-серверы. Ответьте на следующие вопросы:

1. Компания установила беспроводные точки доступа для удобства клиентов. Однако руководство беспокоится, что злоумышленники могут попытаться зарегистрировать свои компьютеры в системе DNS компании. Как защититься от этого?
2. Ваш руководитель знает о необходимости репликации зон DNS на два автономных сервера BIND. Он беспокоится, что злоумышленники могут попытаться реплицировать информацию о зонах DNS на неавторизованный сервер, чтобы получить имена и IP-адреса компьютеров компании. Что следует выполнить, чтобы противостоять таким атакам?
3. Для повышения безопасности в филиалах компании используются контроллеры домена только для чтения. Руководство обеспокоено поддержкой актуальности зон DNS на этих компьютерах. Что вы можете сказать по этому поводу?
4. Компания хочет использовать приложение, требующее разрешения адресов IPv6 в имена хостов. Как предоставить такую функциональность?

Рекомендуемые упражнения

Чтобы успешно справиться с экзаменационными заданиями по темам этой главы, выполните следующие упражнения.

Настройка IPv6

Выполните все упражнения из этого раздела.

Изучите команды Netsh

- Структура команд netsh предоставляет много возможностей. Используйте команду help, чтобы изучить информацию о командах netsh interface ipv6 set, netsh interface ipv6 add и netsh interface ipv6 show. Изучите также команды netsh dhcp.

Подробнее изучите параметры сервера и областей DHCPv6

- Выполняя упражнения главы 1, вы установили роль DHCP-сервера. Если нет, установите ее. Используйте утилиту администрирования DHCP для получения списка параметров сервера и областей DHCP. Изучите эти параметры, используя справочную систему и ресурсы Интернета. Найдите информацию по сетям NIS. Хотя в экзамен 70-646 не включены вопросы о NIS, вы, как специалист по сетям, должны знать, что это такое.

Протестируйте выделение адресов DHCPv6

- Настройте клиентский компьютер VAN-SRV1 для автоматического получения конфигурации IPv6. Убедитесь, что настроенная область DHCPv6 предоставляет конфигурацию для этого компьютера, а настроенный IPv6-адрес хоста не входит в диапазон fec0:0:0:fffe::1-fec0:0:0:fffe:ff.

Настройка DNS

Выполните оба упражнения из этого раздела.

Используйте утилиты командной строки

- Чтобы полностью описать возможности утилит nslookup, dnscmd, ipconfig и netsh, понадобится отдельная книга. Единственный способ познакомиться с этими утилитами — использовать их.

Настройте зоны обратного просмотра IPv6

- Процедура настройки описана в занятии 2. При настройке зон обратного просмотра IPv6 в DNS могут возникать ошибки из-за способа указания префиксов. Чтобы такой способ записи стал для вас привычным, практикуйтесь.

Пробный экзамен

Тренировочные тесты на прилагаемом к книге компакт-диске позволяют проверить знания только по одной или сразу по всем темам сертификационного экзамена 70-646. Тестирование можно организовать так, чтобы оно проводилось как настоящий экзамен, а можно проходить в режиме обучения, просматривая правильные ответы и объяснения после каждого ответа.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Пробный экзамен

Подробнее о пробном экзамене рассказано во Введении.

Планирование основы инфраструктуры Active Directory

Занятие 1. Служба каталогов Active Directory **103**

Занятие 2. Службы сертификации Active Directory **138**

Эта глава посвящена Active Directory, в частности, службе каталогов Active Directory (AD DS) и службе центра сертификации Active Directory (AD CS). Мы рассмотрим новые функции и улучшения, появившиеся в Windows Server 2008 и 2008 R2, и обсудим реализацию службы центра сертификации в Active Directory, сфокусировавшись на планировании, а не реализации. Вы узнаете, как использовать инструменты с графическим интерфейсом и утилиты командной строки, но важнее всего не то, как можно изменять конфигурацию, а то, когда и зачем это делать. По мере продвижения по карьерной лестнице вы будете уделять все больше и больше внимания планированию, а не настройке.

Темы экзамена

- Планирование ролей сервера для служб инфраструктуры.

Прежде всего

Для выполнения упражнений этой главы потребуется:

- Сервер с именем VAN-DC1, работающий под управлением Windows Server 2008 R2 Enterprise Edition, настроенный как контроллер домена adatum.com, как описано в Приложении А.
- Установить на сервер VAN-DC1 компонент Управление групповой политикой, если он еще не установлен. Консоль управления групповой политикой (GPMC) должна установиться автоматически при повышении VAN-DC1 до контроллера домена.
- Компьютер с именем VAN-SRV1, работающий под управлением Windows Server 2008 R2 Enterprise Edition, настроенный как рядовой сервер домена adatum.com, как описано в Приложении. Этот сервер может действовать как клиент контроллера домена, и в этой главе мы будем называть его клиентом.

- Учетная запись пользователя Kim Akers с паролем Pa\$\$w0rd в домене adatum.com, включенная в группы администраторов домена, администраторов предприятия и администраторов схемы (см. Приложение А).
- Учетная запись пользователя Don Hall с паролем Pa\$\$w0rd в домене adatum.com, включенная в группу Операторы архива (Backup Operators) для получения возможности интерактивно заходить на контроллер домена.
- Для выполнения практических упражнений рекомендуем использовать изолированную сеть, не входящую в рабочую сеть. Доступ к Интернету не требуется, как и настройка шлюза по умолчанию. Для экономии времени и затрат на настройку физических компьютеров используйте виртуальные машины, например, созданные с использованием роли сервера Hyper-V.

Реальный мир

Йен Маклин

Active Directory — уже не новая технология. Специалисты по сетям знакомы с большинством задач администрирования доменов Active Directory и используемыми для их выполнения инструментами, такими как оснастка **Active Directory — Пользователи и компьютеры**. Даже относительно неопытные корпоративные пользователи могли слышать об Active Directory и знать, что если они забудут пароль или захотят получить доступ к какой-либо папке, администратор будет что-то делать с каталогом.

Однако иногда администраторам приходится объяснять, что такое Active Directory, пользователям, не имеющим особых знаний или интереса в изучении технических принципов работы сети. Обычно такие пользователи — это менеджеры, не понимающие, почему все компьютеры организации нельзя просто связать друг с другом (некоторые даже слышали о рабочих группах), и зачем нужны контроллеры домена и другие серверы, которые, с их точки зрения, ничего не делают.

Я нашел хорошее сравнение структуры каталогов с библиотекой. Простая система хранения, такая как база данных SAM в Windows NT 4, — это эквивалент хранения всех книг в куче на полу. Если читатель захочет найти определенную книгу, ему придется просматривать все книги по очереди, пока не найдется нужная. Структура каталогов эквивалентна хранению книг на полках с сортировкой по фамилии автора в алфавитном порядке, к тому же стеллажи с полками расположены в четко определенных частях библиотеки.

Таким образом, если я захочу найти книгу по истории, я пойду в секцию научной литературы, остановлюсь перед полками с книгами по истории и легко найду нужный том. В крупной библиотеке стеллажи могут быть разделены по секциям: античная история, история средних веков, история Европы и т.д.

Чтобы повысить эффективность поиска, я могу обратиться к библиотечному указателю и найти, на какой именно полке находится нужная мне книга. Я могу посмотреть на карту библиотеки, чтобы определить физическое расположение этой полки. Примерно так функционирует

схема Active Directory. Аналогию можно расширить, включив в нее залы со специализированными материалами — организационными единицами (подразделениями). В таких залах будут читать книги специалисты, изучающие общую тему. Политика входа в специализированные залы может отличаться от политики входа в общие залы. В некоторых залах могут быть служащие, контролирующие доступ к материалам, но не имеющие полномочий на другие залы библиотеки.

Наконец, важнее всего то, что упорядоченная библиотека, как и упорядоченная структура каталогов, может иметь установленную, централизованно контролируемую политику безопасности. Из кучи на полу кто угодно может взять любую книгу, написать что-то на полях, вырвать страницы или просто выбросить книгу. В системе с централизованным управлением права на чтение, запись и изменение можно строго контролировать.

Конечно, аналогия не идеальна, но я успешно пользуюсь ей несколько лет.

Занятие 1. Служба каталогов Active Directory

На этом занятии не рассматриваются базовые функции Active Directory. Как опытный специалист, вы должны уметь добавлять пользователей и группы, назначать права и разрешения, пользоваться поиском и т.д. Если вы не знаете, как это делать, обратитесь к файлам справки, официальной документации и книгам. Цель этого занятия — описать новые и улучшенные функции AD DS Windows Server 2008 и 2008 R2 и обсудить аспекты планирования реализации AD DS. Например, достаточно легко повысить функциональный уровень домена, но важно знать, когда и зачем это делать, особенно с учетом того, что вернуть прежний уровень можно только восстановлением из резервной копии или переустановкой операционной системы.

На этом занятии вам не потребуется создавать в тестовой сети несколько доменов или лесов. Тем не менее, перед администратором крупной сети может встать задача планирования функциональных уровней леса и доверительных связей между лесами. Поэтому вам следует ознакомиться с планированием операций, в которые вовлечено несколько лесов.

Изучив материал этого занятия, вы сможете:

- ✓ Перечислить и описать новые компоненты и функции AD DS Windows Server 2008 и 2008 R2.
- ✓ Планировать и настраивать функциональные уровни домена.
- ✓ Планировать функциональные уровни леса.
- ✓ Планировать доверенные связи лесов.
- ✓ Использовать сервер каталогов.

Продолжительность занятия — примерно 55 мин.

Планирование роли сервера AD DS

Контроллер домена под управлением Windows Server 2008 или 2008 R2 с установленной ролью сервера AD DS (иногда ее называют ролью сервера каталогов) используется для управления пользователями, компьютерами, принтерами и приложениями в сети. В AD DS Windows Server 2008 появились компоненты, облегчающие развертывание AD DS, повышающие безопасность и эффективность администрирования. В Windows Server 2008 R2 эти функции сохранены и добавлены новые. Ниже перечислены общие для Windows Server 2008 и 2008 R2 функции:

- **Контроллеры домена только для чтения.** В Windows Server 2008 появились контроллеры домена только для чтения (RODC), содержащие части базы данных Active Directory, доступные только для чтения. Такие контроллеры домена можно использовать там, где нельзя гарантировать физическую безопасность (например, в офисах филиалов), или в местах, где опасно хранить доменные пароли (например, во внешних сетях или в роли, взаимодействующей с приложениями). Администрирование RODC можно делегировать пользователю домена или группе безопасности, т.е. можно использовать RODC в местах, где локальный администратор не входит в группу администраторов домена.
- **Новые и улучшенные утилиты и мастера.** В Windows Server 2008 появился мастер установки AD DS, расширяющий инструменты оснастки MMC, используемой для управления пользователями и ресурсами. Например, этот мастер позволяет указать, какой контроллер домена устанавливается: с возможностью записи или только для чтения. В первом случае можно указать для контроллера домена политику репликации паролей, определяющую, разрешено ли RODC запрашивать информацию об учетных данных пользователей.
- **Детальные политики безопасности.** AD DS Windows Server 2008 и 2008 R2 позволяет применять разные политики блокировки учетных записей и паролей к пользователям и глобальным группам безопасности одного домена, тем самым снижая число доменов, которыми приходится управлять.
- **Перезапускаемая служба каталогов Active Directory.** AD DS можно останавливать и повторно запускать. Это позволяет выполнять в автономном режиме такие операции, как дефрагментация объектов Active Directory, не перезагружая контроллер домена в режиме восстановления служб каталогов (DSRM).
- **Интеллектуальный анализ данных AD DS.** Средство интеллектуального анализа данных AD DS можно использовать для просмотра данных Active Directory, хранящихся в моментальных снимках, сравнивать данные из моментальных снимков, полученные в разное время, и определять, какие данные следует восстановить, не перезагружая контроллер домена.

ПРИМЕЧАНИЕ Восстановление удаленных объектов и контейнеров

Нельзя напрямую использовать средство интеллектуального анализа данных AD DS для восстановления удаленных объектов и контейнеров. Это средство можно использовать, чтобы просмотреть данные из моментальных снимков, и выполнить восстановление данных, как последующий шаг. Однако больше не требуется восстанавливать данные из нескольких резервных копий, чтобы найти удаленные данные.

- **Улучшения аудита.** При выполнении аудита AD DS в Windows Server 2008 и 2008 R2 можно использовать подкатегорию политики аудита **Изменения службы каталогов** (Directory Service Changes). Она позволяет записывать старые и новые значения, когда в объектах AD DS и их атрибутах происходят изменения. Эту возможность можно использовать и для аудита служб Active Directory облегченного доступа к каталогам (AD LDS).

ПРИМЕЧАНИЕ Службы Active Directory облегченного доступа к каталогам

Подробнее о службах Active Directory облегченного доступа к каталогам см. по адресу [http://technet.microsoft.com/ru-ru/library/cc754361\(WS.10\).aspx](http://technet.microsoft.com/ru-ru/library/cc754361(WS.10).aspx).

В Windows Server 2008 R2 появились следующие улучшения в роли сервера AD DS:

- **Новые функциональные уровни домена и леса.** На функциональном уровне домена Windows Server 2008 R2 появилась возможность обеспечения надежности механизма проверки подлинности и управления именами участника службы. На функциональном уровне леса Windows Server 2008 R2 появилась Корзина Active Directory. Подробнее см. далее на этом занятии.
- **Улучшенное управление из командной строки.** Теперь можно управлять ролями сервера Active Directory при помощи PowerShell.
- **Улучшение автоматизации мониторинга и уведомлений.** Обновленный пакет управления System Center Operations Manager 2007 R2 Management Pack расширяет возможности мониторинга и управления ролями сервера Active Directory.
- **Улучшенный Диспетчер сервера.** Диспетчер сервера позволяет выполнять предварительную подготовку контроллеров домена. Когда роль контроллера домена добавляется из консоли Диспетчера сервера, на сервер копируются файлы, необходимые для установки службы каталогов. Когда запускается мастер установки AD DS (Dcpromo.exe), эти файлы уже кэшированы и доступны.
- **Интегрированный анализатор соответствия рекомендациям.** Windows Server 2008 и 2008 R2 полностью соответствуют установленным стандартам и рекомендациям. В Windows Server 2008 R2 включен интегрированный анализатор соответствия рекомендациям для каждой из ролей сервера. Эта утилита создает в Диспетчере сервера контрольный список для роли, помогающий выполнять все задачи по настройке.
- **Создание файла ответов.** Если устанавливается несколько контроллеров домена с одинаковыми параметрами, с итоговой страницы мастера установки AD DS можно экспортировать параметры текущей установки в файл ответов. В файл ответов не экспортируется пароль учетной записи администратора DSRM, и можно указать, что пользователь, устанавливающий контроллер домена, всегда должен вводить пароль администратора. Следовательно, пароли недоступны пользователям, имеющим доступ к расположению, где хранятся файлы ответов.
- **Упрощенная установка RODC.** Стало проще определять, кому разрешено устанавливать контроллеры домена только для чтения и управлять ими. На

первом этапе установки указывается учетная запись, которая может выполнять установку RODC. После этого пользователь, связанный с RODC, имеет права на установку службы каталогов.

Следующие улучшения AD DS, появившиеся в Windows Server 2008 R2, имеют особую важность, а потому описаны подробнее:

- **Административный центр Active Directory** — предоставляет дополнительный усовершенствованный метод управления объектами службы каталогов.
- **Модуль Active Directory для PowerShell** — предоставляет командлеты, позволяющие выполнять задачи администрирования, настройки и диагностики.
- **Корзина Active Directory** — расширяет возможности сохранения и восстановления случайно удаленных объектов Active Directory.

Центр администрирования Active Directory

В предыдущих версиях ОС Windows Server, таких как Windows Server 2003 и Windows Server 2008, можно публиковать информацию в Active Directory и управлять ей, используя консоль MMC **Active Directory — пользователи и компьютеры**. В Windows Server 2008 R2 объектами службы каталогов можно управлять, используя Центр администрирования Active Directory, доступный в меню **Администрирование**.

Центр администрирования позволяет выполнять следующие задачи:

- создавать новые учетные записи пользователей и управлять существующими;
- создавать новые группы и управлять существующими;
- создавать новые учетные записи компьютеров и управлять существующими;
- создавать новые подразделения и контейнеры и управлять существующими;
- подключаться к одному или нескольким доменам или контроллерам домена для просмотра и управления информацией из каталога, относящейся к этим доменам и контроллерам домена;
- фильтровать данные Active Directory, используя поиск на основе запросов.

Графический интерфейс Центра администрирования Active Directory (рис. 3-1) можно использовать для настройки функциональности этой утилиты.

Центр администрирования Active Directory автоматически устанавливается на любой сервер под управлением Windows Server 2008 R2 при установке AD DS при помощи Диспетчера сервера. Также он автоматически устанавливается при повышении сервера под управлением Windows Server 2008 R2 до контроллера домена утилитой Dsromo.exe. Центр администрирования можно также устанавливать на серверах под управлением Windows Server 2008 R2 и клиентах под управлением Windows 7, используя средства удаленного администрирования сервера (RSAT).

После открытия Центра администрирования Active Directory на сервере под управлением Windows Server 2008 R2 локальный домен будет показан в области навигации. Здесь можно просматривать и управлять объектами Active Directory этого домена.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Установка роли сервера AD DS

Подробнее об установке роли сервера AD DS см. по адресу <http://technet.microsoft.com/ru-ru/library/cc754438%28WS.10%29.aspx>.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Веб-службы Active Directory (ADWS)

Если хотите использовать Центр администрирования Active Directory, необходимо установить ADWS минимум на одном контроллере домена. Подробнее см. по адресу [http://technet.microsoft.com/ru-ru/library/dd391908\(W5.10\).aspx](http://technet.microsoft.com/ru-ru/library/dd391908(W5.10).aspx).

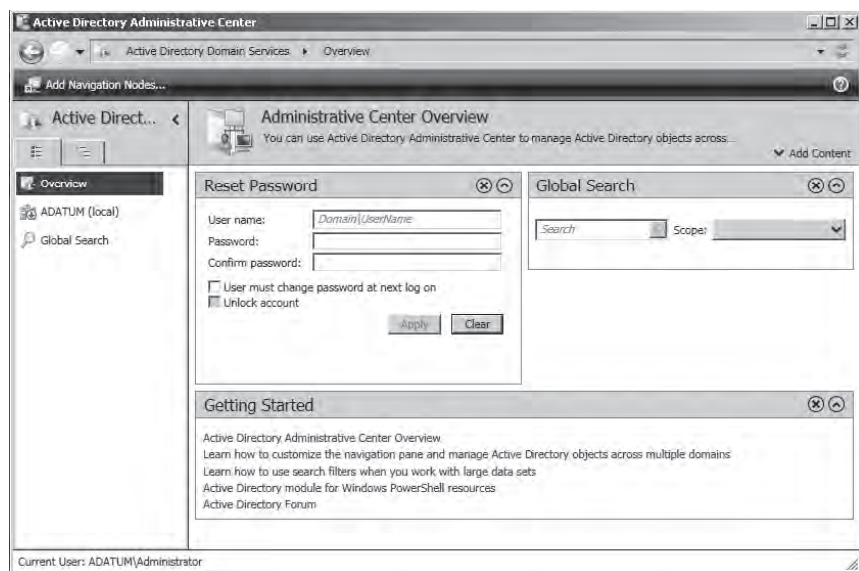


Рис. 3-1. Центр администрирования Active Directory

Можно использовать текущие учетные данные для просмотра или управления объектами Active Directory из других доменов. Просматривать можно домены из того же леса или установить доверительные отношения с локальным доменом. Поддерживается одностороннее и двустороннее доверие. Можно также открыть Центр администрирования Active Directory, используя другие учетные данные.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Управление другими доменами

Подробнее об управлении нелокальными доменами см. по адресу [http://technet.microsoft.com/ru-ru/library/dd560632\(W5.10\).aspx](http://technet.microsoft.com/ru-ru/library/dd560632(W5.10).aspx).

Объекты в области навигации можно просматривать в виде списка или в виде дерева. Чтобы просмотреть дерево, наведите указатель мыши на левую вкладку в верхней части области навигации и щелкните, когда появится всплывающая подсказка «Представление в виде дерева» (Tree View). Чтобы просмотреть список, переместите указатель влево и щелкните на вкладке, когда появится всплывающая подсказка «Представление списка» (List View).

В представлении списка можно использовать функцию Обозреватель столбцов, которая упрощает навигацию, показывая все дочерние контейнеры родительского контейнера в одном столбце. Представление списка содержит также список часто используемых элементов. Этот список автоматически появляется под узлом навигации при посещении минимум одного контейнера из этого узла. Он содержит последние три посещенные контейнера для каждого узла. Текущий список часто используемых элементов можно просмотреть, развернув строку

иерархической навигации центра администрирования Active Directory (см. далее).

Область навигации можно настраивать, добавляя контейнеры из локального или любого внешнего домена в виде отдельных узлов. Добавленные вручную узлы можно переименовывать, удалять, перемещать вверх или вниз по области навигации и создавать дубликаты.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Настройка области навигации центра администрирования Active Directory

Подробнее о настройке области навигации центра администрирования Active Directory см. по адресу [http://technet.microsoft.com/ru-ru/library/dd560665\(W5.10\).aspx](http://technet.microsoft.com/ru-ru/library/dd560665(W5.10).aspx).

Строка иерархической навигации — поле в верхней части окна центра администрирования Active Directory. Можно перейти непосредственно к определенному контейнеру в локальном или любом доверенном внешнем домене, щелкнув в этой строке и указав один из следующих вариантов:

- различающееся имя (DN) нужного контейнера, например, `cn=Users, DC=adatum, DC=com`;
- иерархический путь к нужному контейнеру, например, `Доменные службы Active Directory\adatum (локальный)\Пользователи`;
- путь LDAP к нужному контейнеру, например, `LDAP://cn=Users, DC=adatum, DC=com`.

С помощью строки иерархической навигации можно перейти непосредственно к контейнеру только в том случае, если этот контейнер хранится в разделе каталога локального домена (или доверенного внешнего домена), управление которым выполняется в центре администрирования Active Directory. Эту строку нельзя использовать для перехода непосредственно к контейнерам, хранящимся в разделах каталога для конфигурации, схемы и приложения локального домена (или доверенных внешних доменов), управление которыми выполняется в центре администрирования Active Directory.

Чтобы перейти непосредственно к контейнеру, указав путь к нему в строке иерархической навигации, необходимо выполнять управление локальным доменом (или доверенным внешним доменом), к которому принадлежит этот контейнер, в выбранном экземпляре центра администрирования Active Directory. Однако это ограничение не применяется, если для перехода к контейнеру в строке иерархической навигации указывается путь LDAP или различающееся имя.

Например, если между доменами `adatum.com` (локальный) и `fabrikam.com` (внешний) установлено доверие, то в строке иерархической навигации можно указывать пути LDAP или различающиеся имена контейнеров. Можно успешно переходить к нужным контейнерам из обоих доменов, независимо от того, какой из них в текущий момент добавлен в область навигации. Однако чтобы иметь возможность переходить к контейнерам из этих доменов, указывая их иерархические пути в строке иерархической навигации, необходимо добавить оба домена в область навигации.

Страница свойств объекта в центре администрирования Active Directory содержит несколько разделов свойств и функцию предварительного просмотра.

Эту страницу можно настраивать, отображая, скрывая и сворачивая любые разделы свойств и область просмотра.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Настройка страниц свойств объектов

Подробнее о настройке страниц свойств объектов в центре администрирования Active Directory см. по адресу [http://technet.microsoft.com/ru-ru/library/dd560647\(WS.10\).aspx](http://technet.microsoft.com/ru-ru/library/dd560647(WS.10).aspx).

Для быстрого поиска объектов Active Directory можно использовать механизм поиска и фильтрации с составлением запросов. Составленные запросы можно сохранять и повторно использовать в дальнейшем. Каждый сохраненный запрос содержит выбранные параметры поиска, сортировки и отображения столбцов.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Поиск объектов Active Directory

Подробнее о поиске объектов в центре администрирования Active Directory см. по адресу [http://technet.microsoft.com/ru-ru/library/dd560661\(WS.10\).aspx](http://technet.microsoft.com/ru-ru/library/dd560661(WS.10).aspx).

Модуль Active Directory для PowerShell

Модуль Active Directory для PowerShell предоставляет словарь и синтаксис для создания сценариев командной строки, позволяющих выполнять задачи администрирования, настройки и диагностики. Этот модуль объединяет несколько командлетов для управления доменами Active Directory, наборы конфигурации AD LDS и экземпляры средства подключения базы данных Active Directory.

Модуль Active Directory устанавливается на компьютерах под управлением Windows Server 2008 R2 (Standard, Enterprise и Datacenter) во время установки роли сервера AD DS или AD LDS. Этот модуль можно установить также на рабочих станциях с Windows 7 как часть RSAT, если в домене есть хотя бы один контроллер домена под управлением Windows Server 2008 R2 или хотя бы один экземпляр набора конфигурации AD LDS, запущенный на сервере под управлением Windows Server 2008 R2. Для корректного функционирования модуль Active Directory использует службу ADWS, которая требует открытия порта TCP 9389 на том контроллере домена, где запущена.

Модуль Active Directory состоит из поставщика и командлетов. Чтобы подключиться к поставщику модуля, выберите **Модуль Active Directory для Windows PowerShell** в меню **Все программы | Администрирование**.

Командлеты модуля Active Directory можно использовать для управления существующими учетными записями Active Directory пользователей и компьютеров, группами, подразделениями, доменами и лесами, контроллерами домена и политиками паролей, а также для создания новых.

В табл. 3-1 описаны некоторые командлеты, доступные в выпуске модуля Active Directory в Windows Server 2008 R2 во время написания книги. Полный список можно найти по ссылке, приведенной ниже.

Табл. 3-1. Некоторые командлеты модуля Active Directory

Командлет	Описание
Enable-ADAccount	Включает учетную запись Active Directory
Set-ADAccountControl	Изменяет значения контроля учетных записей для учетной записи Active Directory
Set-ADAccountPassword	Изменяет пароль учетной записи Active Directory
Set-ADComputer	Изменяет компьютер Active Directory
Get-ADComputerServiceAccount	Возвращает учетные записи служб, размещенных на компьютере Active Directory
Set-ADDefaultDomainPasswordPolicy	Изменяет используемую по умолчанию политику паролей в домене Active Directory
New-ADFineGrainedPasswordPolicy	Создает новую подробную политику паролей Active Directory
Set-ADGroup	Изменяет группу Active Directory
Set-ADObject	Изменяет объект Active Directory
Enable-ADOptionalFeature	Включает дополнительный компонент Active Directory
New-ADServiceAccount	Создает новую учетную запись службы Active Directory

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Модуль Active Directory для Windows PowerShell

Подробнее о модуле Active Directory для Windows PowerShell, включая полный список и описания поддерживаемых командлетов, см. по адресу [http://technet.microsoft.com/ru-ru/library/dd378783\(WS.10\).aspx](http://technet.microsoft.com/ru-ru/library/dd378783(WS.10).aspx).

Корзина Active Directory

Корзина Active Directory в Windows Server 2008 R2, основанная на существующей инфраструктуре восстановления объектов-захоронений, расширяет возможности по сохранению и восстановлению случайно удаленных объектов Active Directory. Она помогает минимизировать время простоя службы каталогов, позволяя восстанавливать случайно удаленные объекты Active Directory (например, подразделения) без восстановления данных из резервных копий, перезапуска доменных служб Active Directory и перезагрузки контроллеров домена.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Восстановление объектов-захоронений

Подробнее о восстановлении объектов-захоронений см. по адресу <http://technet.microsoft.com/ru-ru/magazine/2007.09.tombstones.aspx>.

После включения корзины Active Directory все атрибуты удаленных объектов Active Directory сохраняются, и эти объекты можно восстановить в том же логическом состоянии, в котором они находились непосредственно перед удалением. Например, восстановленные учетные записи пользователей автоматически получают членство в группах и соответствующие права доступа к объектам локального и внешних доменов, имевшиеся у них перед удалением. Корзина Active Directory работает как для доменных служб Active Directory, так и для служб Active Directory облегченного доступа к каталогам. Как будет показано ниже, корзину Active Directory можно включить, используя модуль Active Directory

для PowerShell, если установлен функциональный уровень леса Windows Server 2008 R2. Для использования этого модуля необходим запуск служб ADWS на сервере под управлением Windows Server 2008 R2, входящем в домен.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Восстановление удаленных объектов Active Directory

Пошаговые инструкции по восстановлению удаленных объектов Active Directory см. по адресу [http://technet.microsoft.com/ru-ru/library/dd392261\(WS.10\).aspx](http://technet.microsoft.com/ru-ru/library/dd392261(WS.10).aspx).

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Новые компоненты AD DS в Windows Server 2008 R2

Подробнее о дополнительных компонентах AD DS, появившихся в Windows Server 2008 R2, см. по адресу [http://technet.microsoft.com/ru-ru/library/dd378796\(WS.10\).aspx](http://technet.microsoft.com/ru-ru/library/dd378796(WS.10).aspx).

Планирование и использование RODC

В организациях, использующих домены Windows Server 2003 или более ранние, пользователи из удаленных филиалов обычно проходят аутентификацию на контроллере домена в центральном офисе, подключаясь через каналы глобальной связи (WAN). Это далеко не идеальный вариант, при котором могут возникать задержки. Если WAN-связь отключается, пользователи не могут войти в систему.

Однако с точки зрения безопасности, лучше выполнять вход через WAN-подключение, чем размещать доступный для записи контроллер домена в небольшом офисе, где нельзя гарантировать физическую безопасность сервера. Кроме того, иметь администратора домена в небольшом офисе нерационально, а удаленное администрирование контроллера домена через WAN-подключение может отнимать много времени и сил, особенно если связь медленная.

В Windows Server 2008 для решения этой проблемы появились контроллеры домена только для чтения (RODC). Такие контроллеры домена повышают безопасность, ускоряют вход в систему и облегчают доступ к локальным ресурсам. Администрирование RODC можно делегировать пользователям или группам, не имеющим административных прав в домене.

Развертывать RODC в офисах филиалов можно и в том случае, если производственные приложения работают только при установке на контроллере домена. Такой контроллер домена может быть единственным сервером в офисе филиала, содержащем все серверные приложения. Часто владельцу производственного приложения необходимо интерактивно заходить на контроллер домена или использовать службы терминалов (службы удаленных рабочих столов в Windows Server 2008 R2) для настройки и управления приложением. Это создает риск для безопасности леса Active Directory. Однако этот риск значительно уменьшается, если владелец приложения (обычно не являющийся администратором домена) заходит на контроллер домена только для чтения.

ПРИМЕЧАНИЕ Планирование офисов филиалов

Когда бюджет на приобретение оборудования для небольших офисов филиалов ограничен, на одном сервере приходится размещать несколько ролей, некоторые из которых могут конфликтовать с другими. Контроллеры домена только для чтения могут помочь в решении этой проблемы, но следует также рассмотреть возможность виртуализации.

RODC получает свою конфигурацию с контроллера домена, доступного для записи. Следовательно, в домене должен быть минимум один контроллер домена с возможностью записи, работающий под управлением Windows Server 2008 или 2008 R2. Кроме того, должен быть установлен функциональный уровень леса Windows Server 2003 или более высокий. Важная для безопасности информация, такая как пароли пользователей, не реплицируется на RODC. При первом входе пользователя в систему проверка подлинности выполняется через WAN-подключение. RODC может запрашивать учетные данные пользователя, чтобы в дальнейшем этот пользователь мог проходить проверку подлинности локально, но это должно быть специально разрешено доменной политикой репликации паролей, применяющейся к этому RODC. Сделать это можно на контроллере домена, доступном для записи, при создании учетной записи компьютера для RODC в Active Directory с помощью оснастки **Active Directory — пользователи и компьютеры**.

Проверьте себя

- Вы планируете установить в офисах филиалов компании контроллеры домена только для чтения. Какой минимальный функциональный уровень леса для этого необходим?

Ответ

- Windows Server 2003.

Когда RODC запрашивает информацию об учетных данных у контроллера домена, доступного для записи, последний распознает, что запрос исходит от RODC и проверяет политику репликации паролей, действующую для этого RODC. Это позволяет избавиться от риска хранения паролей всех пользователей домена на контроллере домена в удаленном расположении.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ **Фильтруемые атрибуты, не реплицируемые на RODC**

Подробнее о фильтруемых атрибутах, не реплицируемых на RODC, см. по адресу [http://technet.microsoft.com/ru-ru/library/cc753223\(WS.10\).aspx?ppud=4](http://technet.microsoft.com/ru-ru/library/cc753223(WS.10).aspx?ppud=4).

Контроллеры домена только для чтения особенно полезны в удаленных расположениях с относительно небольшим числом пользователей, с отсутствием опытных пользователей, с недостаточной физической защитой, с низкой скоростью подключения или с любой комбинацией этих условий. Такие контроллеры домена предоставляют базу данных AD DS, доступную только для чтения, обеспечивают однонаправленную репликацию (только с контроллера домена, доступного для записи, на RODC), кэширование учетных данных и зоны DNS только для чтения.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ **Развертывание RODC**

Подробнее о развертывании RODC см. по адресам [http://technet.microsoft.com/ru-ru/library/cc732801\(WS.10\).aspx](http://technet.microsoft.com/ru-ru/library/cc732801(WS.10).aspx) и [http://technet.microsoft.com/ru-ru/library/cc772234\(WS.10\).aspx](http://technet.microsoft.com/ru-ru/library/cc772234(WS.10).aspx). Подробнее о команде `adprep /rodcrep` см. по адресу [http://technet.microsoft.com/en-us/library/cc731728\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc731728(WS.10).aspx) (на англ. языке).

На RODC можно установить службу DNS-сервера, которая реплицирует все разделы каталога для приложений, используемые DNS, включая ForestDNSZones и DomainDNSZones. Если DNS-сервер установлен на RODC, клиенты смогут отправлять запросы на разрешение имен, как на любой другой DNS-сервер.

Однако DNS-сервер на RODC напрямую не поддерживает клиентские обновления и не регистрирует записи сервера имен (NS) для любых размещенных на нем зон, интегрированных с Active Directory. Когда клиент пытается обновить свои записи DNS на RODC, сервер возвращает направление на DNS-сервер с возможностью записи. Затем RODC запрашивает обновленную запись DNS (только одиночную запись) с DNS-сервера с возможностью записи. Во время этого специального запроса на репликацию одного объекта не выполняется репликация полного списка измененных зон или данных домена.

ПРИМЕЧАНИЕ Команда ADPREP /RODCPREP

Эта команда обновляет разрешения для разделов каталога для приложений, чтобы эти разделы можно было реплицировать на RODC. Эта операция обращается к хозяину инфраструктуры в каждом домене, чтобы обновить необходимые разрешения. Выполнять эту команду могут члены группы администраторов предприятия. В лесу требуется выполнить эту команду только один раз (кроме ситуации, когда она не может быть успешно выполнена из-за недоступности хозяина инфраструктуры).

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ ADPREP

Подробнее о команде adprep см. по адресу [http://technet.microsoft.com/en-us/library/cc731728\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc731728(WS.10).aspx) (на англ. языке).

Планирование применения RODC

Планировать применение RODC в удаленных расположениях можно при обновлении серверов до Windows Server 2008/2008 R2 или в существующем домене AD DS Windows Server 2008/2008 R2. Политику репликации паролей для определенного RODC можно указать при создании доменной учетной записи компьютера для этого RODC на первом этапе двухэтапной процедуры установки RODC (см. далее). Также можно открыть оснастку **Active Directory — пользователи и компьютеры** на существующем контроллере домена с возможностью записи, щелкнуть правой кнопкой мыши учетную запись RODC в контейнере **Контроллеры домена** (Domain Controllers), выбрать команду **Свойства** (Properties) и на вкладке **Политика репликации паролей** (Password Replication Policy) разрешить кэширование паролей для этого RODC. На рис. 3-2 показана вкладка **Политика репликации паролей** (Password Replication Policy) для RODC VAN-RODC1 из домена adatum.com. Заметьте, что доступ к этому экрану нельзя получить, пока не создана учетная запись для RODC VAN-RODC1 (см. далее).

Например, компания Margie's Travel имеет несколько небольших филиалов в удаленной сельской местности, где связь WAN бывает медленной и ненадежной. Из-за размера и удаленности этих офисов бюджет на приобретение оборудования ограничен, и серверы должны выполнять несколько ролей. На местах администраторов доменов нет. Для централизованного администрирования из головного офиса требуется, чтобы компьютеры филиалов были частью структуры Active Directory. Одна из текущих функций серверов в филиалах — рабо-

та в качестве вторичных DNS-серверов. Удаленные серверы являются также файловыми серверами и серверами приложений, и некоторые приложения требуют интерактивного входа на сервер. В удаленных офисах нельзя обеспечить такой же уровень физической безопасности, как в головном офисе; при входе в систему в удаленных офисах учетные данные проверяются контроллерами домена из головного офиса. Это может привести к возникновению неприятных задержек.

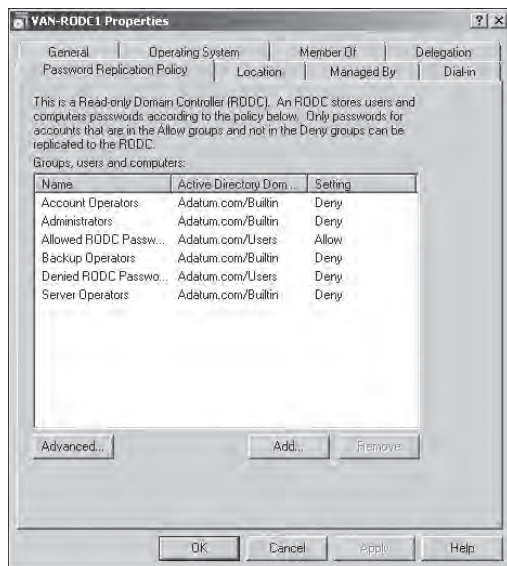


Рис. 3-2. Политика репликации паролей для VAN-RDCC1

Кроме обновления контроллеров домена в главном офисе, можно запланировать установку RODC в каждом удаленном офисе. Сначала можно создать в главном офисе учетные записи для всех RODC и определить на этом этапе политику репликации паролей для каждого RODC, чтобы разрешить удаленным RODC запрашивать информацию об учетных записях и кэшировать учетные данные пользователей, входящих в систему в удаленных офисах. Это ускорит вход в систему. В то же время, пользователям или группе безопасности можно предоставить разрешения на установку RODC и интерактивный вход на эти RODC.

Установка DNS на RODC (по умолчанию) позволяет создать дополнительный DNS-сервер, который может реплицировать все разделы каталога для приложений, используемые DNS, включая ForestDNSZones и DomainDNSZones. Кроме того, при изменении или добавлении записи о локальном клиенте этот DNS-сервер может запросить соответствующую одиночную обновленную запись у DNS-сервера с возможностью записи, без передачи полного списка измененных зон или данных домена.

Можно разрешить интерактивный вход в систему, если этого требуют установленные на RODC приложения, не предоставляя доступных для записи данных Active Directory пользователю, не являющемуся администратором. Следует также рассмотреть возможность виртуализации. Файловые серверы и серверы приложений виртуализуются редко, но это можно сделать с RODC и DNS-серверами.

Улучшения мастера установки AD DS

В Windows Server 2008 был улучшен мастер установки AD DS, упрощающий работу с AD DS и позволяющий выполнять новые задачи, такие как установку RODC. Кроме этого, появились изменения в функциях оснасток MMC, используемых для управления AD DS. В Windows Server 2008 R2 эти функции сохранились, и появились новые улучшения, описанные ранее на этом занятии. Например, улучшенный мастер установки AD DS позволяет быстро находить контроллеры домена в крупной сети и настраивать политику репликации паролей для RODC.

Чтобы запустить мастер установки AD DS, щелкните **Добавить роли** (Add Roles) в диалоговом окне **Задачи начальной настройки** (Initial Configuration Tasks) или в Диспетчере сервера, или выполните команду Dcpromo. Этот мастер запускается также во время предварительного создания учетной записи компьютера для RODC. Некоторые страницы появляются в окне мастера только в том случае, если установить флажок **Использовать расширенный режим установки** (Use advanced mode installation) на первой странице (рис. 3-3). Включить расширенный режим установки можно также командой dcpromo /adv.



Рис. 3-3. Включение расширенного режима установки

СОВЕТ Подготовка к экзамену

Настройка политики репликации паролей для RODC выполняется администратором домена на контроллере домена с возможностью записи. На экзамене можно отбрасывать все ответы, в которых пользователь, не являющийся администратором домена, открывает на RODC оснастку **Active Directory — пользователи и компьютеры** и настраивает политику репликации паролей.

Расширенный режим установки дает большую степень контроля над процессом установки. Если не включить этот режим, мастер будет использовать стандартные параметры, подходящие для большинства конфигураций. В расширенном режиме доступны следующие дополнительные параметры установки:

- можно выбрать контроллер домена-источник, который будет использоваться для первоначальной репликации данных на новый контроллер домена;
- можно использовать резервную копию, полученную на существующем контроллере того же домена, чтобы уменьшить сетевой трафик, связанный с первоначальной репликацией;
- можно создать новое дерево доменов;
- можно изменить имя NetBIOS, выбранное по умолчанию;
- можно установить функциональные уровни леса и домена при создании нового леса или домена;
- можно настроить политику репликации паролей для RODC.

В процессе установки AD DS есть и другие возможности. Например, если устанавливается дополнительный контроллер домена, можно выбрать имя домена, а не вводить его в диалоговом окне. По умолчанию новый мастер установки AD DS использует учетные данные текущего пользователя, если это пользователь домена. Если требуется, можно указать другие учетные данные.

На последней странице мастера можно экспортировать параметры в файл ответов и использовать его в качестве шаблона для последующих установок или удалений. Заметьте, что если указать пароль администратора DSRM на соответствующей странице мастера, а затем экспортировать параметры в файл ответов, пароль не будет добавлен в этот файл. Если требуется включить пароль, необходимо отредактировать файл ответов вручную.

Включать в файлы ответов пароли в виде чистого текста не рекомендуется. Поэтому из файла ответов можно исключить пароль. Если ввести в файле ответов password=*, мастер установки предложит ввести учетные данные. Наконец, мастер позволяет принудительно понижать контроллер домена, запущенный в режиме восстановления службы каталогов.

Делегирование установки RODC

Планируя установку RODC, можно применить двухэтапную установку. Работая в головном офисе, можно делегировать соответствующие разрешения пользователю или группе. В удаленном офисе пользователь с делегированными разрешениями может выполнить установку, а затем управлять RODC, не требуя прав администратора.

Чтобы делегировать установку RODC, сначала создайте учетную запись RODC в оснастке **Active Directory — пользователи и компьютеры**, щелкнув правой кнопкой мыши контейнер **Контроллеры домена** (Domain Controllers) и выбрав команду **Создать заранее учетную запись контроллера домена только для чтения** (Pre-Create Read-Only Domain Controller Account). На рис. 3-4 показана страница мастера, на которой указывается имя компьютера.

Создавая учетную запись RODC, можно делегировать установку и администрирование этого RODC пользователю или группе безопасности. На рис. 3-5 права на установку и администрирование делегируются учетной записи пользователя Don Hall.

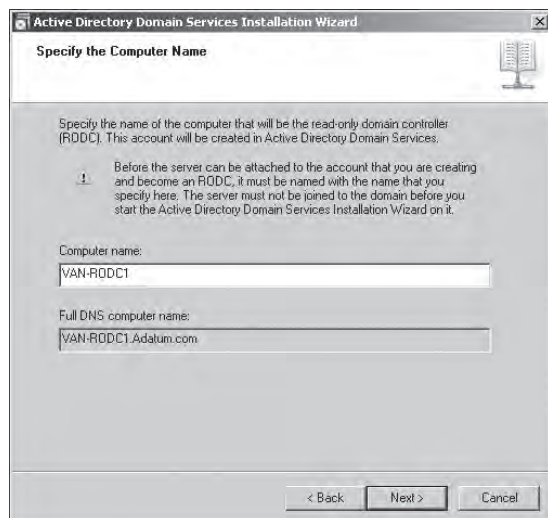


Рис. 3-4. Указание имени компьютера во время предварительного создания учетной записи RODC

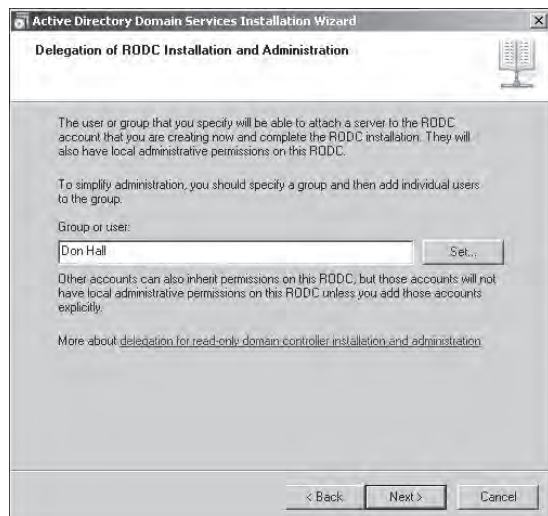


Рис. 3-5. Делегирование прав на установку и администрирование

Пользователь с делегированными правами на установку и администрирование может создать RODC на выделенном сервере, выполнив команду `dsprom /UseExistingAccount:Attach`. Этот пользователь (или пользователи из выбранной группы безопасности) может интерактивно заходить на RODC и администрировать его, не имея административных прав в оставшейся части домена или леса.

ПРИМЕЧАНИЕ Удаление учетной записи RODC

При удалении учетной записи RODC можно автоматически форсировать изменение паролей для всех учетных записей, которые были реплицированы на RODC.

Проверьте себя

- Вы администратор домена. Вы планируете использовать в офисах филиалов контроллеры домена только для чтения. Повышать серверы до RODC будет персонал из этих офисов. Что необходимо сделать в качестве первого этапа двухэтапной установки RODC?

Ответ

- Необходимо создать для RODC доменные учетные записи компьютеров. Сотрудникам из офисов филиалов (обычно одному человеку в каждом офисе) необходимо предоставить соответствующие права на установку RODC.

Улучшения в оснастках MMC

В Windows Server 2008 и 2008 R2 улучшены функции оснасток MMC, таких как **Active Directory — пользователи и компьютеры**. В следующем разделе обсуждаются улучшения в этой оснастке и схеме, позволяющие более точно назначать разрешения, планировать структуру разрешений и, в некоторых случаях, упрощать доменную структуру.

Оснастка **Active Directory — сайты и службы** в Windows Server 2008 и 2008 R2 имеет команду поиска на панели инструментов и в меню **Действия** (Action). Эта команда позволяет найти сайт, в который помещен контроллер домена, что помогает решать проблемы репликации. В Windows 2000 Server и Windows Server 2003 эта оснастка не предоставляет такой информации.

При создании учетной записи компьютера для RODC мастер установки AD DS предоставляет страницу для определения политики репликации паролей для этого RODC. Если не настроить эти параметры на данном этапе, потом можно использовать вкладку **Политика репликации паролей** (Password Replication Policy) диалогового окна свойств RODC (см. рис. 3-2).

Если на этой вкладке щелкнуть кнопку **Дополнительно** (Advanced), можно определить, какие пароли были отправлены на RODC или сохранены на нем, и какие учетные записи проходили аутентификацию на этом RODC. Это позволяет выяснить, кто использовал RODC. Эту информацию можно использовать при планировании политики репликации паролей. Записи в этом диалоговом окне не видны, пока RODC не будет физически создан и не будет использован для проверки подлинности локальных пользователей.

Планирование детальных политик паролей и блокировки учетных записей

До появления Windows Server 2008 в Active Directory можно было применить только одну политику паролей и блокировки учетных записей ко всем пользователям домена. Если разным наборам пользователей требовались разные политики, приходилось использовать настраиваемый фильтр паролей или создавать несколько доменов.

В Windows Server 2008 и 2008 R2 можно использовать детальные политики паролей. Можно создать несколько политик паролей и применить разные политики ограничений паролей и блокировки учетных записей к разным наборам

пользователей в одном домене. Например, можно увеличить минимальную длину паролей для административных учетных записей. Эта возможность позволяет также применять особую политику паролей к учетным записям, чьи пароли синхронизируются с другими источниками данных.

В Windows Server 2008 в схеме AD DS появились два новых класса объектов, поддерживаемые и в Windows Server 2008 R2:

- контейнер параметров паролей;
- параметры паролей.

Класс объектов контейнера параметров паролей (Password Settings Container, PSC) по умолчанию создается в домене в контейнере **Система** (System). В нем хранятся объекты параметров паролей (Password Settings Object, PSO) для этого домена. Этот контейнер нельзя переименовать, переместить или удалить. Можно создать PSO, сохранив параметры (такие как длина паролей) в текстовом файле с разрешением *.ldf* и выполнив команду `ldifde` в командной строке. Можно также использовать оснастку **Редактирование ADSI**, как описано на практикуме далее в этом занятии.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Создание объектов параметров паролей

Подробнее о создании объектов параметров паролей см. по адресу [http://technet.microsoft.com/ru-ru/library/cc754461\(Ws.10\).aspx](http://technet.microsoft.com/ru-ru/library/cc754461(Ws.10).aspx).

СОВЕТ Подготовка к экзамену

На экзамене вряд ли будут вопросы, связанные с созданием объектов параметров паролей, хотя у вас могут спросить, какими инструментами можно это делать. Более вероятны вопросы о планировании подробных политик паролей и предоставляемых ими преимуществ.

Прежде чем планировать политику паролей, следует ознакомиться с параметрами по умолчанию. На рис. 3-6 показаны параметры по умолчанию для домена *adatum.com*.

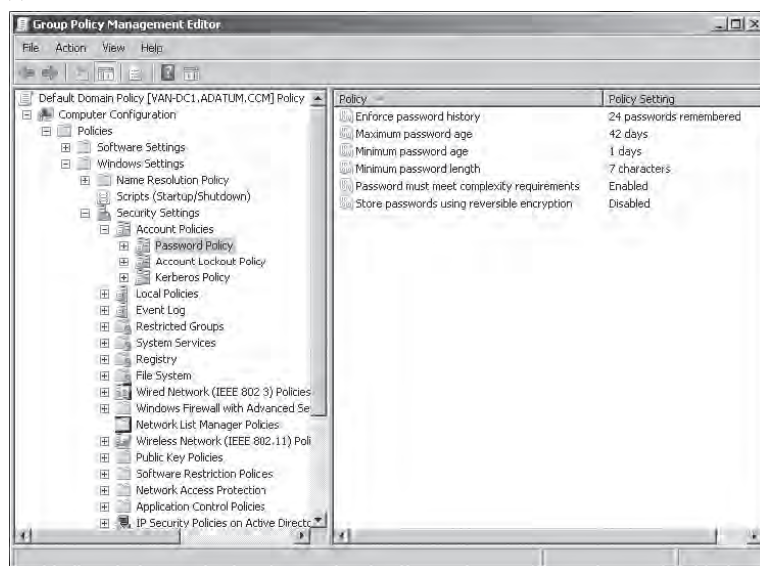


Рис. 3-6. Параметры паролей, используемые по умолчанию

В качестве первого этапа планирования подробных политик паролей и блокировки учетных записей следует определить, сколько разных политик паролей требуется. Обычно политика включает минимум 3, но редко более 10 PSO. Чаще всего минимальная настройка включает следующее:

- политика паролей администраторов со строгими параметрами; например, минимальная длина паролей 12 символов, максимальный срок действия пароля 28 дней и включенные требования к сложности пароля;
- политика паролей пользователей; например, с минимальной длиной 6 символов, максимальным сроком действия пароля 90 дней и не включенные требования к сложности пароля;
- политика паролей служб с минимальной длиной пароля 32 символа и включенными требованиями к сложности (пароли служб редко вводятся с клавиатуры). Благодаря высокой сложности такого пароля, можно установить очень длительный или неограниченный срок действия.

Необходимо также учитывать существующую инфраструктуру групп. Если есть группы **Администраторы** и **Пользователи**, нет смысла создавать новые. В конечном итоге требуется определить структуру Active Directory и групп, соответствующую подробным политикам паролей и блокировки учетных записей.

PSO нельзя применять к подразделениям напрямую. Если пользователи организованы при помощи подразделений, можно создать теневые группы для этих подразделений и применять политики к этим группам. Теневая группа — глобальная группа безопасности, логически сопоставленная с подразделением для применения подробных политик паролей и блокировки учетных записей. Добавляйте пользователей из подразделений в созданную теневую группу и применяйте к этой группе политики. Когда пользователь перемещается из одного подразделения в другое, необходимо обновить членство в соответствующих теневых группах.

ПРИМЕЧАНИЕ Теневые группы

В оснастке **Active Directory** — **пользователи и компьютеры** нет команды «создать теневую группу». *Теневая группа* — это обычная глобальная группа безопасности, содержащая все учетные записи пользователей из одного или нескольких подразделений. Применяя PSO к теневой группе, вы применяете его к пользователям из соответствующего подразделения.

Объекты групповой политики (GPO) применяются к группам, а не подразделениям, поскольку группы предоставляют больше гибкости в управлении различными наборами пользователей. В AD DS Windows Server 2008 и 2008 R2 создано несколько групп для административных учетных записей: Администраторы домена, Администраторы предприятия, Администраторы схемы, Операторы сервера и Операторы резервного копирования. К этим группам можно применять PSO или добавлять их в глобальную группу безопасности и применять PSO к этой группе. Поскольку используются группы, а не подразделения, для применения подробных паролей не требуется изменять иерархию подразделений. Изменение иерархии подразделений требует подробного планирования и повышает вероятность возникновения ошибок.

Если вы собираетесь использовать детальные политики паролей, возможно, вам придется повысить функциональный уровень домена. Для корректной работы параметров детальных политик паролей необходим, как минимум, функциональный уровень домена Windows Server 2008. Планирование функциональных уровней домена и леса обсуждается далее на этом занятии. Изменение функциональных уровней влечет необратимые изменения. Поэтому сначала необходимо убедиться, что больше не потребуется добавление контроллеров домена под управлением Windows Server 2003.

По умолчанию создавать PSO и применять их к группам и пользователям могут только члены группы администраторов домена. Однако для применения PSO к объекту (пользователю или группе) не требуются разрешения на этот объект. Можно делегировать разрешение **Чтение свойства** (Read property) на используемый по умолчанию дескриптор безопасности объекта PSO любой другой группе (например, сотрудникам службы поддержки). Это дает пользователям, не являющимся администраторами домена, возможность просматривать параметры паролей и блокировки учетных записей, примененные через PSO к группе безопасности.

Подробные политики паролей можно применять только к объектам пользователей и глобальным группам безопасности (или объектам inetOrgPerson, если они используются вместо объектов пользователей). Если вы планируете идентифицировать группу компьютеров, требующих других параметров паролей, используйте специальные средства, такие как фильтры паролей. Детальные политики паролей нельзя применять к объектам компьютеров.

Если в домене используются настраиваемые фильтры паролей, детальные политики паролей не мешают их работе. Если планируется обновление доменов Windows 2000 Server или Windows Server 2003, в которых на контроллерах доменов развернуты настраиваемые фильтры паролей, можно продолжать использовать эти фильтры для наложения дополнительных ограничений на пароли.

Если глобальной группе безопасности назначен PSO, но для одного пользователя из этой группы требуются особые параметры, можно назначить особый PSO непосредственно этому пользователю. Например, исполнительный директор компании Northwind Traders является членом группы старших менеджеров, а политика компании требует, чтобы старшие менеджеры использовали сложные пароли. Однако директор не хочет использовать сложный пароль. В этом случае можно создать особый PSO и применить его напрямую к учетной записи директора. Когда будут определяться параметры паролей для учетной записи директора (msDS-ResultantPSO), особый PSO переопределит параметры, назначенные группе безопасности.

Проверьте себя

- Члены какой группы по умолчанию могут создавать PSO?

Ответ

- Администраторы домена.

Наконец, можно делегировать управление детальными политиками паролей. Создав необходимые PSO и связав их с глобальными группами безопасности,

можно делегировать управление этими группами безопасности доверенным пользователям или группам. Например, группа отдела кадров может добавлять и удалять учетные записи из группы менеджеров, когда происходит замена персонала. Если с группой менеджеров связан PSO, указывающий детальную политику паролей, то группа отдела кадров определяет, к кому применяется эта политика.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Настройка детальной политики паролей и блокировки учетных записей

Подробнее о детальной политике паролей и блокировки учетных записей см. по адресу [http://technet.microsoft.com/ru-ru/library/cc770842\(WS.10\).aspx](http://technet.microsoft.com/ru-ru/library/cc770842(WS.10).aspx).

ПРИМЕЧАНИЕ Приоритет PSO

Атрибут приоритета PSO (Precedence) — целое число, используемое для разрешения конфликтов, если к пользователю или группе применяется несколько PSO. Параметры PSO с более низким значением этого атрибута переопределяются параметрами PSO с более высоким приоритетом. Изменять атрибуты PSO можно на вкладке **Атрибут (Attribute)** в оснастке **Active Directory — пользователи и компьютеры**. Эта вкладка отображается в расширенном режиме просмотра.

Планирование использования средства интеллектуального анализа данных

Средство интеллектуального анализа данных (Dsamain.exe) позволяет сохранять удаленные данные AD DS и AD LDS в виде моментальных снимков AD DS, создаваемых службой теневого копирования томов (VSS). Просматривать доступные только для чтения данные из моментальных снимков можно при помощи утилит LDAP (например, ldp.exe) и оснастки **Active Directory — пользователи и компьютеры**. Само средство интеллектуального анализа данных не восстанавливает удаленные объекты и контейнеры; последующее восстановление данных выполняет администратор.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Использование Ntdsutil

Вместе со средством интеллектуального анализа данных можно использовать улучшенную версию Ntdsutil, появившуюся в Windows Server 2008, для создания и просмотра моментальных снимков данных, хранящихся в AD DS или AD LDS. Подробнее см. по адресу [http://technet.microsoft.com/ru-ru/library/cc753609\(WS.10\).aspx](http://technet.microsoft.com/ru-ru/library/cc753609(WS.10).aspx).

Планируя стратегию восстановления, определите, как лучше всего сохранять удаленные данные и восстанавливать их при необходимости. Например, можно настроить регулярный запуск утилиты Ntdsutil, создающей моментальные снимки тома, содержащего базу данных AD DS. Эта же утилита предоставляет список доступных моментальных снимков и позволяет подключать моментальный снимок, который требуется просмотреть.

Второй этап стратегии включает определение моментального снимка, который следует восстановить при потере или повреждении данных. Можно запустить Dsamain.exe для представления тома моментального снимка в качестве

сервера LDAP. В команде `dsamain` можно указать номер порта LDAP. Можно также указать порты LDAP-SSL, Global Catalog и Global Catalog-SSL; если этого не сделать, команда получит эти значения на основе значения порта LDAP. После этого можно запустить `Ldp.exe` и подключиться к указанному порту LDAP. Это позволяет просматривать моментальные снимки так же, как и любой активный контроллер домена.

Если известно, какие объекты или подразделения нужно восстановить, можно найти их в моментальных снимках и записать их атрибуты и обратные ссылки. Затем можно вернуть эти объекты, используя функцию восстановления объектов-захоронений и вручную заполнить их атрибутами и обратными ссылками, найденными в моментальных снимках. Средство интеллектуального анализа данных позволяет сделать это без перезагрузки контроллера домена в режиме службы каталогов.

В процессе планирования следует учитывать не только способы получения моментальных снимков и их использования для восстановления данных. Например, следует также учитывать безопасность. Получение злоумышленником доступа к моментальному снимку AD DS настолько же серьезно, как и получение доступа к резервной копии AD DS. Злоумышленник может скопировать моментальные снимки AD DS из леса А в лес Б и просматривать их, используя учетные данные администратора домена или предприятия из леса Б. Следует шифровать моментальные снимки AD DS для уменьшения вероятности неавторизованного доступа. Как и при любом шифровании данных, следует составить план восстановления на случай потери или повреждения ключа шифрования.

Планирование аудита AD DS

В Windows Server 2008 и 2008 R2 по умолчанию включена глобальная политика аудита **Аудит доступа к службе каталогов** (Audit Directory Service Access). Эта политика определяет, включен или отключен аудит событий службы каталогов. Если настроить эту политику, изменив политику контроллеров домена по умолчанию, можно включить аудит успехов и неудач или отключить аудит всех типов событий. Чтобы указать, какие операции подлежат аудиту, изменить список SACL объекта. Это можно сделать на вкладке **Безопасность** (Security) диалогового окна свойств этого объекта.

Одна из задач администратора — настройка политики аудита. Включить аудит успехов или неудач несложно. Гораздо сложнее определить, какие объекты должны подвергнуться аудиту, аудит какого типа событий следует включить и требуется ли записывать новые и старые значения, если произошли изменения. Аудит всего подряд — не выход, так как одинаково плохо получать слишком много и слишком мало информации. Необходим выборочный аудит.

В Windows 2000 Server и Windows Server 2003 можно выполнять только аудит доступа к службе каталогов. В Windows Server 2008 и 2008 R2 возможностей больше. Можно выполнять аудит следующих событий:

- доступ к службе каталогов;
- изменения в службе каталогов (старые и новые значения);
- репликация службы каталогов.

Аудит репликации службы каталогов имеет дальнейшее разделение, так что можно выбрать один из двух уровней аудита: обычный или подробный.

Приведем пример. Вы администратор домена компании Litware. Вы обнаружили, что настроенный ранее аудит имеет ограничения. Вы можете определить, что изменились атрибуты объекта в Active Directory, но не можете определить, что это за изменения. Если изменение ошибочно, для его исправления вы обращаетесь к документации, которую ведет группа администраторов домена. Однако такая документация не всегда точна и не всегда существует.

Компания недавно обновила домен до Windows Server 2008 R2. Теперь вы можете спланировать процедуры аудита так, что при изменении атрибута объекта будут записываться его предыдущее и текущее значения. Записываются только непосредственно измененные значения, так что не придется искать нужное изменение в длинном списке значений атрибутов.

Проверьте себя

- Вы настраиваете аудит репликации службы каталогов. Какие уровни аудита доступны?

Ответ

- Обычный и подробный.

Если создается новый объект, записываются значения атрибутов, настроенных или добавленных при создании. Атрибуты, принимающие значения по умолчанию, не записываются. Если объект перемещается в пределах домена, будут записаны предыдущее и новое расположения. Если объект переносится в другой домен, можно обратиться к событию создания, которое генерируется и записывается на контроллере домена в целевом домене. Если было отменено удаление объекта, можно определить расположение, в которое он перемещен. Если атрибуты добавляются, изменяются или удаляются в процессе отмены удаления, значения атрибутов можно посмотреть в журнале безопасности.

Если включен параметр **Изменения службы каталогов** (Directory Service Changes), AD DS записывает события в журнал безопасности, когда вносятся изменения в объекты, для которых администратор включил аудит. Эти события перечислены в табл. 3-2.

Табл. 3-2. События безопасности, имеющие отношение к объектам AD DS

Код события	Тип события	Описание события
5136	Изменение	Успешное изменение атрибута в каталоге
5137	Создание	Создание нового объекта в каталоге
5138	Отмена удаления	Отмена удаления объекта в каталоге
5139	Перемещение	Перемещение объекта в пределах домена

Администратор должен определить, нужно ли реагировать на такие события, и как это делать. По умолчанию события записываются в журнал безопасности, и их можно просматривать, открыв средство просмотра событий (Event Viewer). Однако можно указать, что событие, записываемое в журнал безопасности,

инициирует задачу, такую как генерация оповещения или запуск программы. Для этого выберите событие в окне **Просмотр событий** (Event Viewer) и выберите в меню **Действие** (Action) команду **Привязать задачу к событию** (Attach Task To This Event) (рис. 3-7).

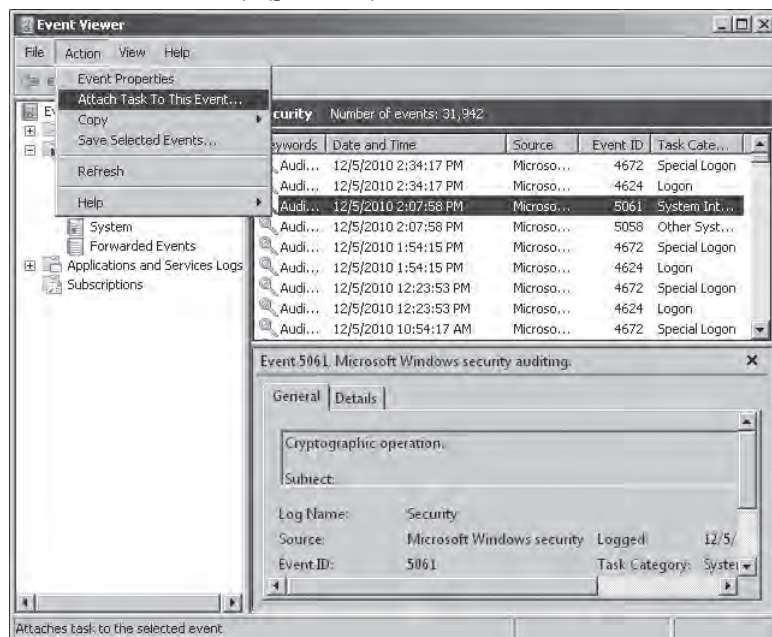


Рис. 3-7. Привязка задачи к событию

Планирование функциональности домена и леса

При обновлении доменов и лесов до Windows Server 2008 или 2008 R2 всегда возникает соблазн поднять функциональные уровни домена и леса. Это очень легко сделать, а в сети не будет доступна полная функциональность, пока функциональные уровни не подняты. Например, для корректной работы конфигурации детальной политики паролей необходим, как минимум, функциональный уровень леса Windows Server 2008.

Будьте осторожны. Очень легко повысить функциональный уровень домена и леса, но почти невозможно понизить его. (Для этого придется выполнять деинсталляцию и переустановку или восстановление из резервных копий, полученных до изменения функционального уровня.) Если в домен требуется добавить контроллеры домена, работающие под управлением Windows Server 2003, а вы повысили функциональный уровень домена до Windows Server 2008 или 2008 R2, у вас проблема. Если вы повысили функциональный уровень леса, а потом потребовалось добавить в этот лес домен Windows Server 2000, вы можете пожалеть о принятом решении. Планирование функциональных уровней — сложная задача по поиску компромиссов. Необходимо учесть и дополнительную функциональность, обретаемую при повышении уровня, и возможные проблемы совместимости.

ПРИМЕЧАНИЕ Откат функционального уровня леса Windows Server 2008 R2

Вообще говоря, если повысить функциональный уровень леса, нельзя понизить его или выполнить откат (кроме варианта с восстановлением из резервной копии, созданной до повышения функционального уровня). Но есть одно исключение: если повысить функциональный уровень до Windows Server 2008 R2 и не включить Корзину Active Directory, можно выполнить откат до функционального уровня Windows Server 2008.

Чтобы определить, какой функциональный уровень следует установить для своих доменов и лесов, нужно знать, какие контроллеры домена поддерживаются на каждом функциональном уровне, и какие дополнительные возможности предоставляет повышение уровня. Необходимо также понимать связь между функциональными уровнями домена и леса. Например, если повысить функциональный уровень леса до Windows Server 2008 R2, функциональным уровнем по умолчанию для всех доменов этого леса будет Windows Server 2008 R2.

ВНИМАНИЕ! Функциональные уровни не влияют на рядовые серверы

Функциональные уровни домена и леса предназначены для контроллеров домена. Они не влияют на рядовые серверы. Например, файловый сервер в домене Windows Server 2008 может работать под управлением Windows 2000 Server или Windows Server 2003.

Функциональный уровень домена

Функциональный уровень домена определяет функции, влияющие на работу домена. В AD DS Windows Server 2008 R2 доступны следующие функциональные уровни домена:

- Windows 2000, основной режим;
- Windows Server 2003;
- Windows Server 2008;
- Windows Server 2008 R2.

При установке роли сервера AD DS Windows Server 2008 R2 по умолчанию создается домен с функциональным уровнем основного режима Windows 2000. На практикуме этого занятия вы повысите функциональный уровень домена. Чтобы определить, следует ли повышать функциональный уровень домена, нужно знать, какие функциональные уровни поддерживаются всеми имеющимися в сети контроллерами домена, и контроллерами домена, которые могут быть добавлены. В табл. 3-3 перечислены функциональные уровни домена и поддерживаемые ими контроллеры домена.

Табл. 3-3. Функциональные уровни домена и поддерживаемые контроллеры домена

Функциональный уровень домена	Поддерживаемые контроллеры домена
Windows 2000, основной режим	Windows 2000 Server
	Windows Server 2003
	Windows Server 2008
	Windows Server 2008 R2

Табл. 3-3. (окончание)

Функциональный уровень домена	Поддерживаемые контроллеры домена
Windows Server 2003	Windows Server 2003 Windows Server 2008 Windows Server 2008 R2
Windows Server 2008	Windows Server 2008 Windows Server 2008 R2
Windows Server 2008 R2	Windows Server 2008 R2

Например, если в домене есть контроллеры домена, работающие под управлением Windows Server 2003, нельзя повысить функциональный уровень домена до Windows Server 2008. Если все контроллеры домена работают под управлением Windows Server 2008 R2, но позже потребуются добавить контроллер домена, работающий под управлением Windows Server 2003, лучше не поднимать функциональный уровень домена выше Windows Server 2003.

Следует найти компромисс между этими ограничениями и преимуществами от повышения функционального уровня. Например, для корректной работы детальных политик паролей требуется функциональный уровень Windows Server 2008 или выше. В табл. 3-4 приведен список возможностей, предоставляемых каждым функциональным уровнем, который может помочь вам при планировании.

ПРИМЕЧАНИЕ Возможности функциональных уровней

В табл. 3-4 возможности только перечислены, но не объяснены; для подробного описания потребовалось бы слишком много места. Большинство этих функций объяснено в других местах книги. Если что-то в списке вам незнакомо, обратитесь к предметному указателю книги, справочным файлам Windows Server 2008 и 2008 R2 или поищите в Интернете (можно начать отсюда: [http://technet.microsoft.com/en-us/library/cc787290\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc787290(Ws.10).aspx)).

Табл. 3-4. Возможности функциональных уровней домена

Функциональный уровень домена	Предоставляемые возможности
Windows 2000, основной режим	Все стандартные функции Active Directory Универсальные группы рассылки и безопасности Вложение групп Преобразование групп История SID
Windows Server 2003	Все стандартные функции Active Directory Все возможности функционального уровня основного режима Windows 2000 Средство управления доменом (Netdom.exe) Обновление временного штампа входа в систему Использование атрибута userPassword в качестве действующего пароля объекта inetOrgPerson и объектов пользователей Диспетчер авторизации хранит политики авторизации в AD DS Ограниченное делегирование Выборочная аутентификация между лесами

Табл. 3-4. Возможности функциональных уровней домена

Функциональный уровень домена	Предоставляемые возможности
Windows Server 2008	Все стандартные функции Active Directory Все возможности функционального уровня Windows Server 2003 Поддержка репликации распределенной файловой системы (DFS) для SYSVOL Поддержка шифрования AES 128 и 256 протоколом аутентификации Kerberos Сведения о последнем интерактивном входе в систему Детальные политики паролей
Windows Server 2008 R2	Все стандартные функции Active Directory Все возможности функционального уровня Windows Server 2008 Контроль механизма проверки подлинности Автоматическое управление SPN

Функциональный уровень леса

Функциональный уровень леса определяет возможности всех доменов леса. В лесах Windows Server 2008 доступны следующие функциональные уровни:

- Windows 2000;
- Windows Server 2003;
- Windows Server 2008;
- Windows Server 2008 R2.

При установке роли сервера AD DS Windows Server 2008 R2 по умолчанию создается новый лес с функциональным уровнем Windows 2000. Функциональный уровень леса можно повысить до Windows Server 2003, Windows Server 2008 или Windows Server 2008 R2. Функциональный уровень леса меньше ограничивает список контроллеров домена, которые могут функционировать внутри леса, чем функциональный уровень домена. Однако чтобы определить, какие контроллеры поддерживаются и могут быть добавлены, следует учитывать оба функциональных уровня. В табл. 3-5 перечислены контроллеры домена, поддерживаемые на разных функциональных уровнях леса. Заметьте, что в домене Active Directory могут функционировать резервные контроллеры домена Windows NT 4.

Табл. 3-5. Функциональные уровни леса и поддерживаемые контроллеры домена

Функциональный уровень леса	Поддерживаемые контроллеры домена
Windows 2000	Windows NT 4 Windows 2000 Server Windows Server 2003 Windows Server 2008 Windows Server 2008 R2
Windows Server 2003	Windows Server 2003 Windows Server 2008 Windows Server 2008 R2
Windows Server 2008	Windows Server 2008 Windows Server 2008 R2
Windows Server 2008 R2	Windows Server 2008 R2

При повышении функционального уровня леса контроллеры домена, работающие под управлением более ранних операционных систем, не могут добавляться в лес. Например, если повысить функциональный уровень леса до Windows Server 2003, в этот лес нельзя добавлять контроллеры домена, работающие под управлением Windows 2000 Server. Функциональный уровень домена не может быть ниже функционального уровня леса. Например, в лесу Windows Server 2003 нельзя иметь домен, работающий в основном режиме Windows 2000, но можно иметь домен Windows Server 2008 R2 в лесу Windows 2000.

Повышение функционального уровня леса — операция, требующая тщательного планирования. Вы можете быть уверены, что в домен Windows Server 2008 не потребуется добавлять контроллеры домена под управлением Windows Server 2003, но можете ли вы гарантировать, что никогда не понадобится добавить домен Windows Server 2008 в лес Windows Server 2008 R2 (например, после приобретения другой компании)?

Как и при повышении функционального уровня домена, для принятия окончательного решения нужно знать о преимуществах более высоких функциональных уровней леса. В табл. 3-6 перечислены возможности каждого функционального уровня.

Табл. 3-6. Возможности функциональных уровней леса

Функциональный уровень леса	Предоставляемые возможности
Windows 2000	Все стандартные функции Active Directory
Windows Server 2003	Все стандартные функции Active Directory Доверительные отношения между лесами Переименование доменов Репликация связанного значения Контроллеры домена только для чтения Улучшенные алгоритмы КСС и масштабируемость, в частности, улучшенные алгоритмы ISTG Возможность преобразования экземпляра объекта inetOrgPerson в экземпляр объекта пользователя, и наоборот Возможность создания базовых групп приложений и групп запросов LDAP для поддержки авторизации на основе ролей Все домены леса функционируют на функциональном уровне домена Windows Server 2003
Windows Server 2008	Все возможности функционального уровня Windows Server 2003 Все домены леса функционируют на функциональном уровне домена Windows Server 2008
Windows Server 2008 R2	Все возможности функционального уровня Windows Server 2008 Все домены леса функционируют на функциональном уровне домена Windows Server 2008 R2 Корзина Active Directory

Например, партнерские компании Coho Vineyard и Coho Vineyard and Winery планируют объединить свои структуры Active Directory в один лес. Все серверы компании Coho Vineyard недавно были обновлены до Windows Server 2008 R2. Менеджеры этой компании увидели значительные преимущества в использовании детальных политик паролей, в частности, упрощение структуры до одного домена. Долгосрочная стратегия предусматривает включение Корзины Active Directory, что позволит восстанавливать случайно удаленные объекты AD DS без необходимости использования резервных копий. Однако это не срочное требование.

Большинство серверов компании Coho Vineyard and Winery, включая все контроллеры домена, работают под управлением Windows Server 2003. Компания не планирует повышать имеющиеся серверы Windows 2000 Server до контроллеров домена, как и обновлять контроллеры домена до Windows Server 2008 R2. Структура сети компании Coho Vineyard and Winery состоит из одного домена, планов по увеличению числа доменов нет. Обе компании тесно сотрудничают с компанией Trey Research и хотят создать доверие между своим лесом и лесом Windows Server 2003 этой компании.

В этой ситуации перепроектированный домен компании Coho Vineyard может иметь функциональный уровень Windows Server 2008 или Windows Server 2008 R2. Это позволит использовать детальную политику паролей. В текущий момент, поскольку функциональный уровень компании Coho Vineyard and Winery должен поддерживать контроллеры домена Windows Server 2003, функциональный уровень леса нельзя поднять выше Windows Server 2003. Следовательно, Корзину Active Directory (для которой требуется функциональный уровень леса Windows Server 2008 R2) включить нельзя. Компания Coho Vineyard, вероятно, выберет функциональный уровень Windows Server 2008 R2 с учетом возможного повышения функционального уровня леса в будущем.

Домен компании Coho Vineyard and Winery может иметь функциональный уровень Windows Server 2003, так как не планируется добавление контроллеров домена под управлением Windows 2000 Server. Это позволяет установить в новом лесу функциональный уровень Windows Server 2003, что обеспечит возможность создания доверия с лесом компании Trey Research.

ПРИМЕЧАНИЕ Повышение функциональных уровней домена и леса в производственной среде

Повышать функциональный уровень домена следует на сервере глобального каталога. Когда все домены имеют требуемый функциональный уровень, функциональный уровень леса следует повысить на сервере глобального каталога в корневом домене.

Включение корзины Active Directory

Чтобы включить Корзину Active Directory, сначала необходимо повысить функциональный уровень всех доменов леса до Windows Server 2008 R2. Затем следует повысить до Windows Server 2008 R2 функциональный уровень леса. После этого можно запустить от имени администратора модуль Active Directory для Windows PowerShell и включить Корзину при помощи команды на основе командлета Enable-ADOptionalFeature. Вы сделаете это на практикуме этой главы. Заметьте, что для использования модуля Active Directory для Win-

dows PowerShell необходим запуск ADWS на сервере Windows Server 2008 R2 в домене и открытый порт TCP 9389 на этом сервере.

Включить Корзину Active Directory можно также с помощью утилиты Lpd.exe, но Microsoft рекомендует использовать командлет Enable-ADOptionalFeature. Заметьте также, что после включения Корзины Active Directory каждый контроллер домена, не являющийся сервером глобального каталога, действует как хозяин инфраструктуры. В результате этого размещение одиночного гибкого хозяина операций инфраструктуры (IM FSMO) не имеет значения.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Enable-ADOptionalFeature

Подробнее о командлете Enable-ADOptionalFeature см. по адресу <http://technet.microsoft.com/en-us/library/ee617209.aspx> (на англ. языке).

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Функциональные уровни домена и леса

Подробнее о функциональных уровнях домена и леса см. по адресу [http://technet.microsoft.com/en-us/library/cc757019\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc757019(WS.10).aspx). Дополнительные сведения можно найти по адресу [http://technet.microsoft.com/en-us/library/understanding-active-directory-functional-levels\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/understanding-active-directory-functional-levels(WS.10).aspx) (на англ. языке).

Планирование доверия лесов

Доверие лесов (или доверие на уровне леса) позволяет каждому домену одного леса доверять каждому домену второго леса. Доверие лесов появилось в Windows Server 2003. Доверие может быть односторонним входящим, односторонним исходящим или двусторонним. Например, все домены леса А могут доверять всем доменам леса Б, если создать одностороннее доверие в лесу А или лесу Б. Если также все домены леса Б должны доверять всем доменам леса А, следует создать двустороннее доверие.

Доверие лесов можно использовать при взаимодействии с партнерскими или тесно связанными компаниями. Например, компании Coho Vineyard и Coho Vineyard and Winery могли не объединять свои домены в один лес, а создать доверие лесов, чтобы предоставить сотрудникам одной компании права и разрешения в лесу другой компании.

Доверие лесов может быть частью стратегии приобретения или поглощения компаний. Компания Northwind Traders приобрела компанию Litware. Конечный план — реорганизовать структуры доменов обеих компаний, объединив их в один лес, но пока этот процесс не завершен, можно использовать доверие лесов.

Доверие лесов можно использовать также для изоляции Active Directory. Например, стратегия перехода может предусматривать запуск Exchange Server 2010 для тестирования новых функций и ознакомления с ними техперсонала. Однако вы не хотите устанавливать Exchange Server 2010 в производственный лес, поскольку это может повлиять на имеющуюся среду Exchange Server 2007. Можно создать для Exchange Server 2010 отдельный лес и получить доступ к ресурсам из производственного леса, установив доверие.

Планирование типа и направления доверия

Наиболее распространенный тип доверия, используемый в лесах — доверие лесов. Его мы будем рассматривать на этом занятии. Однако следует знать и о

других типах доверия, которые можно применять к сущностям за пределами леса.

- **Сокращенное доверие.** Доверие леса позволяет любому домену из одного леса доверять любому домену из другого леса. Однако, если леса сложные, с несколькими уровнями дочерних доменов, клиенту из дочернего домена может потребоваться какое-то время, чтобы найти ресурсы в дочернем домене в другом лесу, особенно при соединении через WAN-связь. Если пользователям из одного дочернего домена часто требуется доступ к ресурсам из другого дочернего домена, расположенного в другом лесу, можно создать сокращенное доверие между этими двумя доменами.
- **Внешнее доверие.** Доверие домена устанавливается, когда домену леса требуются доверительные отношения с доменом, не принадлежащим этому лесу. Обычно внешнее доверие используется во время перемещения ресурсов из доменов Windows NT (их до сих пор существует немало). В Windows NT не используется концепция лесов, и домен Windows NT является самостоятельной автономной единицей. При планировании переноса ресурсов из таких доменов в существующий лес Active Directory можно установить внешнее доверие между одним из доменов Active Directory и доменом Windows NT.
- **Доверие к сфере.** Если сфера UNIX использует аутентификацию Kerberos, можно создать доверие между доменом Windows и сферой UNIX. Такой тип доверия аналогичен внешнему доверию, но между доменом Windows и сферой UNIX.

Выбрав требуемый тип доверия (обычно это доверие леса, поскольку другие типы доверия используются в конкретных ситуациях), нужно определить, будет это доверие односторонним или двусторонним, и, в первом случае, направление доверия. Одностороннее доверие может быть входящим или исходящим.

Если пользователям из леса А требуется доступ к ресурсам леса Б, и пользователям из леса Б требуется доступ к ресурсам из леса А, необходимо создать двустороннее доверие. Так как это двустороннее доверие, направление указывать не требуется.

Но если пользователям из леса А требуется доступ к ресурсам леса Б, а пользователям из леса Б доступ к ресурсам из леса А не требуется, то лес А будет доверенным лесом, а лес Б — доверяющим лесом или лесом ресурсов. Лес Б доверяет пользователям из леса А и позволяет им обращаться к своим ресурсам. Если одностороннее доверие создано в лесу ресурсов, это входящее доверие. Если одностороннее доверие создано в доверенном лесу, это исходящее доверие.

Представьте, что доверие — это стрелка. Ресурсы находятся на острие стрелки. Доверенные пользователи, использующие эти ресурсы, находятся на другом конце (рис. 3-8). Стрелка является входящей в доверяющем лесу (лесу ресурсов) и исходящей в доверенном лесу.

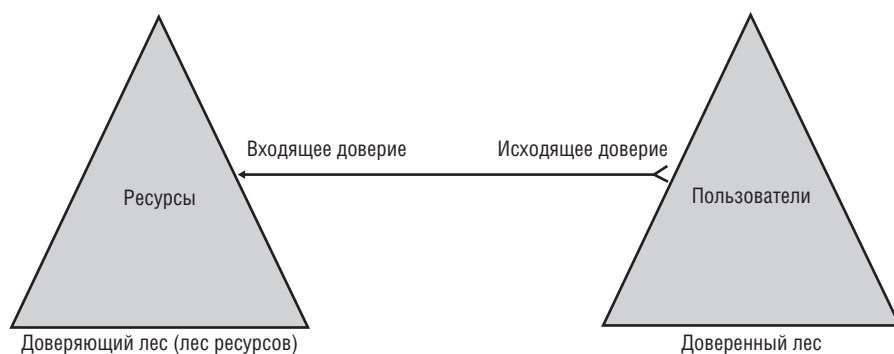


Рис. 3-8. Односторонние доверительные отношения

Создание доверия леса

Прежде чем создать доверие леса, необходимо убедиться, что оба леса имеют функциональный уровень Windows Server 2003 или выше. (Функциональные уровни леса обсуждались ранее на этом занятии.) Следующий шаг — убедиться, что корневой домен каждого леса имеет доступ к корневому домену другого леса. Потребуется создать необходимые записи DNS и использовать утилиту nslookup, чтобы убедиться, что в другом лесу может выполняться разрешение доменных имен. Необходимо также знать имя и пароль учетной записи администратора предприятия (администратора корневого домена) в каждом лесу, если только разные стороны доверия не настраиваются разными администраторами.

Доверие леса создается в оснастке **Active Directory — домены и доверие** (Active Directory Domains And Trusts), доступной в меню **Администрирование** (Administrative Tools). Эту оснастку необходимо подключить к контроллеру корневого домена леса. Затем щелкните правой кнопкой мыши корневой домен в левой части оснастки и выберите команду **Свойства** (Properties). На вкладке **Доверие** (Trust) щелкните **Создать доверие** (New Trust), чтобы запустить мастер создания нового доверия.

Мастер предложит ввести имя домена, леса или сферы для доверия. Чтобы создать доверие леса, следует ввести имя корневого домена леса, с которым требуется установить доверительные отношения. Мастер спросит, какое доверие создается: со сферой или с доменом Windows; выберите второй вариант. После этого будет предложено создать доверие леса или внешнее доверие. Выберите доверие леса и щелкните **Далее** (Next).

Теперь мастер предложит создать одностороннее входящее, одностороннее исходящее или двустороннее доверие. Если создается одностороннее доверие в лесу ресурсов, доверие будет входящим (рис. 3-8). Однако на практике в большинстве случаев лучше использовать двустороннее доверие.

После этого мастер спросит, будете ли вы настраивать только свою сторону или обе стороны доверия. Для создания доверия требуются пароли администраторов корневых доменов обоих лесов. Если вам известен пароль только для своего домена, установите переключатель **Только для данного домена** (This Domain Only). Администратор корневого домена другого леса должен будет повторить эту процедуру на другом конце. Если известны оба пароля, можете настроить обе стороны доверия сразу.

Затем следует выбрать способ проверки подлинности: проверка подлинности в лесу или выборочная проверка подлинности. Второй вариант позволяет подробнее указать параметры проверки подлинности, но требует больше работы. Обычно выбирается проверка подлинности в лесу.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Выборочная проверка подлинности

Подробнее о настройке выборочной проверки подлинности для доверия леса см. по адресу [http://technet.microsoft.com/en-us/library/cc794747\(W.S.10\).aspx](http://technet.microsoft.com/en-us/library/cc794747(W.S.10).aspx).

На последнем этапе мастер покажет общую сводку по выбранным параметрам. Щелкните **Далее**, чтобы установить доверительные отношения. После этого можно подтвердить связь.

Службы федерации Active Directory

Доверительные отношения можно создавать между двумя и более лесами Windows Server 2008 R2 (или любой комбинацией лесов Windows Server 2008 R2, Windows Server 2008 и Windows Server 2003). Это обеспечивает перекрестный доступ к ресурсам, расположенным в лесах, представляющих разные бизнес-структуры или организации. Однако иногда доверие леса — не самый лучший вариант; например, когда доступ к ресурсам других организаций должны иметь только некоторые сотрудники. Службы федерации Active Directory (AD FS) позволяют организациям предоставлять доверенным партнерам ограниченный доступ к своей инфраструктуре. Службы федерации действуют как доверие между лесами, позволяют работать через Интернет и распространяют доверительные отношения на веб-приложения (федеративное доверие). Службы федерации предоставляют технологии единого входа (single sign-on, SSO) через Интернет, позволяющие единожды выполнять проверку подлинности пользователя за все время сеанса работы онлайн. Службы федерации обеспечивают безопасное использование цифровых удостоверений и прав (называемых *утверждениями*) в пределах границ безопасности и границ сети.

Службы федерации появились в Windows Server 2003 и были расширены в Windows Server 2008. Ниже перечислены возможности AD FS, появившиеся в Windows Server 2008 и сохранившиеся в Windows Server 2008 R2.

- **Улучшенная поддержка приложений.** В Windows Server 2008 и 2008 R2 службы федерации интегрированы с SharePoint Server 2007 и службами управления правами Active Directory (AD RMS).
- **Улучшенная установка.** В Windows Server 2008 и 2008 R2 службы федерации реализованы как роль сервера. Мастер установки AD FS включает несколько новых проверок сервера.
- **Улучшенная политика доверия.** Улучшенная функциональность импорта и экспорта политики доверия помогает минимизировать проблемы с конфигурацией, часто возникающие при создании федеративного доверия.

Службы федерации расширяют функциональность SSO для приложений, доступных через Интернет. Партнеры, обращающиеся к веб-приложениям организации, могут работать с ними так же, как при обращении через доверие леса. Серверы федерации можно использовать для выполнения федеративных транзакций типа «бизнес-бизнес».

Службы федерации предоставляют решение для управления федеративными удостоверениями, которое взаимодействует с другими продуктами для обеспечения безопасности в соответствии со спецификацией федерации веб-служб (WS-Federation). Эта спецификация позволяет средам, в которых не используется Windows, создавать федеративные отношения со средами Windows. Также она предоставляет расширяемую архитектуру, поддерживающую тип маркера SAML (Security Assertion Markup Language) 1.1 и аутентификацию Kerberos. Службы федерации могут выполнять сопоставление утверждений (например, изменяя утверждения с помощью настраиваемой бизнес-логики в качестве переменных в запросе доступа). Организации могут изменять службы AD FS, чтобы они существовали с текущей инфраструктурой безопасности и бизнес-политиками.

Наконец, службы AD FS поддерживают распределенную проверку подлинности и авторизацию через Интернет. Эти службы можно интегрировать в существующее решение по управлению доступом, чтобы транслировать утверждения, используемые в организации, в утверждения, согласованные в федерации. Службы AD FS могут создавать, обеспечивать безопасность и проверять утверждения, перемещающиеся между организациями. Также их можно использовать для аудита и мониторинга взаимодействия между организациями и отделами, обеспечивая безопасность транзакций.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Службы AD FS

Подробнее о службах AD FS в Windows Server 2008 и 2008 R2 см. по адресу <http://technet.microsoft.com/ru-ru/library/cc733115.aspx>.

Резюме

- В AD DS Windows Server 2008 появились новые возможности, включая контроллеры домена только для чтения, детальные политики безопасности и средство интеллектуального анализа данных. Эти возможности сохранились в Windows Server 2008 R2.
- Контроллеры домена только для чтения можно устанавливать в офисах филиалов для ускорения входа в систему и разрешения имен DNS, если размещение там контроллера домена с возможностью записи представляет угрозу для безопасности.
- Можно настраивать PSO, хранящие политики паролей и блокировки учетных записей, отличающиеся от политик домена. С PSO можно связывать пользователей и группы безопасности.
- Средство интеллектуального анализа данных позволяет сохранять удаленные данные AD DS или AD LDS в виде моментальных снимков AD DS, полученных при помощи VSS.
- В состав Windows Server 2008 вошли улучшенные оснастки MMC, включая **Active Directory — пользователи и компьютеры** и **Active Directory — сайты и службы**. Эти компоненты продолжают использоваться в Windows Server 2008 R2.
- Улучшенный аудит AD DS позволяет определить, какие изменения и когда произошли в AD DS.

- В Windows Server 2008 R2 появились новые функциональные уровни домена и леса. Если поднять функциональный уровень леса до Windows Server 2008 R2, можно включить Корзину Active Directory в этом лесу.
- Доверие на уровне леса позволяет пользователям из домена одного леса обращаться к ресурсам из домена другого леса.

Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных на занятии 1. Эти вопросы предоставлены также в электронном виде на прилагаемом к книге компакт-диске.

ПРИМЕЧАНИЕ Ответы

Ответы на вопросы и пояснения к их вариантам размещены в разделе «Ответы» в конце книги.

1. Корневой домен contoso.com имеет функциональный уровень Windows Server 2008. Все контроллеры этого домена работают под управлением Windows Server 2008 или Windows Server 2008 R2. Все остальные серверы этого домена (не являющиеся контроллерами домена) работают под управлением Windows Server 2003 и Windows Server 2008. Два дочерних домена, denver.contoso.com и dallas.contoso.com, имеют функциональные уровни Windows Server 2008 и Windows Server 2003, соответственно. Все контроллеры домена denver.contoso.com работают под управлением Windows Server 2008. Некоторые контроллеры домена dallas.contoso.com работают под управлением Windows Server 2003, остальные — под управлением Windows Server 2008. В обоих дочерних доменах все серверы, не являющиеся контроллерами домена, работают под управлением Windows Server 2003. Технический директор компании Contoso хочет использовать Корзину Active Directory. Что требуется для активации этой возможности? (Каждый ответ является частью решения. Выберите четыре.)
 - a. Только в домене contoso.com обновить все контроллеры домена, работающие под управлением Windows Server 2008, до Windows Server 2008 R2.
 - b. Во всех трех доменах обновить все контроллеры домена до Windows Server 2008 R2.
 - c. Обновить все контроллеры домена contoso.com до Windows Server 2008 R2. Все контроллеры двух дочерних доменов обновить до Windows Server 2008.
 - d. В корневом домене установить функциональный уровень домена Windows Server 2008 R2. В двух дочерних доменах установить функциональный уровень Windows Server 2008.
 - e. Во всех трех доменах установить функциональный уровень Windows Server 2008 R2.
 - f. На сервере глобального каталога (контроллере домена) в корневом домене повысить функциональный уровень леса до Windows Server 2008 R2.

- g. В каждом из трех доменов на сервере глобального каталога (контроллере домена) повысить функциональный уровень леса до Windows Server 2008 R2.
 - h. Выполнить команду на основе командлета Enable-ADOptionalFeature.
 - i. Выполнить команду на основе командлета Enable-ADAccount.
 - j. Перенастроить размещение IM FSMO.
2. Вы создали и настроили PSO, содержащий политики блокировки учетных записей, отличающиеся от политики по умолчанию. К каким сущностям можно применять этот PSO? (Каждый ответ является законченным решением. Выберите два.)
- a. Глобальная группа безопасности.
 - b. Учетная запись пользователя домена.
 - c. Подразделение.
 - d. Глобальная группа рассылки.
 - e. Учетная запись компьютера.
3. Какой инструмент позволяет просматривать данные Active Directory, хранящиеся в моментальных снимках?
- a. SACL.
 - b. PSC.
 - c. Средство интеллектуального анализа данных AD DS.
 - d. Мастер установки AD DS.
4. Вы планируете перенести ресурсы из домена Windows NT 4 в существующий лес Active Directory. Доверие какого типа следует установить?
- a. Доверие леса.
 - b. Внешнее доверие.
 - c. Доверие к сфере.
 - d. Сокращенное доверие.
5. Вы администратор домена компании Litware. Совместно с коллегами (не являющимися администраторами домена) из филиалов вы установили контроллеры домена только для чтения (RODC) во всех филиалах. Теперь требуется изменить политику репликации паролей для одного из контроллеров домена только для чтения. Как это сделать?
- a. В каждом филиале попросить коллегу, имеющего право входа на RODC, открыть оснастку **Active Directory — пользователи и компьютеры** и убедиться, что эта оснастка подключена к соответствующему RODC, после чего изменить параметры на вкладке **Политика репликации паролей** (Password Replication Policy) диалогового окна свойств RODC.
 - b. В каждом филиале добавить пользователя, имеющего право интерактивного входа на RODC, в группу администраторов домена. Попросить этого пользователя зайти на RODC, запустить Диспетчер сервера и раскрыть узел **Конфигурация** (Configuration), откуда можно обратиться к диалоговому окну **Политика репликации паролей** (Password Replication Policy).

- c. Подключиться к каждому RODC через удаленный рабочий стол. Запустить диспетчер сервера и раскрыть узел **Конфигурация** (Configuration), откуда можно обратиться к диалоговому окну **Политика репликации паролей** (Password Replication Policy).
 - d. Откройте оснастку **Active Directory — пользователи и компьютеры** и убедитесь, что она подключена к контроллеру домена с возможностью записи, расположенному в главном офисе. Найти соответствующий RODC в контейнере **Контроллеры домена** (Domain Controllers) и открыть его диалоговое окно свойств. Внести необходимые изменения на вкладке **Политика репликации паролей** (Password Replication Policy).
6. Вы планируете создать двустороннее доверие лесов между лесом вашей компании и лесом недавно приобретенной организации. Какой минимальный функциональный уровень леса необходим в обеих компаниях?
 - a. Windows 2000.
 - b. Windows 2000, основной режим.
 - c. Windows Server 2003.
 - d. Windows Server 2008.
 - e. Windows Server 2008 R2.
 7. Вы планируете переименовать домен при помощи утилиты Netdom.exe. Контроллеры домена работают под управлением Windows Server 2003, Windows Server 2008 и Windows Server 2008 R2. Вы не планируете обновлять контроллеры домена, работающие под управлением Windows Server 2003. Какой функциональный уровень домена позволит реализовать такой план?
 - a. Windows Server 2008 R2.
 - b. Windows Server 2008.
 - c. Windows Server 2003.
 - d. Windows 2000, основной режим.
 - e. Windows 2000, смешанный режим.

Занятие 2. Службы сертификации Active Directory

Центры сертификации (Certificate Authority, CA) важны для сетевой инфраструктуры организации так же, как контроллеры домена, DNS- и DHCP-серверы. На этом занятии вы узнаете, как шаблоны сертификатов влияют на выдачу цифровых сертификатов, как настраивать автоматическую выдачу сертификатов пользователям, и как настраивать сопутствующие технологии, такие как сетевые ответчики и перемещение учетных данных. Знакомство с этими технологиями поможет вам внедрить сертификаты в свою среду Windows Server 2008 или 2008 R2.

Изучив материал этого занятия, вы сможете:

- ✓ Устанавливать центры сертификации Active Directory и управлять ими.
- ✓ Настраивать автоматическую регистрацию сертификатов.
- ✓ Настраивать перемещение учетных данных.
- ✓ Настраивать сетевого ответчика для служб сертификации.

Продолжительность занятия — примерно 45 мин.

Типы центров сертификации

Планируя развертывание служб сертификации в сети организации, необходимо определить, какой центр сертификации (ЦС) лучше всего удовлетворяет вашим требованиям. Существует четыре типа ЦС:

- корневой ЦС предприятия;
- подчиненный ЦС предприятия;
- автономный корневой ЦС;
- автономный подчиненный ЦС.

Тип развертываемого ЦС зависит от того, как будут использоваться сертификаты в сети, и от состояния существующего окружения. Во время установки служб ролей сертификации необходимо выбрать ЦС предприятия или автономный ЦС (рис. 3-9). Изменить тип после развертывания ЦС нельзя.

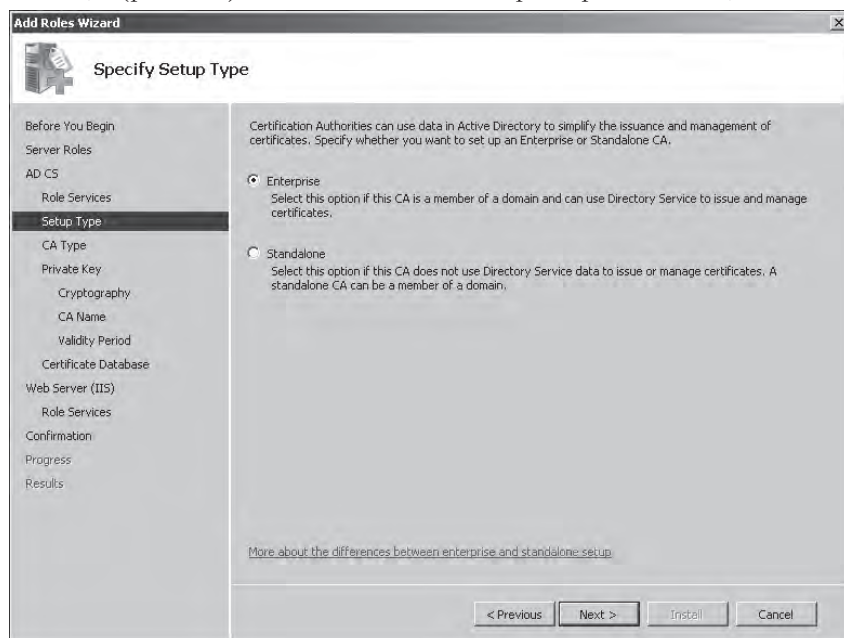


Рис. 3-9. Выбор ЦС предприятия или автономного ЦС

ЦС предприятия требует доступа к Active Directory. ЦС такого типа используют групповую политику для передачи списков доверенных сертификатов пользователям и компьютерам домена и публикуют в Active Directory списки отзыва сертификатов (CRL). ЦС предприятия выдают сертификаты на основе шаблонов сертификатов, которые предоставляют следующие возможности:

- ЦС предприятия принудительно проверяют учетные данные пользователей во время регистрации сертификатов. Каждый шаблон сертификатов имеет набор разрешений безопасности, определяющий, разрешено ли пользователю получать сертификаты, созданные на основе этого шаблона.
- Имена сертификатов автоматически генерируются на основе информации, хранящейся в Active Directory. Способ, которым это делается, определяется конфигурацией шаблона сертификатов.

- Для выдачи сертификатов может использоваться автоматическая регистрация, значительно упрощающая процесс распространения сертификатов. Автоматическая регистрация настраивается путем применения разрешений шаблонов сертификатов.

ЦС предприятия полностью интегрированы в среду Windows Server 2008/2008 R2. ЦС этого типа максимально упрощают выдачу сертификатов клиентам Active Directory и управление ими.

Автономные ЦС не требуют использования Active Directory. Когда автономный ЦС получает запрос на сертификат, запрашивающая сторона должна предоставить всю необходимую информацию для идентификации и вручную указать требуемый тип сертификата. При использовании ЦС предприятия это происходит автоматически. По умолчанию запросы к автономному ЦС требуют утверждения администратором. Вмешательство администратора необходимо, поскольку нет автоматизированного способа проверки учетных данных запрашивающей стороны. Автономные ЦС не используют шаблоны сертификатов, что ограничивает возможности администратора по настройке сертификатов для конкретных нужд организации.

Автономные ЦС можно развертывать на компьютерах, входящих в домен. Если автономный ЦС установлен администратором предприятия или пользователем, которому делегированы аналогичные права, информация об этом ЦС будет добавлена в хранилище сертификатов доверенных корневых центров сертификации для всех пользователей и компьютеров домена. Также этот ЦС сможет публиковать свой список отозванных сертификатов в Active Directory.

Выбор между корневым и подчиненным ЦС зависит от того, есть ли существующая инфраструктура сертификации. Корневые ЦС — наиболее доверенные ЦС в иерархии инфраструктуры открытого ключа (PKI). Корневые ЦС находятся на верхнем уровне инфраструктуры в качестве точек с безоговорочным доверием, а значит должны быть максимально защищенными. Корневой ЦС выдает сертификаты только подчиненным ЦС, а когда не используется для этой цели, должен быть отключен от сети и находиться в безопасном месте для уменьшения вероятности того, что он будет скомпрометирован.

Если корневой ЦС скомпрометирован, все сертификаты в инфраструктуре PKI организации должны считаться скомпрометированными. Цифровые сертификаты — это заявления о доверии. Если нельзя доверять главному центру, от которого должно исходить доверие, то нельзя доверять и любым сертификатам, полученным от этого центра.

Подчиненные ЦС — серверы в сетевой инфраструктуре, выдающие пользователям, компьютерам и службам сертификаты, необходимые им для повседневной работы. Организация может иметь много подчиненных ЦС, каждому из которых корневой ЦС выдает сертификат. Если один из подчиненных ЦС скомпрометирован, корневой ЦС может аннулировать доверие к этому ЦС. Ненадежными будут считаться только сертификаты, выданные этим подчиненным ЦС. Скомпрометированный подчиненный ЦС можно заменить, не заменяя всю инфраструктуру сертификации. Подчиненные ЦС можно заменять, но если скомпрометирован корневой ЦС, это обычно означает, что необходимо заново развертывать лес Active Directory с чистого листа. Если скомпрометирован автономный корневой ЦС, необходимо заменить также инфраструктуру PKI.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Обзор служб сертификации

Подробнее о службах сертификации Active Directory в Windows Server 2008 R2 см. по адресу <http://technet.microsoft.com/ru-ru/library/cc755071.aspx>.

Ролевое администрирование служб сертификации

Из-за тесной связи служб сертификации с инфраструктурой безопасности во многих организациях управлением разными компонентами служб сертификации занимаются разные люди. Одна группа отвечает за управление самим ЦС, другая — за управление сертификатами, которые выдает этот ЦС. Такое разделение реализуется посредством назначения служб ролей центра сертификации.

Две критически важные роли — администратор ЦС и диспетчер сертификатов. Роли назначаются путем назначения разрешений на вкладке **Безопасность** (Security) в диалоговом окне свойств сервера сертификатов (сервера, играющего роль ЦС). Роль администратора ЦС назначается предоставлением пользователю или группе разрешения **Управление ЦС** (Manage CA). Роль диспетчера сертификатов назначается предоставлением разрешения **Выдача и управление сертификатами** (Issue and Manage Certificates). По умолчанию эти роли могут назначать администраторы домена, администраторы предприятия и локальные администраторы. На рис. 3-10 глобальная группа безопасности **Alpha** играет роль диспетчера сертификатов, так как имеет разрешение **Выдача и управление сертификатами** (Issue and Manage Certificates).

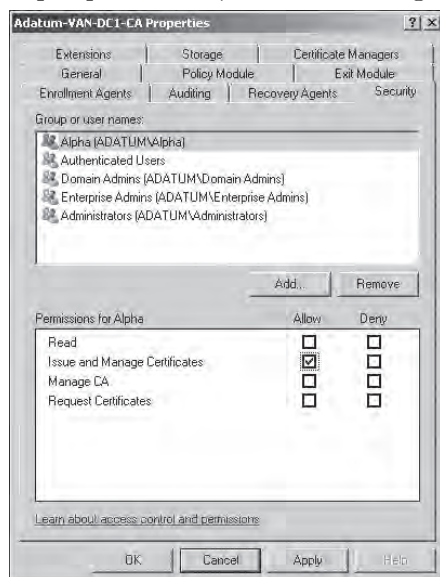


Рис. 3-10. Группе Alpha назначена роль диспетчера сертификатов

Эти роли имеют следующие характеристики:

- **Администратор ЦС.** Эту роль следует назначать сотрудникам, отвечающим за настройку и обслуживание самого ЦС. Пользователи, которым назначена эта роль, могут запускать и останавливать сервер сертификатов, настраивать расширения, назначать роли, обновлять ключи ЦС, определять агентов восстановления ключей и настраивать ограничения диспетчера сертификатов.

- **Диспетчер сертификатов.** Эту роль следует назначать сотрудникам, отвечающим за утверждение запросов на регистрацию и отзыв сертификатов. Можно ограничивать диспетчеров сертификатов, разрешая управление только отдельными группами или шаблонами. Можно дать одной группе разрешение на утверждение сертификатов, выданных на основе одного шаблона, а другой группе — разрешение на утверждение сертификатов, выданных на основе другого шаблона. Эти ограничения настраиваются на вкладке **Диспетчеры сертификатов** (Certificate Managers) (рис. 3-11).

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Ролевое администрирование

Подробнее о реализации ролевого администрирования в службах сертификации см. по адресу <http://technet.microsoft.com/ru-ru/library/cc732590.aspx>.

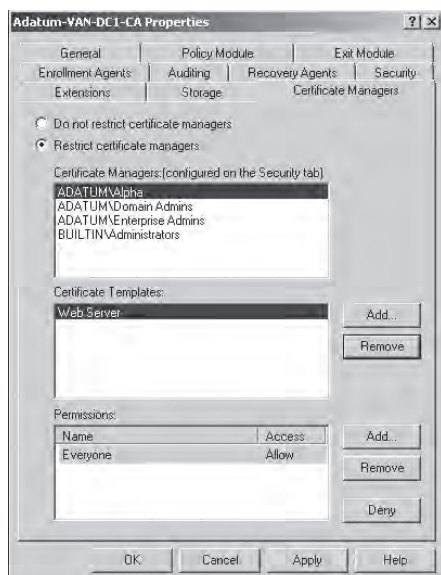


Рис. 3-11. Группа пользователей Alpha может управлять сертификатами веб-сервера

Установка сертификата корневого ЦС

Обычно сертификат корневого ЦС — первая служба роли сертификации Active Directory (AD CS), устанавливаемая в организации. Если организация имеет базовую инфраструктуру PKI, корневой ЦС может быть единственным ЦС, который необходимо развернуть. Сертификат корневого ЦС устанавливает основные правила выдачи и использования сертификатов для PKI. Он определяет стандарты, определяющие, что допустимо и недопустимо в иерархии PKI, а службы AD CS применяют эти стандарты ко всем остальным ЦС и службам ролей AD CS.

Корневой ЦС может быть ЦС предприятия или подчиненным ЦС. Многие организации минимизируют риск компрометации корневого ЦС, держа его отключенным от сети, за исключением случаев, когда он требуется для обработки запросов на получение сертификата подчиненного ЦС.

Чтобы установить автономный корневой ЦС на сервере под управлением Windows Server 2008 или 2008 R2, необходимо, как минимум, быть членом

локальной группы администраторов на этом сервере. Для установки ЦС предприятия необходимо (как минимум) входить в группу администраторов домена. Высокоуровневая процедура установки сертификата корневого ЦС включает в себя следующее:

1. В Диспетчере сервера щелкните **Добавить роли** (Add Roles). Выберите службу роли центра сертификации Active Directory.
2. На странице **Выбор служб ролей** (Select Role Services) щелкните **Центр сертификации** (Certification Authority).
3. На странице **Задание типа установки** (Specify Setup Type) выберите необходимый тип ЦС: автономный (Standalone) или предприятия (Enterprise). Заметьте, что при выборе ЦС предприятия необходимо иметь сетевое подключение к контроллеру домена.
4. На странице **Задание типа ЦС** (Specify CA Type) выберите **Корневой ЦС** (Root CA).
5. На странице **Установка закрытого ключа** (Set Up Private Key) щелкните **Создать новый закрытый ключ** (Create A New Private Key).
6. На странице **Настройка шифрования** (Configure Cryptography) выберите поставщика служб шифрования, длину ключа и алгоритм хеширования.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ **Параметры шифрования**

Подробнее о поставщиках служб шифрования, длине ключей и алгоритмах хеширования см. по адресу <http://technet.microsoft.com/ru-ru/library/cc731828.aspx>.

7. На странице **Задание имени ЦС** (Configure CA Name) укажите уникальное имя для идентификации ЦС.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ **Имя ЦС**

Подробнее об именах ЦС см. по адресу <http://technet.microsoft.com/ru-ru/library/cc770402.aspx>.

8. На странице **Установить срок действия** (Set Validity Period) укажите число лет или месяцев, в течение которых сертификат корневого ЦС будет оставаться действительным.
9. На странице **Настройка базы данных сертификатов** (Configure Certificate Database) обычно оставляются предложенные расположения. Если хотите, можете указать другое расположение базы данных сертификатов и журнала.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ **База данных сертификатов**

Подробнее о базе данных сертификатов см. по адресу <http://technet.microsoft.com/ru-ru/library/cc770463.aspx>.

10. На странице **Подтверждение параметров установки** (Confirm Installation Options) просмотрите выбранные параметры. Если все правильно, щелкните **Установить** (Install).

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ **Установка сертификата корневого ЦС**

Подробные инструкции по установке корневого ЦС см. по адресу <http://technet.microsoft.com/ru-ru/library/cc731183.aspx>.

Улучшения в Windows Server 2008 R2

В Windows Server 2008 R2 сохранились все улучшения служб AD CS, появившиеся в Windows Server 2008, и появились новые функции и службы, повышающие гибкость развертывания PKI, снижающие затраты на администрирование и облегчающие поддержку развертывания NAP.

- **Веб-служба регистрации сертификатов и веб-служба политик регистрации сертификатов.** Эти службы позволяют регистрировать сертификаты по протоколу HTTP.
- **Поддержка регистрации сертификатов через границы лесов** позволяет объединять ЦС в средах с несколькими лесами.
- **Улучшенная поддержка центров массовой сертификации** позволяет уменьшать размер базы данных ЦС для некоторых развертываний NAP и других массовых ЦС.

Веб-служба регистрации сертификатов и веб-служба политик регистрации сертификатов

Эти новые службы ролей AD CS делают возможной основанную на политике регистрацию сертификатов по протоколу HTTP, используя автоматическую регистрацию (см. далее). Веб-службы действуют как посредник между клиентом и ЦС. Это делает ненужным прямое взаимодействие между клиентом и ЦС и позволяет регистрировать сертификаты через Интернет и через границы лесов. Веб-службы регистрации сертификатов доступны во всех редакциях Windows Server 2008 R2.

Рассмотрим пример. Компания Northwind Traders — крупная многонациональная организация, имеющая сетевую инфраструктуру с несколькими лесами. Компания имеет инфраструктуру открытых ключей (PKI), но может получить преимущества повышенной доступности регистрации сертификатов, предоставляемые веб-службами регистрации сертификатов, которые позволят клиентам Windows 7 использовать HTTP для регистрации сертификатов от ЦС из разных лесов Windows Server 2008 R2. Чтобы использовать эту возможность, ЦС предприятия должен работать под управлением версии Enterprise или Datacenter Windows Server 2008 R2, Windows Server 2008 или Windows Server 2003.

Trey Research и Contoso — партнерские компании, чья сетевая инфраструктура формирует внешнюю сеть. В Contoso работает несколько мобильных сотрудников. Новые веб-службы позволяют бизнес-партнерам и мобильным работникам регистрировать сертификаты через Интернет. Как и в предыдущем сценарии, клиенты должны работать под управлением Windows 7, леса Active Directory обеих организаций должны иметь схемы Windows Server 2008 R2, а ЦС предприятия обеих компаний должны работать под управлением версий Enterprise или Datacenter Windows Server 2008 R2, Windows Server 2008 или Windows Server 2003.

ВНИМАНИЕ! Веб-служба регистрации сертификатов может сделать внешнюю сеть более уязвимой

Веб-служба регистрации сертификатов отправляет запросы от имени клиентов, а следовательно, ей необходимо доверить делегирование. Поэтому ее развертывание во внешней сети делает сетевую инфраструктуру более уязвимой к атакам. Из-за этого некоторые организации предпочитают не доверять делегирование этой службе. В таких случаях веб-службу регистрации сертификатов и выдающий ЦС можно настроить так, чтобы принимались только запросы на обновление, подписанные существующими сертификатами. Делегирование при этом не требуется.

Регистрация сертификатов через границы лесов с двусторонним доверием

До выхода Windows Server 2008 R2 с улучшенными службами AD CS центры сертификации могли выдавать сертификаты только членам того же леса, а каждый лес имел собственную инфраструктуру открытых ключей. С появлением поддержки ссылок LDAP в Windows Server 2008 R2 центры сертификации могут выдавать сертификаты через границы лесов, имеющих двусторонние доверительные отношения. Это позволяет регистрировать сертификаты напрямую, не используя HTTP.

Например, если в компании Northwind Traders из предыдущего примера ЦС предприятия работает под управлением Windows Server 2008 R2 Datacenter или Enterprise, если каждый лес имеет PKI, и если между лесами установлено доверие, то ЦС может выдавать сертификаты через границы лесов. В такой ситуации есть несколько ограничений. Если ЦС предприятия работает под управлением соответствующей версии Windows Server 2008 R2, потребуется только функциональный уровень леса Windows Server 2003 или выше, а клиенты могут работать не только под управлением Windows 7, но также Windows XP, Windows Server 2003 или Windows Vista.

Поддержка центров массовой сертификации

Если ЦС обрабатывает большое число запросов, можно пропускать некоторые операции с базой данных ЦС, чтобы уменьшить ее размер. Например, ЦС генерирует большой объем трафика, если в сети развернута принудительная защита доступа (NAP) с помощью IPSec. Срок сертификатов NAP обычно истекает через несколько часов после выдачи, и ЦС может выдавать несколько сертификатов для каждого компьютера каждый день. По умолчанию в базе данных ЦС хранятся записи для каждого запроса и выданного сертификата. Высокое число запросов увеличивает скорость роста базы данных ЦС и затраты на администрирование. Можно указать, что выданные сертификаты должны храниться в другом месте, а не в базе данных ЦС на ЦС предприятия, работающего под управлением любой версии Windows Server 2008 R2.

Используя эту возможность, помните, что, поскольку выданные сертификаты не хранятся в базе данных ЦС, их отзыв невозможен. Однако поддержка списка отозванных сертификатов для большого числа сертификатов с коротким сроком действия часто непрактично и не дает никаких преимуществ, поэтому возможностью отзыва можно пренебречь.

Настройка перемещения учетных данных

Перемещение учетных данных позволяет хранить сертификаты и закрытые ключи в Active Directory. Например, сертификат шифрованной файловой системы (EFS) пользователя можно хранить в Active Directory и предоставлять пользователю, когда тот входит на другой компьютер в том же домене. Для шифрования файлов всегда можно использовать один и тот же сертификат. Это означает, что пользователь может зашифровать файлы на съемном USB-устройстве с файловой системой NTFS на одном компьютере, а затем расшифровать их на другом, поскольку сертификат EFS будет передан на второй компьютер во время входа в систему. Перемещение учетных данных позволяет также удалять все сертификаты и ключи пользователя при выходе из системы.

Перемещение учетных данных включается политикой **Клиент служб сертификации: перемещение учетных данных** (Certificate Services Client — Credential Roaming), которую можно найти при помощи компонента Диспетчера сервера **Управление групповой политикой** (Group Policy Management) под узлом **Конфигурация пользователя | Политики | Конфигурация Windows | Параметры безопасности | Политики открытого ключа** (User Configuration | Policies | Windows Settings | Security Settings | Public Key Properties) (рис. 3-12).

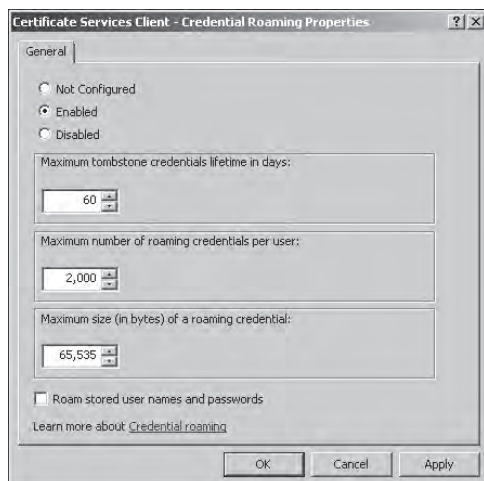


Рис. 3-12. Политика перемещения учетных данных

Когда пользователь входит на клиент в домене, в котором включена политика перемещения учетных данных, сертификаты из пользовательского хранилища на клиенте сравниваются с сертификатами, хранящимися для этого пользователя в Active Directory.

- Если сертификаты в пользовательском хранилище не устарели, дальнейших действий не предпринимается.
- Если в Active Directory хранятся более новые сертификаты, они копируются на клиент.
- Если более новые сертификаты хранятся в пользовательском хранилище, сертификаты в Active Directory обновляются.

Перемещение учетных данных выполняет синхронизацию и решает конфликты между сертификатами и закрытыми ключами на любых клиентских станциях, на которые входит пользователь, а также между сертификатами и закрытыми ключами, хранящимися в Active Directory. Перемещение учетных данных инициируется каждый раз, когда изменяется закрытый ключ или сертификат в локальном хранилище, когда пользователь блокирует или разблокирует компьютер, и когда обновляется групповая политика. Перемещение учетных данных поддерживается в Windows Server 2008 R2, Windows Server 2008, Windows Server 2003 SP1, Windows 7, Windows Vista и Windows XP SP2.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Перемещение учетных данных

Подробнее о перемещении учетных данных см. по адресу <http://technet.microsoft.com/ru-ru/library/cc770797.aspx>.

Настройка авторегистрации

Авторегистрация сертификатов позволяет распространять сертификаты на клиенты без непосредственного вмешательства клиентов. Кроме того, это делает возможной автоматическую регистрацию субъектов для определенных сертификатов, а также позволяет отзывать выданные сертификаты и автоматически обновлять истекшие сертификаты без вмешательства субъекта или администратора. В большинстве случаев авторегистрации проходит без уведомления пользователя, хотя можно настраивать шаблоны сертификатов так, чтобы они взаимодействовали с субъектами.

Настройка шаблона для авторегистрации

Чтобы сертификат можно было регистрировать автоматически, необходимо настроить некоторые параметры шаблона сертификатов. Шаблоны сертификатов изменяются при помощи оснастки **Шаблоны сертификатов** (Certificate Templates), которую нужно добавить в настраиваемую консоль MMC. Создавать и изменять шаблоны сертификатов могут только пользователи с разрешениями роли диспетчера сертификатов.

Заметьте, что при использовании консоли **Шаблоны сертификатов** нельзя настроить разрешения авторегистрации для шаблона сертификатов первого уровня. Для таких сертификатов минимальный поддерживаемый уровень ЦС — Windows 2000. Для сертификатов второго уровня это Windows Server 2003. Второй уровень — минимальный уровень шаблонов сертификатов, поддерживающий авторегистрацию. Шаблоны сертификатов третьего уровня поддерживаются только клиентами под управлением Windows Server 2008, Windows Server 2008 R2, Windows Vista и Windows 7. Шаблоны сертификатов третьего уровня позволяют администраторам настраивать дополнительные параметры шифрования по стандарту Suite B. Эти параметры не обязательны для авторегистрации сертификатов, и в большинстве случаев для удовлетворения потребностей организации достаточно шаблонов сертификатов второго уровня.

Чтобы создать новый шаблон сертификатов на основе существующего, следует настроить скопированный шаблон как вытесняемый. Это позволяет обновлять параметры ранее настроенных сертификатов. Также потребуется настроить ЦС, чтобы опубликовать этот новый шаблон, используя консоль **Центр серти-**

фикации (Certification Authority). Чтобы настроить для определенного шаблона автоматическую регистрацию сертификатов, выполните следующее:

1. Откройте оснастку **Шаблоны сертификатов** (Certificate Templates).
2. Щелкните правой кнопкой мыши шаблон сертификатов, который хотите изменить, и выберите команду **Свойства** (Properties).
3. Настройте параметры на вкладках **Общие** (General), **Обработка запроса** (Request Handling) и **Требования выдачи** (Issuance Requirements). Заметьте, что не каждый шаблон сертификатов имеет все три вкладки в диалоговом окне свойств. Например, шаблон сертификатов **Базовое шифрование EFS** (Basic EFS) не имеет вкладки **Требования выдачи**. Кроме того, этот этап не обязателен для авторегистрации, но параметры на этих вкладках следует просмотреть, так как они позволяют более точно настроить автоматическую выдачу сертификатов.
4. На вкладке **Безопасность** (Security) шаблона сертификата выберите группу, которой разрешено автоматически регистрировать сертификаты, и установите флажок **Разрешить** (Allow) для разрешения **Автоматическая подача заявок** (Autoenroll). На рис. 3-13 показано включение авторегистрации для группы аутентифицированных пользователей, использующих аутентификацию Kerberos (шаблон сертификатов второго уровня).

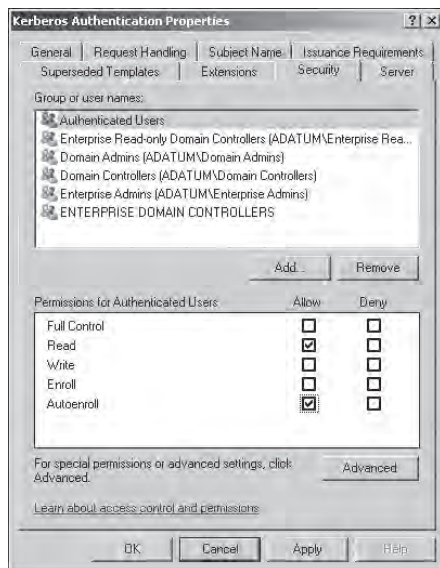


Рис. 3-13. Настройка разрешений для включения автоматической регистрации

Настройка групповой политики для авторегистрации

После настройки разрешений для шаблонов сертификатов следующим этапом развертывания авторегистрации сертификатов в сети организации будет настройка политики домена по умолчанию. Чтобы настроить групповую политику для авторегистрации, выполните следующее:

1. Измените объект групповой политики домена по умолчанию, используя консоль управления групповой политикой, которую можно найти в разделе **Компоненты** (Features) Диспетчера сервера.
2. Под узлом **Конфигурация пользователя | Политики | Конфигурация Windows | Параметры безопасности | Политики открытого ключа** (User Configuration | Policies | Windows Settings | Security Settings | Public Key Policies) дважды щелкните **Клиент служб сертификации: автоматическая подача заявок** (Certificate Services Client – Auto-Enrollment). Откроется диалоговое окно свойств авторегистрации.
3. В раскрывающемся списке **Модель конфигурации** (Configuration Model) выберите **Включено** (Enabled), а затем настройте параметры истечения срока и обновления (рис. 3-14).

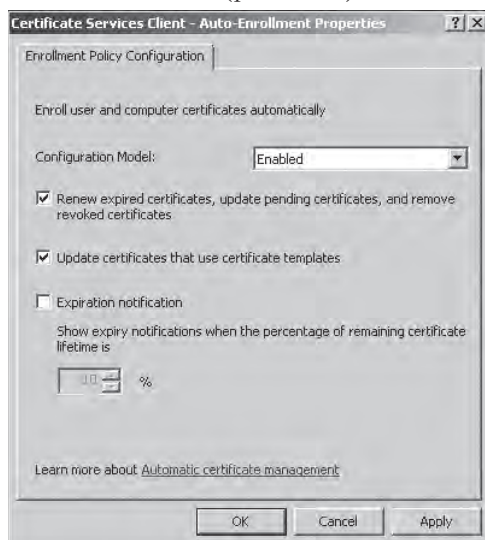


Рис. 3-14. Настройка политик авторегистрации

После включения политики авторегистрации сертификаты, имеющие шаблоны, настроенные для авторегистрации, будут разворачиваться автоматически. В политике авторегистрации можно настроить следующие параметры:

- **Обновлять сертификаты с истекшим сроком действия или в состоянии ожидания и удалять отозванные сертификаты** (Renew Expired Certificates, Update Pending Certificates, And Remove Revoked Certificates). Эта политика относится, в основном, к управлению сертификатами. Если включена авторегистрация, возможно, вы захотите, чтобы истекшие сертификаты и сертификаты в состоянии ожидания автоматически обновлялись, а отозванные сертификаты удалялись. Включение этой политики значительно упрощает работу администраторов сертификатов.
- **Обновлять сертификаты, использующие шаблоны сертификатов** (Update certificates that use certificate templates). Если эта политика включена, а шаблон, на основе которого выдан сертификат, изменен или заменен, выданный сертификат будет обновлен.

- **Уведомлять об окончании срока действия** (Expiration Notification). Эта политика менее важна, если настроено автоматическое обновление сертификатов с истекшим сроком действия, но может быть полезной, когда шаблоны сертификатов настроены так, что автоматическое обновление (в отличие от автоматической регистрации) не выполняется.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Настройка авторегистрации

Подробнее о настройке авторегистрации см. по адресу <http://technet.microsoft.com/ru-ru/library/cc731522.aspx>.

Проверьте себя

1. Какой ЦС следует установить первым, если требуется интегрировать сертификаты с Active Directory?
2. Какие клиенты и центры сертификации поддерживают шаблоны третьего уровня?

Ответы

1. Корневой ЦС предприятия.
2. Шаблоны третьего уровня поддерживают Windows Vista, Windows 7, Windows Server 2008 и Windows Server 2008 R2.

Настройка поддержки регистрации через Интернет

Регистрация через Интернет дает пользователям Internet Explorer 6 и выше подавать заявки на сертификаты непосредственно через веб-приложения. При помощи веб-регистрации можно выполнять следующее:

- запрашивать сертификаты и просматривать существующие запросы на сертификаты;
- обращаться к спискам отзыва сертификатов;
- выполнять регистрацию смарт-карт.

Регистрация через Интернет разворачивается, в основном, для предоставления механизма регистрации компаниям, которым требуется выдавать и обновлять сертификаты для пользователей и компьютеров, не входящих в домен Active Directory, или использующих операционные системы, выпущенные не Microsoft. Пользователи обозревателей, отличных от Internet Explorer 6 и выше, могут подавать запросы на регистрацию при помощи приложения для регистрации через Интернет, но сначала они должны создать запрос с помощью файла PKCS #10. Если запрос подан успешно, пользователи могут повторно подключаться к приложению для регистрации через Интернет, загружать и устанавливать запрошенные сертификаты.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ PKCS #10

Подробнее о PKCS #10 см. по адресу <http://tools.ietf.org/html/rfc2986>. Однако на экзамене вряд ли будут вопросы о подробностях PKCS.

Чтобы настроить на сервере поддержку регистрации через Интернет, необходимо добавить к роли сервера роль веб-службы регистрации сертификатов. Если эта веб-служба установлена на компьютере, действующем как ЦС, никакой дальнейшей настройки не требуется. Если она установлена на отдельном компьютере, требуется указать ЦС в процессе установки веб-службы.

Регистрация через Интернет имеет следующие ограничения:

- регистрация через Интернет не может выполняться для шаблонов сертификатов третьего уровня; поддерживаются только шаблоны сертификатов первого и второго уровня;
- при помощи регистрации через Интернет нельзя запрашивать сертификаты компьютеров у ЦС под управлением Windows Server 2008 или 2008 R2;
- если службы IIS установлены в 64-разрядной версии Windows Sever 2008 или 2008 R2, некоторые 32-разрядные веб-приложения нельзя установить, поскольку это приведет к запуску IIS в 32-разрядном режиме. Веб-служба регистрации через Интернет попытается установиться как 64-разрядное веб-приложение, и установка завершится неудачей. Это не относится к 32-разрядным версиям Windows Server 2008.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Настройка регистрации через Интернет

Подробнее о настройке поддержки регистрации через Интернет см. по адресу <http://technet.microsoft.com/ru-ru/library/cc732895.aspx>.

Настройка списков отзыва сертификатов

Службы сертификации не только выдают сертификаты. Сертификаты — это знаки доверия, действие которых в некоторых случаях приходится отменять. Этот процесс называется *отзывом сертификатов*. Наиболее распространенный способ публикации сведений о том, какие из выданных ЦС сертификатов больше не действуют — использование списков отзыва сертификатов (CRL). Эти списки содержат серийные номера сертификатов, которые были отозваны или приостановлены. CRL выпускаются центром сертификации, выдавшим соответствующие сертификаты, а не выше- или нижестоящим ЦС. Перед использованием сертификата выполняется проверка CRL ЦС, выпустившего этот сертификат. Расположение CRL указывается в сертификате, чтобы клиент знал, где проверить действительность сертификата.

Задание точки распространения CRL

На вкладке **Расширения** (Extensions) диалогового окна свойств сервера сертификации (рис. 3-15) можно добавлять, удалять и изменять точки распространения CRL. Изменяя список точек распространения, учитывайте, что эти изменения действуют только для сертификатов, которые будут выданы позже, но не для уже выданных. Изменять параметры точек распространения CRL могут пользователи, которым назначена роль диспетчера сертификатов. Адреса URL списков отозванных сертификатов можно указывать в форматах HTTP, FTP, LDAP и FILE.

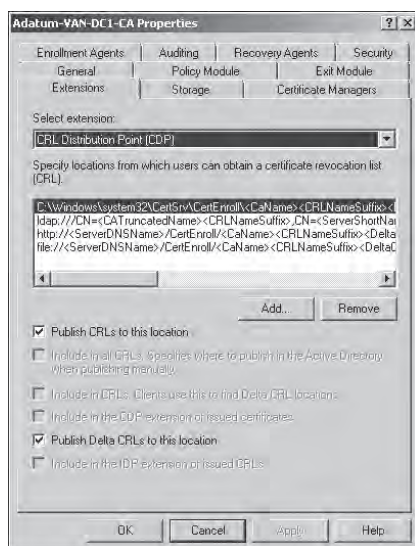


Рис. 3-15. Настройка точки распространения CRL

Настройка публикации CRL и разностных CRL

Поскольку CRL может очень быстро увеличиваться в размерах, можно публиковать уменьшенную версию — разностный CRL, но делать это чаще. Разностный CRL содержит только данные о сертификатах, отозванных с момента публикации последнего полного CRL. Это позволяет клиентам загрузить небольшой разностный CRL и добавить его к кэшированной копии полного CRL, чтобы получить список всех отозванных сертификатов. Разностные CRL позволяют чаще публиковать данные об отзыве, что делает службу сертификации более защищенной. Устаревший CRL не может проинформировать клиентов о последних отозванных сертификатах, так как они будут указаны только при следующей публикации полного CRL.

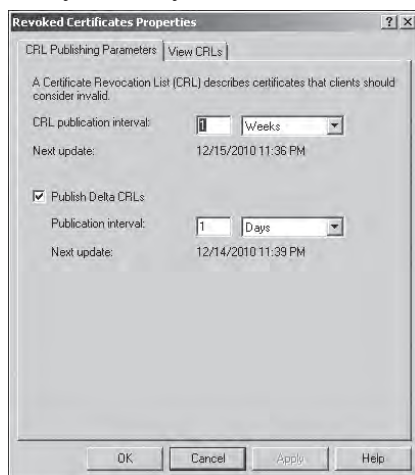


Рис. 3-16. Настройка интервала публикации CRL

Интервалы публикации CRL и разностных CRL настраиваются в диалоговом окне, показанном на рис. 3-16. Чтобы открыть это диалоговое окно, щелкните правой кнопкой мыши узел **Отозванные сертификаты** (Revoked Certificates) под узлом ЦС в Диспетчере сервера и выберите команду **Свойства** (Properties). По умолчанию CRL публикуется раз в неделю, а разностный CRL раз в день.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Отзыв сертификатов

Подробнее о настройке отзыва сертификатов см. по адресу <http://technet.microsoft.com/ru-ru/library/cc771079.aspx>.

Настройка сетевого ответчика для служб сертификации

В период пиковой активности, когда большое число пользователей выполняет вход с использованием смарт-карт, шифрует файлы или использует цифровые подписи, могут возникать значительные задержки в публикации CRL. Это вызвано тем, что приходится проверять весь список отзыва сертификатов, и, как говорилось выше, CRL может значительно увеличиваться в размерах. Нагрузку по проверке CRL нельзя разделить с другим ЦС. Предпринимались попытки решить эту проблему при помощи разделенных, разностных и непрямых CRL. Все эти решения приводили к усложнению реализации ЦС, но не особо успешно решали проблему со скачками трафика. На смену им пришел протокол OCSP (Online Certificate Status Protocol).

Сетевой ответчик получает и отвечает только на запросы о состоянии отдельных сертификатов. Например, вместо того чтобы загружать с ЦС весь CRL для проверки действительности сертификата пользователя Don Hall, клиент подает запрос сетевому ответчику и получает ответ, содержащий только информацию об этом сертификате. Это значительно снижает нагрузку на выдающий ЦС и уменьшает сетевой трафик. CRL могут становиться очень большими, и их передача каждому из 100 клиентов вызовет большой объем трафика. В зависимости от размера CRL, передача информации об отзыве 100 разных сертификатов может потребовать меньше трафика, чем пересылка текущего CRL одному клиенту.

Протокол OCSP в Windows Server 2008 и 2008 R2 предоставляет следующие возможности:

- **Кэширование веб-прокси.** Кэш веб-прокси сетевого ответчика представляет собой интерфейс, через который клиент получает доступ к данным сетевого ответчика. Он реализован в виде расширения ISAPI, размещенного в службах IIS.
- **Поддержка запросов с параметрами и без параметров.** Запросы с параметрами и без параметров можно использовать для предотвращения атак с повторением пакетов на сетевые ответчики. Атаки с повторением основаны на повторении или задержке передачи настоящих данных. С помощью такой атаки можно указать, что отозванный сертификат все еще действителен.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Запросы с параметрами и без параметров

Параметр (nonce) — уникальный идентификатор, включенный в запрос OCSP. Подробнее о запросах с параметрами и без параметров см. по адресу [http://technet.microsoft.com/en-us/library/ee619783\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/ee619783(WS.10).aspx) (на англ. языке).

- **Расширенная поддержка криптографии.** Сетевой ответчик можно настроить на использование криптографического алгоритма с эллиптическими кривыми (ECC) и криптографического алгоритма SHA-256.
- **Интеграция с протоколом Kerberos.** Запросы и ответы OSCP можно обрабатывать вместе с данными проверки подлинности паролей Kerberos для быстрой проверки сертификатов сервера при входе в систему.
- **Одиночные сетевые ответчики и массивы сетевых ответчиков.** В качестве сетевого ответчика может действовать отдельный компьютер или несколько связанных компьютеров, что позволяет распределять нагрузку по проверке сертификатов между несколькими хостами.

Службу сетевого ответчика можно установить на ЦС, но Microsoft рекомендует развертывать ее на отдельном компьютере. Одиночный компьютер, на котором развернута служба сетевого ответчика, может предоставлять данные об отзыве сертификатов, выданных одним или несколькими ЦС. Как уже говорилось, данные одного ЦС можно распределить между несколькими сетевыми ответчиками.

Служба сетевого ответчика устанавливается на компьютеры под управлением Windows Server 2008 и 2008 R2 и управляется через оснастку **Сетевой ответчик** (Online Responder) (рис. 3-17). Заметьте, что эта консоль будет доступна только после развертывания службы сетевого ответчика, которое вы выполните на практических занятиях этой главы.

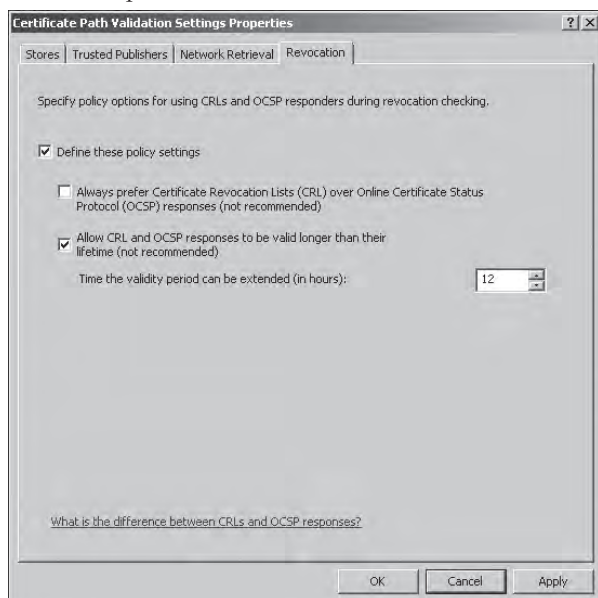


Рис. 3-17. Консоль управления сетевым ответчиком

Сетевые ответчики следует развертывать после развертывания ЦС, но перед выдачей клиентам сертификатов. Для развертывания службы сетевого ответчика на компьютере под управлением Windows Server 2008 или 2008 R2 необходимо выполнение следующих условий:

- на компьютере, где будет размещена служба сетевого ответчика, должны быть установлены службы IIS;
- в ЦС должен быть настроен шаблон сертификата подписи ответа OCSP, а для выдачи сертификата подписи ответа OCSP компьютеру, на котором будет установлен сетевой ответчик, должна использоваться авторегистрация. Сетевой ответчик не может предоставлять информацию о состоянии сертификата, выданного центром сертификации, стоящим в цепочке ЦС выше, чем центр, выдавший его сертификат подписи;
- в расширение доступа к сведениям о центрах сертификации (AIA) для сертификатов, выдаваемых центром сертификации, должен включаться URL-адрес сетевого ответчика. Этот URL-адрес используется клиентом для поиска сетевого ответчика, способного проверить состояние сертификата.

После развертывания сетевого ответчика администратор создает конфигурацию отзыва для всех ЦС и сертификатов ЦС, обслуживаемых этим сетевым ответчиком. Конфигурации отзыва включают все параметры, необходимые для ответа клиентам, запрашивающим состояние сертификатов, выданных с использованием определенного ключа ЦС. Эти параметры включают сертификат ЦС, сертификат подписи для сетевого ответчика и поставщика отзыва, предоставляющего данные об отзыве, используемые конфигурацией отзыва. При настройке одного сетевого ответчика для нескольких ЦС убедитесь, что сетевой ответчик имеет ключ и сертификат подписи для каждого обслуживаемого ЦС. На практикуме в конце занятия вы настроите сетевой ответчик.

Настройка массивов сетевых ответчиков

Если один сетевой ответчик не справляется с большим числом запросов, можно развернуть массив компьютеров, действующих как сетевые ответчики. Как уже говорилось на этом занятии, массив сетевых ответчиков может обрабатывать данные, полученные от одного или нескольких ЦС. Массивы сетевых ответчиков часто развертывают для обеспечения отказоустойчивости. Узлы массивов сетевых ответчиков можно развертывать в офисах филиалов или вспомогательных компаний, не имеющих постоянного подключения к выдающему ЦС.

В массиве сетевых ответчиков один член настроен как контроллер массива, остальные — как члены массива. Каждый сетевой ответчик в массиве можно настраивать отдельно, но когда возникают конфликты, параметры контроллера массива имеют преимущество перед параметрами рядовых членов.

Чтобы создать массив сетевых ответчиков, выполните следующее:

1. Настройте поддержку сетевых ответчиков на ЦС, используемых для выдачи сертификатов.
2. Добавьте службу сетевого ответчика на все серверы, которые планируется добавить в массив.
3. Добавьте сетевые ответчики в массив, открыв консоль **Сетевой ответчик** (Online Responder), выбрав узел **Элементы конфигурации массива** (Array Configuration Members) и щелкнув **Добавить элементы массива** (Add Array Members) в области **Действия** (Actions).

Параметры групповой политики OCSP

В Windows Server 2008 и 2008 R2 включено несколько параметров групповой политики, помогающих в управлении OCSP и использовании данных CRL. Чтобы обратиться к этим параметрам, измените политику домена по умолчанию в дереве консоли Диспетчера сервера и откройте вкладку **Отзыв (Revocation)** диалогового окна свойств узла **Конфигурация компьютера | Политики | Конфигурация Windows | Параметры безопасности | Политики открытого ключа | Параметры подтверждения пути сертификата (Computer Configuration | Policies | Windows Settings | Security Settings | Public Key Policies | Certificate Path Validation Settings)**.

Одна из причин для настройки этих политик состоит в том, что списки CRL имеют определенный срок действия, и если этот срок истекает раньше, чем становится доступным обновление, цепь проверки сертификатов может прерываться, даже если развернут сетевой ответчик. Если сетевой ответчик полагается на CRL с истекшим сроком, могут возникнуть проблемы. Установив флажок **Разрешить превышение срока действия над сроком жизни для ответов CRL и OCSP (Allow CRL and OCSP responses to be valid longer than their lifetime)**, можно увеличить срок действия списков CRL на случай, если они не будут своевременно обновлены.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Управление сетевыми ответчиками

Подробнее об управлении сетевыми ответчиками см. по адресу <http://technet.microsoft.com/ru-ru/library/cc725644.aspx>.

Служба подачи заявок на сетевые устройства

Служба подачи заявок на сетевые устройства позволяет ЦС под управлением Windows Server 2008 или 2008 R2 выдавать и управлять сертификатами для маршрутизаторов и других сетевых устройств, не имеющих учетных записей в базе данных Active Directory. Эта служба позволяет сетевым устройствам получать сертификаты на основе протокола SCEP (Simple Certificate Enrollment Protocol). Служба подачи заявок на сетевые устройства предоставляет следующие возможности:

- создание и предоставление одноразовых паролей подачи заявок для администраторов;
- подача заявок в центр сертификации Windows Server 2008 по протоколу SCEP от имени сетевых устройств;
- получение выданных сертификатов от ЦС и передача их сетевым устройствам.

По умолчанию служба подачи заявок на сетевые устройства может кэшировать только пять паролей одновременно. Это ограничивает до пяти число сетевых устройств, участвующих в процессе регистрации. Можно очистить кэш паролей, перезапустив IIS, или изменить параметры службы подачи заявок, чтобы кэшировалось больше пяти паролей.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Подача заявок на сетевые устройства

Подробнее об использовании службы подачи заявок на сетевые устройства см. по адресу <http://technet.microsoft.com/ru-ru/library/cc753784.aspx>.

Использование PKI предприятия для мониторинга работоспособности ЦС

Оснастку **PKI предприятия** (Enterprise PKI) (рис. 3-18) можно добавить в настраиваемую консоль и использовать для мониторинга работоспособности всех ЦС в пределах PKI. Эта оснастка позволяет наблюдать за состоянием окружения PKI организации. В сетях с многоуровневой структурой выдающих ЦС возможность быстро просматривать все серверы сертификации облегчает управление иерархией ЦС и исправление ошибок. Оснастка **PKI предприятия** предоставляет данные о действительности и доступности расположений AIA и точек распространения CRL.

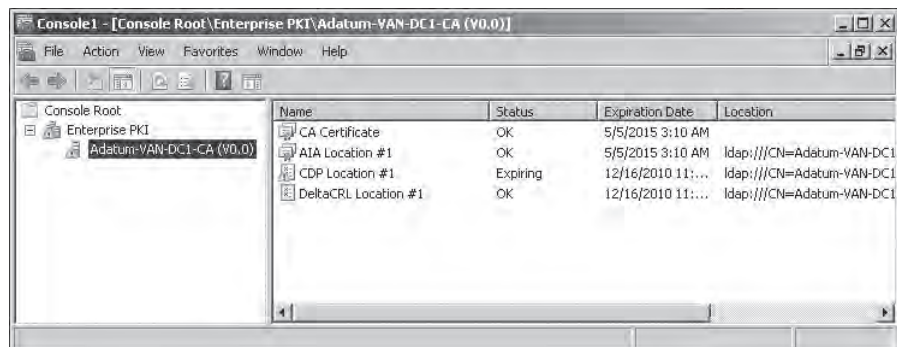


Рис. 3-18. Настраиваемая консоль PKI предприятия

Оснастка **PKI предприятия** работает с ЦС предприятия под управлением Windows Server 2008 и 2008 R2. Она предоставляет следующую информацию о состоянии каждого ЦС в иерархии PKI:

- **знак вопроса** — выполняется проверка состояния работоспособности;
- **зеленый индикатор** — проблем с ЦС нет;
- **желтый индикатор** — ЦС имеет некритическую проблему;
- **красный индикатор** — ЦС имеет критическую проблему;
- **красный крест поверх значка ЦС** — ЦС отключен.

Наиболее распространенные проблемы конфигурации связаны с расположением второго AIA, расположением второго разностного CRL и расположением CDP. При возникновении проблем с конфигурацией ЦС используйте следующие стратегии решения:

- если проблема относится к ЦС, например, проблема с подключением к текущему CRL, используйте консоль **Центр сертификации** (Certification Authority) для подключения к проблемному ЦС;
- если проблема связана с сетевым ответчиком, используйте для ее решения консоль управления сетевым ответчиком;

- если консоль **PKI предприятия** сообщает, что скоро истечет срок действия сертификатов ЦС, используйте оснастку **Сертификаты (Certificates)** в настраиваемой консоли для обновления этих сертификатов;
- для получения подробной информации о проблемах, связанных с PKI, можно включить диагностику CryptoAPI 2.0; для этого в средстве просмотра событий включите операционный журнал, расположенный под узлом **Приложения и журналы служб | Microsoft | Windows | CAPI2 (Applications And Service Logs | Microsoft | Windows | CAPI2)** (рис. 3-19).

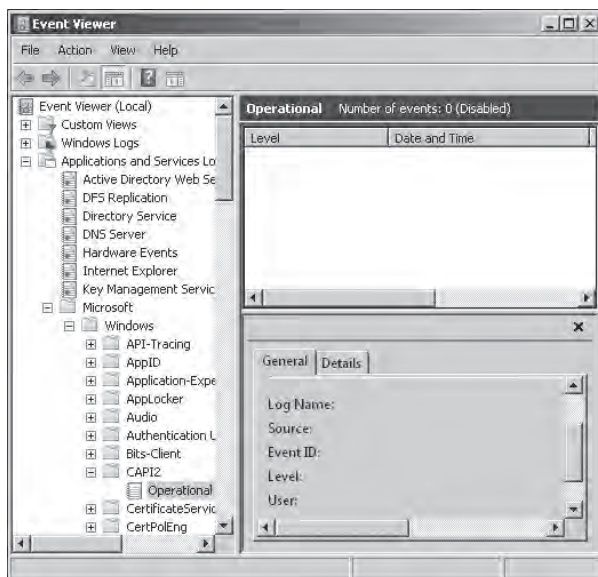


Рис. 3-19. Операционный журнал для диагностики CryptoAPI 2.0

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ PKI предприятия

Подробнее о PKI предприятия см. по адресу <http://technet.microsoft.com/ru-ru/library/cc771400.aspx>.

Резюме

- Центры сертификации предприятия используются для поддержки Active Directory. ЦС предприятия автоматически добавляются в хранилища доверенных сертификатов пользователей домена. В большинстве случаев при развертывании служб сертификации в Windows Server 2008 и 2008 R2 используются ЦС предприятия.
- Автономные ЦС не требуют развертывания Active Directory и не могут быть настроены для использования шаблонов сертификатов.
- Сетевые ответчики обрабатывают запросы на получение данных CRL более эффективно, чем традиционные способы публикации данных CRL.
- Кэширование учетных данных обеспечивает актуальность пользовательских сертификатов посредством частого сравнения локальных сертификатов с сертификатами, хранящимися в Active Directory.

- Авторегистрация позволяет автоматически развертывать сертификаты на клиенты без вмешательства администратора или пользователя. Авторегистрация должна быть включена в шаблоне сертификатов и в групповой политике.
- В AD CS Windows Server 2008 R2 появились новые компоненты и службы, повышающие гибкость развертывания PKI, уменьшающие затраты на администрирование и улучшающие поддержку развертываний NAP.

Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных на занятии 2. Эти вопросы предоставлены также в электронном виде на прилагаемом к книге компакт-диске.

ПРИМЕЧАНИЕ Ответы

Ответы на вопросы и пояснения к их вариантам размещены в разделе «Ответы» в конце книги.

1. В главном офисе компании широко используются цифровые сертификаты, распространяемые при помощи авторегистрации. ЦС какого типа следует развернуть в офисе регионального филиала, чтобы выдавать сертификаты с поддержкой политик авторегистрации, настроенных в GPO домена по умолчанию?
 - a. Корневой ЦС предприятия.
 - b. Подчиненный ЦС предприятия.
 - c. Автономный корневой ЦС.
 - d. Автономный подчиненный ЦС.
2. Какие из перечисленных действий необходимо выполнить перед развертыванием авторегистрации? (Каждый ответ составляет часть решения. Выберите два.)
 - a. Настроить групповую политику для поддержки авторегистрации.
 - b. Настроить разрешения авторегистрации в шаблонах сертификатов.
 - c. Изменить параметры публикации CRL.
 - d. Настроить сетевой ответчик.
 - e. Настроить регистрацию через Интернет.
3. Вы хотите настроить сервер ocspr.adatum.com в качестве сетевого ответчика для ca1.adatum.com. На сервере ocspr.adatum.com установлены службы IIS. Какие действия следует предпринять для этого? (Каждый ответ составляет часть решения. Выберите три.)
 - a. Установить сертификат подписи ответа OCSP на ca1.adatum.com.
 - b. Настроить шаблон сертификата подписи ответа OCSP на ca1.adatum.com.
 - c. Установить сертификат подписи ответа OCSP на ocspr.adatum.com.
 - d. Настроить расширение AIA с URL-адресом ocspr.adatum.com.
 - e. Настроить расширение AIA с URL-адресом ca1.adatum.com.

4. В филиале организации, находящемся в Квинсленде, широко используются цифровые сертификаты. Дополнительные офисы в Квинсленде используют сертификаты аналогичным образом. В офисе филиала установлен один корневой ЦС предприятия, выдающий все сертификаты для Квинсленда. Из-за низкой скорости WAN-соединения клиентам в дополнительных офисах иногда приходится долго ждать проверки подлинности выданных сертификатов. Что можно сделать, чтобы ускорить проверку сертификатов для клиентов в дополнительных офисах?
 - a. Развернуть в офисе филиала подчиненный ЦС предприятия.
 - b. Развернуть в каждом дополнительном офисе подчиненный ЦС предприятия.
 - c. Развернуть в офисе филиала автономный подчиненный ЦС.
 - d. Разместить в каждом дополнительном офисе сетевой ответчик. Настроить массив сетевых ответчиков.
5. Какой из перечисленных инструментов позволяет следить за работоспособностью нескольких ЦС в среде PKI организации?
 - a. Консоль **Центр сертификации** (Certification Authority).
 - b. Консоль **Управление сетевым ответчиком** (Online Responder Management).
 - c. Оснастка **PKI предприятия** (Enterprise PKI).
 - d. Оснастка **Сертификаты** (Certificates).

Практикум. Повышение функционального уровня домена и леса, включение корзины Active Directory и настройка детальной политики паролей

На этом практикуме вы создадите и настроите PSO, содержащий политику паролей, отличную от используемой по умолчанию в домене contoso.internal. Но перед этим необходимо повысить функциональный уровень домена и леса.

ПРИМЕЧАНИЕ Вход в систему на контроллере домена

Для краткости и удобства в этом и других практикумах книги предлагается выполнить интерактивный вход на контроллер домена. Учтите, что в производственной среде, скорее всего, вход будет выполняться с рабочей станции через подключение к удаленному рабочему столу или через подключение с использованием утилит RSAT.

Упражнение 1. Повышение функционального уровня домена

В этом упражнении вы повысите функциональный уровень домена. Это выполняется в первую очередь, так как функциональный уровень леса не может быть выше функционального уровня любого домена, входящего в этот лес.

1. Зайдите на VAN-DC1 под учетной записью Kim Akers.

2. В меню **Администрирование** (Administrative Tools) выберите **Active Directory — домены и доверие** (Active Directory — Domains and Trusts).
3. В дереве консоли щелкните правой кнопкой мыши домен **adatum.com** и выберите команду **Повышение режима работы домена** (Raise Domain Functional Level) (рис. 3-20).

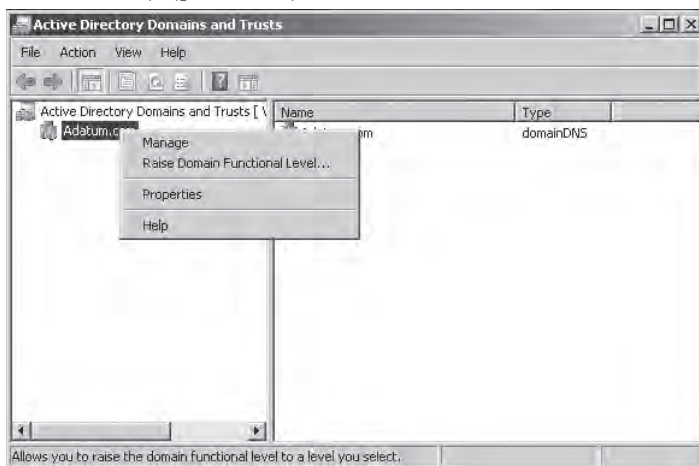


Рис. 3-20. Повышение режима работы домена

4. Проверьте функциональный уровень домена. Если функциональный уровень Windows Server 2008 R2 уже установлен, оставшуюся часть упражнения выполнять не нужно. Щелкните **Заккрыть** (Close), закройте консоль **Active Directory — домены и доверие** и переходите к упражнению 2.
5. Если функциональный уровень ниже Windows Server 2008 R2, выберите самый высокий доступный функциональный уровень в поле **Выбор доступного режима домена** (Select an available domain functional level), щелкните **Повысить** (Raise), щелкните **ОК** в диалоговом окне **Повышение режима работы домена** (Raise Domain Functional Level), после чего еще раз щелкните **ОК**. Повторяйте этот процесс, пока не повысите функциональный уровень домена до Windows Server 2008 R2.
6. Щелкните **Заккрыть** (Close). Закройте консоль **Active Directory — домены и доверие**.

Упражнение 2. Повышение функционального уровня леса

В этом упражнении вы повысите функциональный уровень леса. Не приступайте к этому упражнению, если не выполнили упражнение 1.

1. Если требуется, зайдите на **VAN-DC1** под учетной записью **Kim Akers** и откройте консоль **Active Directory — домены и доверие** (Active Directory — Domains and Trusts).
2. В дереве консоли щелкните правой кнопкой мыши узел **Active Directory — домены и доверие** (Active Directory — Domains and Trusts).
3. Правой кнопкой мыши щелкните **Изменение режима работы леса** (Raise Forest Functional Level).

4. Проверьте функциональный уровень леса. Если функциональный уровень Windows Server 2008 R2 уже установлен, оставшуюся часть упражнения выполнять не нужно. Щелкните **Заккрыть** (Close), закройте консоль **Active Directory — домены и доверие** и переходите к упражнению 3.
5. Если функциональный уровень леса ниже Windows Server 2008 R2, выберите самый высокий доступный функциональный уровень в раскрывающемся списке **Выбор доступного режима леса** (Select an available forest functional level). На рис. 3-21 в этом списке выбран уровень Windows Server 2008 R2. В диалоговом окне **Повышение режима работы леса** (Raise Forest Functional Level) щелкните **Повысить** (Raise), щелкните **ОК**, после чего еще раз щелкните **ОК**.

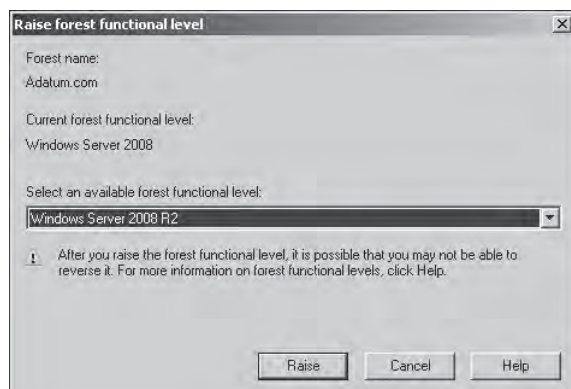


Рис. 3-21. Выбор функционального уровня леса Windows Server 2008 R2

6. Повторяйте этот процесс, пока не повысите функциональный уровень леса до Windows Server 2008 R2.
7. Щелкните **ОК**. Закройте консоль **Active Directory — домены и доверие**.

ПРИМЕЧАНИЕ **Альтернативные способы повышения функционального уровня домена и леса**

Повысить функциональный уровень домена и леса можно также при помощи Центра администрирования Active Directory и модуля Active Directory для Windows PowerShell. В качестве дополнительного задания попробуйте выяснить, как это сделать.

Упражнение 3. Включение Корзины Active Directory

Подняв функциональный уровень леса до Windows Server 2008 R2, можно включить Корзину Active Directory. Не приступайте к этому упражнению, не выполнив упражнения 1 и 2.

1. Если требуется, завершите сеанс пользователя Kim Akers на VAN-DC1 и зайдите под встроенной учетной записью администратора. (Заметьте, что это один из очень редких случаев, когда прав учетной записи Kim Akers недостаточно и необходимо использовать встроенную учетную запись администратора.)

2. Из меню **Пуск | Все программы | Администрирование** откройте модуль Active Directory для Windows PowerShell.

ПРИМЕЧАНИЕ Открытие модуля Active Directory для Windows PowerShell

Если контроллер домена VAN-DC1 настроен, как описано в прил. А, этот модуль должен открываться без сообщения об ошибке. Если вы получаете сообщение о том, что модуль не может найти сервер с веб-службами Active Directory, может потребоваться установка сертификата корневого ЦС и открытие порта 9389 на VAN-DC1. Если не знаете, как выполнить эти задачи, обратитесь к справочной системе.

3. Если модуль Active Directory для Windows PowerShell запустился без ошибок, введите следующую команду:

```
Enable-ADOptionalFeature -Identity 'CN=Recycle Bin Feature,CN=Optional  
Features,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,  
DC=adatum,DC=com' -Scope ForestOrConfigurationSet -Target 'adatum.com'
```

Упражнение 4. Создание PSO

В этом упражнении вы создадите PSO с политиками паролей, отличающимися от политик паролей по умолчанию для домена adatum.com. Этот PSO вы свяжете с глобальной группой безопасности special_password, содержащей пользователя Don Hall. Не приступайте к этому упражнению, не выполнив первые три упражнения.

1. Если требуется, зайдите на VAN-DC1 под учетной записью Kim Akers. Если вы уже вошли под встроенной учетной записью администратора, можете не выходить из системы. Однако рекомендуется использовать встроенную учетную запись как можно реже.
2. Если еще не сделали этого, создайте учетную запись пользователя Don Hall, как описано в начале главы.
3. Создайте глобальную группу безопасности special_password и включите в нее пользователя Don Hall.
4. В поле **Выполнить** введите **adsiedit.msc**.
5. Если это первый запуск консоли **Редактирование ADSI (ADSI Edit)** в вашей тестовой сети, щелкните правой кнопкой мыши **Редактор ADSI (ADSI Edit)** и выберите команду **Подключиться (Connect To)**. В поле **Имя (Name)** введите **adatum.com** и щелкните **ОК**.
6. В дереве консоли дважды щелкните **adatum.com**.
7. Дважды щелкните **DC=adatum,DC=com**.
8. Дважды щелкните **CN=Система**.
9. Щелкните правой кнопкой мыши **CN=Контейнер параметров паролей (CN=Password Settings Container)**. Выберите команду **Создать (New)**, а затем команду **Объект (Object)** (рис. 3-22).

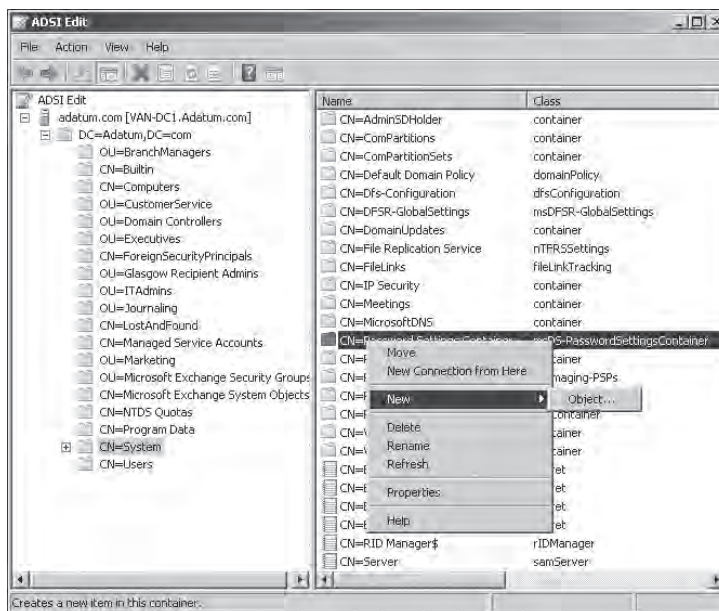


Рис. 3-22. Создание объекта параметров паролей

10. Убедитесь, что в диалоговом окне **Создание объекта** (Create Object) выбран атрибут **msDS-PasswordSettings**. Щелкните **Далее**.
11. В поле **CN** введите **PSO1** и щелкните **Далее**.
12. В поле **msDS-PasswordSettingsPrecedence** введите **10** и щелкните **Далее**.
13. В поле **msDS-PasswordReversibleEncryptionEnabled** введите **FALSE** и щелкните **Далее**.
14. В поле **msDS-PasswordHistoryLength** введите **6** и щелкните **Далее**.
15. В поле **msDS-PasswordComplexityEnabled** введите **FALSE** и щелкните **Далее**.
16. В поле **msDS-MinimumPasswordLength** введите **6** и щелкните **Далее**.
17. В поле **msDS-MinimumPasswordAge** введите **1:00:00:00** и щелкните **Далее**.
18. В поле **msDS-MaximumPasswordAge** введите **20:00:00:00** и щелкните **Далее**.
19. В поле **msDS-LockoutThreshold** введите **2** и щелкните **Далее**.
20. В поле **msDS-LockoutObservationWindow** введите **0:00:15:00** и щелкните **Далее**.
21. В поле **msDS-LockoutDuration** введите **0:00:15:00** и щелкните **Далее**.
22. Щелкните **Готово**.
23. Откройте консоль **Active Directory — пользователи и компьютеры** и выберите в меню **Вид** (View) команду **Дополнительные параметры** (Advanced Features).
24. Раскройте узел **adatum.com**, раскройте узел **Система** (System) и щелкните **Контейнер параметров паролей** (Password Settings Container).

25. Щелкните правой кнопкой мыши **PSO1** и выберите команду **Свойства** (Properties).
26. На вкладке **Редактор атрибутов** (Attribute Editor) выберите атрибут **msDS-PSOAppliesTo** (рис. 3-23).

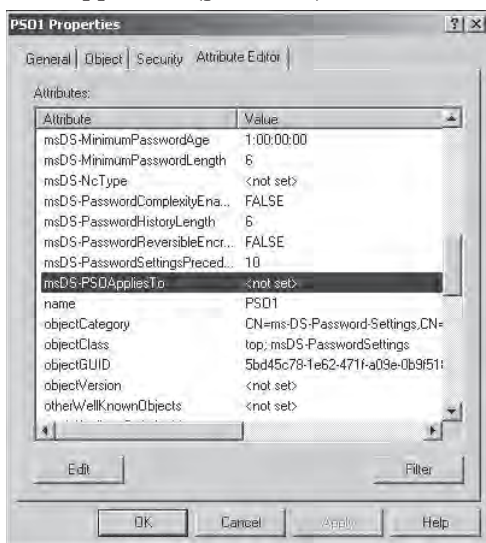


Рис. 3-23. Выбор атрибута для редактирования

27. Щелкните кнопку **Правка** (Edit).
28. Щелкните **Добавить учетную запись Windows** (Add Windows Account).
29. В поле **Введите имена выбираемых объектов** (Enter The Object Names To Select) введите **special_password**. Щелкните **Проверить имена** (Check Names).
30. Щелкните **ОК**. Диалоговое окно **Редактор многозначных различаемых имен участников безопасности** (Multi-Valued Distinguished Name With Security Principal Editor) должно выглядеть аналогично рис. 3-24.
31. Щелкните **ОК**. Еще раз щелкните **ОК**, чтобы закрыть диалоговое окно свойств PSO1.
32. Проверьте введенные параметры, задав пользователю Don Hall несложный шестизначный пароль, например **simple**.

Интересно заметить, что если вы откроете консоль **Active Directory — пользователи и компьютеры** от имени Kim Akers (или администратора домена) и измените пароль пользователя Don Hall на **simple**, то затем вы сможете выйти из системы и проверить введенные параметры, войдя под учетной записью Don Hall. Однако вы не сможете войти под учетной записью Don Hall, используя исходный (сложный) пароль, а затем нажать Ctrl+Alt+Del и сменить пароль на **simple**. Поэкспериментируйте с новыми параметрами и определите, что вы можете делать, а что нет.

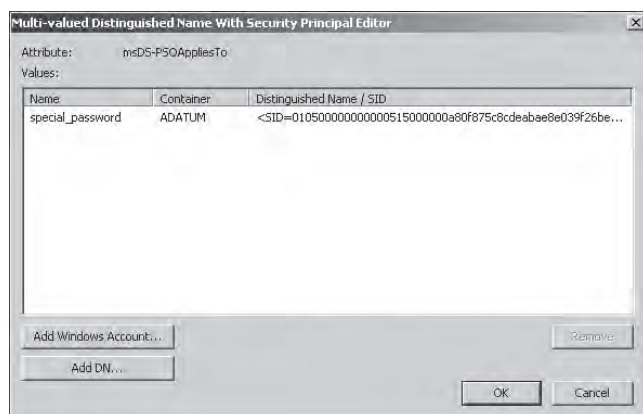


Рис. 3-24. Добавление группы special_password в PSO1

Практикум. Развертывание служб сертификации Active Directory и сетевого ответчика

На этом практикуме вы установите роль служб сертификации Active Directory на VAN-DC1, если это еще не сделано. Затем вы развернете и настроите сетевой ответчик.

Упражнение 1. Развертывание AD CS

1. Зайдите на VAN-DC1 под учетной записью Kim Akers. Если вы уже вошли под встроенной учетной записью администратора, выйдите и зайдите как Kim Akers. Откройте Диспетчер сервера и раскройте узел **Роли (Roles)**. Если роль служб сертификации Active Directory присутствует в списке, это упражнение выполнять не требуется, и можно перейти к упражнению 2.
2. Правой кнопкой мыши щелкните **Роли (Roles)** и выберите **Добавить роли (Add Roles)**. На странице **Выбор ролей сервера (Select Server Roles)** выберите службу сертификации Active Directory и щелкните **Далее (Next)** два раза. Убедитесь, что на странице **Выбор служб ролей (Select Role Services)** выбраны службы **Центр сертификации (Certification Authority)** и **Служба подачи заявок в центр сертификации через Интернет (Certification Authority Web Enrollment)**. Если будет предложено установить дополнительные службы ролей и компоненты для веб-сервера (IIS) и службы активации процессов Windows, щелкните **Добавить требуемые службы роли (Add Required Role Services)**. Щелкните **Далее**.
3. Убедитесь, что на странице **Задание типа установки (Specify Setup Type)** выбран тип **Предприятия (Enterprise)**, и щелкните **Далее**.
4. Убедитесь, что на странице **Задание типа ЦС (Specify CA Type)** выбран **Корневой ЦС (Root CA)**, и щелкните **Далее**.
5. Убедитесь, что на странице **Установка закрытого ключа (Set Up Private Key)** установлен переключатель **Создать новый закрытый ключ (Create A New Private Key)**, и щелкните **Далее**.

6. Убедитесь, что на странице **Настройка шифрования для ЦС** (Cryptography for CA) выбран поставщик служб шифрования **RSA#Microsoft Software Key Storage Provider**, длина ключа 2048 знаков и алгоритм хеширования SHA1. Щелкните **Далее**.
7. Убедитесь, что в поле **Общее имя для этого ЦС** (Common Name For This CA) указано **Adatum-VAN-DC1**, и щелкните **Далее**.
8. Примите предложенный по умолчанию срок действия 5 лет и щелкайте **Далее**, пока не дойдете до страницы **Подтвердите выбранные элементы** (Confirm Installation Selections). Щелкните **Установить** (Install). Когда установка завершится, щелкните **Заккрыть** (Close).

Упражнение 2. Развертывание сетевого ответчика

В этом упражнении вы установите службу сетевого ответчика как компонент роли службы сертификации Active Directory.

1. Если требуется, зайдите на VAN-DC1 под учетной записью Kim Akers.
2. Откройте консоль **Центр сертификации** (Certification Authority) из меню **Администрирование** (Administrative Tools). Убедитесь, что Adatum-VAN-DC1-CA имеет зеленый значок.
3. Выберите узел **Шаблоны сертификатов** (Certificate Templates). Убедитесь, что список шаблонов сертификатов соответствует списку на рис. 3-25.

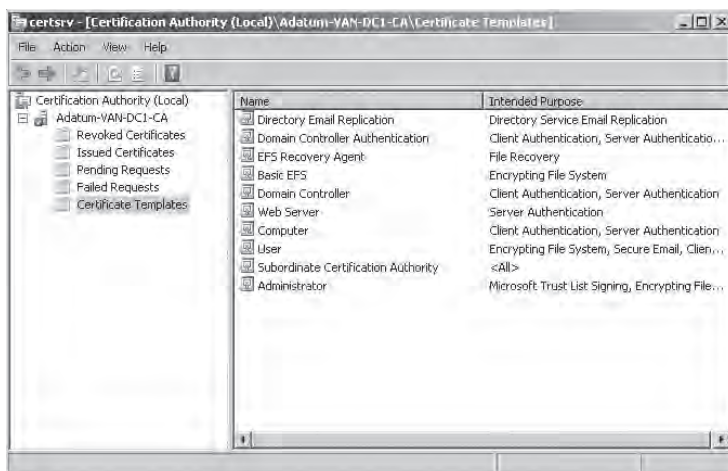


Рис. 3-25. Стандартный список шаблонов

4. Закройте консоль **Центр сертификации** (Certification Authority).
5. Откройте Диспетчер сервера. Под узлом **Роли** (Roles) щелкните правой кнопкой мыши элемент **Службы сертификации Active Directory** (Active Directory Certificate Services) и выберите команду **Добавить службы роли** (Add Role Services).
6. На странице **Выбор служб ролей** (Select Role Services) выберите сетевой ответчик (Online Responder). Если будет предложено, щелкните **Добавить требуемые службы роли** (Add Required Role Services).

7. Щелкните **Далее**.
8. Если откроется страница веб-сервера (IIS), щелкните **Далее**.
9. Если откроется страница **Выбор служб ролей** (Select Role Services), щелкните **Далее**.
10. На странице **Подтвердите выбранные элементы** (Confirm Installation Selections) щелкните **Установить** (Install), чтобы установить службу сетевого ответчика (рис. 3-26). Когда установка завершится, щелкните **Заккрыть** (Close).

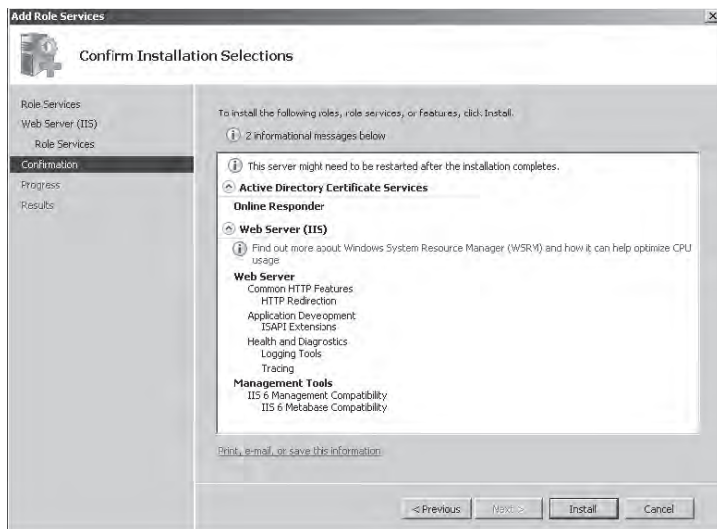


Рис. 3-26. Страница подтверждения выбранных элементов

11. Щелкните **Пуск | Выполнить**, введите **mmc** и щелкните **ОК**. Щелкните **Да**, чтобы закрыть диалоговое окно службы контроля учетных записей. В меню **Файл** (File) выберите команду **Добавить или удалить оснастку** (Add/Remove Snap-In). Добавьте оснастку **Шаблоны сертификатов** (Certificate Templates), как показано на рис. 3-27, и щелкните **ОК**.

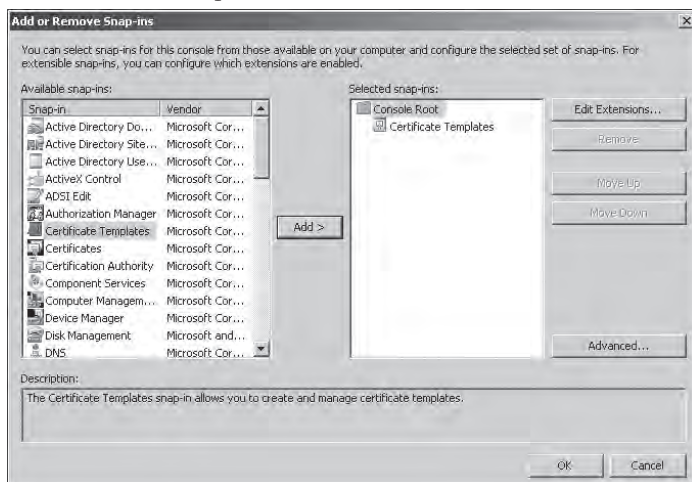


Рис. 3-27. Добавление оснастки Шаблоны сертификатов

12. Раскройте оснастку **Шаблоны сертификатов**. Щелкните правой кнопкой мыши шаблон **Подписывание отклика OCSP** (OCSP Response Signing) и выберите команду **Свойства** (Properties).
13. На вкладке **Безопасность** (Security) щелкните **Добавить** (Add). Щелкните **Типы объектов** (Object Types) и убедитесь, что выбран тип **Компьютеры** (Computers). Щелкните **ОК**, чтобы закрыть диалоговое окно **Типы объектов** (Object Types). В поле **Введите имена выбираемых объектов** (Enter The Object Names To Select) введите **VAN-DC1** и щелкните **ОК**.
14. Выбрав объект VAN-DC1, установите флажки **Разрешить** (Allow) для разрешений **Чтение** (Read), **Заявка** (Enroll) и **Автоматическая подача заявок** (Autoenroll) (рис. 3-28), после чего щелкните **ОК**.

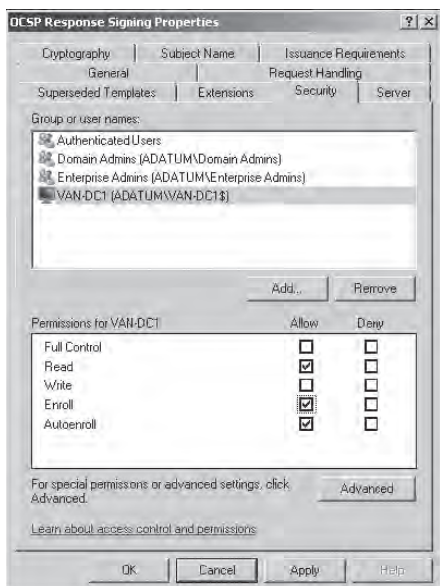


Рис. 3-28. Настройка автоматической регистрации OCSP

15. Закройте настраиваемую консоль, не сохраняя параметров. Откройте консоль **Центр сертификации** (Certification Authority) из меню **Администрирование**.
16. Щелкните узел Adatum-VAN-DC1-CA правой кнопкой мыши и выберите команду **Свойства**. На вкладке **Расширения** (Extensions) в раскрывающемся списке **Выбор расширений** (Select Extensions) выберите **Доступ к сведениям о центрах сертификации (AIA)** [Authority Information Access (AIA)].
17. Щелкните **Добавить** (Add), чтобы открыть диалоговое окно **Добавление размещения** (Add Location), введите **http://van-dc1.adatum.com/ocsp** и щелкните **ОК**.
18. Установите флажки **Включать в AIA-расширение выданных сертификатов** (Include In the AIA Extension Of Issued Certificates) и **Включать в расширение протокола OCSP** [Include in the online certificate status protocol (OCSP) extension] и щелкните **ОК** (рис. 3-29).

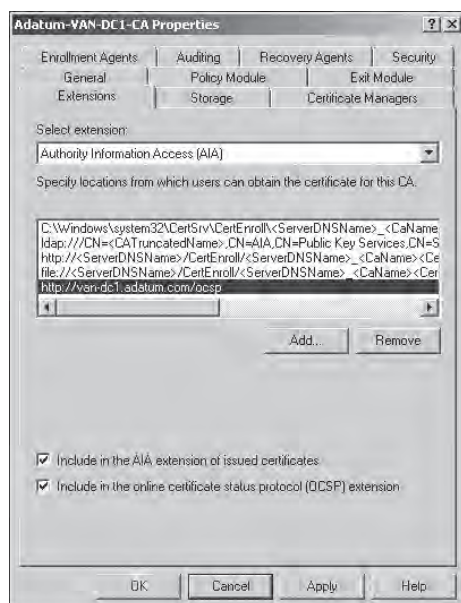


Рис. 3-29. Настройка расширений ЦС OCSP

19. Появится сообщение о том, что необходимо перезапустить службы сертификации Active Directory для вступления изменений в силу. Щелкните **Да**, чтобы перезапустить службу.
20. В консоли **Центр сертификации** (Certificate Authority) щелкните правой кнопкой мыши узел **Шаблоны сертификатов** (Certificate Templates), выберите команду **Создать** (New), а затем выберите **Выдаваемый шаблон сертификата** (Certificate Template To Issue). Выберите шаблон **Подписывание отклика OCSP** (OCSP Response Signing) и щелкните **ОК**.

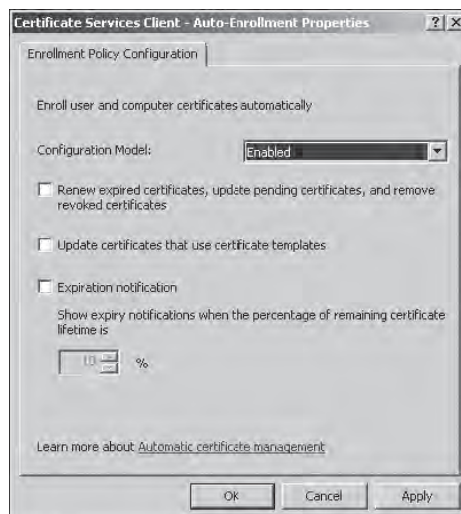


Рис. 3-30. Включение автоматической подачи заявок

21. Просмотрите список шаблонов сертификатов под узлом **Шаблон сертификатов** (Certificate Template) и убедитесь, что в списке есть шаблон **Подписывание отклика OCSP** (OCSP Response Signing).
22. Сверните консоль **Центр сертификации** (Certification Authority).
23. Запустите консоль **Управление групповой политикой** (Group Policy Management) из меню **Администрирование**.
24. Измените GPO политики домена по умолчанию. Включите политику **Клиент служб сертификации: автоматическая подача заявок** (Certificate Services Client – Auto-Enrollment), расположенную под узлом **Конфигурация пользователя | Политики | Конфигурация Windows | Параметры безопасности | Политики открытого ключа** (User Configuration | Policies | Windows Settings | Security Settings | Public Key Policies) (рис.3-30). Сделайте то же самое для политики **Клиент служб сертификации: автоматическая подача заявок** из раздела **Конфигурация компьютера GPO**.
25. Закройте редактор управления групповой политикой и консоль управления групповой политикой, после чего перезагрузите VAN-DC1.

Закрепление материала главы

Чтобы попрактиковаться и закрепить знания, полученные при изучении этой главы, выполните следующее:

- прочитайте резюме главы;
- просмотрите список основных терминов, представленных в этой главе;
- выполните задания лабораторной работы, моделирующей реальные ситуации, требующие применения полученных знаний;
- выполните рекомендуемые упражнения;
- пройдите пробный тест.

Резюме главы

- Функции AD DS дают больше контроля над политиками безопасности, позволяют сделать более удобной работу пользователей в офисах филиалов и помогают найти архивированную информацию, которую требуется восстановить.
- Улучшенные утилиты с графическим интерфейсом и средства аудита, появившиеся в Windows Server 2008, облегчают и ускоряют выполнение административных задач.
- В Windows Server 2008 R2 появились новые функциональные уровни домена и леса. Если повысить функциональный уровень леса до Windows Server 2008 R2, можно использовать Корзину Active Directory.
- Функциональный уровень домена и леса можно повысить, чтобы получить доступ к новой функциональности, но, за единственным исключением, его нельзя понизить (не выполняя переустановку или восстановление из резервной копии). Между лесами можно настраивать доверительные отношения.

- Центры сертификации предприятия используются для выдачи цифровых сертификатов учетным записям Active Directory пользователей и компьютеров.
- Процессы автоматической регистрации и перемещения учетных данных могут уменьшить нагрузку на администраторов служб сертификации в Windows Server 2003 и Windows Server 2008 R2.
- Сетевые ответчики и массивы сетевых ответчиков уменьшают трафик, вызванный проверками CRL. Одиночный сетевой ответчик или массив сетевых ответчиков может предоставлять информацию из списков CRL с одного или нескольких ЦС.

Основные термины

Проверьте, знаете ли вы, что означают перечисленные ниже термины из этой главы:

- Авторегистрация.
- Центр сертификации (ЦС).
- Список отозванных сертификатов (CRL).
- Функциональный уровень.
- Контроллер домена только для чтения (RODC).
- Теневая группа.
- Двухэтапная установка.

Лабораторная работа

Для выполнения заданий лабораторной работы используйте знания о планировании служб каталогов и служб сертификации, полученные из этой главы. Ответы можно найти в разделе «Ответы» в конце книги.

Задание 1. Планирование обновления с Windows Server 2003 до Windows Server 2008 R2

Вы старший администратор домена компании Northwind Traders. Компания планирует обновить свои контроллеры домена с Windows Server 2003 до Windows Server 2008 R2, хотя некоторые старшие менеджеры все еще не убеждены в целесообразности этого. Ответьте на следующие вопросы:

1. Некоторые сотрудники, в том числе исполнительный директор, хотят использовать несложные пароли, хотя политика домена northwindtraders.com по умолчанию требует использования сложных паролей. У вас спрашивают, будет ли это возможно после обновления до Windows Server 2008 R2. Что вы ответите?
2. Технический директор обеспокоен тем, что если вы обновите контроллеры домена до Windows Server 2008 R2, а затем повысите функциональный уровень леса до Windows Server 2008 R2, чтобы использовать новые функции, то оставшиеся контроллеры домена с Windows Server 2003 перестанут функ-

ционировать. Также директора беспокоит то, что в домене есть рядовые серверы под управлением Windows 2000 Server и Windows Server 2003, и компания не планирует обновлять эти компьютеры. Что вы ответите?

3. Пользователи из удаленных офисов сообщают о том, что вход в систему иногда выполняется неприемлемо медленно. В каждом таком офисе установлен дополнительный DNS-сервер, но контроллеры домена в удаленных офисах нет по соображениям безопасности, к тому же там нет администраторов домена. У вас спрашивают, как обновление до Windows Server 2008 R2 поможет в решение этой проблемы. Что вы ответите?

Задание 2. Развертывание служб сертификации в Coho Vineyard

Компания Coho Vineyard недавно развернула сеть Windows Server 2008 R2 во всех офисах в Долине Ярра, винодельческом регионе Австралии. Менеджеры компании обратились к вам за помощью в решении некоторых проблем с конфигурацией сети. Руководство считает, что необходимо повысить безопасность сетевого взаимодействия через глобальную и локальную сеть компании. Компания хочет использовать IPSec и проверку подлинности на основе сертификатов. WAN-связь между главным и дополнительными офисами уже перегружена трафиком. Вас попросили разработать решение, позволяющее уменьшить влияние проверок CRL на трафик, передаваемый по WAN-каналу. В компании развернута принудительная защита доступа к сети (NAP) с помощью IPSec, что приводит к возможным проблемам с размером базы данных ЦС. Учитывая все это, ответьте на вопросы:

1. Что следует предпринять, чтобы обеспечить развертывание сертификатов IPSec на все компьютеры, входящие в домен?
2. Что следует предпринять, чтобы проверки CRL выполнялись с минимальным использованием трафика?
3. Может ли новая функциональность Windows Server 2008 R2 помочь в уменьшении размера баз данных? Если да, то есть ли связанные с этим решением недостатки?

Рекомендуемые упражнения

Чтобы успешно справиться с экзаменационными заданиями по темам этой главы, выполните следующие упражнения.

Настройте PSO

- PSO может содержать много параметров, некоторые из которых вы настраивали в упражнениях этой главы. Поэкспериментируйте с параметрами PSO и определите их влияние на политики безопасности, действующие для пользователей, связанных с GPO.

Изучите RODC подробнее

- В вашей маленькой тестовой сети сложно практиковаться в установке и настройке RODC, хотя вы можете использовать виртуальные машины. Поищите в Интернете статьи и обсуждения, относящиеся к RODC. Это новая технология, и с каждым днем появляется все больше информации о ней.

Настройте аудит

- Исследуйте новые возможности аудита AD DS, появившиеся в Windows Server 2008 R2. Настройте аудит для записи изменений AD DS, внесите какие-либо изменения, а затем просмотрите журнал безопасности.

Настройте регистрацию через Интернет

- Настройте на VAN-DC1 регистрацию сертификатов через Интернет.
- Используйте клиент VAN-SRV1 для запроса сертификата веб-сервера через интерфейс регистрации через Интернет. Подтвердите запрос, используя консоль **Цент сертификации** (Certification Authority), после чего загрузите сертификат веб-сервера с веб-страницы регистрации.

Пробный экзамен

Тренировочные тесты на прилагаемом к книге компакт-диске позволяют проверить знания только по одной или сразу по всем темам сертификационного экзамена 70-646. Тестирование можно организовать так, чтобы оно проводилось как настоящий экзамен, а можно проходить в режиме обучения, просматривая правильные ответы и объяснения после каждого ответа.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Пробный экзамен

Подробнее о пробном экзамене рассказано во Введении.

Стратегии групповой политики

Занятие 1. Планирование объектов групповой политики	177
Занятие 2. Стратегия объектов групповой политики	189

Эта глава посвящена групповой политике доменных служб Active Directory (AD DS). Основное внимание уделяется планированию и стратегиям, а не внедрению. Вы, как опытный администратор, наверняка уже имели дело с групповой политикой, поэтому мы будем рассматривать, в основном, улучшения, появившиеся в Windows Server 2008 и 2008 R2. Мы обсудим инструменты с графическим интерфейсом и утилиты командной строки, но суть не в том, какими инструментами изменять конфигурацию, а в том, почему и когда это надо делать. Чем опытнее администратор, тем больше времени он посвящает планированию, а не настройке.

Темы экзамена

- Планирование и реализация стратегии групповой политики.

Прежде всего

Для выполнения упражнений этой главы потребуется:

- Сервер с именем VAN-DC1, работающий под управлением Windows Server 2008 R2 Enterprise, настроенный как контроллер домена Adatum.com, как описано в Приложении.
- Если сервер VAN-DC1 настроен, как описано в Приложении, то на него должны быть установлены средства управления групповыми политиками. Если эти средства не установлены, выполните первое упражнение из практикума этой главы, чтобы установить их.
- Установить на VAN-DC1 роль сервера Службы удаленных рабочих столов (Remote Desktop Services, RDS). Это позволит изучить такие инструменты, как Диспетчер удаленных приложений. Роль сервера RDS понадобится в следующих главах.
- Клиентская рабочая станция с Windows 7 Business, Enterprise или Ultimate в домене adatum.com. К сожалению, сервер VAN-SRV1, работающий под управлением Windows Server 2008 R2, который вы настраивали в предыдущих главах, не содержит файлов административных шаблонов, которые мы

будем изучать в этой главе. Клиентская рабочая станция может быть как виртуальной, так и физической машиной. При отсутствии доступа к компьютеру под управлением Windows 7 можно использовать рабочую станцию с Windows Vista Business, Enterprise или Ultimate. В упражнениях практика этот клиент называется VAN-CL1. Если у вашего клиента другое имя, внесите в упражнения соответствующую поправку.

- Учетная запись пользователя Kim Akers с паролем Pa\$\$w0rd в домене adatum.com, включенная в группы администраторов домена, администраторов предприятия и администраторов схемы. Процедура создания этой учетной записи описана в Приложении.
- Учетная запись пользователя Don Hall с паролем Pa\$\$w0rd в домене adatum.com, включенная в группу Операторы архива (Backup Operators) для получения возможности интерактивно заходить на контроллер домена.
- Для выполнения практических упражнений рекомендуем использовать изолированную сеть, не входящую в рабочую сеть. Доступ к Интернету не требуется, как и настройка шлюза по умолчанию. Для экономии времени и затрат на настройку физических компьютеров используйте виртуальные машины, например, созданные с использованием роли сервера Hyper-V.

Реальный мир

Йен Маклин

Как правило, в книгах, посвященных новым операционным системам, описываются появившиеся в них новые функции. К счастью, с большинством экзаменов ситуация та же. Обычно авторы лишь вкратце описывают технологии, имевшиеся ранее, чтобы книги не были слишком объемными и очень дорогими.

Однако реальная жизнь не отражает ситуации с книгами и экзаменами. Каждый день я пользуюсь навыками и принципами, усвоенными при использовании Windows 2000 Server и даже Windows NT 4. Кроме того, нет никакой гарантии того, что экзаменационные вопросы будут касаться только новых функций. Если в темах указана групповая политика, то экзаменатор вправе включить туда любые вопросы по групповой политике, будь то инструменты, появившиеся в Windows 2000 Server или в Windows Server 2008 R2.

Несколько лет назад я встретил экзаменационный вопрос по теме, которую я когда-то изучал, но с тех пор особо не сталкивался с ней. К счастью, я знал ответ, однако я не встречал его ни в одной из книг, по которым готовился. Иногда ко мне обращаются коллеги, прочитавшие одну из моих книг, и рассказывают, что им на экзамене попала тема, отсутствовавшая в книге. В таких случаях я лишь сдержанно улыбаюсь и говорю им, что эта тема была в моей книге, написанной для предыдущего экзамена.

Предполагается, что экзаменуемые являются опытными администраторами, и экзаменуют их соответствующим образом. Я не могу описать в одной книге обширный трехлетний опыт и вдобавок все новые сложные компоненты, появившиеся в Windows Server 2008 и 2008 R2. Для этого

потребовалась бы целая библиотека. Выход — в приобретении соответствующего опыта. На практике зачастую приходится регулярно выполнять одни и те же задачи, а прочие обязанности возлагать на других людей. Готовясь к экзамену, постарайтесь приобрести хоть какой-то опыт по всем дисциплинам. Книги, конечно, тоже нужны, однако есть лишь один способ повышения квалификации и продвижения по карьерной лестнице — практика, практика и еще раз практика.

Занятие 1. Планирование объектов групповой политики

На этом занятии рассматривается стратегия планирования конфигурации объектов групповой политики (GPO), используемых для применения групповой политики в Windows Server 2008 и 2008 R2. В частности, описываются административные шаблоны и файлы административных шаблонов (ADM). Мы обсудим начальные GPO, в том числе системные начальные GPO, включенные в Windows Server 2008 R2.

В Windows Server 2008 и 2008 R2 можно установить консоль управления групповыми политиками (GPMC), используя мастер добавления функций в Диспетчере сервера. Вы сделаете это на одном из упражнений этого занятия. С помощью этой консоли можно эффективно внедрять настройки безопасности, применять ИТ-политики и обеспечивать согласованность распространения программ по сайтам, доменам и подразделениям (OU).

Файлы ADM появились в Windows NT 4. Они используются для описания параметров групповой политики, хранящихся в реестре. В Windows Sever 2008 и 2008 R2 (а также в Windows Vista и Windows 7), файлы ADM заменены файлами XML, известными как файлы ADMX. Файлы ADMX облегчают управление параметрами политики, хранящимися в реестре. В Windows Server 2008 R2 в диалоговое окно свойств добавлена возможность настройки политики административных шаблонов и увеличено число типов реестра, поддерживаемых административными шаблонами. В Windows Server 2008 R2 и Windows 7 появились средства удаленного администрирования серверов (Remote Server Administration Tools, RSAT), добавляющие более 300 параметров политики административных шаблонов.

На этом занятии обсуждаются начальные и системные начальные GPO, а также способы их использования при планировании внедрения групповой политики. Также здесь описываются независимые и зависимые от языка ADMX-файлы.

Изучив материал этого занятия, вы сможете:

- ✓ Установить GPMC (если требуется) и использовать эту консоль для управления параметрами групповой политики.
- ✓ Создавать, редактировать, резервировать и восстанавливать начальные GPO.
- ✓ Работать с ADMX-файлами.
- ✓ Настраивать фильтр просмотра для настроек политики административных шаблонов.

Продолжительность занятия — примерно 45 мин.

Использование начальных объектов групповой политики

В групповой политике Windows Server 2008 появились начальные (или стартовые) объекты групповой политики (Starter GPO), а в групповой политике Windows Server 2008 R2 — системные начальные GPO. Начальные GPO позволяют сохранять базовые шаблоны, которые можно использовать при создании новых GPO. Можно также экспортировать начальные GPO в другие домены из доменов, в которых они были созданы.

Системные начальные GPO — это начальные GPO, доступные только для чтения, предоставляющие основные параметры для определенной ситуации. Как и начальные GPO, они хранят набор параметров политики административных шаблонов в одном объекте, который можно импортировать. Однако невозможно редактировать системные начальные GPO или создать собственный системный начальный GPO. Можно определить, является ли начальный GPO системным, просмотрев значение **Тип стартового GPO** (Starter GPO Type) на вкладке **Сведения** (Details) панели информации о начальном GPO. На Рис. 4-1 показана эта вкладка с данными пользовательского (редактируемого) начального GPO.

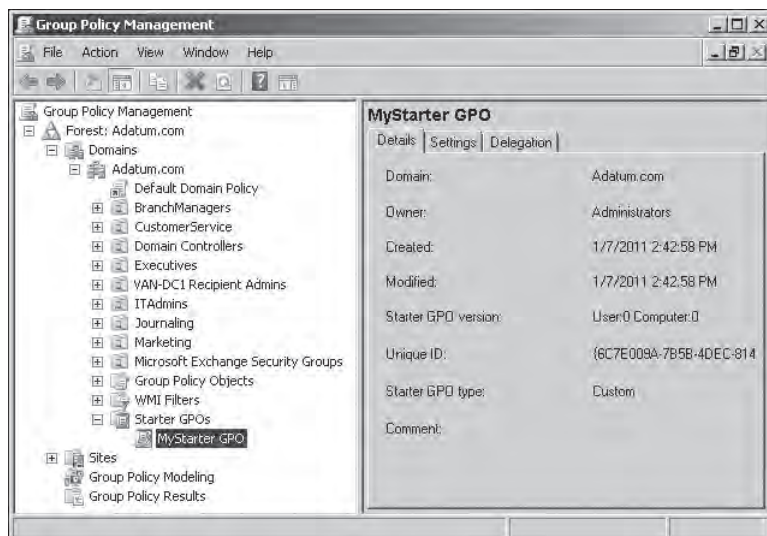


Рис. 4-1. Вкладка Сведения с информацией о стартовом GPO

ПРИМЕЧАНИЕ Контейнер Начальные объекты групповой политики

В зависимости от настроек, может появиться окно с предложением создать контейнер начальных GPO. Если создать его, в нем автоматически появятся восемь системных начальных GPO: четыре для клиентов под управлением Windows XP и четыре для клиентов под управлением Windows Vista. Загружать эти системные начальные GPO не требуется.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Системные начальные GPO

Подробнее о системных начальных GPO см. по адресу [http://technet.microsoft.com/ru-ru/library/dd367854\(WS.10\).aspx](http://technet.microsoft.com/ru-ru/library/dd367854(WS.10).aspx).

Чтобы создать начальный GPO, щелкните правой кнопкой мыши контейнер **Начальные объекты групповой политики (Starter GPOs)** в дереве GPMC и выберите **Создать (New)**. Появится окно для ввода имени начального GPO и комментария, если он требуется (рис. 4-2). В процессе создания начального GPO на контроллере домена, к которому подключена консоль GPMC, автоматически создается новая папка. По умолчанию эта папка создается в папке C:\Windows\SYSVOL\domain\StarterGPOs. Она реплицируется на другие контроллеры доменов во время репликации SYSVOL.

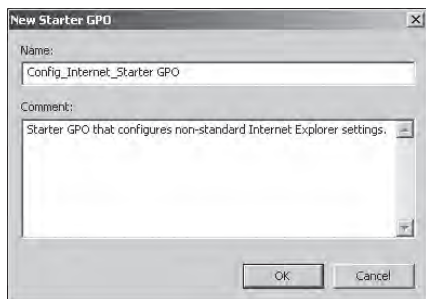


Рис. 4-2. Создание нового начального GPO

Начальный GPO можно настраивать точно так же, как и любой другой GPO, с той лишь разницей, что в конфигурации компьютера и конфигурации пользователя имеются только параметры административных шаблонов. Для настройки щелкните правой кнопкой мыши начальный GPO и выберите команду **Изменить (Edit)**. На рис. 4-3 показан объект групповой политики Config_Internet_Starter GPO с параметром **Не разрешать пользователям включать и отключать надстройки (Do Not Allow Users To Enable Or Disable Add-Ons)** из редактируемого раздела **Internet Explorer**. Если выбрать команду **Изменить (Edit)**, можно включить или отключить этот параметр политики или оставить не настроенным.

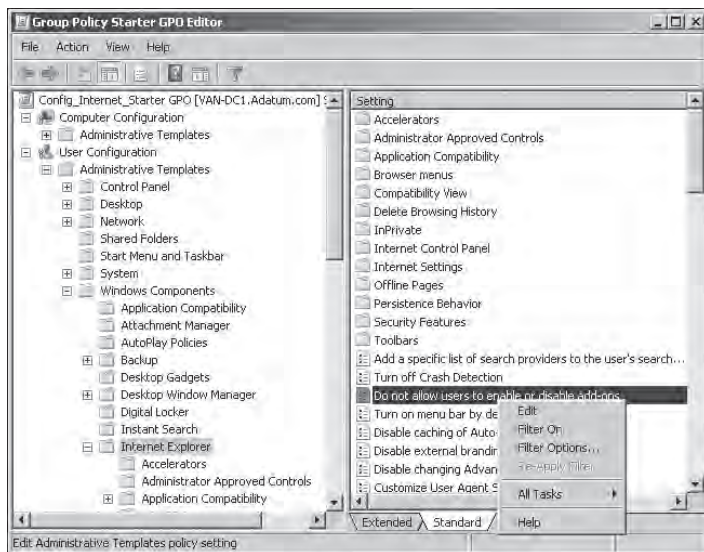


Рис. 4-3. Настройка начального GPO

Начальный GPO позволяет легко создавать несколько GPO с одинаковой базовой конфигурацией. Требуется настроить только те параметры GPO, которые не содержатся в административных шаблонах. Можно создать новый (стандартный) GPO, используя начальный GPO в качестве шаблона. Для этого щелкните начальный GPO правой кнопкой мыши и выберите команду **Новый объект групповой политики из начального объекта групповой политик** (New GPO From Starter GPO). Можно также щелкнуть правой кнопкой мыши контейнер объектов групповой политики, выбрать **Создать** (New), а затем выбрать начальный GPO в раскрывающемся списке **Исходный начальный объект групповой политики** (Source Starter GPO) (рис. 4-4). Если щелкнуть правой кнопкой мыши подразделение (или домен) и выбрать **Создать объект GPO в этом домене и связать его** (Create A GPO In This Domain, And Link It Here), то можно перейти к этому же диалоговому окну и указать начальный GPO.

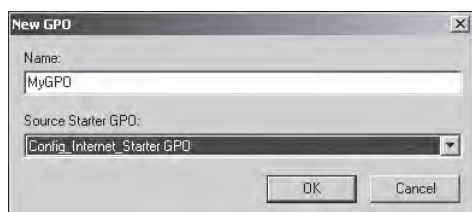


Рис. 4-4. Выбор начального GPO при создании нового GPO

Резервное копирование и восстановление начальных GPO

В отличие от стандартных GPO, нельзя создать резервную копию начальных GPO, щелкнув правой кнопкой мыши контейнер **Объекты групповой политики** (Group Policy Objects) и выбрав команду **Архивировать все** (Back Up All). Нельзя также восстановить их командой **Управление архивацией** (Manage Backups), щелкнув контейнер доменов или объектов групповой политики. Чтобы создать резервную копию всех начальных GPO, щелкните правой кнопкой мыши контейнер **Начальные объекты групповой политики** (Starter GPOs) и выберите команду **Архивировать все** (Back Up All). Можно также архивировать отдельные начальные GPO, щелкая на них правой кнопкой мыши и выбирая команду **Архивировать** (Back Up). Резервную копию можно сохранить в папку на жестком диске, на компакт-диск или в общую сетевую папку. На Рис. 4-5 изображено диалоговое окно **Архивация стартовых объектов GPO** (Back Up Starter GPO).

Чтобы восстановить начальный GPO из резервной копии, щелкните правой кнопкой мыши контейнер **Начальные объекты групповой политики** (Starter GPOs) и выберите команду **Управление архивацией** (Manage Backups). Мастер восстановления запросит путь к резервной копии и предложит выбрать начальный GPO для восстановления (рис. 4-6). Щелкните **Далее** (Next), а затем **Готово** (Finish), чтобы восстановить выбранный GPO.

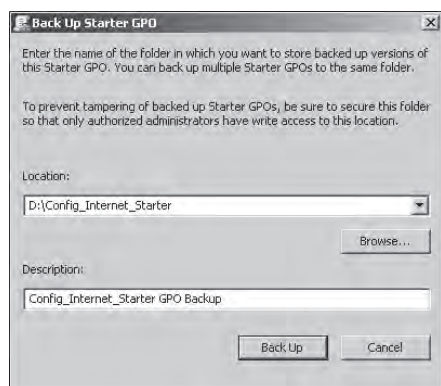


Рис. 4-5. Диалоговое окно Архивация стартовых объектов GPO

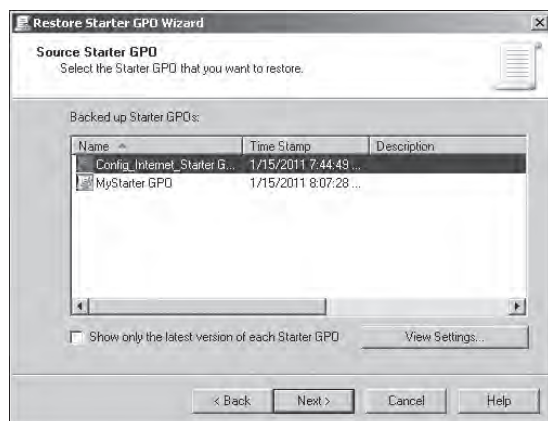


Рис. 4-6. Выбор начального GPO для восстановления

Планирование административных шаблонов

В редакторе групповых политик административные шаблоны (называемые также параметрами политики на основе реестра) обычных и начальных GPO отображаются в разделе **Административные шаблоны** (Administrative Templates) конфигурации компьютера и конфигурации пользователя. Административные шаблоны создаются на основе XML-файлов административных шаблонов. Параметры административных шаблонов любого GPO (кроме системных начальных GPO) можно редактировать. Для этого дважды щелкните любой параметр политики и измените его состояние, включив или отключив его. После этого можно выбрать любые другие доступные параметры на вкладке параметров.

Однако не рекомендуется произвольно изменять параметры политики административных шаблонов в соответствии с отдельными изолированными требованиями. Легко забыть, что какой-то GPO имеет нестандартный параметр политики, и связать его с подразделением, для которой данный параметр политики не подходит. Помните: если политика пользователей конфликтует с политикой компьютера, последняя, как правило, имеет приоритет. Однако это нельзя гарантировать для каждого приложения. Если авторы приложения не следуют этому правилу, групповая политика не может принудительно применить его.

Следовательно, следует запланировать создание нескольких проверенных и хорошо документированных параметров административных шаблонов, внедренных в начальные GPO. Если параметры соответствуют промышленному стандарту, их можно хранить в системных начальных GPO. Собственные GPO следует создавать на основе начальных GPO. Параметры программ и параметры Windows из конфигурации пользователя и конфигурации компьютера можно редактировать в обычных GPO, однако не следует изменять административные шаблоны, которые определены начальным GPO, на котором основаны эти обычные GPO.

Проверьте себя

- Какие группы параметров политики содержат начальные GPO?
- Начальные GPO какого типа доступны только для чтения?

Ответы

- Параметры административных шаблонов для конфигураций пользователя и компьютера.
- Системные начальные GPO.

Фильтрация параметров административных шаблонов

Если в редакторе управления групповыми политиками (Group Policy Management Editor) доступно много параметров административных шаблонов, и вы хотите, чтобы отображались только те шаблоны, которые соответствуют определенным критериям, можно отфильтровать представление административных шаблонов в соответствии с этими критериями. Фильтрация определяет, какие параметры отображаются на консоли, и никак не влияет на параметры, применяемые к GPO. Вы можете не видеть отфильтрованный параметр политики шаблонов, однако он все равно существует и применяется. Кроме того, фильтрация не влияет на то, применяются ли параметры к пользователям или к компьютерам. Фильтрация представления административных шаблонов — это не то же самое, что и фильтрация области групповой политики в соответствии с членством в группах безопасности.

Можно отображать только настроенные или полностью управляемые параметры политики. Можно использовать фильтры требований (Requirement Filters), чтобы отображать параметры, соответствующие выбранным платформам. Можно выполнять фильтрацию по наличию указанного текста в заголовках параметров политики или связанном тексте справки. В Windows Server 2008 появилась возможность фильтрации по тексту комментариев, которые можно добавлять в конфигурацию политики. Такая возможность поддерживается и в Windows Server 2008 R2. На рис. 4-7 показана конфигурация для отображения всех параметров политики, имеющих фразу «Internet Explorer» в тексте комментариев.

ПРИМЕЧАНИЕ Параметры фильтрации административных шаблонов не сохраняются

После закрытия редактора управления групповыми политиками параметры фильтрации представления административных шаблонов не сохраняются.

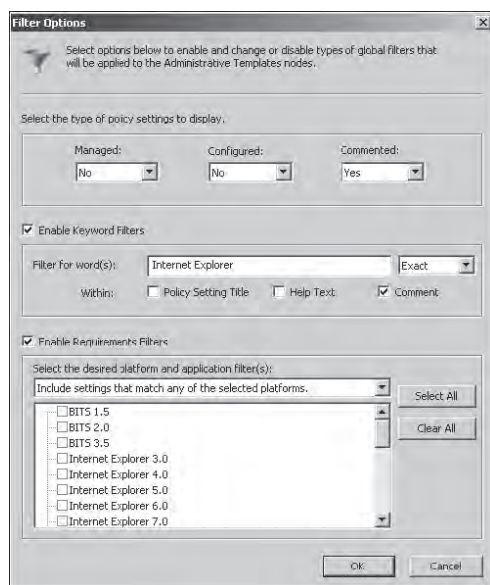


Рис. 4-7. Фильтрация по тексту комментариев

Управление групповыми политиками с помощью ADMX-файлов

ADMX-файлы на основе XML служат заменой ADM-файлов, использовавшихся в Windows Server 2003 и ранее. В отличие от ADM-файлов, ADMX-файлы не хранятся в отдельных GPO. Можно создать центральное хранилище ADMX-файлов, доступ к которому будут иметь все пользователи с разрешением на создание или редактирование GPO. Инструменты групповой политики по-прежнему распознают все имеющиеся ADM-файлы, однако они игнорируют все ADM-файлы, замененные ADMX-файлами. Редактор управления групповыми политиками автоматически считывает и отображает параметры политики административных шаблонов из ADMX-файлов, хранящихся локально или в центральном хранилище ADMX. Все параметры групповой политики, применяемые в предшествующих операционных системах через ADM-файлы, в Windows Server 2008 и 2008 R2 доступны в файлах ADMX.

ПРИМЕЧАНИЕ ADMX-файлы в Windows Vista и Windows 7

Windows Vista и Windows 7 используют ADMX-файлы для применения локальной политики. Если создать центральное хранилище на контроллере домена под управлением Windows Server 2008 или 2008 R2, то можно копировать в это хранилище ADMX-файлы с административной рабочей станции, работающей под управлением Windows Vista или Windows 7.

Файлы административных шаблонов используют формат на основе XML, описывающий параметры групповой политики, хранящиеся в реестре. ADMX-файлы делятся на независимые (.admx-файлы) и зависимые от языка ресурсы (.adml-файлы). Это дает инструментам групповой политики возможность настраивать пользовательский интерфейс в соответствии с выбранным языком. Можно добавить новый язык в набор определений политики, при условии наличия файла ресурсов, ориентированного на этот язык.

Пути к ADMX-файлам

ADMX-файлы на контроллерах домена, работающих под управлением Windows Server 2008 и 2008 R2, можно содержать в центральном хранилище. Это существенно уменьшает объем дискового пространства, требуемого для поддержки GPO. В Windows Server 2008 и 2008 R2 редактор управления групповыми политиками не копирует ADMX-файлы в каждый редактируемый GPO, а предоставляет средства для чтения из одного расположения на уровне домена. Если центральное хранилище недоступно, редактор будет считывать данные с локальной административной рабочей станции, работающей под управлением Windows Vista или Windows 7.

По умолчанию центральное хранилище отсутствует, и его нужно создать вручную. Вы сделаете это на одном из упражнений этого занятия. Помимо хранения стандартных ADMX-файлов Windows Server 2008 в центральном хранилище, можно совместно использовать пользовательский ADMX-файл, скопировав его в центральное хранилище. Это автоматически сделает его доступным всем администраторам групповой политики в домене. В табл. 4-1 показаны пути к ADMX-файлам на контроллере домена (в типичной установке Windows Server 2008 или 2008 R2 с ADMX-файлами для языка U.S. English). Microsoft рекомендует вручную создавать центральное хранилище на основном контроллере домена, то есть на первом контроллере домена, работающем под управлением Windows 2008 или 2008 R2, настроенном в домене. Это ускоряет репликацию файлов на все остальные контроллеры в домене за счет использования репликации распределенной файловой системы (DFSР).

Табл. 4-1. Пути к ADMX-файлам на контроллере домена

Тип файла	Путь к файлу
ADMX-файл, независимый от языка (.admx)	C:\Windows\SYSVOL\domain\policies\PolicyDefinitions
ADMX-файл, зависимый от языка (.adml)	C:\Windows\SYSVOL\domain\policies\PolicyDefinitions\en-us

Центральное хранилище для ADMX-файлов позволяет всем администраторам, редактирующим GPO домена, получать доступ к одному и тому же набору ADMX-файлов. После создания центрального хранилища инструменты групповой политики будут использовать только ADMX-файлы из центрального хранилища, игнорируя все локальные версии. Для редактирования GPO с использованием ADMX-файлов из центрального хранилища сначала нужно создать центральное хранилище и все необходимые подпапки для языковых файлов. После этого можно скопировать ADMX-файлы с административной рабочей станции в центральное хранилище. Все это вы сделаете во время выполнения упражнений этого занятия.

Создание пользовательских ADMX-файлов

Если стандартных параметров групповой политики, поставляемых с Windows Server, недостаточно, можно создавать пользовательские ADMX-файлы. В этом случае необходимо соблюдать осторожность, так как ADMX-файлы вносят изменения в реестр. Тщательно следите за тем, что изменяете, и дважды или даже

трижды проверяйте свой код. Не устанавливайте пользовательские ADMX-файлы в корпоративной сети, не проверив их работу в изолированной тестовой сети.

Чтобы научиться использовать синтаксис ADMX, Microsoft рекомендует загружать и устанавливать файлы-образцы и изменять элементы, которые не влияют на реестр. Установочный файл можно загрузить с сайта Microsoft: <http://www.microsoft.com/downloads/en/details.aspx?FamilyId=3D7975FF-1242-4C94-93D3-B3091067071A&displaylang=en>.

Схема ADMX определяет синтаксис ADMX-файлов. Если хотите просмотреть эту схему, скачайте ее отсюда: <http://www.microsoft.com/downloads/details.aspx?FamilyId=B4CB0039-E091-4EE8-9EC0-2BBCE56C539E&displaylang=en>. Впрочем, имейте в виду, что экзамен не содержит вопросов об управлении схемой.

Создавать и редактировать ADMX-файлы можно при помощи редактора XML или текстового редактора, такого как Блокнот. Если не хотите скачивать файлы-образцы, можно с помощью Блокнота открывать ADMX-файлы, которые вы разместите в центральном хранилище, выполняя упражнения этого занятия. Не забудьте изменить имя файла, прежде чем сохранять какие-либо изменения.

ПРИМЕЧАНИЕ Изучение ADMX-файлов

ADMX-файлы довольно длинные, поэтому включать их в данную книгу было бы непрактично и не особенно полезно. Вместо этого советуем открывать эти файлы в Блокноте и изучать их содержимое.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Пользовательские ADMX-файлы

Если вы планируете создать несколько ADMX-файлов, которые будут отображаться в редакторе управления групповыми политиками под одним узлом, потребуется создать пользовательский файл. Подробнее см. по адресу [http://technet.microsoft.com/ru-ru/library/cc770905\(WS.10\).aspx](http://technet.microsoft.com/ru-ru/library/cc770905(WS.10).aspx).

ADMX-файлы создаются в виде одного независимого от языка файла (.admx) и одного или нескольких языковых файлов (.adml). Заметьте, что язык XML чувствителен к регистру. Независимый от языка ADMX-файл содержит следующие элементы:

- **декларация XML** подтверждает, что файл является файлом на основе XML; содержит информацию о версии и кодировке;
- **элемент PolicyDefinitions** содержит все остальные элементы для .admx-файла;
- **элемент PolicyNamespaces** определяет уникальное пространство имен для файла и обеспечивает сопоставление с пространствами имен внешних файлов;
- **элемент Resources** определяет требования к языковым ресурсам, такие как минимальная требуемая версия связанного .adml-файла;
- **элемент SupportedOn** определяет ссылки на локализованные текстовые строки, определяя операционные системы или приложения, к которым применяется конкретный параметр политики;
- **элемент Categories** определяет категории, под которыми будет отображаться параметр политики в файле в редакторе управления групповыми полити-

ками. Заметьте, что если указать имя категории, которое уже существует в другом ADMX-файле, будет создан дубликат узла;

- **элемент Policies** содержит индивидуальные определения параметров политики.

Зависимый от языка ADMX-файл (языковой ресурс) содержит следующие элементы:

- **декларация XML** подтверждает, что файл является файлом на основе XML. В файлах .admx и .adml этот элемент одинаковый;
- **элемент PolicyDefinitionResources** содержит все остальные элементы для языкового ADMX-файла;
- **элемент Resources (.adml)** содержит элемент StringTable и элемент PresentationTable для конкретного языка.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Элементы ADMX-файлов

Подробнее об элементах ADMX-файлов и, в частности, о связывании сведений параметров файлов ADMX ADML см. по адресу [http://technet.microsoft.com/ru-ru/library/cc731761\(WS.10\).aspx](http://technet.microsoft.com/ru-ru/library/cc731761(WS.10).aspx).

СОВЕТ Подготовка к экзамену

Вряд ли на экзамене вас попросят создать ADMX-файл. Однако вам могут показать фрагмент кода XML и задать вопрос о нем. Как правило, код нетрудно понять. Например, раздел кода, начинающийся с <policies>, скорее всего, образует часть элемента Policies.

Резюме

- Консоль GPMC тесно интегрирована с Windows Server 2008 и 2008 R2. Ее можно установить с помощью диспетчера сервера.
- Независимые и зависимые от языка ADMX-файлы определяют настраиваемые параметры групповой политики в доменах Windows Server 2008. Эти файлы можно хранить в центральном хранилище на контроллерах домена. Для этого необходимо создать центральное хранилище на одном контроллере домена. Оно будет передаваться на другие контроллеры домена при репликации распределенной файловой системы.
- Начальные GPO могут содержать параметры административных шаблонов для конфигураций пользователя и компьютера. Объекты GPO можно создавать на основе начальных GPO, содержащих известные и проверенные параметры административных шаблонов, и настраивать только параметры, не относящиеся к административным шаблонам.
- В Windows Server 2008 R2 появились системные начальные GPO, доступные только для чтения.
- Можно создавать резервные копии всех начальных GPO или отдельных системных начальных GPO. Команда **Управление архивацией** (Manage Backups) из контекстного меню контейнера **Начальные объекты групповой политики** (Starter GPOs) позволяет восстанавливать отдельные GPO из резервной копии.

Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных на занятии 1. Эти вопросы предоставлены также в электронном виде на прилагаемом к книге компакт-диске.

ПРИМЕЧАНИЕ Ответы

Ответы на вопросы и пояснения к их вариантам размещены в разделе «Ответы» в конце книги.

1. Вы хотите восстановить стандартный GPO с именем MyGPO из резервной копии. Как это сделать? (Каждый ответ является законченным решением. Выберите три.)
 - a. Щелкните правой кнопкой мыши объект MyGPO в любом подразделении, с которым он связан. Выберите команду **Восстановить из архива** (Restore From Backup). Следуйте инструкциям мастера восстановления.
 - b. Щелкните правой кнопкой мыши MyGPO в контейнере **Объекты групповой политики** (Group Policy Objects). Выберите команду **Восстановить из архива** (Restore From Backup). Следуйте инструкциям мастера восстановления.
 - c. Щелкните правой кнопкой мыши контейнер **Домены** (Domains). Выберите команду **Управление архивацией** (Manage Backups). Укажите путь к резервной копии. Выберите MyGPO. Щелкните **Восстановить** (Restore).
 - d. Щелкните правой кнопкой мыши контейнер **Начальные объекты групповой политики** (Starter GPOs). Выберите команду **Управление архивацией** (Manage Backups). Укажите путь к резервной копии. Выберите MyGPO. Щелкните **Восстановить** (Restore).
 - e. Щелкните правой кнопкой мыши контейнер **Объекты групповой политики** (Group Policy Objects). Выберите команду **Управление архивацией** (Manage Backups). Укажите путь к резервной копии. Выберите MyGPO. Щелкните **Восстановить** (Restore).
2. Вы хотите создать резервную копию начального GPO с именем MyStarterGPO. Как это сделать? (Каждый ответ является законченным решением. Выберите два.)
 - a. Щелкните правой кнопкой мыши контейнер **Объекты групповой политики** (Group Policy Objects). Выберите команду **Архивировать все** (Back Up All). Укажите путь к резервной копии. Щелкните **Архивировать** (Back Up).
 - b. Щелкните правой кнопкой мыши контейнер **Начальные объекты групповой политики** (Starter GPOs). Выберите команду **Архивировать все** (Back Up All). Укажите путь к резервной копии. Щелкните **Архивировать** (Back Up).
 - c. Щелкните правой кнопкой мыши объект MyStarterGPO в контейнере **Начальные объекты групповой политики** (Starter GPO). Выберите команду **Архивировать** (Back Up). Укажите путь к резервной копии. Щелкните **Архивировать** (Back Up).

- d. Щелкните правой кнопкой мыши контейнер Starter GPOs. Выберите команду **Управление архивацией** (Manage Backups). Укажите путь к резервной копии. Щелкните **Архивировать** (Back Up).
 - e. Щелкните правой кнопкой мыши контейнер **Объекты групповой политики** (Group Policy Objects). Выберите **Управление архивацией** (Manage Backups). Укажите путь к резервной копии. Щелкните **Архивировать** (Back Up).
3. Вы хотите отобразить только параметры политики конфигурации пользователя из начального GPO MyStarterGPO, имеющие в тексте комментария фразу «Internet Explorer». Щелкните правой кнопкой мыши контейнер **Начальные объекты групповой политики** (Starter GPO) и выберите команду **Изменить** (Edit). Щелкните правой кнопкой мыши узел **Административные шаблоны** (Administrative Templates) из конфигурации пользователя и выберите команду **Параметры фильтра** (Filter Options). Какие параметры фильтра позволяют отображать требуемые параметры политики? (Каждый ответ является частью решения. Выберите четыре.)
- a. В секции **Выберите тип отображаемых параметров политики** (Select The Type Of Policy Settings To Display) выберите **Да** (Yes) под заголовком **С комментарием** (Commented).
 - b. В секции **Выберите тип отображаемых параметров политики** (Select The Type Of Policy Settings To Display) выберите **Нет** (No) под заголовком **С комментарием** (Commented).
 - c. Установите флажок **Включить фильтры по ключевым словам** (Enable Keyword Filters).
 - d. В секции **Фильтры по словам** [Filter For Word(s)] введите «Internet Explorer» и выберите **Точное** (Exact).
 - e. В секции **Фильтры по словам** [Filter For Word(s)] установите только флажок **Комментарий** (Comment).
 - f. В секции **Фильтры по словам** [Filter For Word(s)] установите флажки **Заголовок параметра политики** (Policy Setting Title) и **Текст справки** (Help Text). Не устанавливайте флажок **Комментарий** (Comment).
4. Элемент независимого от языка ADMX-файла содержит следующий код:
- ```
<?xml version="1.0" encoding="utf-8"?>
```
- Что это за элемент?
- a. Элемент Policies.
  - b. Элемент SupportedOn.
  - c. Элемент PolicyNamespaces.
  - d. Декларация XML.
5. Какой элемент независимого от языка ADMX-файла определяет ссылки на локализованные текстовые строки, определяя операционные системы или приложения, к которым применяется параметр политики?
- a. Элемент Categories.
  - b. Элемент SupportedOn.

- c. Элемент PolicyNamespaces.
- d. Элемент Resources.

## Занятие 2. Стратегия объектов групповой политики

Будучи опытным администратором, вы уже знаете, что групповая политика упрощает администрирование за счет автоматизации многих задач по управлению пользователями и компьютерами. Например, вы должны знать, что с помощью групповой политики можно по требованию устанавливать разрешенные приложения на клиенты и обновлять их.

Вы наверняка знаете, что параметры групповой политики, содержащиеся в GPO, можно связать с подразделениями, которые могут либо наследовать параметры от родительских подразделений, либо блокировать наследование и получать собственные параметры из связанных с ними GPO. Также вы должны знать, что некоторые политики, в частности, политики безопасности, могут применяться принудительно (в Windows Server 2003 это называлось «без переопределения»), поэтому их нельзя блокировать или переписать и принудительно применить к дочерним подразделениям унаследованные родительские параметры.

В Windows Server 2008 и 2008 R2 не изменен ни один из этих параметров, но добавлены объекты настроек пароля (Password Setting Objects, PSO), описанные в гл. 3. Эти объекты позволяют настраивать некоторые параметры безопасности (например, параметры блокирования пароля и учетной записи) отдельно от параметров домена по умолчанию и применять их к группам безопасности.

На этом занятии не будут подробно рассматриваться базовые аспекты групповой политики. Мы рассмотрим стратегию групповой политики, улучшения, появившиеся в групповой политике Windows Server 2008 и 2008 R2, и некоторые наиболее значимые новые параметры.

---

### Изучив материал этого занятия, вы сможете:

- ✓ Объяснять и применять общие принципы стратегии проектирования групповой политики.
- ✓ Описывать наиболее значимые из новых параметров групповой политики, появившихся в Windows Server 2008 и 2008 R2, и их функции.
- ✓ Определять различные проблемы, которые могут возникнуть в конфигурации групповой политики, а также способы их решения.

**Продолжительность занятия — примерно 40 мин.**

---

## Планирование стратегии групповой политики

Планирование групповой политики частично связано с планированием организационной структуры. Если в структуре много подразделений, одни из которых наследуют политику, другие блокируют наследование, третьи связаны с одним и тем же GPO, а некоторые GPO связаны с одним подразделением, то у вас есть средство, чтобы разобраться со всем этим. Хотя иметь слишком мало подразделений и GPO — тоже ошибка, большинство из нас ошибаются, создавая

слишком много. Делайте структуры простыми. Не связывайте подразделения и GPO из разных сайтов. Назначайте подразделениям и объектам групповой политики содержательные имена.

Политики блокирования наследования, принудительного применения, фильтров безопасности, замыкания на себя и др. могут быть полезны в определенных ситуациях. Однако они усложняют структуру групповой политики и затрудняют ее понимание. Эти функции следует использовать лишь тогда, когда это дает реальные преимущества.

Если GPO не имеет политик в конфигурации компьютера, то желательно отключить параметры конфигурации компьютера. Эти параметры обрабатываются, даже когда не настроены, и их отключение экономит время и ресурсы. Для отключения правой кнопкой мыши щелкните GPO в редакторе управления групповыми политиками и выберите команду **Свойства (Properties)** (рис. 4-8). Гораздо реже политики бывают не настроены в конфигурации пользователя, но и в этом случае можно отключить параметры конфигурации пользователя.

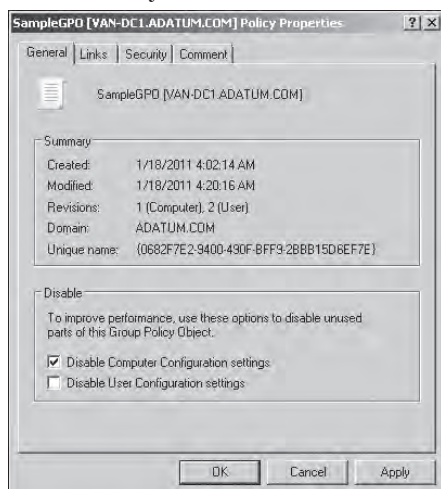


Рис. 4-8. Отключение параметров конфигурации компьютера

#### ПРИМЕЧАНИЕ Планирование стратегии подразделений

При планировании стратегии подразделений желательно определять отдельные подразделения для объектов пользователей и групп и для объектов компьютеров. Если GPO связан с подразделением, можно отключить для этого GPO конфигурацию компьютера или пользователя. Исключения составляют GPO, связанные с контейнером домена, для которого обычно настраиваются и параметры пользователя, и параметры компьютера.

После изменения конфигурации групповой политики используйте команду `Groupdate`. Даже если изменения GPO были реплицированы в домене, они не вступят в силу до следующего обновления групповой политики. Команда `Groupdate` вызывает обновление политики. Это команду можно выполнять на контроллере домена, любом рядовом сервере или клиенте домена, где нужно, чтобы изменения групповой политики вступили в силу немедленно.

Используйте стандартные комбинации параметров административных шаблонов, предварительно определенных в начальных или начальных системных GPO, и избегайте необходимости редактирования этих параметров в обычных GPO, создаваемых на основе начальных GPO. Всегда храните свои ADMX-файлы в центральном хранилище.

При планировании групповой политики следует учитывать новые параметры, появившиеся в Windows Server 2008 и 2008 R2. Их очень много, и нет смысла запоминать их все, но следует ознакомиться с их категориями. Даже если вы не редактируете политики, рекомендуем изучить структуру групповой политики в редакторе управления групповыми политиками. Это поможет понять, какие возможности доступны, и определить, следует ли создавать пользовательские политики, создавая ADMX-файлы (см. предыдущий урок).

Необходимо также хорошо понимать, как групповая политика обрабатывается на клиенте. Это происходит в два этапа:

- **Обработка ядра.** Когда клиент начинает обрабатывать групповую политику, он должен определить, может ли он достичь контроллера домена, были ли изменены какие-либо GPO, и какие параметры политики необходимо обработать. Механизм ядра групповой политики выполняет такую обработку на начальном этапе.
- **Обработка клиентских расширений (CSE).** На этом этапе параметры групповой политики распределяются по различным категориям, таким как административные шаблоны, параметры безопасности, перенаправление папок, дисковые квоты и установка программного обеспечения. Определенное расширение обрабатывает параметры в каждой категории, при этом каждое расширение имеет свои правила обработки параметров. Механизм ядра групповой политики вызывает расширения, необходимые для обработки параметров, применяемых к клиенту.

Клиентские расширения не могут начать обработку, пока не завершена обработка ядра групповой политики. Таким образом, важно планировать групповую политику и структуру домена так, чтобы это происходило как можно быстрее и надежнее. Далее на этом занятии обсуждаются некоторые проблемы, которые могут задержать или остановить обработку ядра групповой политики.

## Новые параметры групповой политики

В Windows Server 2008 появилось много новых параметров групповой политики, которые сохранились и в Windows Server 2008 R2. Ниже приведен список наиболее значимых из них.

- **Разрешать удаленный запуск любых программ (Allow Remote Start Of Unlisted Programs).** Этот параметр из конфигурации компьютера определяет, разрешено ли пользователям, начавшим сеанс удаленной работы через службы удаленных рабочих столов (в Windows Server 2008 R2) или службы терминалов (в Windows Server 2008), запускать любые программы или только программы из списка удаленных приложений RemoteApp. Создать такой список можно при помощи диспетчера удаленных приложений RemoteApp. По умолчанию пользователь, начавший сеанс удаленной работы, может запускать только программы из списка удаленных приложений RemoteApp.

На рис. 4-9 показано диалоговое окно для настройки этого параметра.

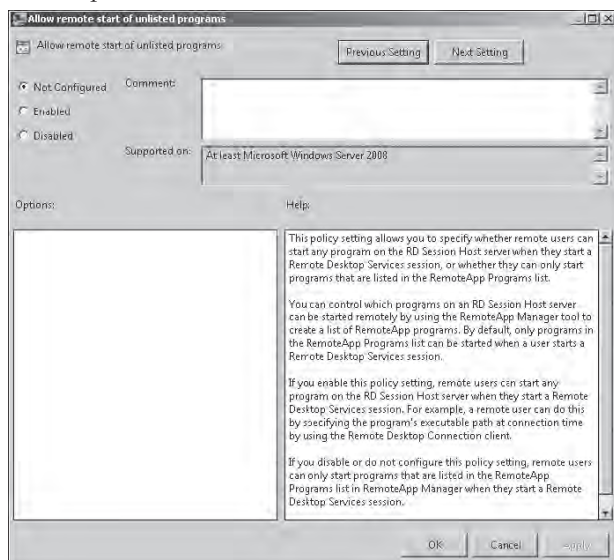


Рис. 4-9. Настройка параметра Allow Remote Start Of Unlisted Program

Полезно сравнить это диалоговое окно с аналогичным диалоговым окном из Windows Server 2008 (рис. 4-10). В Windows Server 2008 R2 можно настроить этот параметр, добавить комментарий и прочитать пояснение, не открывая разные вкладки.

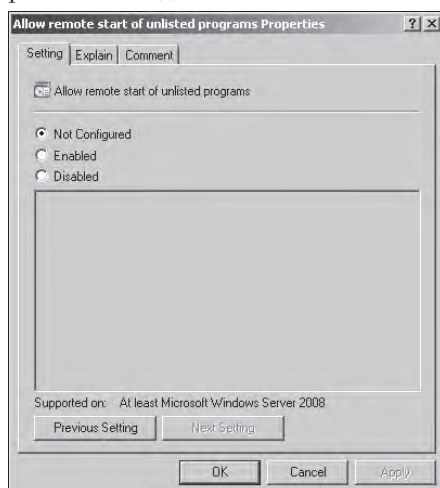


Рис. 4-10. Аналогичное диалоговое окно в Windows Server 2008

#### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Диспетчер RemoteApp, службы удаленных рабочих столов и службы терминалов

Подробнее о диспетчере удаленных приложений RemoteApp см. по адресу <http://technet.microsoft.com/ru-ru/library/cc755261.aspx>. Службы удаленных рабочих столов обсуждаются в гл. 5 и 6. Подробнее о службах терминалов в Windows Server 2008 см. <http://technet.microsoft.com/en-us/windowsserver/dd448619.aspx>.



- **Разрешить перенаправление часового пояса (Allow Time Zone Redirection).** Этот параметр из конфигурации пользователя определяет, будет ли клиентский компьютер перенаправлять свои параметры часового пояса в сеанс служб терминалов или служб удаленных рабочих столов. Если этот параметр политик включен, клиенты, способные перенаправлять часовой пояс, отправляют на сервер сведения о своем часовом поясе. На рис. 4-11 показан этот параметр в редакторе управления групповыми политиками.

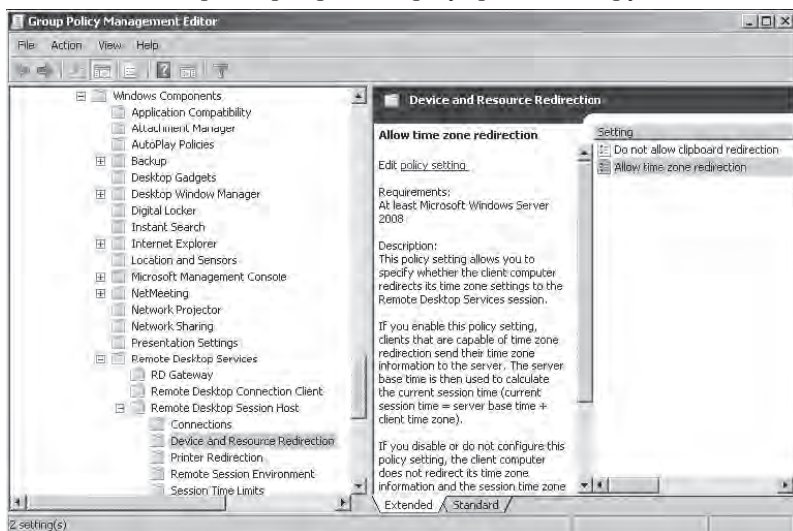


Рис. 4-11. Параметр политики Разрешить перенаправление часового пояса

- **Всегда отображать рабочий стол при подключении (Always Show Desktop On Connection).** Этот параметр политики, применяемый к пользователю, определяет, всегда ли рабочий стол отображается при подключении клиента к удаленному компьютеру, даже если начальная программа уже указана в профиле пользователя по умолчанию, в подключении к удаленному рабочему столу, в клиенте служб терминалов (в Windows Server 2008), в клиенте служб удаленных рабочих столов (в Windows Server 2008 R2) или в групповой политике. Если начальная программа не указана, удаленный рабочий стол всегда отображается при подключении.
- **Настроить пользовательский текст предупреждения (Configure Custom Alert Text).** Этот параметр политики из конфигурации компьютера требует установки на сервер Windows Server 2008 или 2008 R2 компонента **Возможности рабочего стола** (Desktop Experience). Он подставляет пользовательский текст в сообщение диагностики диска, появляющееся, когда диск сообщает об ошибке SMART.



## ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ SMART

Большинство производителей встраивает в свои жесткие диски логику SMART. Она играет роль ранней системы предупреждения о возможных проблемах с диском. Подробнее см. по адресу <http://www.pcguides.com/ref/hdd/perf/qual/featuresSMART-c.html>. Эта ссылка ведет не на сайт Microsoft, и адрес может измениться. В этом случае можно выполнить поиск в Интернете по ключевым словам: «технология самоконтроля, анализа и отчетности, SMART». Однако учитывайте, что SMART не является технологией Microsoft и вряд ли будет затронута на экзамене.

- **Диагностика диска: Настроить уровень выполнения (Disk Diagnostic: Configure Execution Level).** Этот параметр из конфигурации компьютера требует установки на сервер Windows Server 2008 или 2008 R2 компонента **Возможности рабочего стола** (Desktop Experience). Он определяет уровень выполнения для диагностики диска на основе SMART. Служба политики диагностики (DPS) обнаруживает и записывает возникающие ошибки SMART в журнал событий. Если этот параметр политики включен, DPS будет также предупреждать пользователей и руководить созданием резервных копий и восстановлением, чтобы минимизировать возможные потери данных.
- **Не разрешать перенаправление буфера обмена (Do Not Allow Clipboard Redirection).** Этот параметр политики из конфигурации пользователя определяет, следует ли отключать совместное использование содержимого буфера обмена (перенаправление буфера обмена) удаленным компьютером и клиентом в сеансе служб терминалов или служб удаленных рабочих столов. По умолчанию службы терминалов и службы удаленных рабочих столов разрешают перенаправление буфера обмена. Если выбрано состояние политики **Не задана** (Not Configured), перенаправление буфера обмена на уровне групповой политики не определено.
- **Не отображать окно «Задачи начальной настройки» автоматически при входе (Do Not Display Initial Configuration Tasks Window Automatically At Logon).** Этот параметр политики из конфигурации компьютера отключает автоматическое отображение окна **Задачи начальной настройки** (Initial Configuration Tasks) при входе в систему. Если этот параметр не настроен, окно **Задачи начальной настройки** будет отображаться при входе администратора на сервер. Тем не менее, если администратор установит флажок **Не показывать это окно при входе в систему** (Do Not Show This Window At Logon), то при последующих входах окно отображаться не будет.
- **Не отображать диспетчер сервера автоматически при входе (Do Not Display Server Manager Automatically At Logon).** Этот параметр политики из конфигурации компьютера отключает автоматическое отображение диспетчера сервера при входе в систему. Если этот параметр включен, диспетчер сервера не будет автоматически открываться при входе администратора на сервер. Этот параметр связан с сервером, а не с конкретной учетной записью пользователя.
- **Принудительная отмена фонового рисунка удаленного рабочего стола (Enforce Removal Of Remote Desktop Wallpaper).** Этот параметр политики

из конфигурации компьютера указывает, будет ли отображаться фоновый рисунок рабочего стола на удаленных клиентах, подключающихся через службы терминалов или службы удаленных рабочих столов. Можно использовать этот параметр для принудительного удаления фонового рисунка с рабочего стола во время удаленного сеанса. Если политика включена, фоновый рисунок никогда не отображается в удаленном сеансе. Если политика отключена, фоновый рисунок может отображаться в зависимости от настройки клиента.

- **Редактор управления групповыми политиками (Group Policy Management Editor).** Этот параметр из конфигурации пользователя разрешает или запрещает использование редактора управления групповыми политиками. Если этот параметр включен, использование редактора разрешено. Если этот параметр не настроен, использование редактора разрешается или запрещается параметром **Ограничить использование оснасток списком явно разрешенных оснасток** (Restrict Users To The Explicitly Permitted List Of Snap-Ins).

---

#### **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ** Ограничить использование оснасток списком явно разрешенных оснасток

Параметр политики **Ограничить использование оснасток списком явно разрешенных оснасток** (Restrict Users To The Explicitly Permitted List Of Snap-Ins) не является новым для Windows Server 2008 или 2008 R2 и, следовательно, не рассматривается на этом занятии. Если вы не знакомы с этим параметром, см. <http://technet.microsoft.com/en-gb/library/cc975962.aspx> (на англ. языке).

- 
- **Редактор стартового GPO групповой политики (Group Policy Starter GPO Editor).** Этот параметр политики из конфигурации пользователя разрешает или запрещает использование этой оснастки редактора. Если этот параметр не настроен, использование оснастки разрешается или запрещается параметром **Ограничить использование оснасток списком явно разрешенных оснасток** (Restrict Users To The Explicitly Permitted List Of Snap-Ins).
  - **Перенаправлять только используемый по умолчанию принтер клиента (Redirect Only The Default Client Printer) — конфигурация пользователя.** Этот параметр определяет, является ли принтер клиента по умолчанию единственным принтером, перенаправляемым в сеансах служб терминалов и служб удаленных рабочих столов.
  - **Перенаправлять только используемый по умолчанию принтер клиента (Redirect Only The Default Client Printer) — конфигурация компьютера.** Этот параметр определяет, является ли принтер клиента по умолчанию единственным принтером, перенаправляемым в сеансах служб терминалов. Поскольку это параметр из конфигурации компьютера, он не зависит от того, какой пользователь вошел в систему.
  - **Set The Number Of Synchronization Retries For Servers Running Password Synchronization (Установить число попыток синхронизации для серверов, выполняющих синхронизацию паролей).** Этот параметр политики из конфигурации компьютера определяет число попыток синхронизации при отказе сервера. Если этот параметр включен, все задействованные серверы

синхронизации паролей используют указанное число попыток. Если этот параметр отключен или не настроен, к серверам синхронизации паролей будут применяться пользовательские настройки.

- **Set The Interval Between Synchronization Retries For Password Synchronization (Установить интервал между попытками синхронизации для синхронизации паролей).** Этот параметр из конфигурации компьютера определяет интервал в секундах между попытками в случае неудачной синхронизации. Если этот параметр отключен или не настроен, к серверам синхронизации паролей будут применяться пользовательские настройки.
- **Set The Map Update Interval For NIS Subordinate Servers (Установить интервал обновления карт для подчиненных серверов NIS).** Этот параметр политики из конфигурации компьютера определяет интервал обновления для извещающей отправки карт NIS (сетевой информационной службы) на подчиненные серверы NIS. Если этот параметр включен, заданный интервал обновления будет использоваться на всех контроллерах домена с ролью сервера для NIS. Если этот параметр отключен или не настроен, к серверам для NIS будут применяться пользовательские настройки.

---

#### **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Серверы для NIS**

Подробнее о NIS см. по адресу <http://technet.microsoft.com/ru-ru/library/cc772394.aspx>.

- **Использовать балансировку нагрузки посредника подключений к удаленному рабочему столу (или службам терминалов) [Use RD Connection Broker (или TS Session Broker) Load Balancing].** Этот параметр политики из конфигурации компьютера определяет, будет ли использоваться функция балансировки нагрузки посредника подключений к удаленному рабочему столу или службам терминалов для балансировки нагрузки между серверами в составе фермы серверов узлов сеансов удаленных рабочих столов или служб терминалов. Служба роли посредника подключений устанавливается как часть роли служб удаленных рабочих столов на серверы Windows Server 2008 R2 и заменяет посредника сеансов служб терминалов из Windows Server 2008. Если этот параметр политики включен, то посредник перенаправляет пользователей, не имеющих существующего сеанса, на сервер фермы, имеющий наименьшее количество сеансов.

---

#### **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Посредник подключений к удаленному рабочему столу**

Подробнее о посреднике подключений к удаленному рабочему столу см. по адресу [http://technet.microsoft.com/ru-ru/library/dd560675\(WS.10\).aspx?ppud=4](http://technet.microsoft.com/ru-ru/library/dd560675(WS.10).aspx?ppud=4).

- **Turn On Extensive Logging For Password Synchronization (Включить расширенные функции журнала для синхронизации паролей).** Этот параметр политики из конфигурации компьютера управляет расширенными функциями журнала для серверов синхронизации паролей. Если эта политика включена, все задействованные серверы синхронизации паролей записывают промежуточные шаги во время попыток синхронизации.

- **Turn On Extensive Logging For Active Directory Domain Services Domain Controllers That Are Running Server For NIS (Включить расширенные функции журнала для контроллеров домена Active Directory, выполняющих функцию сервера для NIS).** Этот параметр из конфигурации компьютера управляет расширенными функциями журнала сервера для контроллеров домена с функцией сервера для NIS (SNIS).

### Возможности рабочего стола

Компонент **Возможности рабочего стола** (Desktop Experience) на сервере под управлением Windows Server 2008 или 2008 R2 позволяет устанавливать на сервер и настраивать ряд функций Windows 7 (или Windows Vista). Возможности рабочего стола включают следующие компоненты и функции:

- Windows Media Player;
- темы рабочего стола;
- видео для Windows (поддержка AVI);
- Windows SlideShow;
- Защитник Windows;
- Очистка диска;
- Центр синхронизации;
- Запись звука;
- Таблица символов;
- Ножницы.

При установке Возможностей рабочего стола ни одна из этих функций не включается автоматически. После установки необходимо вручную включить все функции, требующие изменений конфигурации. Например, чтобы использовать тему рабочего стола, откройте оснастку Службы (Services), включите и запустите службу **Темы** (Themes), после чего выберите тему.

Чтобы установить Возможности рабочего стола, откройте диспетчер сервера, выберите узел **Компоненты** (Features) и щелкните **Добавить функции** (Add Features) на панели справа. Установите флажок **Возможности рабочего стола** (Desktop Experience) и щелкните **Далее** (Next). Если будет предложено, щелкните **Добавить необходимые компоненты** (Add Required Features), а затем **Далее** (Next), после чего щелкните **Установить** (Install). После установки необходимо перезапустить сервер.

## Решение проблем с групповой политикой

Групповая политика очень редко «ломается». Она является частью AS DS, а значит, обладает прочностью и гибкостью. Гораздо чаще политики применяются не так, как ожидают администраторы или пользователи. Например, параметр в GPO настраивается неправильно или, что бывает чаще, создается неверная структура подразделений и наследования политики. В результате пользователи не могут выполнять нужные им действия или (что серьезнее и что труднее ис-

правильно) могут выполнять действия, которые им не следует выполнять. Если используется машинная обработка замыкания на себя, то компьютеры, находящиеся в безопасном помещении, могут работать без должного уровня защищенности.

Обычно при отладке групповой политики в первую очередь проверяется правильность планирования и реализации инфраструктуры домена. Убедитесь, что необходимые службы и компоненты работают и настроены должным образом. Как и во всех процедурах отладки системы, начните с самого низкого уровня и убедитесь, что сетевая связь полностью работает. Если отдельный клиент работает неправильно, убедитесь, что он подключен к сети, присоединен к домену и имеет правильное системное время.

Ни один администратор не любит исключения, но иногда они необходимы. Обычно приходится работать с фильтрами безопасности, фильтрами WMI, параметрами политик блокирования наследования, принудительно примененными параметрами, обработкой замыкания на себя и параметрами медленной связи. Необходимо проверить, не влияют ли эти параметры на обработку GPO.

## Использование инструментов групповой политики

Инструменты отладки групповой политики хорошо известны, и в Windows Server 2008/ 2008 R2 особых изменений не произошло (кроме добавления в утилиту GPOResult двух новых параметров командной строки). Например, для проверки всех параметров политики, применяющихся к определенному пользователю или компьютеру, используется утилита GPOResult.exe. Утилита GPO-Tool.exe из пакета Windows Server 2003 Resource Kit (доступного для скачивания по адресу <http://www.microsoft.com/downloads/en/details.aspx?familyid=9d467a69-57ff-4ae7-96ee-b18c4790cffd&displaylang=en>) позволяет проверять согласованность объектов GPO на всех контроллерах домена. Эта утилита позволяет также определять, применяются ли определенные политики, и отображает подробную информацию о реплицированных GPO.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Командная строка GPOResult

Подробнее о параметрах командной строки /x и /h утилиты GPOResult, см. по адресу [http://technet.microsoft.com/en-us/library/cc733160\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc733160(WS.10).aspx) (на англ. языке).

---

С помощью мастера **Результаты групповой политики** (Group Policy Results) можно определить результирующий набор политик (RSOP) для конкретного пользователя или компьютера. Этот мастер дает ту же информацию, что и GPOResult.exe. Чтобы воспользоваться этим мастером, дважды щелкните лес в верхней части дерева консоли GPMC, правой кнопкой мыши щелкните **Результаты групповой политики** (Group Policy Results) под узлом **Лес** (Forest) и выберите Команду **Мастер результатов групповой политики** (Group Policy Results Wizard). Мастер запросит имена компьютера и пользователя (по умолчанию используются имена текущего компьютера и пользователя, выполнившего вход) и составит отчет (рис. 4-12).

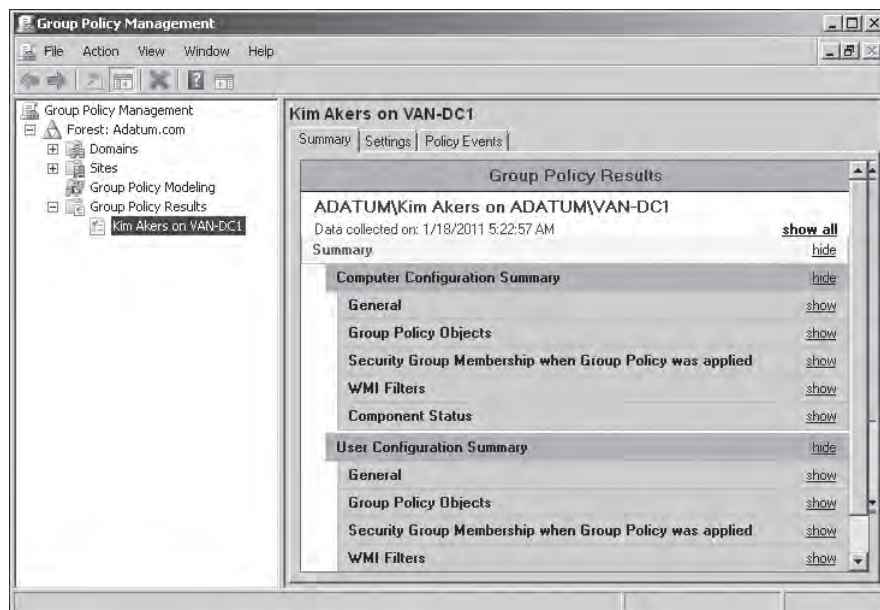


Рис. 4-12. Генерация отчета RSoP

Пожалуй, одним из самых полезных инструментов для изолирования проблем групповой политики является функция создания отчетов консоли GPMC. Можно выбрать GPO в левой части окна и просмотреть информацию отчета GPO на вкладках правой панели (рис. 4-13). Можно также щелкнуть GPO правой кнопкой мыши и выбрать команду **Сохранить отчет** (Save Report) (рис. 4-14).

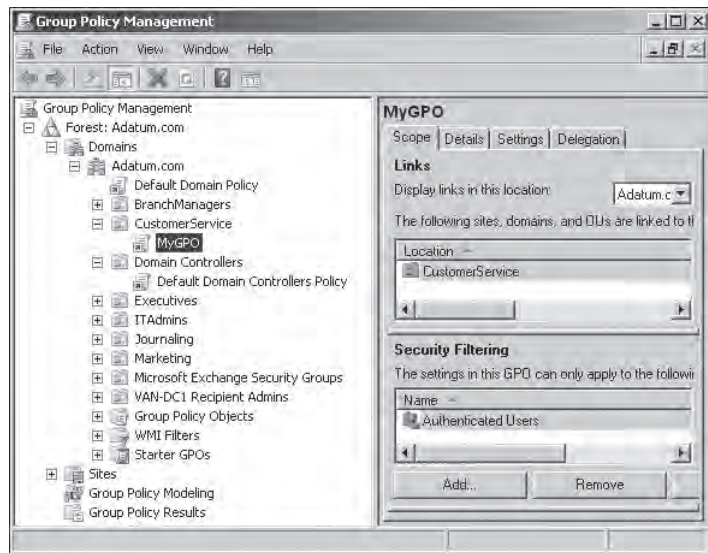


Рис. 4-13. Просмотр информации GPO



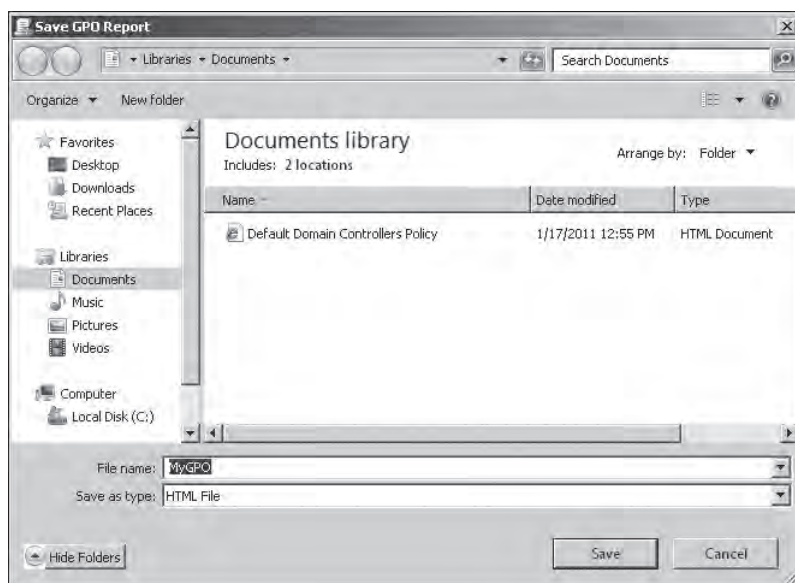


Рис. 4-14. Сохранение отчета GPMC

На рис. 4-15 показана часть выходных данных из отчета GPO. По умолчанию отчеты сохраняются в формате HTML и открываются в Internet Explorer.

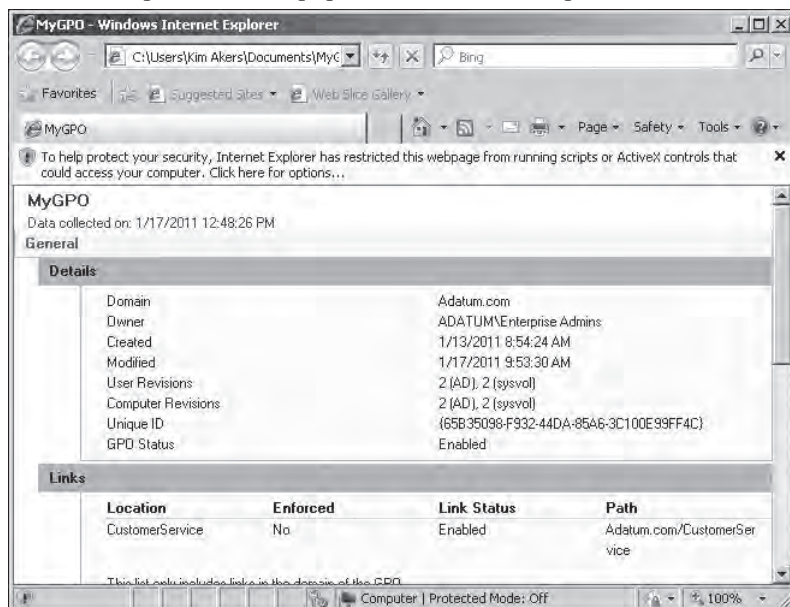


Рис. 4-15. Выходные данные отчета GPMC

В отчетах GPMC можно найти ответы на следующие вопросы:

- Содержат ли результаты все примененные GPO?
- Содержат ли результаты нужный параметр?
- Входит ли GPO в список запрещенных объектов?



## Проблемы обработки ядра

Если обработка ядра происходит медленно и неэффективно, то может не начаться обработка клиентских расширений, и групповая политика не будет применена. На обработку ядра влияет несколько факторов.

Одной из наиболее распространенных причин, по которым GPO не применяется к пользователю или компьютеру, является отсутствие привязки GPO к сайту, домену или подразделению, где находится пользователь или компьютер. Объекты GPO применяются к клиентам на основе принадлежности компьютера и выполнившего вход пользователя к сайту и подразделению.

### Проверьте себя

- Какая утилита командной строки проверяет все параметры политики, применяемые к определенному пользователю или компьютеру?

### Ответы

- GPResult.exe.

Еще одна возможная причина проблем обработки ядра заключается в том, что еще не успела произойти репликация. Если связаны объекты GPO из разных сайтов (что не рекомендуется), это может быть особенно проблематично. Когда GPO связывается с сайтом, доменом или подразделением в иерархии, это изменение должно реплицироваться на контроллер домена, из которого клиент получает свой GPO. Если в подразделение добавляется пользователь или компьютер, то GPO, применяемые к этому подразделению, могут не применяться к клиенту, пока не будет реплицировано это изменение.

Изменения, произошедшие в GPO, должны достичь клиента. Это происходит во время обновления групповой политики. Иногда проблемы с групповой политикой можно решить, выполнив команду `Gpupdate`.

В начале этого раздела упоминалась сетевая связь. Необходимо убедиться, что клиент может подключиться к контроллеру домена. Убедитесь, что TCP/IP, DNS и DHCP настроены и нормально работают, а сетевой кабель не отсоединен.

## Резюме

- Можно улучшить структуру групповой политики, ограничив количество объектов GPO и подразделений. Однако не злоупотребляйте блокированием наследования, принудительным применением, фильтрами безопасности и политиками замыкания на себя. Не связывайте GPO с подразделениями из разных сайтов. Можно отключать конфигурацию пользователя или компьютера, если та не содержит настроенных параметров политики.
- В Windows Server 2008 появилось несколько новых параметров групповой политики, в частности, параметры, относящиеся к роли сервера служб терминалов. В Windows Server 2008 R2 службы терминалов заменены службами удаленных рабочих столов, а соответствующие параметры групповой политики сохранились.
- Для решения проблем с групповой политикой доступны различные инструменты. Одной из наиболее полезных является возможность сохранять от-

четы GPO с помощью GPMC. Можно также создавать отчеты о результатах групповой политики и моделировании групповой политики.

## Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных на занятии 2. Эти вопросы предоставлены также в электронном виде на прилагаемом к книге компакт-диске.

---

### ПРИМЕЧАНИЕ Ответы

Ответы на вопросы и пояснения к их вариантам размещены в разделе «Ответы» в конце книги.

---

1. Какие параметры групповой политики требуют установки компонента **Возможности рабочего стола** (Desktop Experience) на сервер под управлением Windows Server 2008 или 2008 R2? (Каждый вариант является законченным решением. Выберите два.)
  - a. **Диагностика диска: Настроить уровень выполнения** (Disk Diagnostic: Configure Execution Level).
  - b. **Не разрешать перенаправление буфера обмена** (Do Not Allow Clipboard Redirection).
  - c. **Принудительная отмена фоновой рисунка удаленного рабочего стола** (Enforce Removal Of Remote Desktop Wallpaper).
  - d. **Set The Map Update Interval For NIS Subordinate Servers** (Установить интервал обновления карт для подчиненных серверов NIS).
  - e. **Диагностика диска: Настроить пользовательский текст предупреждения** (Disk Diagnostic: Configure Custom Alert Text).
2. Какие параметры групповой политики относятся к службам терминалов в Windows Server 2008 и службам удаленных рабочих столов в Windows Server 2008 R2? (Каждый вариант является законченным ответом. Выберите три.)
  - a. **Разрешить перенаправление часового пояса** (Allow Time Zone Redirection).
  - b. **Диагностика диска: Настроить уровень выполнения** (Disk Diagnostic: Configure Execution Level).
  - c. **Не разрешать перенаправление буфера обмена** (Do Not Allow Clipboard Redirection).
  - d. **Принудительная отмена фоновой рисунка удаленного рабочего стола** (Enforce Removal Of Remote Desktop Wallpaper).
  - e. **Turn On Extensive Logging For Active Directory Domain Services Domain Controllers That Are Running Server For NIS** (Включить расширенные функции журнала для контроллеров домена Active Directory, выполняющих функцию сервера для NIS).
3. Вы планируете стратегию групповой политики. Каким из приведенных ниже советов вы последуете? (Каждый вариант является полным ответом. Выберите три.)

- a. Сведите к минимуму количество GPO за счет включения множества параметров конфигурации в каждый отдельный GPO и связывания GPO с подразделениями из разных сайтов.
  - b. Храните ADMX-файлы в центральном хранилище.
  - c. Назначайте подразделениям и объектам GPO содержательные имена.
  - d. Активно используйте такие функции, как блокирование наследования политики, принудительное выполнение, фильтры безопасности и политики замыкания на себя.
  - e. Убедитесь, что политика обновления и изменения GPO предписывает использовать команду Gpupdate после внесения изменений.
4. Какая утилита проверяет последовательность GPO в каждом контроллере домена, определяет действительность политики и отображает подробную информацию о реплицированных GPO?
- a. GPRresult.exe.
  - b. GPOTool.exe.
  - c. Функция создания отчетов GPMC.
  - d. Gpupdate.exe.
5. Вы хотите создать отчет RSoP для пользователя, выполнившего вход на локальный контроллер домена. Вы открыли GPMC. Что вы сделаете?
- a. Раскройте контейнер **Лес** (Forest). Щелкните правой кнопкой мыши контейнер **Результаты групповой политики** (Group Policy Results) и выберите команду **Мастер результатов групповой политики** (Group Policy Results Wizard). В окне мастера используйте параметры по умолчанию.
  - b. Раскройте контейнер **Лес** (Forest). Щелкните правой кнопкой мыши контейнер **Моделирование групповой политики** (Group Policy Modeling) и выберите команду **Мастер моделирования групповой политики** (Group Policy Modeling Wizard). В окне мастера используйте параметры по умолчанию.
  - c. Раскройте контейнеры **Лес** (Forest) и **Домены** (Domains). Щелкните правой кнопкой мыши контейнер с именем домена и выберите команду **Мастер моделирования групповой политики** (Group Policy Modeling Wizard). В окне мастера используйте параметры по умолчанию.
  - d. Раскройте контейнеры **Лес** (Forest) и **Домены** (Domains). Щелкните правой кнопкой мыши контейнер с именем домена, а затем щелкните правой кнопкой мыши GPO **Политика домена по умолчанию** (Default Domain Policy). Щелкните **Сохранить отчет** (Save Report). Щелкните **Сохранить** (Save), чтобы сохранить отчет в библиотеке документов.

## Практикум. Установка консоли GPMC и создание центрального хранилища для файлов групповой политики

На этом практикуме вы установите консоль GPMC, если она не была установлена в процессе установки AD DS. Также вы создадите и заполните центральное хранилище для файлов определений групповой политики (ADMX).

### Упражнение 1. Установка консоли GPMC

В данном упражнении вы проверите, установлена ли консоль GPMC на VAN-DC1. Это зависит от того, как настроен компьютер (если VAN-DC1 настроен, как описано в Приложении А, то консоль уже установлена). Если консоль не установлена, необходимо установить ее.

1. Зайдите на VAN-DC1 под учетной записью Kim Akers.
2. Просмотрите раздел **Администрирование** (Administrative Tools). Если консоль **Управление групповой политикой** (Group Policy Management) уже существует, как показано на рис. 4-16, это упражнение выполнять не требуется, и можно переходить к упражнению 2. В противном случае перейдите к шагу 3.

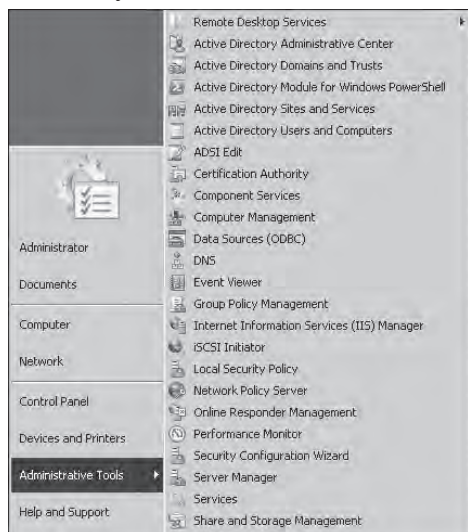


Рис. 4-16. Консоль GPMC, установленная на VAN-DC1

3. При необходимости откройте Диспетчер сервера (Server Manager) из меню **Администрирование** (Administrative Tools).
4. В дереве консоли щелкните **Компоненты** (Features).
5. На панели **Компоненты** (Features) щелкните **Добавить компоненты** (Add Features).
6. В окне мастера добавления компонентов в списке компонентов установите флажок **Управление групповой политикой** (Group Policy Management).

7. Щелкните **Далее** (Next).
8. Щелкните **Установить** (Install).

## Упражнение 2. Создание центрального хранилища для ADMX-файлов

В этом упражнении вы создадите папку, которая послужит центральным хранилищем для независимых от языка ADMX-файлов, и подпапку для языковых ADMX-файлов. Затем вы скопируете в эти папки файлы с клиентской рабочей станции VAN-CL1.

1. Если требуется, зайдите на VAN-DC1 под учетной записью Kim Akers.
2. Откройте Проводник и перейдите в папку C:\Windows\SYSVOL\domain\policies. Создайте подпапку с именем **PolicyDefinitions**.
3. В папке **PolicyDefinitions** создайте подпапку **en-us**. Структура папок показана на рис. 4-17.

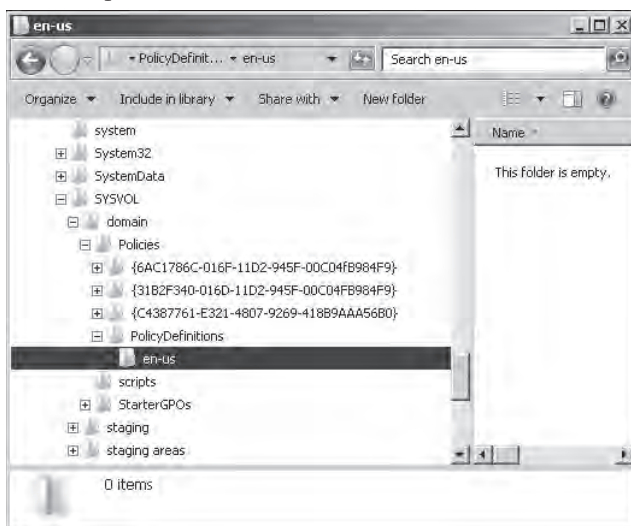


Рис. 4-17. Структура папок центрального хранилища

4. Сделайте папку **PolicyDefinitions** общей и предоставьте пользователю Kim Akers полный доступ (Full Control) (см. рис. 4-18). Обратите внимание: для выполнения этого упражнения допустимо предоставить разрешения отдельному пользователю, но обычно разрешения предоставляются группам безопасности.
5. Зайдите на клиентскую рабочую станцию VAN-CL1 под учетной записью Kim Akers или подключитесь к ней через удаленный рабочий стол. Не выходите из системы на VAN-DC1.
6. Найдите на клиенте VAN-CL1 все файлы.admx. Скопируйте их в общую папку **PolicyDefinitions** на VAN-DC1. На рис. 4-19 показано центральное хранилище с ADMX-файлами.

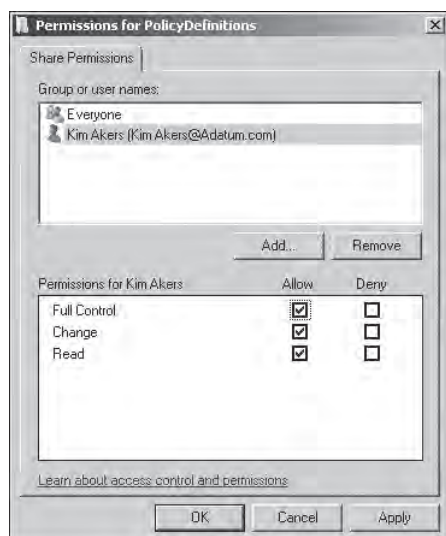


Рис. 4-18. Настройка разрешений для общей папки PolicyDefinitions

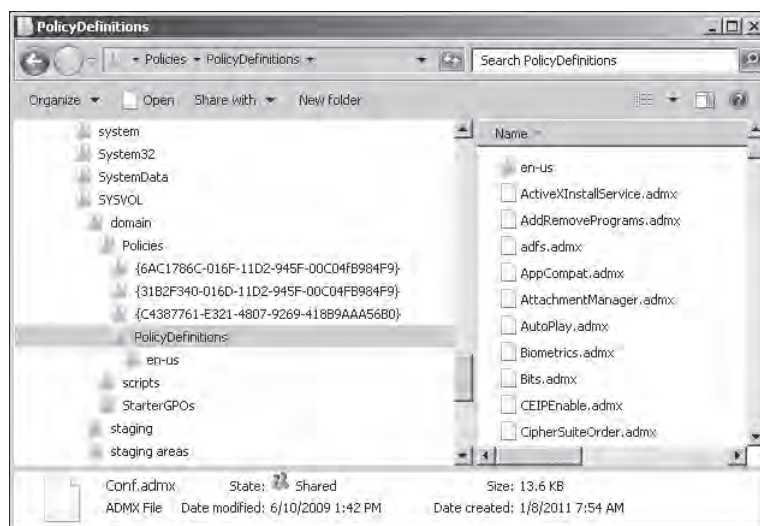


Рис. 4-19. ADMX-файлы в центральном хранилище

7. Найдите на клиенте VAN-CL1 все файлы .adml. Скопируйте их в общую папку **PolicyDefinitions/en-us** на VAN-DC1.
8. На VAN-DC1 откройте любой ADMX-файл (.admх или .adml) с помощью Блокнота и просмотрите содержимое. На рис. 4-20 показан ADMX-файл, открытый в Блокноте.

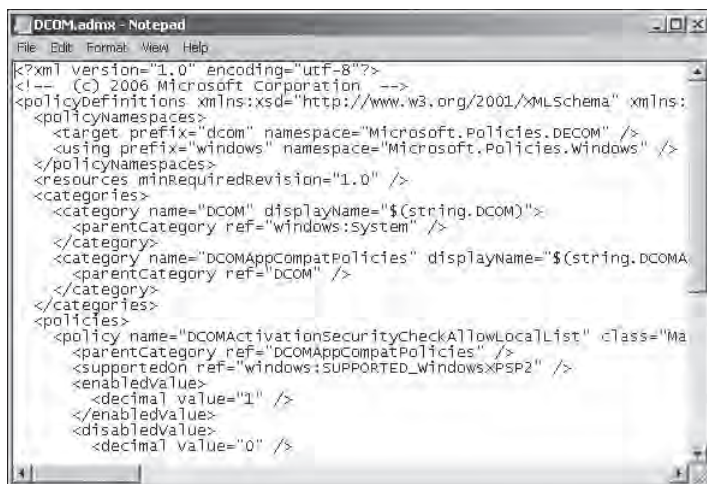


Рис. 4-20. Содержимое ADMX-файла

## Практикум. Создание и настройка GPO и создание отчета

На этом практикуме вы создадите и настроите объект GPO, связанный с одним из подразделений в домене adatum.com. Затем вы создадите отчет при помощи функции создания отчетов GPMC и проверите все параметры политики, действующие для пользователя Kim Akers, при помощи утилиты GPRresult.exe.

### Упражнение 1. Создание и настройка GPO

В этом упражнении вы создадите и настроите объект GPO. Для выполнения этого упражнения требуется установить GPMC.

1. Если требуется, зайдите на VAN-DC1 под учетной записью Kim Akers.
2. В меню **Администрирование** (Administrative Tools) выберите **Управление групповой политикой** (Group Policy Management), чтобы открыть консоль GPMC.
3. В окне GPMC разверните дерево консоли, щелкните правой кнопкой мыши любое подразделение (например, Marketing) и выберите команду **Создать объект GPO в этом домене и связать его** (Create A GPO In This Domain, And Link It Here).
4. Дайте новому GPO имя **SampleGPO**. Можно указать исходный начальный GPO, если такой имеется (см. рис. 4-21). Щелкните **ОК**.
5. Щелкните правой кнопкой мыши SampleGPO в дереве консоли и выберите команду **Изменить** (Edit).
6. В редакторе управления групповой политикой раскройте узлы **Конфигурация пользователя**, **Политики**, **Конфигурация Windows** и **Настройка Internet Explorer** (User Configuration, Policies, Windows Settings и Internet Explorer Maintenance).



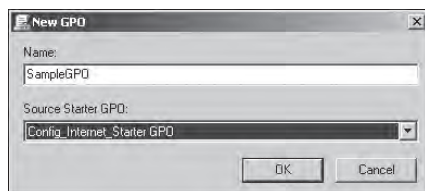


Рис. 4-21. Указание имени и исходного начального GPO

7. На панели консоли щелкните **Пользовательский интерфейс обозревателя** (Browser User Interface). На панели сведений дважды щелкните **Заголовок обозревателя** (Browser Title).
8. Настройте заголовок, отображаемый браузером, как показано на рис. 4-22.

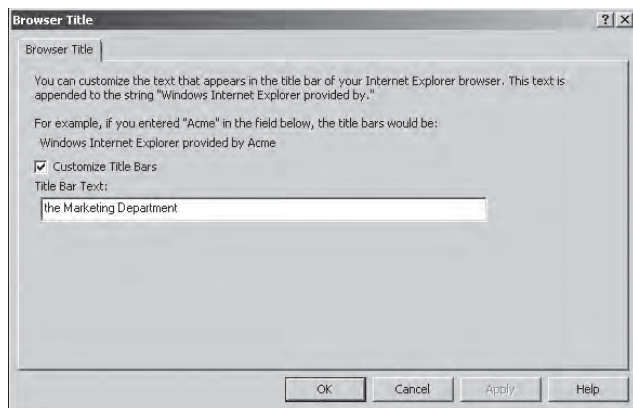


Рис. 4-22. Указание заголовка браузера

9. Щелкните **ОК**. Закройте редактор управления групповой политикой.

## Упражнение 2. Создание отчета GPO

В этом упражнении вы создадите и проверите отчет для объекта GPO, созданного в упражнении 1.

1. Если требуется, зайдите на VAN-DC1 под учетной записью Kim Akers и откройте GPMC.
2. В GPMC разверните дерево консоли и щелкните правой кнопкой мыши объект SampleGPO. Выберите команду **Сохранить отчет** (Save Report).
3. Щелкните **Сохранить** (Save), чтобы сохранить отчет в Библиотеке документов на VAN-DC1 (рис. 4-23). Обратите внимание: на контроллере домена в рабочей сети, скорее всего, потребуется создать отдельную папку для хранения таких отчетов.
4. На VAN-DC1 перейдите в Библиотеку документов. Дважды щелкните SampleGPO. Файл откроется в Internet Explorer.
5. Изучите отчет SampleGPO. В частности, обратите внимание на изменения, внесенные вами в конфигурацию пользователя и (если вносили) в исходный начальный GPO. На рис. 4-24 показан типичный отчет о конфигурации пользователя.

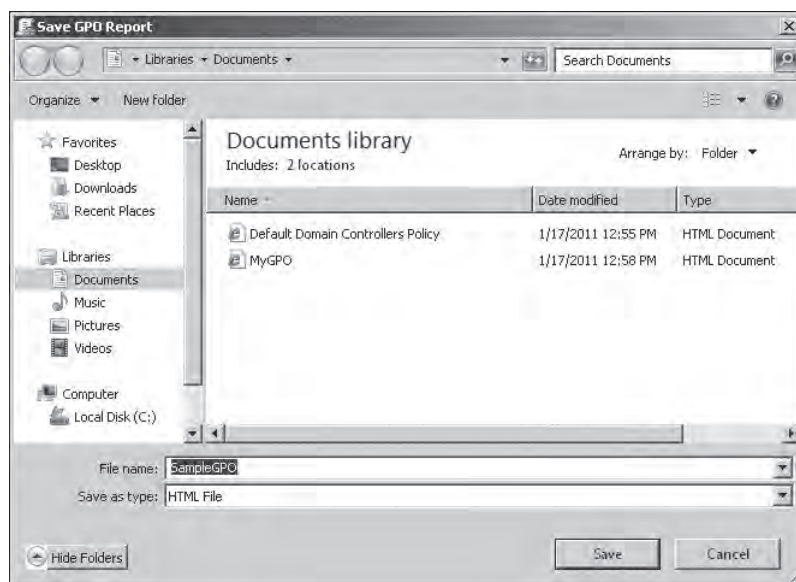


Рис. 4-23. Сохранение отчета групповой политики SampleGPO в виде HTML-файла

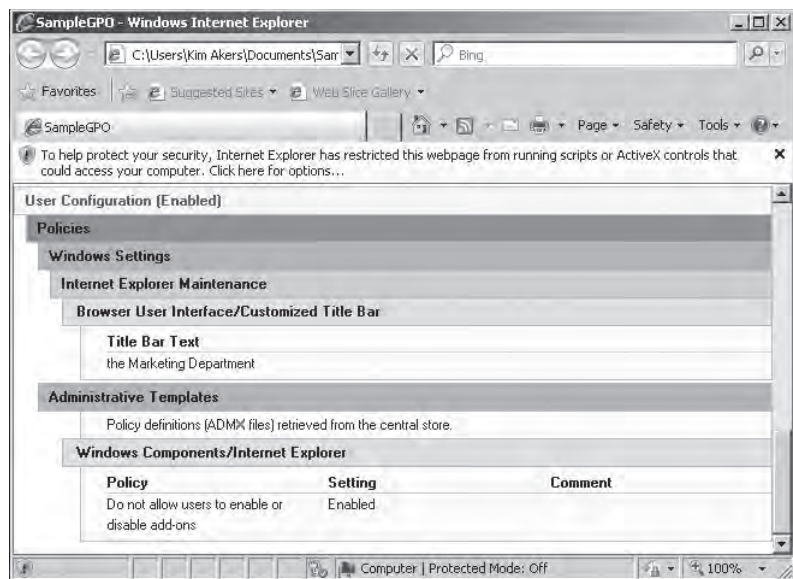


Рис. 4-24. Проверка изменений в конфигурации пользователя

### Упражнение 3. Проверка параметров политики

В этом упражнении вы воспользуетесь утилитой GPRresult.exe для проверки всех параметров политики, применяемых к пользователю Kim Akers, вошедшему в систему.

1. Если требуется, зайдите на VAN-DC1 под учетной записью Kim Akers.

2. Откройте командную строку из меню **Все программы | Стандартные** (All Programs | Accessories).
3. Введите команду `gpresult /R`.
4. Просмотрите выходные данные этой команды, выполненной для пользователя Kim Akers. На рис. 4-25 показана часть этих данных.

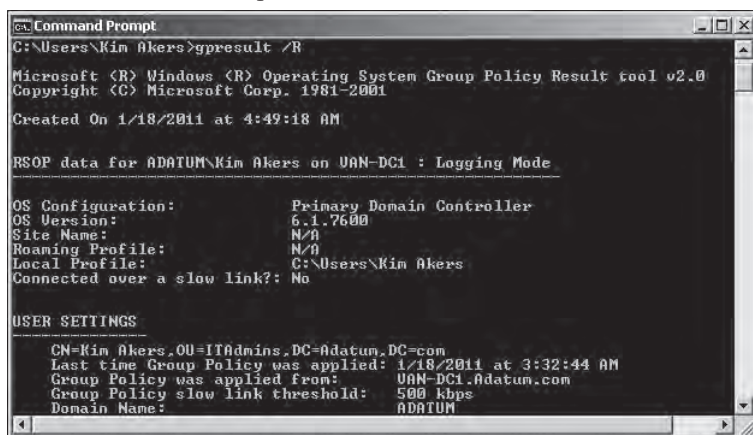


Рис. 4-25. Параметры политики для Kim Akers

## Закрепление материала главы

Чтобы попрактиковаться и закрепить знания, полученные при изучении этой главы, выполните следующее:

- прочитайте резюме главы;
- просмотрите список основных терминов, представленных в этой главе;
- выполните задания лабораторной работы, моделирующей реальные ситуации, требующие применения полученных знаний;
- выполните рекомендуемые упражнения;
- пройдите пробный тест.

## Резюме главы

- Начальные GPO и системные начальные GPO содержат параметры политики административных шаблонов для конфигураций пользователя и компьютера. На основе начальных GPO можно создавать объекты GPO с уже настроенными параметрами.
- Файлы определений групповой политики могут храниться в центральном хранилище AS DS, реплицируемом между контроллерами домена. При необходимости можно создавать собственные файлы.
- Параметры политики, появившиеся в Windows Server 2008 и сохраненные в Windows Server 2008 R2, обеспечивают дополнительную функциональность групповой политики. Доступны инструменты для решения проблем с политиками.

## Основные термины

Проверьте, знаете ли вы, что означают перечисленные ниже термины из этой главы:

- параметры административного шаблона;
- отчеты GPMC;
- параметры групповой политики;
- результирующий набор политик (RSOP);
- начальный объект групповой политики;
- системный начальный объект групповой политики.

## Лабораторная работа

Для выполнения заданий лабораторной работы используйте знания о планировании объектов GPO и стратегии GPO, полученные из этой главы. Ответы можно найти в разделе «Ответы» в конце книги.

### Задание 1. Использование начальных GPO

Дон Холл хочет создать несколько объектов GPO, имеющих одинаковые параметры административных шаблонов в конфигурации пользователя, но разные параметры конфигурации Windows в конфигурации пользователя. Эти GPO не содержат настроенных политик в конфигурации компьютера. Вы советуете Дону создать начальный GPO с определенными параметрами административных шаблонов в конфигурации пользователя и использовать этот объект для создания других GPO. В этом случае потребуется настроить только параметры конфигурации Windows в конфигурации пользователя. Дон задает вам следующие вопросы:

1. Следует ли отключить конфигурацию компьютера в создаваемых GPO, и какие преимущества это даст?
2. Дон попытался создать резервную копию начального GPO, щелкнув правой кнопкой мыши контейнер **Объекты групповой политики** (Group Policy Objects) и выбрав команду **Архивировать все** (Back Up All), но не нашел этот GPO в списке резервных копий GPO. Как создать резервную копию?

### Задание 2. Планирование и документирование процедур по решению проблем

Вы проработали несколько лет в службе поддержки компании Litware. Одной из ваших задач было решение проблем, связанных с групповой политикой. Недавно вы получили повышение в должности, и одна из ваших новых обязанностей — создание документа «Процедуры и планирование», помогающего менее опытным администраторам эффективно выполнять задачи по решению проблем. Ответьте на следующие вопросы:

1. Что делать, когда пользователь сообщает, что не может получить доступ к функциям, к которым есть доступ у его коллег?

2. Что делать, если изменения в параметрах политики не применяются к конкретному клиенту, но работают на аналогичных компьютерах?
3. Администраторы компании Litware обычно используют функцию **Сохранить отчет** (Save Report) консоли GPMC для создания отчетов GPO. На какие вопросы они должны искать ответы, изучая эти отчеты?

## Рекомендуемые упражнения

Чтобы успешно справиться с экзаменационными заданиями по темам этой главы, выполните следующие упражнения.

### Используйте консоль GPMC и редактор управления групповой политикой

- Обычно администратору требуется настраивать лишь небольшое число параметров политики. Главному администратору, отвечающему за планирование, а не за внедрение, нужны более обширные знания доступных параметров. Изучите консоль GPMC и, особенно, редактор управления групповой политикой (Group Policy Management Editor). Просмотрите списки параметров политики. Читайте описания, чтобы узнать, для чего предназначен каждый параметр.

### Изучайте ADMX-файлы

- Умение понимать и создавать код незаменимо, если вы намереваетесь стать специалистом. Администраторы не являются разработчиками ПО, однако и им полезно уметь создавать простые XML-файлы. Установите образцы ADMX-файлов, предоставляемых Microsoft, и изучите их (ссылка приводилась на занятии 1).

### Изучайте отчеты GPO

- Используйте функцию **Сохранить отчет** (Save Report) в GPMC для создания и сохранения отчетов GPO. Изучайте эти отчеты, пока не начнете свободно разбираться в их структуре и понимать, какую информацию они предоставляют. Также создавайте и изучайте отчеты RSoP (см. занятие 2).

### Изучите программы из списка RemoteApp

- Программы из списка удаленных приложений RemoteApp работают на хосте служб удаленных рабочих столов или на сервере терминалов, а доступ к ним осуществляется через удаленный рабочий стол. Эти программы выглядят так, будто работают на локальном клиенте. Узнайте подробнее об этих программах и диспетчере удаленных приложений RemoteApp, а затем используйте клиент под управлением Windows 7, чтобы проверить эту функцию на практике. Обратите внимание: для выполнения данного упражнения на VANDC1 должна быть установлена роль сервера RDS.

## Пробный экзамен

Тренировочные тесты на прилагаемом к книге компакт-диске позволяют проверить знания только по одной или сразу по всем темам сертификационного экзамена 70-646. Тестирование можно организовать так, чтобы оно проводилось как настоящий экзамен, а можно проходить в режиме обучения, просматривая правильные ответы и объяснения после каждого ответа.

---

### **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Пробный экзамен**

Подробнее о пробном экзамене рассказано во Введении.

---

## Планирование администрирования серверов

|                                                   |            |
|---------------------------------------------------|------------|
| <b>Занятие 1. Технологии управления серверами</b> | <b>215</b> |
| <b>Занятие 2. Делегирование полномочий</b>        | <b>236</b> |

Планирование управления серверами не менее важно, чем планирование их развертывания. Если системный администратор не уделит достаточно внимания выбору метода управления серверами, его работа существенно затруднится. Цените свое рабочее время. В крупной организации у вас не будет достаточно времени, чтобы решать каждую мелкую проблему. Подумайте о том, чтобы передать решение менее важных административных задач доверенным пользователям и сосредоточиться на более сложных вопросах. Из этой главы вы узнаете, как правильно выбрать метод удаленного администрирования, и как передавать простые административные задачи подчиненным, чтобы уделять больше времени сложным задачам.

### Темы экзамена

- Планирование стратегий управления серверами.
- Планирование делегированного администрирования.

### Прежде всего

Для выполнения упражнений этой главы потребуется:

- Выполнить задания по установке сервера, приведенные в Приложении. Дополнительной настройки не требуется.

#### Реальный мир

*Орин Томас*

Когда-то я бил рекорды по длительности удаленных сеансов. Два года я использовал удаленный рабочий стол для выполнения задач по управлению сервером из Миннеаполиса, штат Миннесота, тогда как сам жил в Мельбурне, в Австралии. Длительная получилась бы поездка, если бы мне потребовалось вручную сменить ленту для резервного копирования!



Сегодня, в эпоху оффшоров и аутсорсинга, такой способ работы уже не так необычен. Технологии дистанционного управления для системных администраторов — одновременно и благо, и проклятие: благо, потому что серверами можно управлять из любой точки мира, и проклятие, потому что от вас ожидают, что вы сможете управлять серверами из любой точки мира. Если у вас есть ноутбук со встроенным сотовым модемом, то не исключено, что вы можете сидеть где-нибудь в баре и восстанавливать данные на сервере, находящемся на другом континенте.

## Занятие 1. Технологии управления серверами

На этом занятии рассказывается о способах удаленного администрирования, доступных в Windows Server 2008 и 2008 R2. Освоив эти способы, вы сможете учитывать их при планировании управления и мониторинга серверов на уровне организации. Главное — понимать разницу в функциональности разных технологий при локальном использовании и при управлении серверами, расположенными в другом городе или даже на другом континенте.

---

### Изучив материал этого занятия, вы сможете:

- ✓ Планировать локальное и удаленное администрирование Windows Server 2008.
- ✓ Определять способы управления серверами, подходящие для определенных ситуаций.

**Продолжительность занятия — примерно 60 мин.**

---

## Инструменты для администрирования Windows Server 2008 и 2008 R2

Во многих случаях выбор инструментов для управления серверами корпоративной сети зависит скорее от личного предпочтения, чем от технической необходимости. Возможностей много, и у системного администратора часто просят совета о том, как лучше всего управлять серверами в тех или иных обстоятельствах. На этом занятии рассматриваются различные технологии управления Windows Server 2008 и 2008 R2 и ситуации, в которых эти технологии наиболее эффективны.

### Диспетчер сервера

Консоль **Диспетчер сервера** (Server Manager) —расширенная консоль управления (MMC), позволяющая управлять всеми аспектами Windows Server 2008 и 2008 R2 (рис. 5-1). Диспетчер сервера содержит наиболее часто используемые инструменты, необходимые администратору. При добавлении и удалении ролей и функций в диспетчере сервера добавляются и удаляются соответствующие компоненты. В режиме Server Core Диспетчер сервера отсутствует.

## ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Диспетчер сервера

Подробнее о Диспетчере сервера см. по адресу [http://technet.microsoft.com/ru-ru/library/cc732131\(W.S.10\).aspx](http://technet.microsoft.com/ru-ru/library/cc732131(W.S.10).aspx).

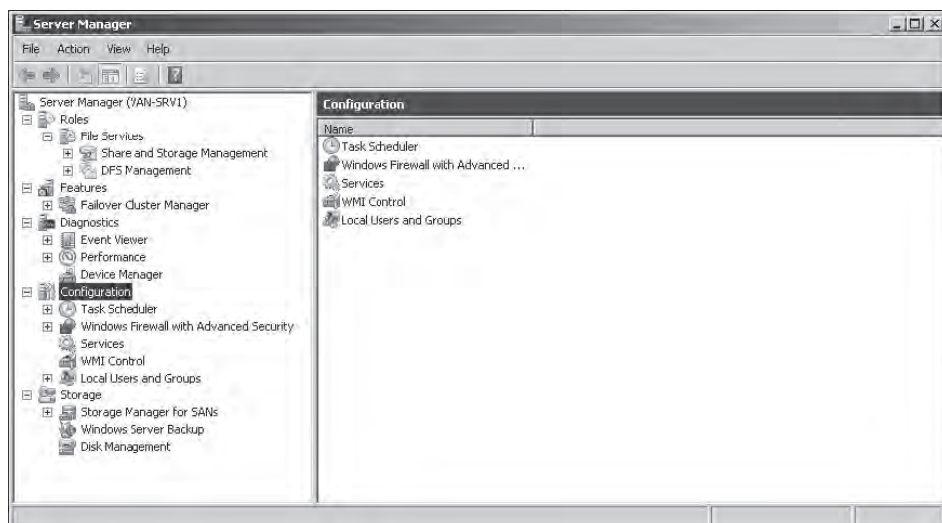


Рис. 5-1. Диспетчер сервера

Servermanagercmd.exe — утилита, для добавления и удаления ролей и функций сервера. Ее можно запускать из командной строки с повышенными привилегиями в полной установке Windows Server 2008 и в режиме Server Core. Команда servermanagercmd.exe -query отображает список всех ролей, служб ролей и компонентов, доступных для компьютера под управлением Windows Server 2008, и показывает, установлены они или нет. Чаще всего при помощи этой утилиты администраторы устанавливают роли и функции в режиме Server Core, а затем используют инструменты вроде RSAT для удаленного управления этими ролями и функциями. В режиме Server Core для тех же целей можно использовать утилиты Oclist.exe и Ocsetup.exe. Хотя утилита Servermanagercmd.exe доступна в Windows Server 2008 и 2008 R2, вместо нее рекомендуется использовать командлет PowerShell Add-WindowsFeature. Этот командлет доступен в составе модуля ServerManager в PowerShell. Подробнее о PowerShell рассказывается далее на этом занятии.

## ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ ServerManagerCmd.exe

Подробнее о ServerManagerCmd.exe см. по адресу [http://technet.microsoft.com/ru-ru/library/cc748918\(W.S.10\).aspx](http://technet.microsoft.com/ru-ru/library/cc748918(W.S.10).aspx).

## Консоли MMC

В меню **Администрирование** (Administrative Tools) доступен стандартный набор консолей MMC, но оснастки, с помощью которых можно создавать собственные консоли, предоставляют больше функциональности и возможностей по настройке. Пользовательские консоли позволяют быстрее получать доступ к часто используемым инструментам. Консоли можно копировать на другие компьюте-

ры, в частности, на административную рабочую станцию, что позволяет всегда иметь одинаковый набор инструментов, независимо от того, с каким компьютером вы работаете. В некоторых оснастках можно указывать учетные данные для работы с удаленными компьютерами. Создать пользовательскую консоль просто:

1. В меню **Пуск** в строке **Выполнить** (Run) введите **mmc**. Откроется пустая консоль MMC.
2. В меню **Файл** (File) выберите **Добавить или удалить оснастку** (Add/Remove Snap-in). Откроется диалоговое окно **Добавление и удаление оснасток** (Add Or Remove Snap-ins) (рис. 5-2). Добавьте оснастки, которые хотите использовать в консоли, и щелкните **ОК**.

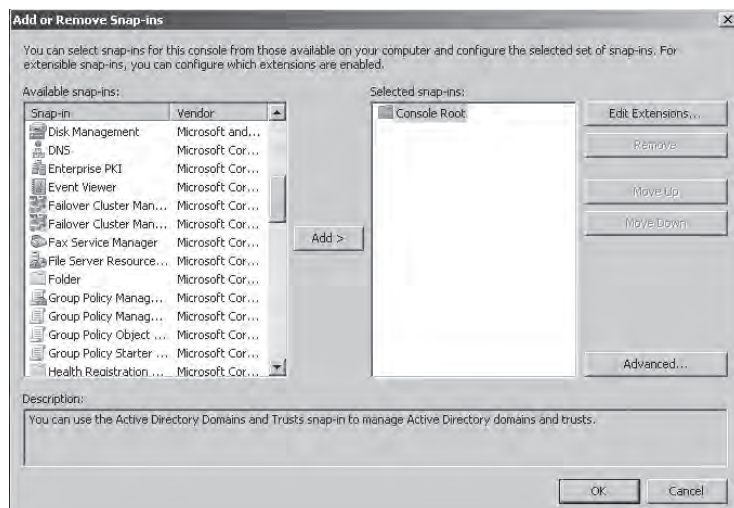


Рис. 5-2. Добавление оснасток

3. Если будет предложено выбрать компьютер, которым должна управлять оснастка, выберите его и щелкните **ОК**.
4. Сохраните консоль при помощи меню **Файл** (File).
5. Для всех ролей и функций, установленных на сервере, имеются свои оснастки. Оснастки для не установленных служб и функций недоступны, если не установлены соответствующие функции RSAT (см. далее).

## PowerShell

PowerShell — язык оболочки командной строки и сценариев, разработанный специально для системного администрирования. Администраторам, не привыкшим выполнять задачи с помощью командной строки, этот язык может показаться сложным, но после нескольких часов работы с PowerShell вам вряд ли захочется возвращаться к утилитам с графическим интерфейсом.

В состав Windows Server 2008 R2 входит оболочка PowerShell 2.0, включенная по умолчанию. PowerShell 2.0 можно добавить в Windows Server 2008, скачав установочный файл с сайта Microsoft. Можно автоматически добавить модули в PowerShell, щелкнув правой кнопкой значок PowerShell на панели задач и выбрав команду **Импорт системных модулей** (Import System Modules).

После этого станут активными модули, связанные с компонентами и ролями, установленными на сервере. Если установить все инструменты RSAT, будут доступны следующие системные модули:

- ActiveDirectory;
- AD RMS;
- ADRMSAdmin;
- AppLocker;
- BestPractices;
- BitsTransfer;
- FailoverClusters;
- NetworkLoadBalancingClusters;
- PSDiagnostics;
- ServerManager;
- TroubleshootingPack;
- WebAdministration.

Можно также добавлять эти модули по отдельности. Например, для загрузки модуля ServerManager выполните следующую команду:

```
Import-Module ServerManager
```

Что касается планирования стратегий управления серверами, можно использовать сценарии PowerShell для автоматизации почти всех сложных задач администрирования. Сценарии PowerShell можно вызывать из планировщика заданий (Task Scheduler), что позволяет автоматизировать выполнение многих повседневных задач. Поскольку PowerShell является также языком сценариев, можно встраивать в сценарии логику условий, чтобы задачи выполнялись в зависимости от условий, существующих на момент запуска сценария. Сценарии PowerShell лучше всего подходят для выполнения запланированных задач, когда точно известно, что необходимо сделать. Если задачи требуют принятия множества оперативных решений, сценарии PowerShell менее эффективны.

PowerShell 2.0 предоставляет широкие возможности для удаленного администрирования. Подробнее о настройке Windows Server 2008 R2 для поддержки удаленных функций PowerShell рассказывается далее на этом занятии.

---

### **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ PowerShell и Windows Server 2008/2008 R2**

PowerShell — это сложная тема, которую нельзя раскрыть на нескольких страницах. Издательство Microsoft Press выпустило несколько хороших книг, посвященных эффективному использованию PowerShell. Для начала обратитесь к странице PowerShell на сайте Microsoft: <http://technet.microsoft.com/ru-ru/library/bb978526.aspx>.

---

### **Сценарии и инструменты командной строки**

Для всех ролей и компонентов сервера, которые можно установить в Windows Server 2008 и 2008 R2, существуют сценарии и утилиты командной строки. Утилиты командной строки не так просты в использовании, как инструменты с графическим интерфейсом, но после некоторой практики с их помощью можно выполнять все те же задачи. Преимущество утилит командной строки в том,

что их можно использовать в сценариях. Если создать сценарий для автоматизации сложной задачи, работающий на одном сервере, можно скопировать его и использовать на других серверах.

На смену традиционным сценариям на основе Windows Scripting Host пришла оболочка PowerShell. Это не значит, что нельзя использовать существующие сценарии в Windows Server 2008 и 2008 R2, однако Microsoft рекомендует использовать оболочку PowerShell, которая, в отличие от Windows Scripting Host, разработана специально для выполнения сценариев и утилит командной строки. В некоторых случаях, особенно в сценариях управления компьютерами, работающими в режиме Server Core, нет иного выбора, кроме использования традиционных сценариев, поскольку Server Core в Windows Server 2008 не полностью поддерживает PowerShell. В Windows Server 2008 R2 поддержка PowerShell реализована гораздо лучше.

### Службы аварийного управления (EMS)

Службы аварийного управления (Emergency Management Services, EMS) позволяют управлять сервером, находящимся в режиме минимального функционирования, например, когда не работают сетевая карта и графический адаптер. Службы EMS позволяют установить внешнее подключение, обычно через последовательный или USB-порт, используя Telnet или другой эмулятор терминала. Имея подходящее оборудование, при помощи EMS можно выполнять многие задачи по управлению сервером из командной строки.

Преимущество служб EMS в том, что они работают, когда недоступны другие методы администрирования. EMS можно использовать, когда компьютер находится в процессе загрузки или завершения работы. Например, можно получить доступ к серверу, зависшему при завершении работы, или даже когда произошла STOP-ошибка. Кроме этого, EMS можно использовать, когда сервер не реагирует на традиционные методы ввода из-за неконтролируемого процесса. Приведем пример: за время работы системным администратором вы могли встречать серверы, кажущиеся зависшими и не позволяющие выполнить вход в систему. В таких ситуациях можно управлять сервером при помощи EMS и даже завершить сбойный процесс. Это не всегда возможно, т.к. иногда зависший сервер можно только выключить вручную, однако службы EMS дают последнюю возможность вернуть сервер к работе, прежде чем прибегнуть к этому.

Службы EMS должны быть включены на сервере. Способ включения зависит от аппаратной конфигурации компьютера. Например, на компьютере с прошивкой EFI (Extensible Firmware Interface) службы EMS включаются и настраиваются не так, как на компьютере с интерфейсом ACPI и перенаправлением последовательного порта. Включение EMS требует использования команды `bcdedit` для редактирования параметров загрузки Windows Server 2008 и 2008 R2, однако точный синтаксис зависит от аппаратной конфигурации сервера. С точки зрения планирования, EMS следует включать на серверах перед развертыванием — тогда эти службы будут доступны, если понадобятся.

---

#### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Включение EMS

О включении EMS на компьютере под управлением Windows Server 2008 или 2008 R2 см. по адресу [http://technet.microsoft.com/ru-ru/library/cc731245\(WS.10\).aspx](http://technet.microsoft.com/ru-ru/library/cc731245(WS.10).aspx).

---

Хотя с помощью EMS можно выполнять почти все задачи по управлению сервером через интерфейс командной строки, большинство организаций использует EMS для управления серверами, не реагирующими на обычные методы управления. В состав EMS входит специальная консоль администрирования (SAC), доступная только при нормальном функционировании Windows. Консоль !SAC, предоставляющая доступ к ограниченному набору команд SAC, доступна, когда операционная система не работает нормально, а консоль SAC не загружается и перестает работать. Чтобы получить список команд, которые можно использовать в EMS при текущем уровне функциональности, введите help или ? в строке SAC или !SAC.

## Технологии удаленного администрирования

При выборе технологии удаленного администрирования для управления серверами вы не ограничены одним вариантом. Каждая технология имеет свои преимущества и недостатки. В некоторых случаях имеет смысл использовать подключение к удаленному рабочему столу, в других лучше подключаться к серверу с помощью приложения Telnet. Далее мы рассмотрим удаленное администрирование с помощью удаленного рабочего стола, RSAT, PowerShell и Telnet.

### Удаленный рабочий стол

Пожалуй, удаленный рабочий стол является самой распространенной технологией удаленного администрирования, используемой в среде Windows Server 2008, так как он наиболее точно имитирует ощущение работы на локальном компьютере. Для подключения к серверам используется клиент удаленного рабочего стола, входящий в состав Windows.

После включения удаленного рабочего стола члены локальных групп **Администраторы (Administrators)** и **Пользователи удаленного рабочего стола (Remote Desktop Users)** могут подключаться автоматически. Важно отметить, что на контроллерах доменов простая принадлежность к членам группы пользователей удаленного рабочего стола не дает права выполнять вход с помощью удаленного рабочего стола. Это можно исправить, изменив политику **Разрешить вход в систему через службу удаленных рабочих столов (Log On Through Remote Desktop)**, расположенную в узле **Конфигурация компьютера | Политики | Конфигурация Windows | Параметры безопасности | Локальные политики | Назначение прав пользователя (Computer Configuration | Policies | Windows Settings | Security Settings | Local Policies | User Rights Assignment)** объекта групповой политики.

Удаленный рабочий стол позволяет удаленно подключаться к компьютеру под управлением Windows Server 2008 или 2008 R2 двум администраторам одновременно. Чтобы выполнить административное подключение, добавьте после адреса сервера переключатель /admin. Если два администратора уже подключились, можно принудительно отключить одного из них (рис. 5-3).

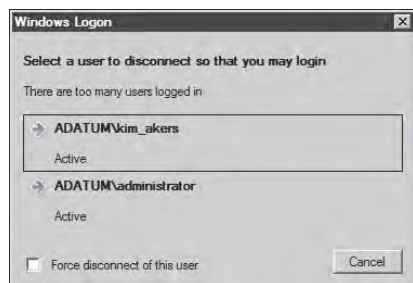


**Рис. 5-3.** Принудительное отключение

Как показано на рис. 5-4, при включении удаленного рабочего стола автоматически добавляется исключение брандмауэра для удаленного рабочего стола. Брандмауэр Windows автоматически разрешает трафик удаленного рабочего стола, но между клиентом и управляемым сервером могут существовать другие брандмауэры. Если столкнетесь с такой ситуацией, настройте брандмауэры на прием трафика по TCP-порту 3389.

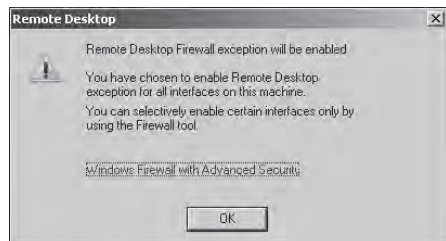


**Рис. 5-4.** Исключение брандмауэра для удаленного рабочего стола

В определенных ситуациях требуется выполнять административные задачи на серверах, расположенных в частных сетях организаций, к которым можно подключиться только через Интернет. Скорее всего, эти сети защищены брандмауэрами, и интернет-хосты не могут обращаться к ним напрямую. Например, невозможно выполнить прямое подключение к компьютеру под управлением Windows Server 2008 или 2008 R2, использующему IP-адрес 192.168.15.100 в удаленной корпоративной сети, если подключиться к этой сети можно только через Интернет.

Когда требуется выполнять повседневные административные задачи на серверах удаленных сетей, к которым нет прямого подключения, есть два варианта:

- Настроить VPN-сервер в удаленной защищенной подсети. После подключения рабочей станции к удаленной частной сети через VPN можно установить административное подключение к серверу, которым нужно управлять.
- Установить в удаленной защищенной подсети шлюз удаленного рабочего стола. Через этот шлюз можно подключаться по протоколу удаленного рабочего стола (RDP) к любому серверу из удаленной частной сети.

Хотя настройка VPN-сервера в удаленной защищенной подсети будет подходящим решением во многих случаях, установка VPN-сервера требует немало усилий. Если требуется выполнять RDP-подключения только к удаленным серверам, проще всего установить шлюз удаленного рабочего стола.



Шлюзы удаленного рабочего стола позволяют пользователям Интернета подключаться к серверам с удаленным рабочим столом в защищенной сети через сервер шлюза, расположенный за брандмауэром в защищенной подсети. Шлюз удаленного рабочего стола работает по протоколу RDP поверх HTTPS, что означает, что внешние брандмауэры должны открыть только порт 443, а не порт удаленного рабочего стола. Выполняется прямое подключение интернет-хоста через брандмауэр к серверу шлюза удаленного рабочего стола, и этот сервер пересылает авторизованный трафик серверам из защищенной частной сети. Хотя шлюз удаленного рабочего стола используется в основном для предоставления обычным пользователям доступа к приложениям удаленного рабочего стола при подключении из Интернета, его можно использовать и для удаленного управления серверами в защищенной сети.

---

### **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Шлюзы удаленного рабочего стола**

Подробнее о шлюзах удаленного рабочего стола см. по адресу [http://technet.microsoft.com/en-us/library/dd560672\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/dd560672(Ws.10).aspx) (на англ. языке).

---

### **Средства удаленного администрирования сервера (RSAT)**

По умолчанию в Windows Server 2008 и 2008 R2 доступны только инструменты управления для установленных служб и функций. Поэтому, если вы хотите управлять удаленным сервером со службами управления правами Active Directory (AD RMS), вы не сможете добавить эту оснастку или получить доступ к ней из меню **Администрирование**, если не установили инструменты RSAT или отдельный компонент AD RMS из инструментов RSAT. Если добавить средства RSAT на сервер, будут доступны все средства управления, даже если соответствующие роли и компоненты не установлены локально. Можно устанавливать только отдельные необходимые компоненты RSAT. Это выполняется при помощи функции добавления компонентов. Можно добавить все инструменты RSAT с помощью следующего командлета PowerShell, если установлен модуль ServerManager:

```
Add-WindowsFeature RSAT
```

Средства RSAT доступны как компоненты Windows Server 2008 и 2008 R2. Кроме того, их можно установить на компьютеры под управлением следующих операционных систем:

- Windows Vista SP1 Business, Enterprise или Ultimate;
- Windows 7 Professional, Enterprise или Ultimate.

Инструменты RSAT нельзя установить в Windows XP Professional или Windows Server 2003.

### **Удаленное взаимодействие с PowerShell**

Удаленное взаимодействие с PowerShell позволяет выполнять команды PowerShell на удаленных компьютерах. Удаленное взаимодействие поддерживается в Windows 7, Windows Vista SP 1 и выше, Windows Server 2008 и Windows Server 2008 R2. Необходимо включить удаленное взаимодействие с PowerShell на компьютере, который будет управляться удаленно. Для этого выполните следующее:

1. Начните сеанс PowerShell с повышенными привилегиями.
2. Настройте службу WinRM на автоматический запуск, а затем запустите ее, выполнив следующие команды:

```
Set-Service Winrm -startuptype automatic
```

```
Start-service winrm
```

3. Включите удаленное взаимодействие с PowerShell, выполнив следующую команду:

```
Enable-PSRemoting -force
```

Включив удаленное взаимодействие с PowerShell, можно использовать удаленные команды через командлет Invoke-Command с параметром -computername. Например, если установлен модуль ServerManager, следующая команда возвращает список всех функций, установленных на удаленном компьютере:

```
Invoke-Command -script {Import-Module ServerManager; Get-WindowsFeature}
-computername VAN-SRV1
```

На практических занятиях в конце главы вы настроите удаленное взаимодействие с PowerShell.

---

#### **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ    Удаленное взаимодействие с PowerShell**

Подробнее об удаленном взаимодействии с PowerShell см. по адресу <http://technet.microsoft.com/ru-ru/library/dd347744.aspx>.

---

### **Средства удаленного администрирования для неадминистративных пользователей**

На занятии 2 вы изучите методы делегирования административных привилегий неадминистративным пользователям. Чтобы пользователи могли выполнять делегированные им задачи, они должны получить доступ к соответствующим инструментам.

Один из способов обеспечить пользователей необходимыми инструментами — создать и распространить собственные MMC. Просто добавьте оснастку, имеющую отношение к делегированной задаче, в пользовательскую консоль, сохраните эту консоль и передайте пользователям. Хотя на неадминистративные рабочие станции можно установить средства RSAT, наличие 30 консолей, из которых нужна только одна, может ввести пользователя в замешательство.

Не следует предоставлять обычным пользователям доступ к серверу через удаленный рабочий стол, хотя это может показаться легким решением. В целом, при планировании удаленного администрирования следует ограничить число людей, имеющих прямой доступ к серверу. Пользователи, которым делегированы ограниченные административные полномочия, почти всегда могут выполнять свои задачи с помощью инструментов, установленных на их рабочие станции.

### **Использование Telnet для удаленного администрирования**

Последний метод удаленного администрирования Windows Server 2008 и 2008 R2 — подключение через Telnet. Telnet предоставляет текстовый интерфейс для подключения к командной консоли. Можно удаленно выполнять любые

текстовые команды, которые обычно вводятся в локальной командной строке. Преимущество Telnet в качестве технологии удаленного администрирования заключается в том, что через Telnet можно работать по очень медленным подключениям (даже со скоростью меньше 56 Кбит), не позволяющим использовать удаленный рабочий стол.

После установки компонента сервера Telnet можно настраивать параметры, выполнив команду `tlntadmn.exe` из командной строки с повышенными привилегиями. Можно настроить таймаут времени простоя сеанса, максимальное число поддерживаемых подключений Telnet, порт, через который работает Telnet, и максимальное число неудачных попыток входа. Механизм аутентификации по умолчанию для сервера Telnet — NTLM. Поскольку протокол Telnet не использует шифрование, подключения к серверу Telnet необходимо защищать с помощью IPSec и настраивать правила брандмауэра, требующие аутентификации для подключений Telnet.

После выхода PowerShell 2.0 и появления в Windows Server 2008 и 2008 R2 поддержки удаленного взаимодействия с PowerShell Telnet реже используется для удаленного администрирования.

### Проверьте себя

- Какой модуль PowerShell 2.0 необходимо добавить в сеанс PowerShell, чтобы использовать командлет `Add-WindowsFeature`?

### Ответ

- Модуль `ServerManager`.

## Управление журналами событий

Важный вопрос при планировании управления серверами — что делать с журналами событий? Цель ведения журнала событий — получить информацию о важных произошедших событиях, а для этого нужно не просто зарегистрировать в журнале соответствующее событие, но и суметь найти его. Здесь возникает две проблемы:

- Если записывать все, как убедиться, что не пропущено одно важное событие среди десятков тысяч записанных?
- Если ограничить объем записываемых данных, где гарантия, что не будет пропущено что-то очень важное?

Когда приходится управлять десятками или даже сотнями серверов, можно быстро утонуть в потоке информации. В следующем разделе вы узнаете, как использовать программу просмотра событий в Windows Server 2008 и 2008 R2, чтобы повысить управляемость данных журнала событий.

В Windows Server 2008 и 2008 R2 в окне программы **Просмотр событий** (Event Viewer) под узлом **Журналы Windows** (Windows Logs) по умолчанию отображаются следующие журналы:

- **Приложение (Application)** — хранит данные, сгенерированные приложениями, установленными на сервер, такими как клиент службы сертификатов, диспетчер рабочего стола, Блокнот и т. д. Работая с журналом приложений,

помните, что есть также узел под названием **Журналы приложений и служб** (Applications And Service Logs), тоже содержащий данные журналов ролей приложений и серверов. Прежде чем проверять сам журнал **Приложение**, проверьте данные, связанные с нужным приложением, под узлом **Журналы приложений и служб**. Можно также установить фильтр (об этом см. далее).

- **Безопасность (Security)** — содержит события аудита безопасности, такие как вход в систему или доступ к объектам (например, файлам), для которых включен аудит. Важно помнить, что если вы хотите, чтобы события записывались в этот журнал, необходимо настроить аудит. Нельзя определить, кто пытался получить доступ к определенному файлу, если для этого файла не настроен аудит. После настройки аудита соответствующие события будут записываться в файл журнала безопасности.
- **Установка (Setup)** — содержит события, относящиеся к установке приложений на сервер.
- **Система (System)** — содержит события, записанные системными компонентами, включая такие события, как неисправность драйвера устройства или неисправность службы.
- **Перенаправленные события (Forwarded Events)** — содержит события, собранные с других компьютеров. Этот журнал очень полезен администраторам, которые хотят просматривать важные данные журнала в одном месте, а не проверять по отдельности журналы каждого сервера. Можно собирать события с других компьютеров, используя только подписки (см. далее).

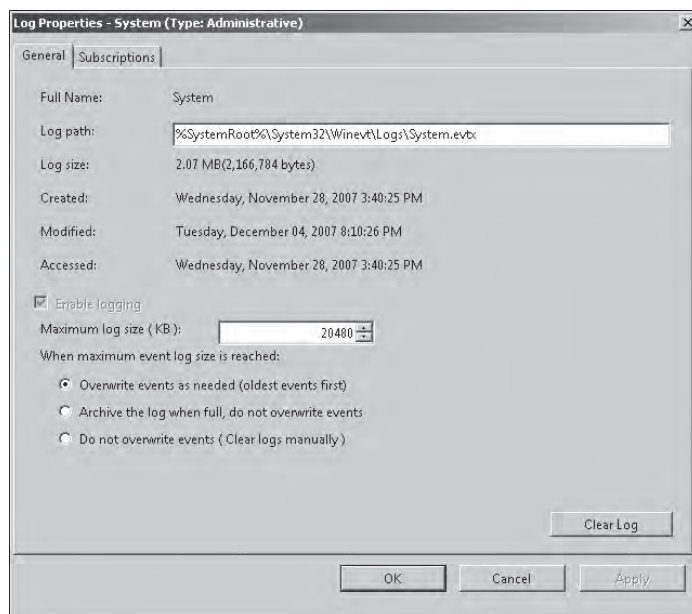


Рис. 5-5. Свойства файла журнала

Еще одно важное решение относительно планирования журналов событий — определение максимального размера журналов и действий при достижении

журналом этого размера. Часто это называется политикой сохранения журнала. Как видно на рис. 5-5, доступны следующие варианты: **Переписывать события при необходимости** (Overwrite Events As Needed), **Архивировать журнал при заполнении** (Archive The Log When Full) и **Не переписывать события (Очистить журнал вручную)** [Do Not Overwrite Events (Clear Log Manually)]. При выборе последнего варианта помните, что в зависимости от конфигурации групповой политики сервер может стать недоступным до очистки соответствующего файла журнала вручную. Чаще всего не следует допускать перезапись журналов событий.

## Фильтры

Фильтры — один из способов ограничения числа отображаемых в журнале событий по заданным критериям. Например, фильтр, показанный на рис. 5-6, отображает только события с уровнем **Критическое** (Critical), **Предупреждение** (Warning) и **Ошибка** (Error) из журнала **Система** (System), записанные в период между 22:49 3 января 2011 г. и 22:49 17 января 2011 г. Чтобы использовать фильтр, нужно что-то знать о типе искомого события. Чем больше условий указано в фильтре, тем меньше событий отображается. В отличие от пользовательских представлений, фильтры нельзя сохранять. Их необходимо генерировать при каждом использовании.

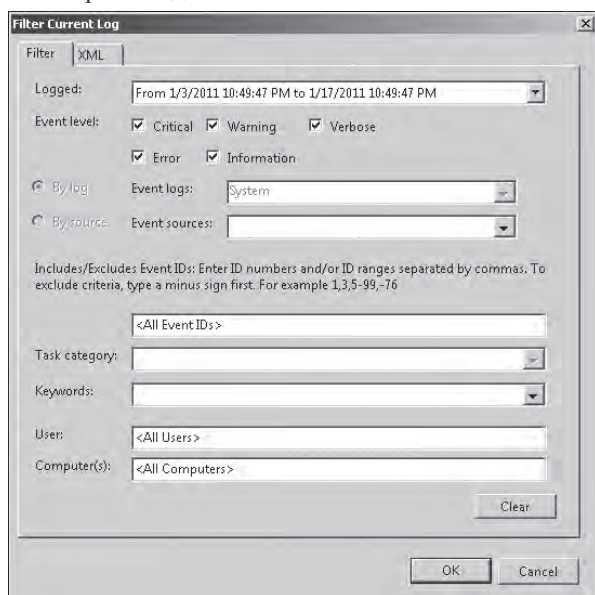


Рис. 5-6. Фильтр журнала

## Настраиваемые представления

Настраиваемое представление (рис. 5-7) можно считать специальным фильтром, который можно сохранить. Такой фильтр можно применять к нескольким журналам, а не только к одному. Вместо того, чтобы создавать фильтр, можно создать настраиваемое представление и выбирать его при каждом открытии консоли **Просмотр событий** (Event Viewer). Настраиваемые представления можно

импортировать и экспортировать, если хотите использовать их на других компьютерах под управлением Windows Server 2008 и 2008 R2.

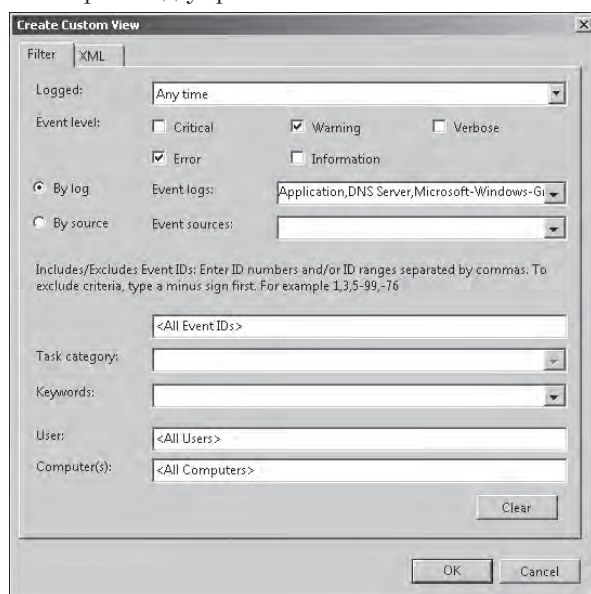


Рис. 5-7. Настраиваемое представление

## Привязка задач к событиям

Как показано на рис. 5-8, привязка задачи к событию позволяет запускать программу, отправлять электронное письмо или отображать сообщение каждый раз, когда указанное событие записывается в определенный журнал событий. Привязка задач к событиям позволяет быстрее реагировать на важные события. Вместо того чтобы узнавать о событии лишь во время просмотра файлов журнала, после того как событие уже произошло, можно сразу узнавать о нем и принимать соответствующие меры. Как и в случае с любыми другими прямыми уведомлениями, следует избегать слишком большого их количества. В противном случае вы будете завалены задачами, не требующими немедленного реагирования. Прямое уведомление следует настраивать только для тех событий, на которые необходимо реагировать незамедлительно. Задачи, привязанные к журналам событий, хранятся в планировщике заданий. Если хотите удалить привязанную задачу, обратитесь к планировщику задач, а не к программе просмотра событий.

Ограничения привязки задач к событиям в том, что событие уже должно существовать в файле журнала. Нельзя привязывать задачи к событиям в аналитических журналах и журналах отладки, а также к событиям из сохраненного файла журнала. Невозможно использовать эту функцию для запуска задачи для события, если событие не произошло, хотя можно имитировать такую ситуацию при помощи сценария PowerShell, выполняющегося в запланированное время. Об использовании PowerShell с файлами журналов рассказывается далее на этом занятии. На практических занятиях в конце главы вы привяжите задачу к событию.

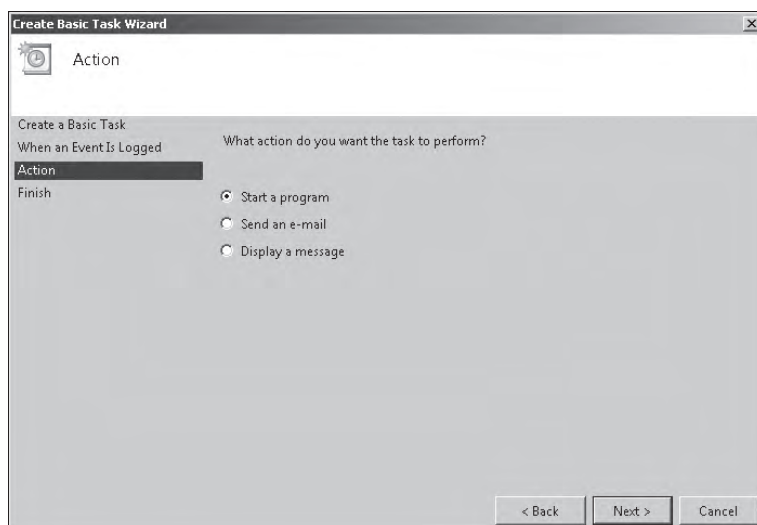


Рис. 5-8. Создание простой задачи

## Настройка подписок журналов

Подписки журналов — один из способов централизованного управления журналами. Вместо того чтобы проверять журналы каждого сервера, можно использовать подписки журналов для объединения всех важных событий в одном месте. Затем при помощи настраиваемых представлений можно быстро находить интересные события.

Существует два типа подписок. В подписке, инициированной сборщиком данных, компьютер, хранящий собранные события (сборщик), получает их от компьютера, который генерирует события (исходный компьютер). В подписке, инициированной компьютером-источником, компьютеры, генерирующие события, пересылают их компьютеру-сборщику.

Для настройки подписки, инициированной сборщиком, выполните следующие действия:

1. На каждом исходном компьютере откройте оболочку командной строки с повышенными привилегиями и введите команду `wingm quickconfig`. Необходимо подтвердить запрос на создание исключения на брандмауэре.
2. На каждом компьютере-источнике добавьте учетную запись компьютера-сборщика в локальную группу администраторов.
3. На компьютере, выполняющем функцию сборщика, откройте оболочку командной строки с повышенными привилегиями и введите команду `wesutil qc`. Эта команда запускает службу сборщика событий Windows и настраивает ее автоматический запуск с отложенным стартом.
4. На компьютере-сборщике откройте **Просмотр событий** (Event Viewer) и выберите узел **Подписки** (Subscriptions). На панели **Действия** (Actions) щелкните **Создать подписку** (Create Subscription), чтобы открыть диалоговое окно **Свойства подписки** (Subscription Properties) (рис. 5-9).



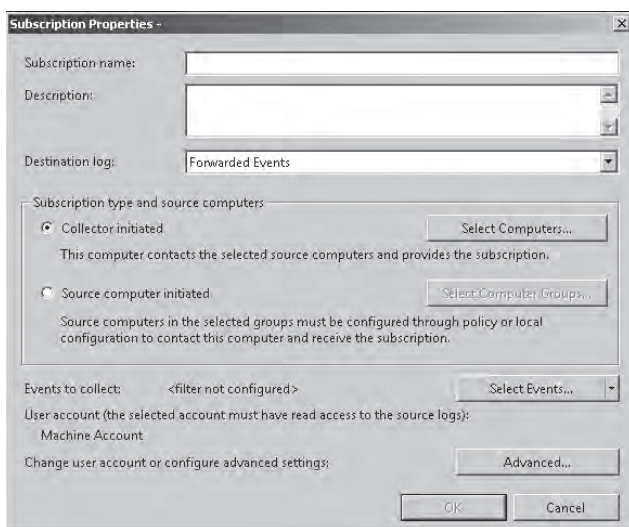


Рис. 5-9. Настройка подписки

- Щелкните **Выбрать компьютеры** (Select Computers), чтобы выбрать компьютеры-источники.
- Выбрав все исходные компьютеры, щелкните **Выбрать события** (Select Events), чтобы настроить фильтр для типа событий, которые должен собирать компьютер-сборщик.
- Завершив создание фильтра, щелкните **ОК** два раза, чтобы активировать подписку.

Настройка фильтра похожа на создание настраиваемого представления в том, что можно указать несколько источников журналов событий, а не только один. Кроме того, подписка сохраняется, тогда как фильтр приходится создавать каждый раз заново. По умолчанию все собранные данные записываются в журнал **Перенаправленные события** (Forwarded Events). Можно пересылать данные в другие журналы, настроив свойства подписки. Несмотря на то, что фильтр используется для получения от исходных компьютеров только определенных событий и помещения их в журнал назначения, все равно можно создавать настраиваемые представления и применять их к данным из журнала назначения. Можно создать настраиваемое представление для каждого исходного компьютера, чтобы просматривать события с отдельных компьютеров, а не все данные одновременно.

Подписки, инициированные сборщиком, настраиваются путем применения групповой политики. Для этого необходимо настроить компьютер-сборщик, как описано выше, но выбрать тип подписки **Инициировано исходным компьютером** (Source Computer Initiated) вместо **Инициировано сборщиком** (Collector Initiated). Для настройки исходных компьютеров примените GPO с настроенным параметром **Настроить адрес сервера, интервал обновления и центр, выдающий сертификат для диспетчера подписки** (Configure the Server Address, Refresh Interval, And Issuer Certificate) из узла **Конфигурация компьютера | Политики | Административные шаблоны | Компоненты Windows | Пересылка**

**событий** (Computer Configuration | Policies | Administrative Templates | Windows Components | Event Forwarding) (рис. 5-10).

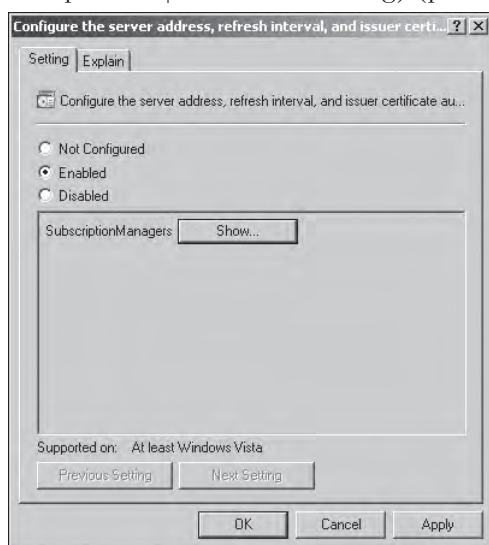


Рис. 5-10. Политика пересылки событий

---

#### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Подписки журнала событий

Подробнее о подписках журнала событий см. по адресу <http://technet.microsoft.com/ru-ru/library/cc749183.aspx>.

---

### Журналы приложений и служб

Когда в Windows Server 2008 и 2008 R2 устанавливаются приложения или роли, для них чаще всего добавляются новые журналы в узел **Журналы приложений и служб** (Applications And Services Logs) консоли **Просмотр событий** (Event Viewer). Журналы приложений и служб — новая категория журналов событий, появившаяся в Windows Server 2008, поэтому приложения, выпущенные до выхода Windows Server 2008, могут по-прежнему записывать события в традиционный журнал приложений, описанный выше. Как показано на рис. 5-11, под этим узлом можно также просматривать аналитические и отладочные журналы. Эти журналы видны, только если выбрать в меню **Вид (View)** команду **Отобразить аналитический и отладочный журналы** (Show Analytic And Debug).

Журналы приложений и служб можно разделить на четыре большие категории:

- **Административные.** В таких журналах описывается проблема и предлагается решение, которое администратор может применить. Сообщения в административных журналах почти всегда предлагают решение проблемы.
- **Оперативные.** Оперативные события предоставляют информацию, помогающую в анализе и диагностике проблем. Хотя эти события не содержат сведений о решении проблемы, сгенерировавшей событие, их можно использовать в качестве триггера для оповещения администратора о событии.

- **Аналитические.** Аналитические события, отображающиеся только если включены, записываются в больших объемах и указывают на проблемы, которые обычно трудно решить.
- **Отладочные.** Такие журналы используются разработчиками, занимающимися решением проблем в своих приложениях.

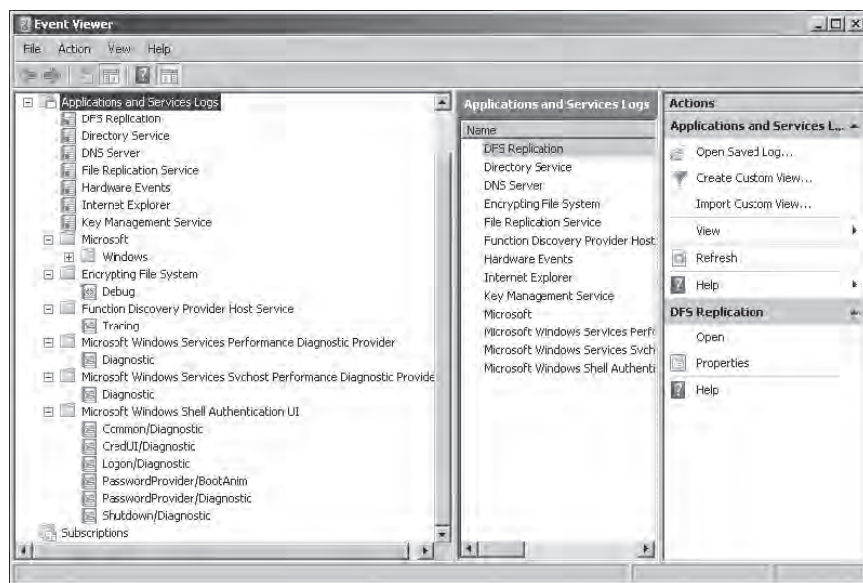


Рис. 5-11. Просмотр аналитических и отладочных журналов

## Просмотр событий на удаленном компьютере

Консоль **Просмотр событий** (Event Viewer), как и другие консоли управления, позволяет подключаться к удаленному компьютеру под управлением Windows Server 2008 или 2008 R2. Для этого выберите в меню **Действия** (Action) команду **Подключиться к другому компьютеру** (Connect To Another Computer). Для удаленного просмотра журналов событий на компьютере с включенным брандмауэром Windows необходимо включить исключение **Удаленное управление журналом событий** (Remote Event Log Management).

После подключения к другому компьютеру с помощью консоли **Просмотр событий** доступны настраиваемые представления, хранящиеся на локальном компьютере, но не на удаленном. Если открыть локальное настраиваемое представление после подключения к удаленному компьютеру, оно будет работать с журналами событий удаленного, а не локального компьютера. Например, если создано представление, которое отображает только ошибки из журнала **Система**, при подключении к удаленному компьютеру оно будет отображать только ошибки из системного журнала удаленного компьютера.

Данные событий чаще всего перенаправляются при помощи подписок в единое хранилище для анализа, поэтому удаленные подключения с помощью консоли **Просмотр событий** будут устанавливаться только в том случае, если обнаружится важное событие, о котором требуется получить больше информации, изучив другие события на компьютере-источнике. Пересылка всех инте-

ресных событий в единое хранилище в сочетании с последующим локальным контролем помогает найти баланс между хранением сведений и отображением потенциально важных данных.

## Архивация журналов событий

Планируя управление данными журнала событий в организации, уделите внимание политике хранения журналов событий. Создайте политику, определяющую длительность хранения данных журналов событий. Например, если работник был уличен в доступе к конфиденциальной информации, свидетельства его деятельности могут иметься в журналах безопасности за последние нескольких месяцев. Если журналы автоматически переписываются по достижении определенного размера или просто удаляются после беглого просмотра, то информация, относящаяся к расследованию, может быть потеряна. Простейший способ управления архивацией журналов событий заключается в том, чтобы применить переадресацию событий и экспортировать собранную информацию в файлы, которые можно архивировать по отдельности и хранить в течение необходимого времени. Чтобы сохранить файлы журнала, выберите в меню **Действие** (Action) команду **Сохранить все события как** (Save Log File As). Доступны следующие форматы:

- Файлы событий (\*.evtx);
- XML (\*.xml);
- Text (с разделением табуляцией) (\*.txt);
- CSV (с разделением запятой) (\*.csv).

При сохранении файла журнала из консоли **Просмотр событий** будет предложено включить отображение сведений. Если не включить эту информацию в сохраненный файл журнала, он может некорректно отображаться на других компьютерах. Файлы журналов можно сохранять после применения фильтров или настраиваемых представлений. Это позволяет уменьшить размер файла, хотя при этом могут не сохраниться события, которые позже окажутся важными. В разных ситуациях полезны файлы разного типа, но только файлы, сохраненные в формате .evtx можно открывать в консоли **Просмотр событий** на другом компьютере.

## Управление журналами событий с помощью Wevtutil и PowerShell

Утилита Wevtutil обладает практически той же функциональностью, что и консоль **Просмотр событий**. Она позволяет администраторам просматривать, фильтровать и управлять данными журнала событий непосредственно из командной строки. Например, для экспорта журнала в файл используйте следующую команду:

```
wevtutil epl имя_журнала имя_файла.evtx
```

Эту команду можно включить в сценарий для ежедневного экспорта всех файлов журналов в общую папку. Консоль **Просмотр событий** не дает возможности для такого рода автоматизации. Автоматизация резервного копирования файлов журналов полезна, когда требуется управлять журналами событий в масштабе организации.

---

**ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Wevtutil**

Подробнее о Wevtutil см. по адресу [http://technet.microsoft.com/en-us/library/cc732848\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc732848(Ws.10).aspx) (на англ. языке).

Хотя утилита Wevtutil дает возможность анализировать данные журнала событий, она предоставляет только простые функции управления событиями. Больше возможностей по мониторингу и управлению журналами событий дает командлет PowerShell Get-Eventlog. Преимущество PowerShell в возможности создавать более сложные сценарии, чем с помощью Wevtutil. Весь анализ и обработка данных происходят внутри сценария PowerShell, тогда как в случае с Wevtutil сценарий вызывает внешнее приложение, а затем пытается работать с его выходными данными. Иными словами, компоненты PowerShell разработаны для взаимодействия друг с другом, что облегчает написание сценариев PowerShell и управление ими.

Одна из команд PowerShell возвращает список всех экземпляров события в указанном журнале. Например, для того чтобы найти в журнале Система все события с ID 1000, выполните следующую команду:

```
Get-Eventlog System | where {$_.EventID -eq 1000}
```

---

**ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Get-Eventlog**

Подробнее о командлете Get-EventLog см. по адресу <http://technet.microsoft.com/ru-ru/library/dd315250.aspx>.

Как язык программирования и сценариев, PowerShell позволяет быстро формировать сложные команды для анализа данных журналов событий Windows. С точки зрения планирования следует рассмотреть возможность использования сценариев PowerShell для управления журналами событий в тех случаях, когда недостаточно возможностей встроенных инструментов, таких как настраиваемые представления, фильтры и привязанные к событиям задачи. Функциональности консоли **Просмотр событий** достаточно в большинстве случаев, но если требуется больше, используйте PowerShell.

---

**Microsoft System Center Operations Manager 2007 R2**

Планируя централизованный мониторинг и управление большим числом компьютеров под управлением Windows Server 2008 и 2008 R2, подумайте о применении System Center Operations Manager 2007 R2. Это приложение позволяет централизованно управлять и наблюдать за тысячами серверов и приложений и предоставляет полную информацию о состоянии сетевого окружения. Последняя версия, System Center Operations Manager 2007 R2, предоставляет следующие возможности:

- предупреждающие оповещения, распознающие условия, которые в будущем могут привести к неисправности критически важных служб, приложений и серверов;
- автоматическое выполнение задач для разрешения проблем при возникновении определенных событий;
- сбор данных на долгосрочной основе со всех серверов и приложений с возможностью генерации сравнительных отчетов о текущей работе;

- сопоставление данных аудита всех компонентов сети для обнаружения тенденций, незаметных при изолированном изучении данных аудита сервера.

Кроме средств, входящих в стандартную установку Operations Manager 2007 R2, можно использовать дополнительные пакеты управления, расширяющие возможности мониторинга. Microsoft предлагает более 60 пакетов управления, которые можно использовать в Operations Manager 2007 R2 для работы с различными приложениями, от Exchange Server 2010 до SQL Server 2008 R2. При помощи пакетов управления можно определять, настроена ли определенная технология в соответствии с рекомендациями. Пакеты управления можно использовать также для анализа производительности технологии и составления рекомендаций по изменению конфигурации для оптимизации работы. Это похоже на использование Best Practices Analyzer (BPA), но анализируется не отдельный компьютер, а определенная технология, развернутая в сети организации.

Подобно другим корпоративным решениям в области мониторинга и управления, таким как Microsoft System Center Virtual Machine Manager 2008 R2, System Center Operations Manager 2007 R2 требует доступа к базе данных под управлением SQL Server 2005 SP1 или выше для хранения данных. Поскольку экземпляры SQL Server способны размещать несколько баз данных, один сервер под управлением SQL Server может хранить базы данных конфигураций для System Center Virtual Machine Manager 2008 R2 и System Center Operations Manager 2007 R2. Даже если организации не требуется сервер баз данных в качестве сервера приложений, в корпоративных окружениях SQL Server все чаще находит место в качестве ключевого компонента сетевой инфраструктуры.

---

#### **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ** System Center Operations Manager 2007 R2

Узнать подробнее о System Center Operations Manager 2007 R2 и скачать 180-дневную пробную версию можно по адресу <http://technet.microsoft.com/ru-RU/evalcenter/bb738014.aspx>.

---

## **Резюме**

- Чтобы иметь возможность удаленно подключаться к серверу под управлением Windows Server 2008 или 2008 R2, необходимо включить удаленный рабочий стол. По умолчанию заходить на сервер с помощью удаленного рабочего стола могут члены локальных групп **Администраторы** и **Пользователи удаленного рабочего стола**. На контроллеры доменов входить могут только члены группы **Администраторы**.
- Службы аварийного управления (EMS) позволяют управлять компьютером, переставшим функционировать.
- Средства RSAT включают консоли для администрирования всех ролей и компонентов Windows Server 2008 и 2008 R2. Средства RSAT можно устанавливать, как компонент Windows Server 2008/2008 R2. Их можно скачать и установить на компьютеры под управлением Windows Vista SP1 и Windows 7.
- Фильтры позволяют выборочно отображать события из журнала событий. Фильтры нельзя сохранять, но настраиваемые представления позволяют применять сохраненный фильтр к нескольким журналам событий.



- Можно привязывать задачи к отдельным журналам или событиям. Когда происходит событие, запускается задача. Редактировать и удалять существующие задачи журнала можно в планировщике задач.

## Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных на занятии 1. Эти вопросы предоставлены также в электронном виде на прилагаемом к книге компакт-диске.

---

### ПРИМЕЧАНИЕ Ответы

Ответы на вопросы и пояснения к их вариантам размещены в разделе «Ответы» в конце книги.

---

1. Какая из перечисленных операционных систем поддерживает RSAT? (Выберите все подходящие ответы.)
  - a. Windows Vista Enterprise с пакетом обновлений SP1.
  - b. Windows XP Professional с пакетом обновлений SP3.
  - c. Windows 7 Home Premium.
  - d. Windows 7 Enterprise.
  - e. Windows Server 2008 Standard.
2. Члены каких групп по умолчанию могут подключаться через удаленный рабочий стол к автономному компьютеру под управлением Windows Server 2008 или 2008 R2? (Каждый ответ является готовым решением. Выберите все подходящие.)
  - a. Администраторы.
  - b. Пользователи удаленного рабочего стола.
  - c. Опытные пользователи.
  - d. Операторы печати.
  - e. Операторы архива.
3. Какая из перечисленных технологий позволяет корректно завершить работу компьютера под управлением Windows Server 2008 R2, продолжающего функционировать после того, как скачок напряжения вывел из строя видеокарту и сетевой адаптер?
  - a. Удаленный рабочий стол.
  - b. Telnet.
  - c. EMS.
  - d. PowerShell.
4. В ближайшие месяцы вам необходимо выполнять администрирование нескольких компьютеров под управлением Windows Server 2008 R2 в офисе дочерней компании. Прямой канал связи между этим офисом и главным офисом вашей компании отсутствует. Однако оба офиса имеют прямое подключение к Интернету, а сторонний брандмауэр разрешает передачу данных через порт 443, если адрес источника находится в пределах диапазона открытых IP-адресов главного офиса компании. Какое решение позволит



удаленно администрировать компьютеры дочерней компании из главного офиса?

- a. Настроить сервер шлюза удаленного рабочего стола и разместить его в офисе дочерней компании.
  - b. Настроить сервер шлюза удаленного рабочего стола и разместить его в главном офисе компании.
  - c. На брандмауэре в офисе дочерней компании разрешить передачу данных через порт 25, если IP-адрес источника входит в диапазон открытых IP-адресов главного офиса компании.
  - d. На брандмауэре в офисе дочерней компании разрешить передачу данных через порт 25, если IP-адрес источника входит в диапазон частных IP-адресов главного офиса компании.
5. Вы настроили компьютер для сбора данных журнала событий с 50 разных компьютеров под управлением Windows Server 2008 R2, распределенных по сети организации. Когда вы открыли журнал **Перенаправленные события** (Forwarded Events) в консоли **Просмотр событий** (Event Viewer), объем данных вас ошеломил. Каждый раз, когда вы открываете консоль **Просмотр событий**, вы хотите иметь возможность быстро выяснить, произошли ли какие-либо критические события в течение последних суток. Какое решение вам следует принять?
- a. Создать пользовательский фильтр.
  - b. Создать настраиваемое представление.
  - c. Создать подписку.
  - d. Настроить политику диспетчера системных ресурсов Windows (WSRM).

## Занятие 2. Делегирование полномочий

Системный администратор часто имеет все возможные привилегии. Однако такому ценному специалисту следует свести к минимуму время, затрачиваемое на решение простых задач, и сосредоточиться на выполнении более сложной работы. Делегирование полномочий дает непривилегированным пользователям возможность выполнять ограниченный и очень специфичный набор простых административных задач. На этом занятии вы узнаете, как планировать делегирование полномочий, чтобы повысить эффективность управления корпоративной сетью.

---

### Изучив материал этого занятия, вы сможете:

- ✓ Планировать политики и процедуры делегирования.
- ✓ Делегировать полномочия.
- ✓ Делегировать управление приложениями.

**Продолжительность занятия — примерно 60 мин.**

---

## Политики делегирования

Сотрудники отдела кадров редко знают о возможностях AD DS. Делегирование полномочий сочетает технические аспекты, реализация которых требует знаний системного администратора, с правовыми и организационными вопросами, которыми занимается отдел кадров. Организация доверяет системным администраторам критически важную информацию. Если системный администратор является единственным, кто может выполнить определенную задачу, такую как создание учетной записи пользователя, изменение разрешений или изменение пароля директора, то, если что-то пойдет не так, виноват, разумеется, будет он. На этом уроке вы узнаете, что системные администраторы имеют возможность делегировать полномочия. Делегирование привилегии следует выполнять только в ситуациях, предусмотренных существующей политикой, не только по этическим соображениям, но и потому, что должна существовать четкая цепочка ответственности.

## Процедуры делегирования

Полномочия можно делегировать путем настройки параметров безопасности объектов в AD DS. На рис. 5-12 изображены дополнительные параметры безопасности подразделения, для которого учетная запись пользователя Kim Akers имеет делегированные разрешения. Недостаток редактирования вручную заключается в том, что требуется гораздо большая точность, чем при использовании мастера делегирования управления, который выполняет настройку автоматически. Делегирование можно выполнять также при помощи команды `dscls.exe`. Как и средства с графическим интерфейсом, эта команда требует точного указания разрешений для объектов AD DS. Чтобы подробнее узнать о синтаксисе команды `dscls.exe`, введите команду `dscls.exe /?` в командной строке с повышенными привилегиями на компьютере под управлением Windows Server 2008 или 2008 R2. Для делегирования можно также создавать сценарии PowerShell, изменяющие разрешения, назначенные подразделениям. Поскольку утилита `dscls.exe` предназначена специально для изменения разрешений объектов каталога, она предоставляет более прямой способ выполнения этой задачи, нежели сценарии PowerShell для простых задач делегирования.

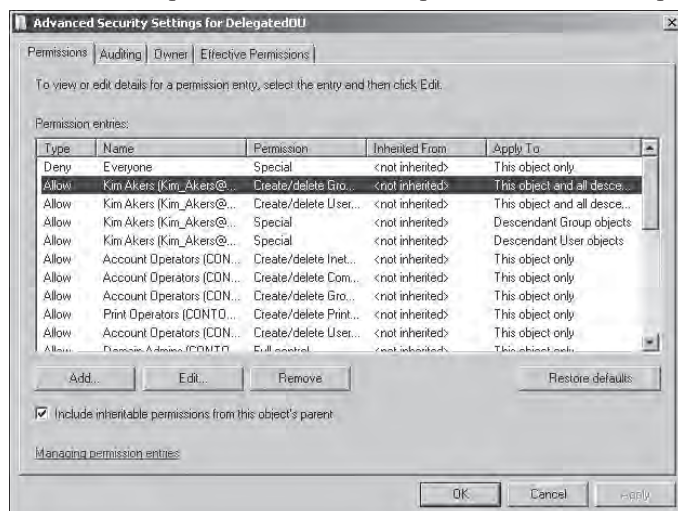


Рис. 5-12. Редактирование разрешений для делегирования

Если задач, которые требуется делегировать, немного, лучше всего использовать мастер делегирования управления, поскольку он снижает вероятность ошибок и относительно прост в использовании. Если требуется делегировать много сложных задач, то стоит потратить время на сценарий, использующий `dsacls.exe` или PowerShell. Выбирая между `dsacls.exe` и PowerShell, оцените сложность делегирования. С помощью `dsacls.exe` можно делегировать много относительно простых задач. Большое число сложных задач лучше делегировать с помощью сценария PowerShell, так как в этом случае проще добавлять другие компоненты, такие как данные, извлеченные сценарием из базы данных, или таблицу, описывающую, какие задачи следует делегировать. Принимая решение, помните:

- для делегирования небольшого числа задач используйте мастер делегирования управления;
- для делегирования большого числа простых задач используйте утилиту командной строки `dsacls.exe`;
- для делегирования большого числа сложных задач, включающих такие компоненты, как CSV-файлы, используйте сценарий PowerShell.

### Делегирование административных привилегий

Как уже говорилось, делегирование можно выполнять при помощи мастера делегирования управления (Delegation Of Control Wizard) (рис. 5-13). Этот мастер можно использовать на уровне домена, хотя в большинстве организаций делегирование выполняется на уровне подразделений. С помощью этого мастера можно делегировать следующие задачи:

- создание, удаление и управление учетными записями пользователей;
- сброс пользовательских паролей и принудительное изменение паролей при следующем входе;
- чтение информации обо всех пользователях;
- создание, удаление и управление группами;
- изменение членства в группах;
- управление ссылками на групповые политики;
- генерация RSoP (планирование);
- генерация RSoP (протоколирование);
- создание, удаление и управление учетными записями `InetOrgPerson`;
- сброс паролей `InetOrgPerson` и принудительное изменение паролей при следующем входе;
- чтение всей информации для `InetOrgPerson`.

Мастер делегирования управления можно использовать для делегирования одной, нескольких или всех этих задач пользователям или группам. Можно также создать пользовательскую задачу для делегирования. В процессе создания пользовательской задачи для делегирования можно делегировать управление папкой, существующими объектами контейнера и создание новых объектов в контейнере или определенных объектов. Можно делегировать управление более чем сотней различных объектов. На рис. 5-14 показаны некоторые из этих объектов в мастере делегирования управления.

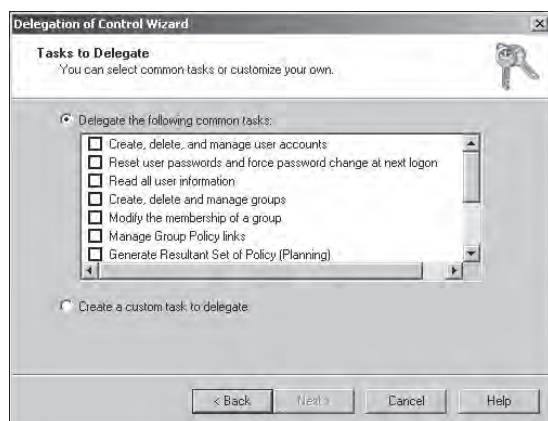


Рис. 5-13. Задачи, которые можно делегировать

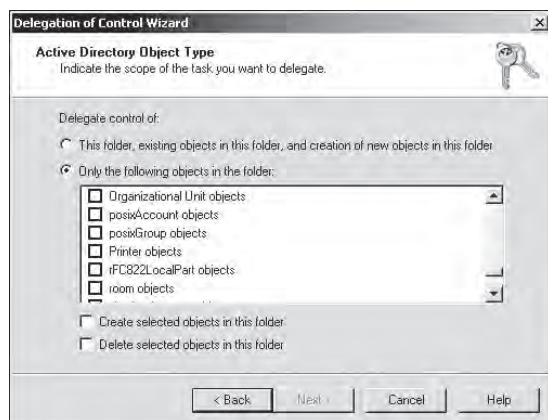


Рис. 5-14. Пользовательское делегирование

Главная причина делегирования управления — желание передать пользователям ограниченные административные права. Это очень важно для тех сред, где ИТ-поддержка централизована и имеется много филиалов без работников ИТ-поддержки. Это важно, потому что выполнение некоторых важных административных задач, таких как изменение паролей, кем-то в удаленном офисе связано с риском для безопасности. Например, злоумышленник может позвонить в службу поддержки, выдавая себя за конкретного пользователя, чтобы изменить пароль учетной записи этого пользователя. Если у вашей организации надежная политика, нужно нечто большее, чем заявление «Я — Руслан», прежде чем пароль Руслана будет изменен. Во многих организациях сюда входит персональный визит в службу поддержки и предоставление каких-либо документов, например, водительского удостоверения. Процесс верификации может быть затруднен, если кто-то забыл пароль, а ИТ-персонала в офисе нет, и некому идентифицировать пользователя и поменять пароль.

С помощью мастера делегирования управления можно планировать политики, позволяющие доверенному лицу в филиале изменять пароли. Поскольку делегируется лишь это конкретное право, доверенное лицо не обладает никакими другими административными правами. Когда кому-то в офисе нужно

изменить пароль, он может подтвердить свою личность у доверенного делегата, который после этого изменяет пароль.

## Удаление существующих делегирований

Несмотря на то, что, просматривая дополнительные параметры безопасности для делегирования, можно определять, каким учетным записям делегированы административные разрешения, иногда бывает трудно точно выяснить, какие права делегированы, особенно если использовалось пользовательское делегирование. Если вы не уверены, как прежде выполнялось делегирование, и не существует никаких записей об этом, будет разумным восстановить настройки по умолчанию. В следующий раз, когда потребуется делегирование, вы сможете убедиться, что имеется подтверждение на бумаге, объясняющее, почему и для кого выполнялось делегирование.

Кнопка **Восстановить умолчания** (Restore Defaults) в диалоговом окне дополнительных параметров безопасности для делегирования, которое открывается кнопкой **Дополнительно** (Advanced) на вкладке **Безопасность** (Security) в диалоговом окне свойств подразделения, позволяет удалить делегирование и вернуть подразделение в состояние по умолчанию. Сбросить существующее делегирование можно также с помощью утилиты командной строки dsaccls.exe. Например, чтобы сбросить параметры делегирования для подразделения Delegation из домена adatum.com, выполните следующую команду:

```
Dsaccls «OU=Delegation,DC=adatum,DC=com» /resetDefaultDACL
```

## Делегирование управления группой

Можно делегировать управление членством в группе, указав менеджера на вкладке **Управляется** (Managed By) в диалоговом окне свойств учетной записи пользователя. Пользователь, указанный как менеджер, может изменять членство в группе, по мере необходимости добавляя и удаляя пользователей. На рис. 5-15 показано, что учетной записи пользователя Kim Akers дана возможность изменять список членов группы ExampleGroup. Менеджером может быть учетная запись пользователя или группа из AD DS.

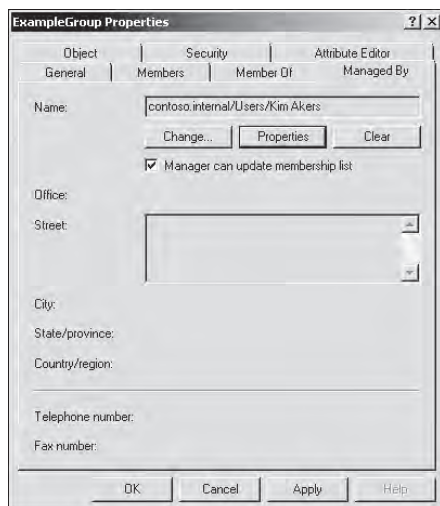


Рис. 5-15. Делегирование управления группой

## Делегирование учетных данных

Делегирование учетных данных — автоматический процесс, отличающийся от делегирования управления. Делегирование управления позволяет владельцу большого набора прав предоставлять часть этих прав другому пользователю. Делегирование учетных данных, называемое также *делегированной аутентификацией*, позволяет компьютеру олицетворять пользователя для получения доступа к ресурсам, к которым может обращаться этот пользователь.

Когда установлен функциональный уровень домена и леса Windows Server 2008 или 2008 R2, в диалоговом окне свойств учетной записи компьютера становится доступной вкладка **Делегирование** (Delegation) (рис. 5-16).

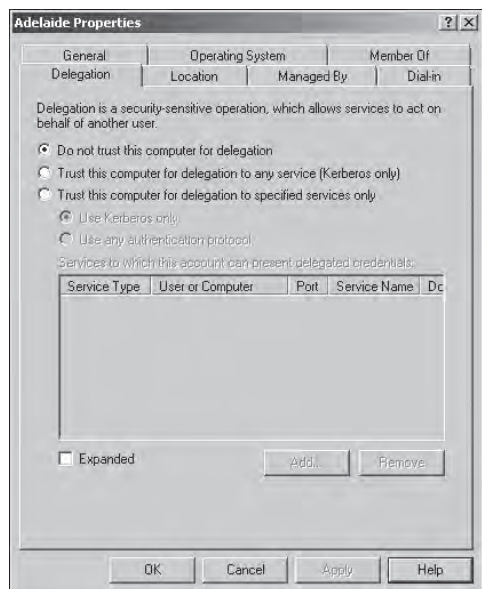


Рис. 5-16. Параметры делегирования в свойствах учетной записи компьютера

Изменив свойства учетной записи компьютера, можно настроить следующие параметры делегирования:

- **Нет, не делать компьютер доверенным для делегирования** (Do Not Trust This Computer For Delegation);
- **Этот компьютер доверенный для делегирования служб (Kerberos)** [Trust This Computer For Delegation To Any Service (Kerberos Only)];
- **Этот компьютер доверенный для делегирования указанных служб** (Trust This Computer For Delegation To Specified Services Only).

С точки зрения планирования, следует отказываться в делегированной аутентификации всем компьютерам, не являющимся безопасными физически. Если это непрактично, можно использовать принудительное делегирование. Принудительное делегирование позволяет выбирать отдельные службы, которые могут быть запрошены доверенным компьютером посредством делегирования. Например, на рис. 5-17 учетная запись компьютера Adelaide настроена так, что ее можно использовать только для представления делегированных учетных данных службе DNS на компьютере GLASGOW.contoso.internal.



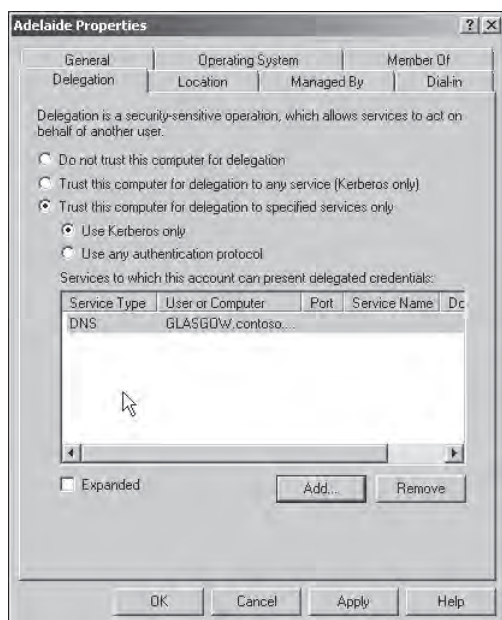


Рис. 5-17. Ограничение делегирования

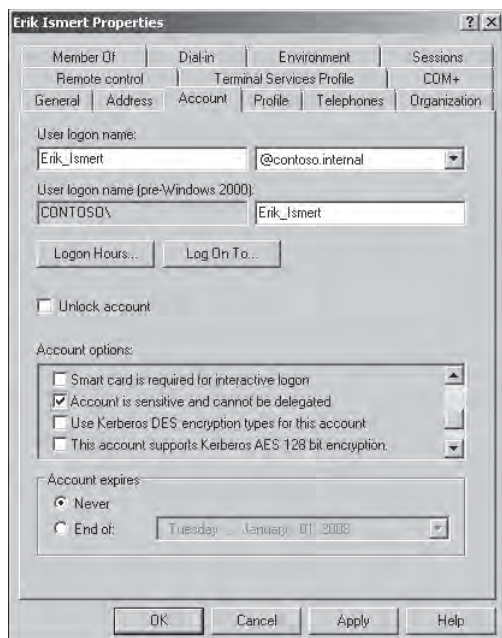


Рис. 5-18. Запрет делегирования важной учетной записи пользователя

Можно запрещать важным учетным записям пользователей участие в делегировании. В оснастке **Active Directory — Пользователи и компьютеры** на вкладке **Учетная запись** (Account) диалогового окна свойств учетной записи пользователя в секции **Параметры учетной записи** (Account Options) можно отметить



учетную запись как важную и не подлежащую делегированию (рис. 5-18). Делегированная аутентификация позволяет сетевой службе действовать от имени пользователя при подключении к другой сетевой службе. Например, если в организации используется шифрованная файловая система (EFS), делегированная аутентификация позволяет хранить зашифрованные файлы на файловых серверах, поскольку файловый сервер должен действовать от имени пользователя для получения необходимых сертификатов, чтобы зашифровать файл. Хотя для обычных учетных записей пользователей это допускается, Microsoft рекомендует отмечать все административные учетные записи домена как важные и запрещать их делегирование. Так предотвращаются сложные атаки, направленные на получение административных прав с использованием делегирования и олицетворения.

### Проверьте себя

- Какие типы учетных записей пользователей следует отмечать как важные и запрещать их участие в делегировании учетных данных?

### Ответ

- Учетные записи администраторов, особенно, администраторов домена и предприятия.

## Делегирование управления приложениями

Во многих организациях разные люди отвечают за разные административные задачи. Часто устанавливает приложение не тот, кто будет его обслуживать. В качестве примера можно привести Exchange Server 2010: человек, отвечающий за сеть в целом и имеющий административные привилегии для управления всеми компьютерами, фактически не отвечает за управление инфраструктурой Exchange Server 2010.

## Делегирование на основе ролей

Почти все серверные продукты Microsoft, в частности, Exchange Server 2010, SQL Server 2008 R2 и System Center Operations Manager 2007 R2, используют делегирование на основе ролей, при котором пользователям назначаются конкретные административные роли. Почти всегда пользователям, которым делегированы административные роли для определенного приложения, не требуются другие административные права на сервере, где располагается это приложение.

Управление доступом на основе ролей (Role Based Access Control, RBAC) — технология, доступная в Exchange Server 2010, позволяющая делегировать определенные административные привилегии с определенной областью действия. Например, можно дать группе возможность управлять всеми почтовыми ящиками на всех серверах сайта Sydney, но не предоставлять ей административные привилегии для почтовых ящиков на любых других почтовых серверах в организации.

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ RBAC в Exchange Server 2010

Подробнее о RBAC в Exchange Server 2010 см. по адресу <http://technet.microsoft.com/ru-ru/library/dd298183.aspx>.

## Делегирование настройки IIS

Делегирование настройки — новая функция IIS 7.0, доступная также в IIS 7.5, позволяющая администраторам компьютеров, на которых размещается роль веб-сервера, делегировать задачи настройки веб-сайта. Это означает, что вместо того, чтобы требовать от администратора компьютера под управлением Windows Server 2008 или 2008 R2 настройки параметров веб-сайта, таких как документ по умолчанию или параметры SSL, можно делегировать эти задачи владельцам сайта или неадминистративным пользователям. Для делегирования функции необходимо выполнить вход или вызвать встроенную учетную запись администратора. Архитектура безопасности Windows Server 2008 и 2008 R2 запрещает делегирование функции при помощи учетной записи, входящей в локальную группу администраторов на компьютере с IIS 7 или 7.5.

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Настройка делегирования IIS

Подробнее о делегированном управлении IIS см. по адресу <http://learn.iis.net/page.aspx/159/configuring-remote-administration-and-featuredellegation-in-iis-7>.

## Диспетчер авторизации

Диспетчер авторизации (Authorization Manager) предоставляет основу модели авторизации для приложений на платформе Windows Server. С помощью диспетчера авторизации разработчики могут создавать роли и области, позволяющие реализовать принципы RBAC в приложениях. Диспетчер авторизации можно использовать только в специально созданных для этого приложениях. В Windows Server 2008 и 2008 R2 диспетчер авторизации запускается командой `azman.msc`. Консоль диспетчера авторизации показана на рис. 5-19.

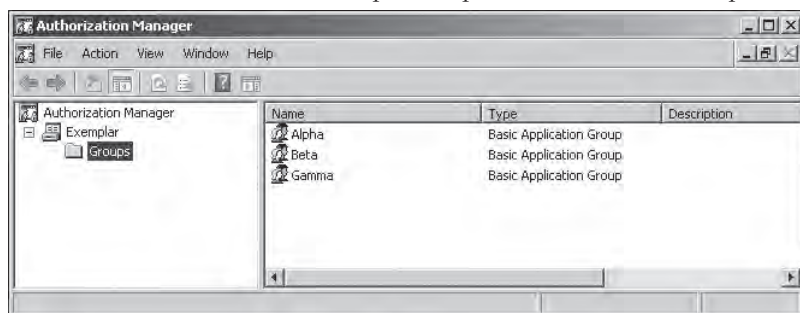


Рис. 5-19. Диспетчер авторизации

Диспетчер авторизации хранит информацию в хранилищах авторизации. В Windows Server 2008 R2 поддерживаются следующие хранилища авторизации: базы данных SQL Server, AD DS, Active Directory Lightweight Directory Services (AD LDS) и XML-файлы. Для поддержки хранилища диспетчера авторизации домен должен иметь функциональный уровень Windows Server 2003 или выше. Поддержка хранилища диспетчера авторизации имеется в SQL Server 2005 SP1 и выше.

Диспетчер авторизации имеет два режима: администратора и разработчика. Режим разработчика позволяет создавать, развертывать и обслуживать приложения, получать доступ ко всем функциям диспетчера авторизации и созда-

вать новые хранилища авторизации. Режим администратора позволяет развертывать и поддерживать существующие приложения, но не дает возможности создавать новые приложения или определять операции.

---

**ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ** Диспетчер авторизации

Подробнее о диспетчере авторизации см. по адресу [http://technet.microsoft.com/ru-ru/library/cc726036\(WS.10\).aspx](http://technet.microsoft.com/ru-ru/library/cc726036(WS.10).aspx).

---

## Резюме

- Прежде чем приступить непосредственно к делегированию, следует проконсультироваться с отделом кадров и письменно утвердить политику.
- Делегирование обычно выполняется с помощью мастера делегирования управления. Можно также выполнять делегирование с помощью команды `dsacls.exe`. Этой командой можно также восстанавливать параметры делегирования по умолчанию.
- Учетные записи администраторов домена следует отмечать как важные и запрещать их участие в делегировании.
- Делегирование приложения обычно включает добавление пользователей в специальные группы, которые добавляются в домен в процессе установки приложения.
- Диспетчер авторизации позволяет реализовать RBAC в пользовательских приложениях.

## Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных на занятии 2. Эти вопросы предоставлены также в электронном виде на прилагаемом к книге компакт-диске.

---

**ПРИМЕЧАНИЕ** Ответы

Ответы на вопросы и пояснения к их вариантам размещены в разделе «Ответы» в конце книги.

---

1. Вы выполнили вход на компьютер под управлением Windows Server 2008 R2, на котором размещается роль веб-сервера, использующая удаленный рабочий стол. Сервер входит в домен вашей организации. Вы находитесь в процессе настройки сервера для размещения сайтов для нескольких разных отделов компании. Вы хотите делегировать полномочия так, чтобы каждый отдел мог управлять своим сайтом. Попытавшись сделать это, вы не смогли выполнить делегирование функции. Какую из следующих стратегий следует использовать для достижения этой цели?
  - a. Войти в систему под локальной учетной записью администратора.
  - b. Добавить свою доменную учетную запись в локальную группу администраторов.
  - c. Добавить свою доменную учетную запись в группу администраторов домена.

- d. Добавить свою локальную учетную запись в локальную группу администраторов.
2. Вы планируете сеть Windows Server 2008 R2 для своей организации. Организация имеет головной офис и пять филиалов по всей стране. ИТ-персонал имеется только в головном офисе. Вы не хотите, чтобы пользователи филиалов обращались в головной офис, когда им нужно изменить пароль, но при этом не хотите также предоставлять работникам, не имеющим отношения к ИТ, лишние привилегии. Какой из предложенных планов соответствует данным целям?
- a. Делегировать задачу **Создание, удаление и управление группами** (Create, Delete, And Manage Groups) доверенному пользователю в каждом филиале с помощью мастера делегирования управления.
  - b. Делегировать задачу **Создание, удаление и управление учетными записями пользователей** (Create, Delete, And Manage User Accounts) доверенному пользователю в каждом филиале с помощью мастера делегирования управления.
  - c. Делегировать задачу **Чтение информации о всех пользователях** (Read All User Information) доверенному пользователю в каждом филиале с помощью мастера делегирования управления.
  - d. Делегировать задачу **Переустановить пароли пользователей и установить изменение пароля при следующей перезагрузке** (Reset User Passwords And Force Password Change At Next Logon) доверенному пользователю в каждом филиале с помощью мастера делегирования управления.
3. Вы хотите предоставить пользователю Hazem Abolrous возможность управлять членством универсальной группы безопасности Interns. Группа расположена в подразделении Contractors, которая содержит учетные записи пользователей и группы безопасности для временных работников вашей организации. Какие из следующих действий вы должны предпринять, чтобы добиться этой цели?
- a. Использовать мастер делегирования управления, чтобы предоставить учетной записи пользователя Hazem право **Изменение членства в группах** (Modify The Membership Of A Group) в подразделении Contractors.
  - b. Использовать мастер делегирования управления, запустив его для группы безопасности Interns. Предоставить учетной записи пользователя Hazem право **Изменение членства в группах** (Modify The Membership Of A Group).
  - c. Использовать мастер делегирования управления, запустив его для группы безопасности Interns. Предоставить учетной записи пользователя Hazem право **Создание, удаление и управление учетными записями пользователей** (Create, Delete, And Manage Groups).
  - d. В параметрах группы безопасности Interns указать, что она управляется пользователем Hazem. Убедиться, что Hazem имеет возможность обновлять список членов.

4. Подразделение Students содержит 300 учетных записей пользователей и 40 групп. Ваша помощница сообщает, что она сделала ошибку во время использования мастера делегирования управления и не знает, какие права делегировала. Что можно сделать, чтобы вернуть подразделение Students в состояние до делегирования? (Каждый ответ является готовым решением. Выберите два.)
- Использовать команду dscls с параметром /resetDefaultDACL.
  - Нажать кнопку **Восстановить умолчания** (Restore Defaults) в диалоговом окне дополнительных параметров безопасности для делегирования соответствующего подразделения.
  - Нажать кнопку **Очистить** (Clear) на вкладке **Управляется** (Managed By) в диалоговом окне свойств подразделения.
  - Нажать кнопку **Изменить** (Change) на вкладке **Управляется** (Managed By) в диалоговом окне свойств подразделения.
  - Использовать команду dsquery.

## Практикум. Удаленное управление и делегирование

На этом практикуме вы выполните несколько задач удаленного управления и делегирования в Windows Server 2008 R2, в том числе, удаленно установите функцию при помощи PowerShell и делегируете административные привилегии для подразделения.

### Упражнение 1. Удаленное управление с помощью PowerShell 2.0

В этом упражнении вы настроите два сервера так, чтобы можно было удаленно управлять им с помощью PowerShell 2.0.

- Включите серверы VAN-DC1, VAN-SRV1 и VAN-SRV2. Войдите на сервер VAN-SRV1 под учетной записью пользователя Kim\_Akers.
- Запустите оболочку PowerShell с административными привилегиями и введите следующие команды:  

```
Import-Module ServerManager

Set-Service Winrm -startuptype automatic

Start-Service winrm

Enable-PSRemoting -force
```
- Зайдите на сервер VAN-SRV2 под учетной записью пользователя Kim\_Akers.
- Начните сеанс PowerShell с повышенными привилегиями и введите следующие команды:  

```
Import-Module ServerManager

Invoke-Command -script {Import-Module ServerManager; Get-WindowsFeature}

-computename VAN-SRV1
```

5. Убедитесь, что на сервере VAN-SRV1 не установлено средства просмотра XPS.
6. Удаленно установите средство просмотра XPS на сервер VAN-SRV1, выполнив следующую команду:  

```
Invoke-Command -script {Import-Module ServerManager; Add-WindowsFeature XPS-Viewer} -computername VAN-SRV1
```
7. Убедитесь, что средство просмотра XPS установлено на сервер VAN-SRV1, введя следующую команду:  

```
Invoke-Command -script {Import-Module ServerManager; Get-WindowsFeature} -computername VAN-SRV1
```

## Упражнение 2. Делегирование управления паролями всех учетных записей пользователей из подразделения

В этом упражнении вы делегируете пользователю возможность управления паролями пользователей из определенного подразделения. Выполнение такой процедуры может понадобиться, когда требуется разрешить сотруднику изменять пароли, но не предоставлять ему возможность создавать учетные записи или управлять группами.

1. Зайдите на VAN-DC1 под учетной записью пользователя Kim\_Akers.
2. В меню **Администрирование** (Administrative Tools) щелкните **Active Directory — Пользователи и компьютеры** (Active Directory Users And Computers).
3. В консоли **Active Directory — Пользователи и компьютеры** создайте учетную запись пользователя Andy\_Jacobs в контейнере **Пользователи** (Users). Назначьте пароль P@ssword.
4. В консоли **Active Directory — Пользователи и компьютеры** создайте новое подразделение с именем Delegation в домене adatum.com.
5. Щелкните подразделение Delegation правой кнопкой мыши и выберите команду **Делегировать управление** (Delegate Control). Запустится мастер делегирования управления. Щелкните **Далее** (Next).
6. На странице **Выбранные пользователи и группы** (Selected Users And Groups) щелкните **Добавить** (Add), добавьте andy\_jacobs@adatum.com и щелкните **ОК**. Снова щелкните **ОК**, после чего щелкните **Далее** (Next).
7. На странице **Делегируемые задачи** (Tasks To Delegate) убедитесь, что установлен переключатель **Делегировать следующие обычные задачи** (Delegate The Following Common Tasks), и установите флажок **Переустановить пароли пользователей и установить изменение пароля при следующей перезагрузке** (Reset User Passwords And Force Password Change At Next Logon). Щелкните **Далее** (Next).
8. Щелкните **Готово** (Finish), чтобы закрыть мастер делегирования управления.

### Упражнение 3. Отмена делегирования с помощью команды dscls

В этом упражнении вы отмените делегирование, которое выполнили в упражнении 2. Это можно сделать несколькими способами. Попробуйте оба предложенных способа.

1. Зайдите на VAN-DC1 под учетной записью пользователя Kim\_Akers.
2. В меню **Администрирование** (Administrative Tools) щелкните **Active Directory — Пользователи и компьютеры** (Active Directory Users And Computers).
3. Выберите команду меню **Вид | Дополнительные параметры** (View | Advanced Features). Отобразятся расширенные свойства объектов AD DS.
4. Щелкните правой кнопкой мыши подразделение Delegation, выберите команду **Свойства** (Properties) и перейдите на вкладку **Безопасность** (Security). Щелкните **Дополнительно** (Advanced). Вы должны увидеть, что учетной записи пользователя Andy Jacobs назначены разрешения. Обратите внимание на кнопку **Восстановить умолчания** (Restore Defaults) в этом диалоговом окне. Ее можно использовать для возврата делегированного подразделения к исходной конфигурации.
5. Щелкните **Отмена** (Cancel) два раза, чтобы закрыть диалоговые окна решений и свойств подразделения.
6. Откройте административную командную строку, щелкнув правой кнопкой мыши командную строку в меню Пуск и выбрав команду **Запуск от имени администратора** (Run As Administrator).
7. Когда откроется командная строка, введите следующую команду:  
`dscls «OU=Delegation,DC=adatum,DC=com» /resetDefaultDACL`
8. Получив сообщение об успешном выполнении команды, закройте командную строку.
9. Просмотрите диалоговое окно дополнительных параметров безопасности подразделения Delegation, используя процедуру, описанную на шаге 4. Убедитесь, что учетная запись пользователя Andy Jacobs больше не имеет никаких разрешений для подразделения Delegation.

### Закрепление материала главы

Чтобы попрактиковаться и закрепить знания, полученные при изучении этой главы, выполните следующее:

- прочитайте резюме главы;
- просмотрите список основных терминов, представленных в этой главе;
- выполните задания лабораторной работы, моделирующей реальные ситуации, требующие применения полученных знаний;
- выполните рекомендуемые упражнения;
- пройдите пробный тест.



## Резюме главы

- Удаленный рабочий стол часто используется для удаленного управления компьютерами под управлением Windows Server 2008. Инструменты RSAT позволяют управлять ролями и компонентами Windows Server 2008 с клиентской рабочей станции. PowerShell — язык административных сценариев, предоставляющий широкие возможности по автоматизации повторяющихся и сложных задач системного администрирования.
- Подписки журналов событий позволяют пересылать все события на один компьютер-сборщик для анализа. Настраиваемые представления — это постоянные фильтры, позволяющие администратору быстро находить данные журнала событий.
- Мастер делегирования управления можно использовать для делегирования административных обязанностей пользователям, не являющиеся администраторами.

## Основные термины

Проверьте, знаете ли вы, что означают перечисленные ниже термины из этой главы:

- компьютер-сборщик;
- группа сборщиков данных;
- делегирование;
- привилегия;
- надежность.

## Лабораторная работа

Для выполнения лабораторной работы используйте полученные знания о планировании установки и обновления серверов. Ответы можно найти в разделе «Ответы» в конце книги.

### Задание 1. Управление событиями

Один из системных администраторов компании Fabrikam увольняется в начале нового года, и вместо того, чтобы найти ему замену, руководство предлагает повысить вам зарплату, если вы сможете внедрить более эффективные технологии управления серверами. Одна из наиболее трудоемких задач — управление данными журналов событий, полученных от большого числа серверов компании. Для повышения эффективности вы решили внедрить ряд новых возможностей управления журналами, предоставляемых Windows Server 2008. Ответьте на следующие вопросы:

1. Какие действия необходимо предпринять, чтобы настроить отдельный компьютер под управлением Windows Server 2008 как сборщик журналов?
2. Имеется 30 серверов, включенных в подразделение AppServers. Как убедиться, что события, записываемые в журналы событий этих серверов, пересылаются сборщику данных журналов?

3. Вы хотите получать текстовые сообщения на сотовый телефон каждый раз, когда происходит определенная ошибка. Вы написали сценарий PowerShell, который генерирует текстовое сообщение на основе данных события, и вам нужно каким-то образом запускать этот сценарий, когда происходит событие. Как это сделать?

## **Задание 2. Делегирование прав доверенным пользователям**

Вы помогаете планировать политику и административные процедуры для новой среды Windows Server 2008, которые будут внедрены в компании Wingtip Toys. Штат Wingtip Toys составляет около 500 человек, работающих в одном офисе и на двух производственных предприятиях. Компания хочет минимизировать численность персонала, имеющего непосредственное отношение к администрированию, и делегировать отдельные задачи доверенным пользователям. Например, помощники администратора в отделах должны иметь возможность восстанавливать пароли сотрудников своих отделов, а руководители групп — добавлять и удалять учетные записи из соответствующих групп безопасности. Руководители групп не должны иметь возможности изменять членство чужих групп безопасности. Все учетные записи пользователей в настоящее время хранятся в контейнере Пользователи, а каждый отдел представлен группой безопасности. С учетом этой информации, ответьте на следующие вопросы:

- Что необходимо предпринять, чтобы позволить помощникам администратора в отделах восстанавливать пароли учетных записей работников соответствующих отделов?
- Как позволить руководителям групп добавлять и удалять учетные записи пользователей из групп безопасности, соответствующих их группам?

## **Рекомендуемые упражнения**

Чтобы успешно справиться с экзаменационными заданиями по темам этой главы, выполните следующие упражнения.

### **Планирование стратегий управления серверами**

- Создайте файл, содержащий данные пяти пользователей, разделенные запятыми. Создайте сценарий PowerShell для импорта этих пользователей в AD DS.
- Создайте второй файл, содержащий данные еще пяти пользователей, разделенные запятыми. Не повторяйте имена пользователей из первого упражнения. При помощи утилиты командной строки csvde.exe импортируйте второй набор пользователей в AD DS.

### **Планирование делегированного администрирования**

- Создайте подразделение CompanyContacts. Создайте группу безопасности ContactAdmins. Делегируйте возможность создавать и удалять объекты типа

**Контакт** (Contact) в подразделении CompanyContacts членам группы безопасности ContactAdmins.

- Создайте в IIS новый виртуальный хост с именем cohovineyard.com. Создайте группу безопасности CohoAdmins. Делегируйте управление недавно созданным сайтом группе CohoAdmins.

## Пробный экзамен

Тренировочные тесты на прилагаемом к книге компакт-диске позволяют проверить знания только по одной или сразу по всем темам сертификационного экзамена 70-646. Тестирование можно организовать так, чтобы оно проводилось как настоящий экзамен, а можно проходить в режиме обучения, просматривая правильные ответы и объяснения после каждого ответа.

---

### **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ** Пробный экзамен

Подробнее о пробном экзамене рассказано во Введении.

---

## Виртуализация представлений и приложений

|                                                            |            |
|------------------------------------------------------------|------------|
| <b>Занятие 1. Виртуализация представлений</b>              | <b>254</b> |
| <b>Занятие 2. Развертывание и виртуализация приложений</b> | <b>273</b> |

Виртуализация представлений — метод, с помощью которого приложение работает на одном компьютере, а графические выходные данные отображаются на другом. К виртуализации представлений относятся службы удаленного рабочего стола (RDS), которые в Windows Server 2008 и Windows Server 2003 назывались службами терминалов. Технология Microsoft Application Virtualization (App-V) позволяет обеспечивать компьютеры приложениями, не устанавливая их напрямую. Приложение работает на локальном компьютере, но не установлено на нем. При корректной настройке App-V по сети передаются только те части приложения, которые необходимы для работы. В этой главе рассказывается о виртуализации представлений и об App-V, в том числе о том, как развертывать приложения таким образом, чтобы клиенты автоматически открывали виртуализованные приложения, когда пользователь дважды щелкает документ соответствующего типа.

### Темы экзамена

- Планирование серверов приложений и служб.
- Подготовка приложений.

### Прежде всего

Для выполнения упражнений этой главы потребуется:

- Выполнить задания по установке из Приложения.
- Дополнительной настройки не требуется.

#### Реальный мир

*Орин Томас*

Первый сервер терминалов (сейчас эта технология называется сервером узлов сеансов удаленного рабочего стола), который я развернул, служил

экспериментальным решением для помощи бухгалтерам компании, в которой я работал. Бухгалтеры работали с пользовательским приложением на одном сервере под управлением Windows NT 4.0, который взаимодействовал с SQL Server 7. Работать с приложением мог одновременно только один человек, что создавало неудобства, поскольку необходимо было заранее планировать время работы с сервером. Само приложение не было сетевым, оно устанавливалось и использовалось на том же сервере, где размещалась база данных. В конечном итоге, пришлось купить новый сервер, так как старый плохо работал из-за слабого оборудования.

Конечно, проще всего было установить Windows NT 4.0 на новый компьютер и продолжать работу как прежде, однако на тот момент вышла Windows 2000, и мне не терпелось проверить, смогу ли я использовать в качестве решения службы терминалов. Убедившись, что в Windows 2000 приложение работает без проблем, мы удалили его, настроили сервер для работы служб терминалов, переустановили приложение и начали пробный сеанс с несколькими пользователями. Приложение работало безупречно, осталась лишь одна проблема: лицензирование. Мы связались с местной компанией, которая написала это приложение. Там никогда не слышали о том, чтобы кто-то пытался использовать их приложение для работы со службами терминалов, поэтому они пришли посмотреть на сервер. У них не было каких-либо правил относительно лицензирования такого рода установки, однако одновременная работа нескольких пользователей с их несетевым приложением явно произвела на них впечатление. Поскольку они собирались рекомендовать эту конфигурацию другим пользователям, они пришли к выводу, что условия лицензии не нарушаются, и все остались довольны.

## Занятие 1. Виртуализация представлений

На этом занятии вы узнаете о том, какие факторы необходимо учитывать при планировании развертывания роли служб удаленных рабочих столов Windows Server 2008 R2. Вы узнаете, на что следует обращать внимание при планировании стратегии лицензирования для клиентов сервера узла сеансов удаленных рабочих столов, и как повлияет использование новых технологий, таких как посредник подключений, на развертывание сервера узла сеансов удаленных рабочих столов в головном офисе и филиалах.

---

### Изучив материал этого занятия, вы сможете:

- ✓ Разворачивать службы удаленных рабочих столов.
- ✓ Обеспечивать надежность и избыточность виртуализации представлений.

**Продолжительность занятия — примерно 60 мин.**

---

## Планирование инфраструктуры удаленных рабочих столов

Сервер узла сеанса удаленных рабочих столов (RD Session Host) предоставляет клиентам удаленный доступ к рабочему столу. Для подключения к такому серверу компьютеру требуется только совместимый клиент протокола рабочего стола (RDP). Многие организации экономят деньги, предоставляя пользователям дешевое клиентское оборудование и подключение к серверу узла сеансов удаленных рабочих столов для работы с прикладными приложениями, включая текстовые процессоры, интернет-браузеры и почтовые клиенты. Такой способ работы дает следующие преимущества:

- Пользовательские рабочие станции работают с минимальным количеством программ и не требуют много внимания. Даже если с рабочей станцией возникнут проблемы, все окружение рабочего стола пользователя находится на сервере узла сеансов, так что неисправную рабочую станцию можно заметить, не перенося с нее никаких данных.
- Данные пользователя всегда хранятся в централизованном хранилище, а не на пользовательских рабочих станциях, что упрощает резервное копирование и восстановление данных.
- На сервере узла сеансов удаленных рабочих столов можно установить и обновлять антишпионское и антивирусное ПО для защиты файлов всех пользователей.
- Вместо обновления по отдельности каждого приложения, установленного на рабочей станции пользователя, выполняется централизованное обновление приложений.

При постоянном использовании подключений к удаленному рабочему столу на сервере узла сеансов требуется высокая пропускная способность и небольшое время ожидания ответа. Пользователи ожидают, что ежедневно используемые приложения будут быстро реагировать на команды. Можно оптимизировать использование удаленного рабочего стола для медленных подключений, но чем быстрее канал связи между клиентами и сервером, тем довольнее будут пользователи. Следовательно, вам нужно подумать о развертывании сервера узла сеансов в каждом филиале. Необходимо также найти оптимальное соотношение между числом клиентов, которые будут подключаться к серверу узла сеансов, и стоимостью развертывания этого сервера. Например, если в филиале есть только три пользователя, нуждающихся в доступе к приложениям, развернутых на ферме серверов узлов сеансов удаленных рабочих столов в головном офисе в другом городе, то проще будет установить приложения непосредственно на компьютер каждого пользователя или оптимизировать подключение RDP для использования канала связи WAN между филиалом и головным офисом. Развертывать оборудование серверного класса для удовлетворения потребностей трех пользователей есть смысл только в том случае, если это действительно необходимо для работы компании.

## Планирование программного обеспечения на сервере сеансов удаленных рабочих столов

Программы, которые будут использоваться клиентами, подключающимися к серверу узла сеансов удаленных рабочих столов, необходимо установить после развертывания этой роли сервера. Во время установки многие приложения проверяют, является ли целью установки сервер узла сеансов удаленных рабочих столов. Иногда для установки на сервер узла сеансов удаленных рабочих столов и на обычный компьютер используются разные исполняемые файлы. Некоторые приложения показывают диалоговое окно с сообщением о том, что установка приложения на сервер узла сеансов удаленных рабочих столов не рекомендуется, и поставщик не поддерживает данную конфигурацию развертывания.

Приложения, развертываемые на сервере узла сеансов удаленных рабочих столов, могут конфликтовать друг с другом. Прежде чем развертывать новую конфигурацию сервера узла сеансов в производственной среде, следует запланировать период тестирования. В течение этого периода следует организовать небольшую группу пользователей, которые будут использовать сервер узла сеансов удаленных рабочих столов для выполнения повседневных задач. Это позволит обнаружить возможные проблемы и конфликты перед развертыванием сервера в производственной среде. На занятии 2 в разделе «App-V» приводится более подробная информация о развертывании приложений, конфликтующих или несовместимых со стандартным развертыванием RDS.

## Лицензирование службы удаленных рабочих столов

Всем клиентам, подключающимся к серверу узла сеансов удаленных рабочих столов, требуется специальная лицензия — клиентская лицензия службы удаленных рабочих столов (RDS CAL). Эта лицензия не входит в состав Windows 7 и Windows Vista и не является частью стандартных лицензий CAL, используемых для лицензирования сервера. Лицензии RDS CAL управляются сервером лицензирования удаленных рабочих столов, который использует службу роли лицензирования удаленных рабочих столов.

Планируя развертывание сервера лицензирования удаленных рабочих столов, необходимо принять несколько решений, включая следующие:

- Какова область обнаружения сервера лицензирования?
- Как будет активироваться сервер лицензирования?
- Сколько требуется серверов лицензирования?
- Какой тип лицензий будет развертываться?

## Область обнаружения сервера лицензирования

Область обнаружения сервера лицензирования определяет, какие серверы и клиенты узла сеансов удаленных рабочих столов могут автоматически обнаруживать сервер лицензирования. Область обнаружения настраивается во время установки службы роли сервера лицензирования удаленных рабочих столов (рис. 6-1). В дальнейшем область можно изменить. Существует три области обнаружения:



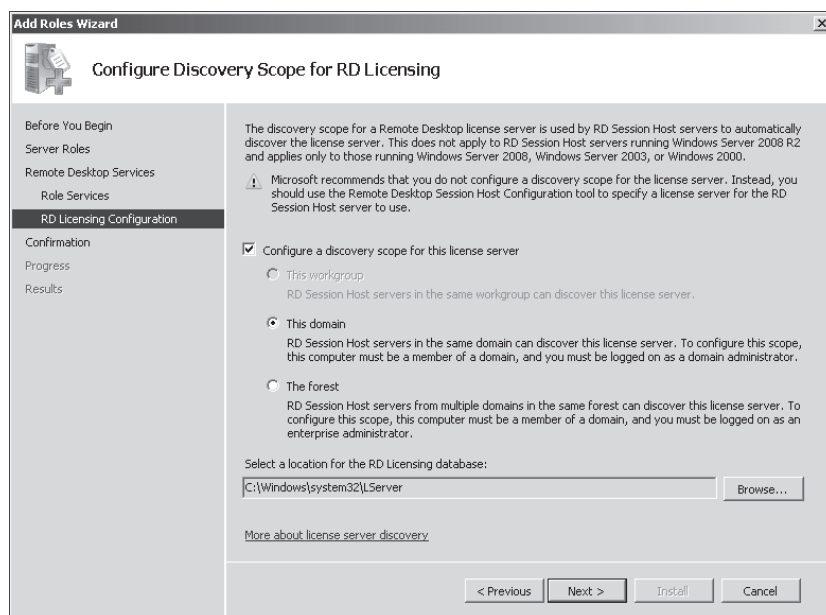


Рис. 6-1. Область обнаружения сервера лицензирования

- **Эта рабочая группа (This Workgroup).** Эта область недоступна, если компьютер присоединен к домену AD DS. Она чаще всего устанавливается на тот же компьютер, что и роль узла сеансов удаленных рабочих столов. Серверы и клиенты узла сеансов удаленных рабочих столов из выбранной рабочей группы могут автоматически обнаруживать этот сервер лицензирования.
- **Этот домен (This Domain).** Эта область обнаружения позволяет серверам и клиентам узла сеансов удаленных рабочих столов из указанного домена автоматически получать лицензии RDS CAL. Эта область наиболее полезна, если лицензии RDS CAL приобретаются для каждого домена.
- **Этот лес (This Forest).** Эта область обнаружения позволяет серверам и клиентам узла сеансов служб терминалов, расположенным в любом месте указанного леса AD DS автоматически получать лицензии RDS CAL. Недостаток этой области состоит в том, что в крупных лесах, включающих много доменов, лицензии RDS CAL невозможно купить незамедлительно. Microsoft рекомендует настраивать эту область организациям с централизованным управлением лицензиями.

## Активация сервера лицензирования

Прежде чем сервер лицензирования сможет выдавать лицензии CAL, его необходимо активировать в Microsoft способом, аналогичным Windows Product Activation. В процессе активации на сервер лицензирования удаленных рабочих столов устанавливается цифровой сертификат, выпущенный Microsoft (используемый для проверки владельцев и идентификации сервера). Этот сертификат будет использоваться в транзакциях с Microsoft для последующего приобретения и установки лицензий. Сервер лицензирования может активироваться тремя способами рис. (6-2).

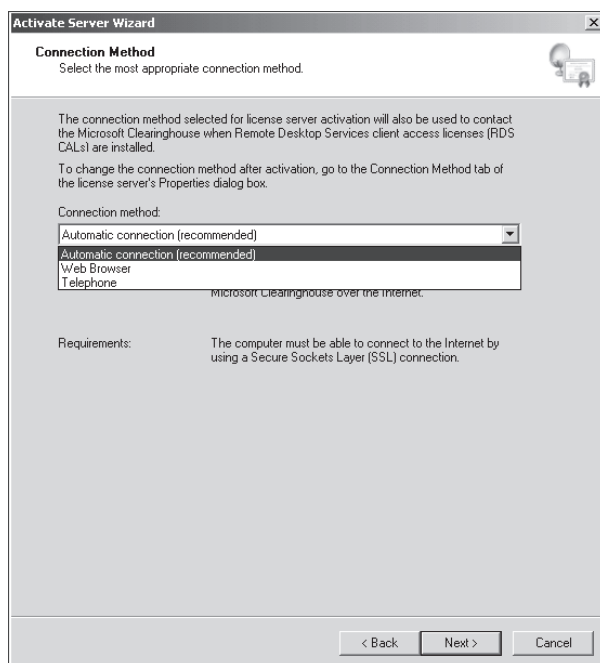


**Рис. 6-2.** Три способа активации сервера лицензирования удаленных рабочих столов

Первый способ выполняется прозрачно, с помощью мастера, аналогичного мастеру Windows Product Activation. Для его использования сервер должен иметь прямое подключение к Интернету через SSL. Следовательно, этот способ не работает с определенными конфигурациями брандмауэра. Второй способ предполагает переход к веб-странице. Его можно использовать на компьютере, не являющимся сервером лицензирования, и в сетях, не поддерживающих прямые SSL-подключения из внутренней сети.

Третий способ — телефонный звонок оператору расчетной палаты Microsoft (бесплатный из многих населенных пунктов). Этот способ можно применять также для проверки лицензий RDS CAL, приобретаемых позднее, хотя его можно изменить, отредактировав свойства сервера лицензирования удаленных рабочих столов. Если сервер не активирован, он может выдавать только временные лицензии, действительные в течение 90 дней.

Если сертификат, полученный в процессе активации, устаревает или будет поврежден, может потребоваться деактивация сервера лицензирования. Деактивированный сервер лицензирования не может выпускать постоянные лицензии для устройств, однако может продолжать выпускать пользовательские лицензии CAL и временные лицензии для устройств. Серверы лицензирования удаленных рабочих столов можно деактивировать автоматически или по телефону, но нельзя деактивировать их с помощью веб-браузера на другом компьютере.

## Клиентские лицензии удаленных рабочих столов

Сервер лицензирования удаленных рабочих столов под управлением Windows Server 2008 R2 может выдавать два типа лицензий CAL: лицензии «на устрой-

ство» и лицензии «на пользователя». Различия между этими лицензиями заключаются в следующем:

- **Клиентская лицензия «на устройство»** дает отдельному компьютеру или устройству возможность подключаться к серверу узла сеансов удаленных рабочих столов. Такие лицензии автоматически возвращаются сервером лицензирования по истечении произвольного периода от 52 до 89 дней. Это не влияет на работу клиентов, которые регулярно используют эти лицензии, потому что любая доступная лицензия CAL просто будет повторно выдана во время следующего подключения устройства. Если лицензии CAL кончились, 20% выданных лицензий «на устройство» для определенной операционной системы можно отозвать на сервере лицензирования с помощью консоли диспетчера лицензирования удаленных рабочих столов. Например, можно в любое время отозвать 20% лицензий CAL «на устройство», выданных для Windows 7, или 20% лицензий для Windows Vista. Отзыв не отменяет необходимости приобретения организацией необходимого количества лицензий CAL «на устройство».
- **Клиентская лицензия «на пользователя»** позволяет отдельной учетной записи пользователя получать доступ к любому серверу узла сеансов удаленных рабочих столов, имеющемуся в организации, с любого компьютера или устройства. Такие лицензии не применяются принудительно компонентом **Лицензирование удаленных рабочих столов**, поэтому в организации может быть больше клиентских подключений, чем лицензий «на пользователя», установленных на сервере лицензирования. Это не освобождает администраторов от выполнения условий лицензионного соглашения, требующих наличия действительной лицензии «на пользователя» для каждого пользователя. Определить число лицензий «на пользователя» можно с помощью консоли диспетчера лицензирования удаленных рабочих столов на сервере лицензирования. Для этого можно обратиться к узлу **Отчеты (Reports)** или использовать консоль для создания отчета.

Если сервер узла сеансов удаленных рабочих столов может подключаться к Интернету напрямую через SSL-соединение, можно приобретать лицензии CAL автоматически. Кроме этого, сразу после активации сервера узла сеансов удаленных рабочих столов можно приобрести лицензии CAL, используя отдельный компьютер, подключенный к Интернету, для обращения к сайту, или позвонить в расчетную палату Microsoft.

---

#### **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Лицензии RDS CAL**

Подробнее о лицензиях RDS CAL см. по адресу <http://technet.microsoft.com/ru-ru/library/cc753650.aspx>.

---

## **Резервное копирование и восстановление сервера лицензирования**

Для резервного копирования сервера лицензирования служб удаленных рабочих столов необходимо архивировать данные состояния системы и папку, в которой находится база данных компонента Лицензирование удаленных рабочих столов.

На странице **Обзор конфигурации** (Review Configuration) мастера добавления ролей можно посмотреть путь к базе данных Лицензирования удаленных рабочих столов. Для восстановления сервера лицензирования переустановите сервер, переустановите роль сервера лицензирования удаленных рабочих столов, восстановите данные состояния системы, а затем восстановите базу данных компонента Лицензирование удаленных рабочих столов. При восстановлении на другом компьютере невыпущенные лицензии не будут восстановлены, и для их пере выпуска необходимо связаться с расчетной палатой Microsoft.

## Развертывание серверов лицензирования

Планируя развертывание серверов узлов сеансов служб удаленных рабочих столов, работающих под управлением Windows Server 2008 R2, в среде, где работают службы терминалов, обратите внимание на то, что серверы лицензирования служб терминалов Windows Server 2003 и Windows 2000 Server не могут выпускать лицензии для серверов узла сеансов удаленных рабочих столов Windows Server 2008 R2 и серверов служб терминалов Windows Server 2008. Однако серверы узлов сеансов удаленных рабочих столов Windows Server 2008 R2 поддерживают более ранние версии RDS. Если при развертывании будет период, когда серверы служб терминалов будут существовать параллельно с серверами узлов сеансов удаленных рабочих столов Windows Server 2008 R2, в первую очередь следует обновить серверы лицензирования до Windows Server 2008 R2, чтобы они могли поддерживать как новые, так и существующие серверы.

### Проверьте себя

1. Какие клиентские лицензии служб удаленных рабочих столов могут отзываться?
2. Когда следует устанавливать приложения, которые будут использоваться клиентами на сервере узла сеансов служб удаленных рабочих столов?

### Ответы

1. Клиентские лицензии «на устройство».
2. После установки роли сервера узла сеансов удаленных рабочих столов.

## Настройка серверов узлов сеансов удаленных рабочих столов

При планировании развертывания серверов узлов сеансов удаленных рабочих столов следует знать, какие параметры конфигурации могут применяться на уровне сервера и на уровне протокола. По большей части, вас будут интересовать параметры конфигурации на уровне протокола. Чтобы редактировать параметры на уровне протокола, откройте консоль **Конфигурация узла сеансов удаленных рабочих столов** (Remote Desktop Session Host Configuration), которая находится в папке **Службы удаленного рабочего стола** (Remote Desktop

Services) в меню **Администрирование** (Administrative Tools), щелкните правой кнопкой мыши элемент **RDP-Тср** в секции **Подключения** (Connections) и выберите команду **Свойства** (Свойства). Откроется диалоговое окно свойств RDP-Тср.

На вкладке **Общие** (General) этого диалогового окна (рис. 6-3) можно настроить уровень безопасности (Security Layer), уровень шифрования (Encryption Level) и другие параметры безопасности соединения. По умолчанию выбран уровень безопасности **Согласование** (Negotiated) и уровень шифрования **Совместимый с клиентским** (Client Compatible). По умолчанию будет предпринята попытка согласовать наиболее высокий уровень безопасности и шифрования, однако администраторы могут выбрать определенный уровень. Клиенты, не соответствующие этому уровню, не смогут установить соединение с сервером узла сеансов удаленных рабочих столов. Клиенты под управлением Windows 7, Windows Vista, и Windows XP SP2+ могут устанавливать стандартные подключения к удаленным рабочим столам, когда выбран наивысший уровень параметров безопасности, хотя это правило не относится к подключениям RemoteApp, выполняемым посредством веб-доступа к удаленным рабочим столам. Подробнее об этом будет рассказано на занятии 2.

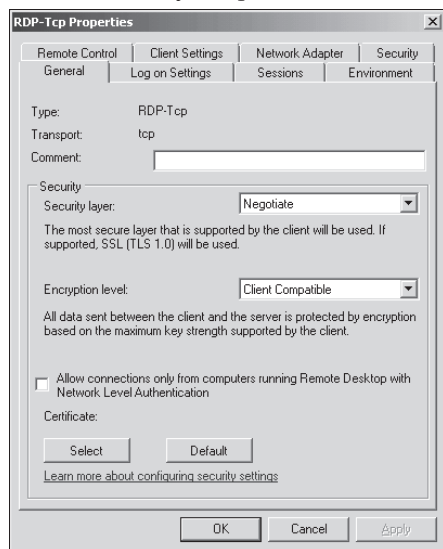


Рис. 6-3. Вкладка Общие диалогового окна свойств RDP-Тср

Параметры уровня безопасности используются для настройки аутентификации сервера, т.е. способа идентификации сервера перед клиентом. Это позволяет установить SSL-сертификат, выданный доверенным центром сертификации, в качестве метода идентификации сервера узла сеансов удаленных рабочих столов перед подключающимся клиентом. Используйте этот параметр, когда клиенты подключаются к серверу узла сеансов удаленных рабочих столов из ненадежных сетей, например, из Интернета. Проверка идентификации сервера узла сеансов удаленных рабочих столов снижает вероятность того, что пользователь из вашей организации предоставит учетные данные аутентификации поддельному серверу в результате фишинг-атаки. Хотя можно использовать

самозаверяющие сертификаты, сгенерированные сервером узла сеансов удаленных рабочих столов, это может привести к проблемам, если на клиентах SSL-сертификат сервера не указан как надежный.

Уровень шифрования устанавливается для защиты содержимого сервера узла сеансов удаленных рабочих столов от перехвата третьими лицами. Доступно четыре уровня:

- **Высокий (High)** — использует 128-битный ключ и поддерживается клиентами RDP 5.2 (Windows XP SP2+, Windows Server 2003 SP1+, Windows Vista, Windows 7, Windows Server 2008 и 2008 R2).
- **FIPS** — трафик шифруется по стандарту FIPS 140-1. В основном его используют правительственные организации.
- **Совместимый с клиентом (Client Compatible)** — согласовывает максимальную длину ключа с клиентом.
- **Низкий (Low)** — данные, отправляемые с клиента на сервер, шифруются с помощью 56-битного ключа; данные, отправляемые с сервера к клиенту, остаются незашифрованными.

На вкладке **Безопасность (Security)** диалогового окна свойств RDP-Тср можно указать, какие группы или пользователи имеют доступ к серверу узла сеансов удаленных рабочих столов, и какой уровень управления они имеют. На вкладке **Сеансы (Sessions)** (рис. 6-4) можно указать, как долго сервер позволяет подключениям оставаться активными, и что делать с бездействующими и отключенными сеансами. В средах, где каждый дополнительный сеанс создает значительную нагрузку на сервер, отключение бездействующих и завершенных сеансов является отличным способом управления ресурсами.

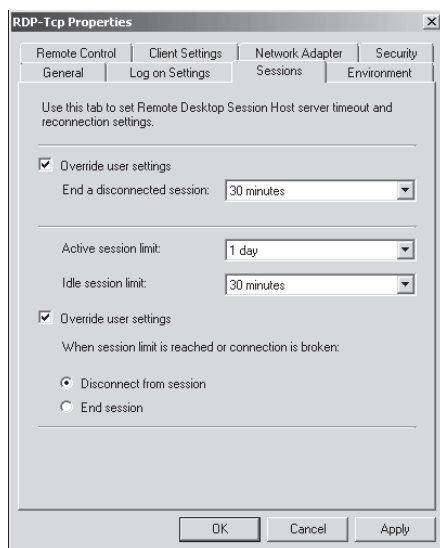


Рис. 6-4. Вкладка Сеансы диалогового окна свойств RDP-Тср

На вкладке **Удаленное управление (Remote Control)** диалогового окна свойств RDP-Тср можно указать, какой уровень управления подключенными сеансами имеет администратор. Можно выполнить настройку так, что сеансы

удаленного управления, используемые в основном персоналом службы поддержки, могут устанавливаться только в том случае, если пользователь разрешает персоналу службы поддержки подключение, аналогично тому, как это происходит при использовании удаленного помощника в Windows Vista и Windows 7. На вкладке **Сетевой адаптер** (Network Adapter) (рис. 6-5) можно ограничить число активных подключений к серверу узла сеансов удаленных рабочих столов и указать, какой сетевой адаптер клиенты будут использовать для подключения. Это важно, когда слишком большое число подключений может исчерпать аппаратные ресурсы сервера. Чтобы производительность сервера не уменьшалась настолько, чтобы доставлять пользователям неудобства, необходимо установить ограничение.

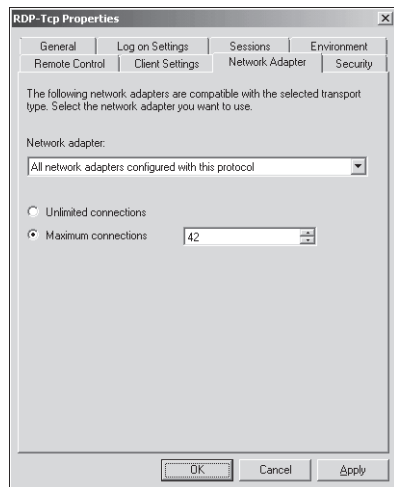


Рис. 6-5. Параметры сетевого адаптера

## Свойства сервера

Помимо свойств подключения RDP, описанных ранее, на работу клиента влияют также свойства каждого сервера узла сеансов удаленных рабочих столов. Как показано на рис. 6-6, сервер может использовать временные папки для каждого сеанса и удалять их после завершения сеанса. Можно также ограничить пользователя одним сеансом на сервере узла сеансов удаленных рабочих столов. Этот параметр важен, так как, если в параметрах подключения RDP не настроено отключение бездействующих сеансов, то пользователь может создать несколько бездействующих сеансов на сервере. Параметры из секции **Режим входа пользователя в систему** (User Logon Mode) используются, когда требуется отключить сервер узла сеансов удаленных рабочих столов для технического обслуживания. Например, если установить переключатель **Разрешить переподключения, но запретить новые попытки входа до перезагрузки сервера** (Allow Reconnections, But Prevent New Logons Until The Server Is Restarted), то можно отследить число активных подключений, а затем отключить сервер и выполнить техническое обслуживание, не прерывая работу пользователя.



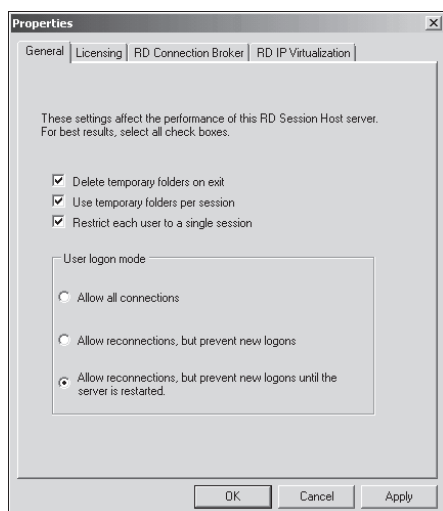


Рис. 6-6. Диалоговое окно свойства сервера узла сеансов удаленных рабочих столов

## Настройка удаленных рабочих столов с помощью групповой политики

Во время масштабного развертывания серверов узлов сеансов удаленных рабочих столов не нужно настраивать параметры подключений RDP-Тср и свойства сервера для каждого сервера в отдельности. Следует применять эти параметры с помощью AD DS. Узел групповой политики **Конфигурация компьютера | Политики | Административные шаблоны | Компоненты Windows | Услуги удаленных рабочих столов | Узел сеансов удаленных рабочих столов** (Computer Configuration | Policies | Administrative Templates | Windows Components | Remote Desktop Services | RD Session Host server) содержит несколько политик, функциональность которых отражает параметры, которые можно применить на сервере. Так как политик очень много велико, здесь о них будет рассказано лишь кратко.

- **Подключения (Connections).** Этот узел содержит следующие политики: **Автоматическое переподключение (Automatic Reconnection)**, **Разрешать удаленное подключение с использованием служб удаленных рабочих столов (Allow Users To Connect Remotely Using Remote Desktop Services)**, **Запретить завершение консольного сеанса администратора (Deny Logoff Of An Administrator Logged In To The Console Session)**, **Настроить интервал проверки активности подключения (Configure Keep-Alive Connection Interval)**, **Ограничить количество подключений (Limit Number Of Connections)**, **Устанавливает правила удаленного управления для пользователей сеансов служб удаленных рабочих столов (Set Rules For Remote Control Of Remote Desktop Services User Sessions)**, **Разрешать переподключение только с исходного клиента (Allow Reconnection From Original Client Only)**, **Ограничить пользователей службы удаленных рабочих столов одним сеансом служб удаленных рабочих столов (Restrict Remote Desktop Services Users To A**

Single Remote Session), **Разрешать удаленный запуск любых программ** (Allow Remote Start Of Unlisted Programs) и **Отключить планирование ЦП со справедливым разделением** (Turn of Fair Share CPU Scheduling).

- **Перенаправление устройств и ресурсов** (Device And Resource Redirection). Этот узел содержит следующие политики: **Разрешать перенаправление воспроизведения звука и видео** (Allow Audio Redirection), **Не разрешать перенаправление буфера обмена** (Do Not Allow Clipboard Redirection), **Не разрешать перенаправление СОМ-портов** (Do Not Allow COM Port Redirection), **Не разрешать перенаправление дисков** (Do Not Allow Drive Redirection), **Не разрешать перенаправление LPT-портов** (Do Not Allow LPT Port Redirection), **Не разрешать перенаправление поддерживаемых устройств Plug and Play** (Do Not Allow Supported Plug And Play Device Redirection), **Не разрешать перенаправление устройства чтения смарт-карт** (Do Not Allow Smart Card Device Redirection) и **Разрешить перенаправление часового пояса** (Allow Time Zone Redirection).
- **Лицензирование** (Licensing). Этот узел содержит следующие политики: **Использовать указанные серверы лицензирования удаленных рабочих столов** (Use The Specified Remote Desktop License Servers), **Скрывать уведомления о проблемах лицензирования удаленных рабочих столов, оказывающих влияние на сервер узла сеансов удаленных рабочих столов** (Hide Notifications About RD Licensing Problems That Affect The RD Session Host Server) и **Задать режим лицензирования узла сеансов удаленных рабочих столов** (Set The Remote Desktop Services Licensing Mode).
- **Перенаправление принтеров** (Printer Redirection). Этот узел содержит следующие политики: **не устанавливать используемый по умолчанию принтер клиента в качестве принтера для сеанса** (Do Not Set Default Client Printer To Be Default Printer In A Session), **Не разрешать перенаправление клиентских принтеров** (Do Not Allow Client Printer Redirection), **Задать поведение сервера узла сеансов удаленных рабочих столов при выборе резервного драйвера принтера** (Specify RD Session Host Server Fallback Printer Driver Behavior), **Использовать в первую очередь драйвер принтера Easy Print удаленного рабочего стола** (Use Remote Desktop Services Easy Print Printer Driver First) и **Перенаправлять только используемый по умолчанию принтер клиента** (Redirect Only The Default Client Printer).
- **Profiles** (Профили). Этот узел содержит следующие политики: **Установить домашний каталог пользователя служб удаленных рабочих столов** (Set Remote Desktop Services User Home Directory), **Использовать обязательные профили на сервере узла сеансов удаленных рабочих столов** (Use Mandatory Profiles On The RD Session Host Server) и **Задать путь для перемещаемого профиля пользователя служб удаленных рабочих столов** (Set Path For Remote Desktop Services Roaming User Profile).
- **Среда удаленных сеансов** (Remote Session Environment). Этот узел содержит следующие политики: **Наибольшая глубина цвета** (Limit Maximum Color Depth), **Принудительная отмена фоновой рисунка удаленного рабочего стола** (Enforce Removal Of Remote Desktop Wallpaper), **Удалить элемент**

«Отключение сеанса» из диалога завершения работы (Remove Disconnect Option From Shut Down Dialog Box), Удалить элемент «Безопасность Windows» из меню «Пуск» (Remove Windows Security Item From Start Menu), Задание алгоритма сжатия для данных RDP (Set Compression Algorithm For RDP Data), Запуска программу при подключении (Start A Program On Connection) и Всегда отображать рабочий стол при подключении (Always Show Desktop On Connection).

- **Безопасность (Security).** Этот узел содержит следующие политики: **Шаблон сертификата проверки подлинности сервера** (Server Authentication Certificate Template), **Установить уровень шифрования для клиентских подключений** (Set Client Connection Encryption Level), **Всегда запрашивать пароль при подключении** (Always Prompt For Password Upon Connection), **Требовать безопасное RPC-подключение** (Require Secure RPC Communication), **Требовать использования специального уровня безопасности для удаленных подключений по методу RDP** [Require Use Of Specific Security Layer For Remote (RDP) Connections], **Не разрешать локальным администраторам настраивать разрешения** (Do Not Allow Local Administrators To Customize Permissions) и **Требовать проверку подлинности пользователя для удаленных подключений путем проверки подлинности на уровне сети** (Require User Authentication For Remote Connections By Using Network Level Authentication).
- **Ограничение сеансов по времени (Session Time Limits).** Этот узел содержит следующие политики: **Задать ограничение по времени для отключенных сеансов** (Set Time Limit For Disconnected Sessions), **Задать ограничение времени для активных, но бездействующих сеансов служб удаленных рабочих столов** (Set Time Limit For Active But Idle Remote Desktop Services Sessions), **Задать ограничение по времени для активных сеансов служб удаленных рабочих столов** (Set Time Limit for Active Remote Desktop Services Sessions), **Завершать сеанс при достижении ограничения по времени** (Terminate Session When Time Limits Are Reached) и **Задать предел времени для выхода из сеансов RemoteApp** (Set Time Limit For Logoff Of RemoteApp Sessions).
- **Временные папки (Temporary Folders).** Этот узел содержит следующие политики: **Не удалять временные папки при выходе** (Do Not Delete Temp Folder Upon Exit) и **Не использовать временные папки для сеанса** (Do Not Use Temporary Folders Per Session).
- **Посредник подключений к удаленному рабочему столу (RD Connection Broker).** Политики из этого узла описаны в разделе «Посредник подключений к удаленному рабочему столу» далее на этом занятии.

Поначалу этот список может показаться пугающим, но он нужен здесь лишь для того, чтобы дать представление о том, как оптимально настроить службы удаленных рабочих столов в соответствии с требованиями, предъявляемыми организацией, а не вовсе для того, чтобы учить его наизусть к экзамену. Ознакомьтесь со списком и подумайте, как каждая политика может повлиять на число обслуживаемых клиентов и на число серверов узлов сеансов удаленных

рабочих столов, которые требуется развернуть. Одни политики не имеют отношения к этим вопросам, другие же, наоборот, очень важны.

Для администратора, планирующего развертывание служб удаленных рабочих столов, наиболее важны группы политик из узлов **Подключения** и **Ограничение сеансов по времени**. С помощью этих политик можно регулировать число клиентов, подключенных к каждому серверу, и длительность подключения. Оба параметра непосредственно влияют на производительность сервера узла сеансов удаленных рабочих столов. Если позволить множеству бездействующих сеансов занимать память, то может потребоваться развертывание дополнительных серверов, так как имеющиеся быстро исчерпают свои ресурсы. Если ограничить время бездействия сеансов, ресурсы не будут расходоваться впустую, однако при этом может быть нарушен режим работы пользователей. Как и все, что касается развертывания и планирования, для установки правильных параметров необходимо найти уникальный для конкретных условий компромисс.

## Веб-доступ к удаленным рабочим столам

Веб-доступ к удаленным рабочим столам позволяет клиентам подключаться к серверу узла сеансов удаленных рабочих столов по ссылке на веб-страницу, а не вводить адрес в клиентской программе Подключение к удаленным рабочим столам (RDC). В отличие от аналогичной функциональности Windows Server 2003, для веб-доступа в Windows Server 2008 R2 используются не элементы управления ActiveX, обеспечивающие подключение к удаленным рабочим столам, а клиентское ПО RDC, установленное на клиентах. Это означает, что для использования веб-доступа к удаленным рабочим столам клиенты должны работать под управлением Windows XP SP2, Windows Vista, Windows 7, Windows Server 2003 SP1, Windows Server 2008 или 2008 R2. Для развертывания веб-доступа к удаленным рабочим столам необходимо установить не только роль сервера веб-доступа, но и роль веб-сервера (IIS), а также компонент Служба активации процессов Windows (Windows Process Activation Service).

## Посредник подключений к удаленному рабочему столу

Один сервер узла сеансов удаленных рабочих столов может поддерживать только ограниченное число клиентов, сверх которого ресурсы заканчиваются, и работа клиентов ухудшается. Точное число будет зависеть от выполняемых клиентами приложений и задач, а также от аппаратной конфигурации сервера. В конечном итоге, с увеличением числа клиентов понадобится добавить второй сервер, чтобы разгрузить первый. С точки зрения планирования, это вполне очевидно, однако при этом возникает вопрос: «Как обеспечить равномерное распределение нагрузки между новым и старым серверами?» Если все перейдут на новый сервер, у него скоро появятся те же проблемы из-за нехватки ресурсов, что и у старого сервера. Служба роли посредника подключений к удаленному рабочему столу упрощает процесс добавления ресурсов, обеспечивая распределение нагрузки между группой серверов узлов сеансов удаленных рабочих столов и повторное подключение клиентов к существующим сеансам внутри этой группы. В терминологии посредника подключений группа серверов узлов сеансов удаленных рабочих столов называется фермой.

Служба посредника подключений к удаленному рабочему столу имеет базу данных для отслеживания сеансов. Посредник подключений может работать в сочетании с циклическим обслуживанием DNS и средствами балансировки нагрузки (NLB), распределяя клиентов по серверам узлов сеансов удаленных рабочих столов. При сочетании с балансировкой нагрузки служба посредника подключения следит за всеми серверами узлов сеансов удаленных рабочих столов, входящими в группу, и распределяет новых клиентов по серверам с наибольшим числом свободных ресурсов. Клиенты распределяются и в сочетании с циклическим обслуживанием DNS. При этом главное преимущество состоит в том, что посредник подключений помнит, куда подключен клиент, и вместо создания нового сеанса на другом сервере отключенный сеанс повторно подключается к тому же серверу. Ограничение в работе посредника подключений в том, что его можно использовать только с серверами узлов сеансов удаленных рабочих столов Windows Server 2008 R2 и серверами служб терминалов Windows Server 2008. Серверы служб терминалов Windows Server 2003 не могут входить в ферму посредника подключений к удаленным рабочим столам.

Для развертывания балансировки нагрузки посредника подключений к удаленным рабочим столам необходимо убедиться, что клиенты поддерживают протокол RDP 5.2 или выше. Посредник подключений поддерживает также параметры режима входа в систему, описанные выше. С помощью этих параметров можно запрещать новые подключения к определенному серверу фермы до завершения технического обслуживания.

Присоединить сервер узла сеансов удаленных рабочих столов к ферме можно с помощью консоли MMC RDS, расположенной в папке **Службы удаленного рабочего стола** (Remote Desktop Services) в меню **Администрирование** (Administrative Tools). Для присоединения к ферме требуется указать адрес сервера посредника подключений, имя фермы, условие участия сервера в балансировке нагрузки, а также относительный вес сервера (на основе его производительности) в ферме. Для более мощных серверов следует указывать больший относительный вес, чем для менее мощных. Параметр Перенаправление IP-адресов следует отключать лишь в том случае, если используются маркеры маршрутизации посредника подключений к удаленным рабочим столам, применяемые в аппаратных решениях балансировки нагрузки, что означает, что сервер с ролью посредника подключений не управляет балансировкой нагрузки. Как уже говорилось, эти параметры конфигурации можно применять также с помощью групповой политики. В Windows Server 2008 R2 соответствующие политики находятся в узле **Конфигурация компьютера | Политики | Административные шаблоны | Компоненты Windows | Узел сеансов удаленных рабочих столов | Посредник подключений к удаленному рабочему столу** (Computer Configuration | Policies | Administrative Templates | Windows Components | Remote Desktop Services | RD Session Host server | RD Connection Broker) объекта групповой политики.

При использовании этих параметров конфигурации необходимо добавить учетную запись сервера узлов сеансов удаленных рабочих столов в локальную группу **Компьютеры каталога сеансов** (Session Directory Computers) на компьютере, где находится служба посредника подключений к удаленному рабочему столу. После этого можно настроить функцию балансировки нагрузки на каждом компьютере фермы.

---

**ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ** Посредник подключений к удаленному рабочему столу

Подробнее о посреднике подключений к удаленному рабочему столу см. по адресу [http://technet.microsoft.com/ru-ru/library/dd560675\(W5.10\).aspx](http://technet.microsoft.com/ru-ru/library/dd560675(W5.10).aspx).

---

## Сервер шлюза удаленных рабочих столов

Серверы шлюза удаленных рабочих столов позволяют предоставлять доступ к серверам узлов сеансов удаленных рабочих столов клиентам, не входящим во внутреннюю сеть вашей организации, без использования виртуальных частных сетей (VPN) или DirectAccess. Подробнее о серверах шлюзов удаленных рабочих столов рассказывается в гл. 9. Сейчас скажем только, что одной из важных особенностей сервера шлюза удаленных рабочих столов является возможность его интеграции с защитой доступа к сети (NAP). Это гарантирует, что клиенты, подключающиеся к серверам узлов сеансов удаленных рабочих столов, удовлетворяют определенным минимальным требованиям к работоспособности. Это может пригодиться, когда необходимо предоставлять доступ клиентам, которыми вы не управляете, но которые нуждаются в доступе к серверам узлов сеансов рабочих столов.

---

**ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ** Сервер шлюза удаленных рабочих столов

Подробнее о серверах шлюза удаленных рабочих столов см. по адресу <http://technet.microsoft.com/ru-ru/library/cc725706.aspx>.

---

## Узел виртуализации удаленных рабочих столов

Узел виртуализации удаленных рабочих столов — роль, впервые появившаяся в Windows Server 2008 R2. Этот узел позволяет клиентам использовать удаленный рабочий стол для подключения к персональным виртуальным машинам, работающим на хостах Hyper-V в Windows Server 2008 R2. Этот тип виртуализации позволяет назначить каждому пользователю индивидуальную виртуальную машину, к которой можно обращаться через удаленный рабочий стол. Виртуализация рабочего стола или сервера не имеет прямого отношения к замене 70-646.

---

**ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ** Узел виртуализации удаленных рабочих столов

Подробнее об узле виртуализации удаленных рабочих столов см. по адресу <http://technet.microsoft.com/ru-ru/library/dd759193.aspx>.

---

## Мониторинг служб удаленных рабочих столов

Необходимо регулярно проводить мониторинг серверов узла сеансов удаленных рабочих столов, следя за тем, чтобы пользовательский интерфейс работал исправно, а у сервера оставалось достаточно ресурсов для нормального функционирования. Чаще всего слабыми местами в оборудовании серверов оказываются ресурсы процессора и память. Во время мониторинга этим ресурсам следует уделять особое внимание. Несмотря на то, что ресурсы сервера можно оценить заранее, до начала работы клиентов невозможно узнать, какую нагрузку может принять сервер, прежде чем производительность станет ухудшаться. Для управ-



ления и мониторинга ресурсов сервера узлов сеансов удаленных рабочих столов используется два инструмента: Системный монитор и Диспетчер системных ресурсов Windows.

## Использование монитора производительности для наблюдения за службами удаленных рабочих столов

В дополнение к стандартным инструментам мониторинга Windows Server 2008 R2, системный монитор имеет счетчики производительности, специфичные для серверов узлов удаленных рабочих столов, помогающие определять уровень нагрузки, создаваемой текущими сеансами клиентов на сервере, где они размещены. Есть две широкие категории счетчиков: Службы удаленных рабочих столов (Remote Desktop Services) и Сеансы служб удаленных рабочих столов (Remote Desktop Services Sessions). Первая категория включает число активных, неактивных и общее число сеансов. Вторая категория включает подробную информацию об использовании ресурсов. Эту категорию можно использовать для слежения за использованием памяти и процессора и для получения сведений, помогающих в решении проблем, таких как число ошибок фреймов и успешных обращений к кэшу протокола.

## Диспетчер системных ресурсов

Диспетчер системных ресурсов (WSRM) — компонент, который можно установить в Windows Server 2008 R2 и использовать для управления распределением ресурсов. Консоль WSRM (рис. 6-7) позволяет администратору применять политики WSRM. WSRM по умолчанию включает четыре политики и позволяет администратору создавать собственные. При планировании и развертывании инфраструктуры служб удаленных рабочих столов наибольший интерес представляют политики Equal\_Per\_User, Weighted\_Remote\_Session, и Equal\_Per\_Session.

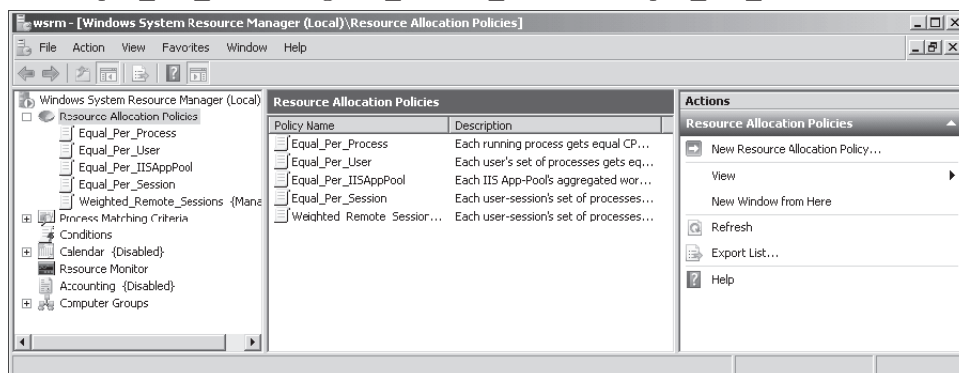


Рис. 6-7. Консоль WSRM

Политика WSRM Equal\_Per\_User обеспечивает равное выделение ресурсов всем пользователям, даже если какой-то пользователь имеет дополнительные сеансы, подключенные к серверу узлов сеансов служб удаленных рабочих столов. Применяйте эту политику, когда разрешаете пользователям иметь несколько сеансов на сервере узлов сеансов удаленных рабочих столов, чтобы предотвратить монополизацию одним пользователем аппаратных ресурсов путем открытия нескольких сеансов. Политика Weighted\_Remote\_Sessions позволяет



группировать процессы в соответствии с приоритетом, назначенным учетной записи пользователя. Политика Equal\_Per\_Session обеспечивает равное выделение ресурсов каждому сеансу. Если эта политика применяется к серверу, разрешающему подключение нескольких сеансов, пользователи могут получать неравные доли системных ресурсов.

---

**ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ** Диспетчер системных ресурсов и узел сеансов удаленных рабочих столов

Подробнее об использовании WSRM для узлов сеансов удаленных рабочих столов см. по адресу <http://technet.microsoft.com/en-us/library/cc742814.aspx>.

---

## Резюме

- Перед установкой клиентских лицензий CAL служб удаленных рабочих столов необходимо активировать серверы лицензирования удаленных рабочих столов. Область обнаружения сервера лицензирования определяет, какие клиенты и серверы узлов сеансов удаленных рабочих столов могут обнаруживать сервер автоматически.
- Посредник подключений к удаленному рабочему столу позволяет создавать фермы серверов узлов удаленных рабочих столов. Посредник подключений можно использовать в сочетании с циклическим обслуживанием DNS и балансировкой сетевой нагрузки. Он гарантирует, что отключенные клиенты будут всегда повторно подключаться к нужному сеансу на соответствующем сервере.
- Веб-доступ к удаленным рабочим столам позволяет клиентам подключаться к серверу узлов сеансов удаленных рабочих столов с помощью ссылки на веб-страницу, но все равно требует установки последней версия клиента удаленного рабочего стола.
- Сервер шлюза удаленных рабочих столов позволяет клиентам из Интернета подключаться к серверам узлов сеансов удаленных рабочих столов, расположенных за брандмауэром, без применения VPN.

## Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных на занятии 1. Эти вопросы предоставлены также в электронном виде на прилагаемом к книге компакт-диске.

---

**ПРИМЕЧАНИЕ** Ответы

Ответы на вопросы и пояснения к их вариантам размещены в разделе «Ответы» в конце книги.

---

1. Ваша организация имеет один сервер узлов сеансов удаленных рабочих столов. Пользователям разрешено подключаться к этому серверу с двумя сеансами. Вы хотите, чтобы пользователи, имеющие два сеанса, использовали не больше ресурсов сервера, чем пользователи с одним сеансом. Что следует сделать?
  - а. Применить политику WSRM Equal\_Per\_User.

- b. Применить политику WSRM Equal\_Per\_Session.
  - c. Настроить свойства сервера в консоли управления сервером узлов сеансов удаленных рабочих столов.
  - d. Настроить свойства RDP-тср.
2. Ваша организация имеет два офиса: в Сиднее и в Мельбурне. Серверы инфраструктуры расположены в центре обработки данных в Канберре. Офисы в Мельбурне и Сиднее имеют собственные фермы серверов узлов сеансов удаленных рабочих столов. Офисы соединены высокоскоростным каналом WAN. У каждого офиса есть собственный домен AD DS, входящий в один и тот же лес. Корневой домен леса расположен в центре обработки данных в Канберре и не содержит стандартных учетных записей пользователей и компьютеров. В связи с производственной необходимостью вы хотите, чтобы клиентские лицензии, приобретенные и установленные в каждом офисе, выделялись только устройствам из этого офиса. Каким будет план развертывания серверов лицензирования?
- a. Развернуть сервер лицензирования в каждом расположении и настроить на каждом сервере область обнаружения Домен.
  - b. Развернуть сервер лицензирования в каждом расположении и настроить на каждом сервере область обнаружения Лес.
  - c. Развернуть сервер лицензирования в центре обработки данных в Канберре и настроить на каждом сервере область обнаружения Лес.
  - d. Развернуть сервер лицензирования в центре обработки данных в Канберре и настроить на каждом сервере область обнаружения Домен.
3. Что следует сделать перед установкой клиентских лицензий на сервер лицензирования удаленных рабочих столов? (Каждый ответ является частью решения. Выберите все подходящие.)
- a. Выбрать область сервера лицензирования.
  - b. Установить функциональный уровень домена Windows Server 2008 R2.
  - c. Активировать сервер лицензирования.
  - d. Выбрать тип лицензии.
4. Организация, в которой вы работаете, переживает период роста. Пользователи имеют доступ к бизнес-приложениям с клиентских терминалов. Вы беспокоитесь, что рост числа пользователей будет опережать вычислительную мощность используемого сервера узлов сеансов удаленных рабочих столов. Какое из следующих решений позволит увеличить производительность клиентов без и перенастройки?
- a. Использовать WSRM, чтобы все пользователи имели равный доступ к ресурсам.
  - b. Установить Hyper-V на компьютер под управлением Windows Server 2008 R2 Enterprise и по мере необходимости добавлять виртуализованные серверы.
  - c. При необходимости добавить серверы узлов сеансов удаленных рабочих столов и перенастроить клиенты для использования определенных серверов.

- d. Создать ферму серверов узлов сеансов удаленных рабочих столов и по мере необходимости добавлять в нее серверы.
- 5. Вы хотите, чтобы все клиенты, подключающиеся к вашим серверам узлов сеансов удаленных рабочих столов, проходили проверку работоспособности. Какой из предложенных вариантов развертывания вы примените?
  - a. Установить на серверы узлов сеансов удаленных рабочих столов Forefront Endpoint Protection.
  - b. Использовать посредник подключений.
  - c. Опосредовать доступ с помощью сервера шлюза служб терминалов.
  - d. Опосредовать доступ с помощью Microsoft ISA Server 2006.

## Занятие 2. Развертывание и виртуализация приложений

На этом занятии рассматривается развертывание и виртуализация приложений. Существует несколько способов развертывания приложения. Наиболее популярный — использование групповой политики. Также на этом занятии рассматриваются действия, которые необходимо выполнить, чтобы развернуть веб-приложения на серверах IIS 7.0 или IIS 7.5. Виртуализация приложений (Application Virtualization, App-V) — это процесс, в котором приложение работает локально в своей собственной среде, но при этом оно не установлено на локальном компьютере. При запуске приложения в его собственной среде не происходит конфликтов, так как для каждой операционной системы или приложения создается эквивалент собственной изолированной среды. Также на этом занятии рассказывается о RemoteApp, особом типе технологии виртуализации представлений, позволяющем запускать приложения удаленных рабочих столов вне стандартного окна удаленных рабочих столов.

---

**Изучив материал этого занятия, вы сможете:**

- ✓ Планировать развертывание App-V.
- ✓ Планировать развертывание виртуальных приложений.
- ✓ Планировать развертывание веб-приложений.

**Продолжительность занятия — примерно 60 мин.**

---

### Традиционное развертывание приложений

Традиционное развертывание приложений подразумевает локальную установку программных файлов для приложения на рабочую станцию пользователя. Это можно сделать напрямую, путем запуска установочной программы вручную. В крупных сетях это обычно выполняется автоматически, сетевым процессом установки без прямого вмешательства человека. Во многих организациях приложения встроены в образ операционной системы.

Когда необходимо обновить приложения, локально установленные на компьютерах, необходимо развернуть эти обновления для каждого клиента, имеющего копию приложения. Традиционные приложения чаще всего развертыва-

ются в процессе развертывания образа операционной системы. Создается образ, содержащий приложения, и этот образ применяется непосредственно к компьютерам пользователей.

Обычно, приложения поставляются в виде исполняемых файлов или пакетов установщика Windows. Пакетами установщика Windows (имеют расширение .msi), легче управлять, поскольку они содержат информацию, которую компьютер может использовать не только для установки пакета, но и для исправления или удаления пакета. Иногда бывает сложно удалить или исправить приложение, установленное с помощью традиционного исполняемого файла, такого как Setup.exe, особенно, когда вы имеете дело с сотнями, а то и тысячами компьютеров.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ    Установщик Windows

Подробнее об установщике Windows см. по адресу [http://technet.microsoft.com/en-us/library/dd316071\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd316071(WS.10).aspx) (на англ. языке).

---

Можно использовать AD DS в качестве метода отправки приложений клиентам, однако это возможно только в том случае, если приложение уже упаковано в формате установщика Windows. Развертывание приложений с помощью групповой политики имеет следующие условия:

- После публикации приложения пользователи могут использовать апплет **Установка и удаление программ** (Add Or Remove Programs), чтобы установить приложение вручную. Можно также связать приложение с определенным типом документа, чтобы оно устанавливалось автоматически, когда пользователь пытается открыть документ такого типа.
- Если приложение назначено, оно установится на компьютер во время его следующей загрузки. Когда приложение присваивается пользователю, оно устанавливается на компьютер при следующем входе этого пользователя в систему.
- Если требуется развернуть приложения, которые еще не упакованы и имеют другой формат, например, .exe, используйте специальные инструменты, такие как System Center Essentials 2010 или System Center Configuration Manager 2007 R3.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ    Развертывание ПО с помощью групповой политики

Подробнее о развертывании ПО с помощью групповой политики см. по адресу <http://support.microsoft.com/kb/816102>.

---

## Развертывание веб-приложений

Веб-сайт является контейнером для веб-приложений. Веб-приложения представляют собой набор содержимого, сценариев и исполняемых файлов, предоставляющих пользователю какую-то функциональность. Веб-приложения хранятся на сервере файлов под управлением Windows Server 2008 R2 в собственных директориях, содержащих эти файлы, сценарии и исполняемые файлы. Большинство организаций создают и обновляют свои веб-приложения в среде разработки, прежде чем развернуть их приложения на веб-серверы приложений.

С точки зрения планирования это означает, что необходима стратегия для развертывания веб-приложений из среды разработки на рабочих веб-серверах.

В целом, развертывание веб-приложений — это перемещение набора файлов и директорий из папок на одном сервере IIS в точно такое же расположение на другом сервере IIS. Несмотря на то, что перемещение файлов с одного сервера на другой при помощи Robocopy.exe не представляет сложности, организациям необходимо учитывать следующее:

- Производственные серверы обычно расположены на периметре сети, в то время как серверы разработки почти всегда размещены во внутренних сетях.
- Производственные серверы обычно являются автономными системами, а не членами доменов. Серверы разработки могут входить или не входить в домен, однако у них есть отдельные базы данных учетных записей с производственных серверов.
- Производственные серверы защищены брандмауэрами. Администраторы вряд ли захотят размещать на периметре сети общий каталог, в который пользователи смогут вести запись.

Есть два основных метода, с помощью которых веб-приложения публикуются на серверах IIS:

- с помощью WebDAV;
- с помощью FTP.

## WebDAV в Windows Server 2008 R2

Протокол WebDAV (Web Distributed Authoring And Versioning) позволяет публиковать содержимое через брандмауэр, используя протокол HTTP или HTTPS. Благодаря этому данный протокол отлично подходит для развертывания веб-приложений с сервера разработки внутренней сети на производственном сервере на периметре сети. Сайты, поддерживающие WebDAV, могут храниться как сетевые расположения в Проводнике или открываться как веб-папки в Internet Explorer на компьютерах под управлением Windows XP, Windows 7, Windows Vista, Windows Server 2003, Windows Server 2008 и Windows Server 2008 R2.

WebDAV поддерживает те же протоколы аутентификации, что и IIS, поэтому не стоит опасаться, что учетные данные будут передаваться на сервер незашифрованными. В качестве дополнительной меры безопасности WebDAV поддерживает SSL-соединения. Протокол WebDAV не был включен в версию RTM Windows Server 2008, однако он есть в составе Windows Server 2008 R2 в качестве службы роли. Параметры WebDAV настраиваются для каждого сайта в диспетчере IIS (рис. 6-8).

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Установка и настройка WebDAV

Подробнее об установке и настройке WebDAV см. на официальном сайте Microsoft IIS: <http://learn.iis.net/page.aspx/350/installing-andconfiguring-webdav-on-iis-7> (на англ. языке).

---

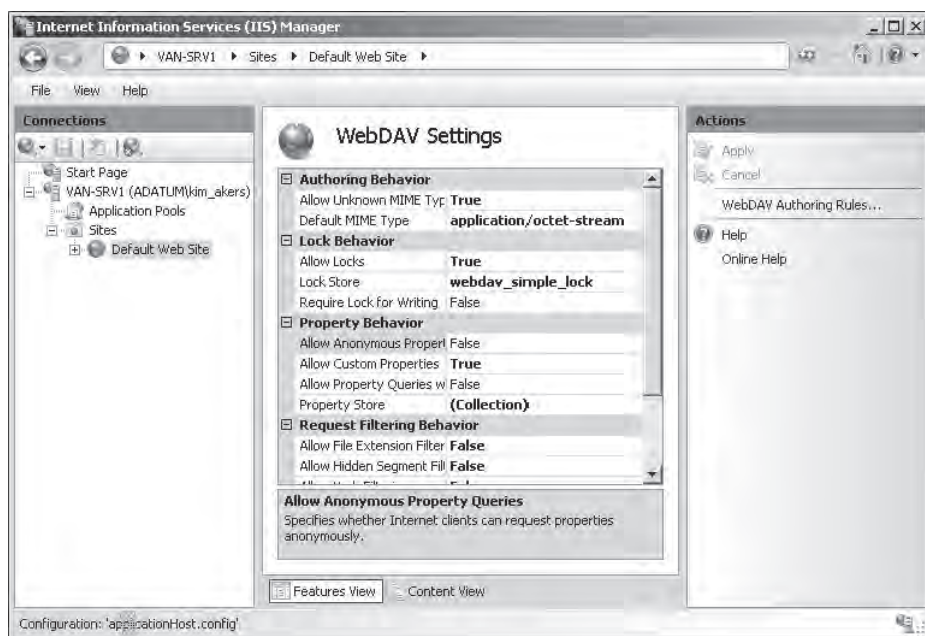


Рис. 6-8. Параметры WebDAV

## FTP 7.5 в Windows Server 2008 R2

FTP (File Transfer Protocol) — протокол, традиционно используемый для публикации содержимого на веб-сайтах. Windows Server 2008 R2 поддерживает FTP 7.5. Эта версия была доступна в качестве дополнения для IIS 7.0 в Windows Server 2008, однако она имеет ряд важных отличий от версии FTP 7.0, по умолчанию устанавливаемой в Windows Server 2008. Одно из главных отличий: FTP 7.5 поддерживает SSL. FTP позволяет передавать файлы и папки с одного сервера на другой, а также на многочисленные клиенты FTP, включая клиент командной строки, имеющийся во всех версиях Windows. Все это означает, что вы почти всегда можете опубликовать содержимое на веб-сервере, если тот поддерживает FTP. Главное — сопоставить FTP-сайт с веб-сайтом, чтобы содержимое можно было разворачивать в папки сайта. Управление FTP 7.5 осуществляется посредством диспетчера IIS. Инструменты управления FTP изображены на рис. 6-9.

В качестве дополнительной меры безопасности можно установить ограничения на IP-адреса и имена доменов, чтобы ограничить количество хостов, которые могут подключаться к серверу. Например, можно создать ограничение, чтобы содержимое могло передаваться только через FTP, и только если подключающийся хост находится на сервере разработки, а не с любого хоста внутренней сети. Можно также настроить правило брандмауэра, которое позволяет FTP-трафику требовать аутентификации от подключающегося хоста, хотя это выходит за рамки действий большинства администраторов, желающих обезопасить FTP-сервер, чтобы тот принимал трафик только от хостов из внутренней сети.

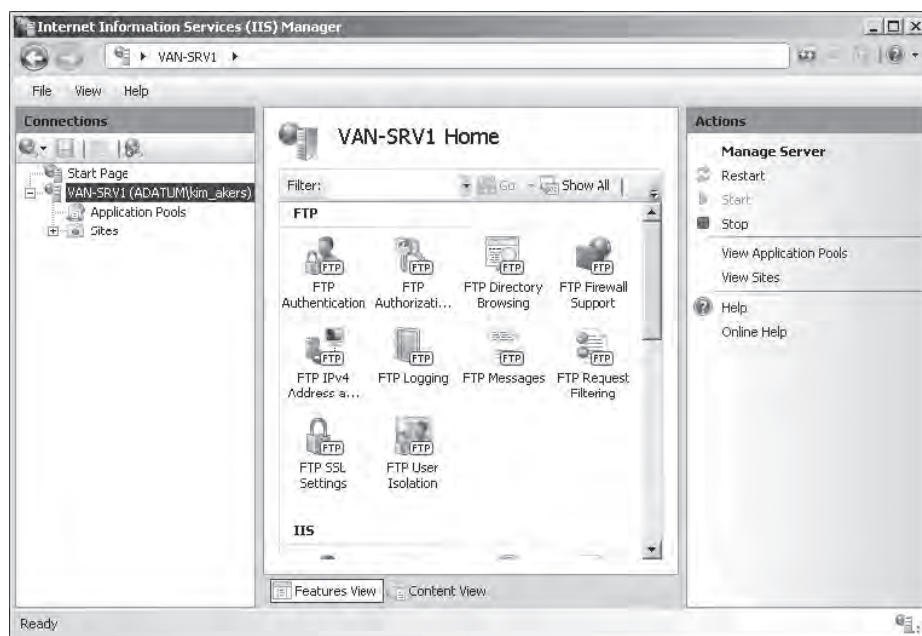


Рис. 6-9. Инструменты управления FTP

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ FTP 7.5

Подробнее о FTP 7.5 см. по адресу [http://technet.microsoft.com/en-us/library/dd722686\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd722686(WS.10).aspx) (на англ. языке).

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Развертывание сайтов в IIS 7.5

Подробнее о развертывании сайтов см. по адресу <http://learn.iis.net/page.aspx/37/deploying-web-sites-on-iis-7> (на англ. языке).

---

## Удаленные приложения RemoteApp

Сеанс RemoteApp отличается от стандартного сеанса сервера узла сеансов служб терминалов тем, что, вместо подключения к окну, отображающему рабочий стол удаленного компьютера, приложение, выполняемое на сервере узла сеансов, выглядит так, будто выполняется на локальном компьютере.

Преимущество этой технологии в том, что все ресурсы памяти, диска и процессора, необходимые приложению, предоставляются не клиентом, а сервером узла сеансов, на котором размещается это приложение. Благодаря этому, приложения, требующие больших объемов оперативной памяти и ресурсов ЦП, быстро запускаются на компьютерах, не имеющих достаточно ресурсов для традиционной установки и выполнения приложений.

Когда с одного сервера вызывается несколько приложений, эти приложения передаются клиентам с использованием одного и того же сеанса. Это означает, что, если сервер узла сеансов удаленных рабочих столов разрешает максимум 20 одновременных сеансов, на пользователя с тремя открытыми приложениями RemoteApp будет приходиться только один сеанс, а не три.



RemoteApp имеет следующие преимущества:

- Проще разворачивать обновления приложений. Обновления требуется применить только на сервере узла сеансов удаленных рабочих столов, а не разворачивать на клиентах.
- Проще путь перехода на следующую версию приложения. Как и в случае с обновлениями, требуется заменить приложение только на сервере. Обновлять клиенты не нужно.
- Любое приложение, которое можно запускать на сервере узла сеансов, может быть запущено как приложение RemoteApp.
- Приложения RemoteApp можно связать с локальными расширениями файлов. Когда пользователь попытается открыть соответствующий документ, запустится приложение RemoteApp.
- Пользователи зачастую не знают, что приложение работает удаленно.

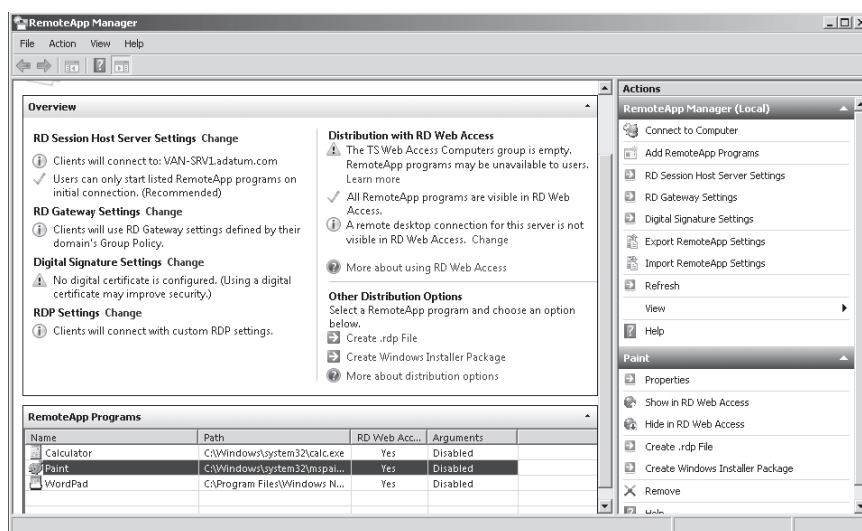


Рис. 6-10. Диспетчер удаленных приложений RemoteApp

С помощью диспетчера удаленных приложений RemoteApp можно настраивать параметры шлюза удаленного рабочего стола. Это даст пользователям, подключенным к Интернету, возможность доступа к приложениям RemoteApp за счет опосредованного подключения через сервер шлюза удаленных рабочих столов. Как показано на рис. 6-10, разворачивать приложения RemoteApp можно тремя способами:

- создать ярлык для файла RDP и передать его клиентам; это можно сделать, поместив ярлык в общую папку или отправив по электронной почте;
- создать и распространить пакет установщика Windows. Преимущество этого способа в том, что можно связать приложение RemoteApp с определенным расширением файла. Когда пользователь попытается открыть этот файл, автоматически запустится приложение RemoteApp;
- подключить клиенты к сайту веб-доступа к удаленным рабочим столам и запустить приложение RemoteApp через ссылку на странице. При помощи дис-

петчера RemoteApp можно указать, размещено ли приложение на сайте веб-доступа.

Пользователи RemoteApp должны быть членами группы **Пользователи удаленного рабочего стола** на сервере узла сеансов удаленных рабочих столов. Если приложения RemoteApp развертываются с компьютера, являющегося контроллером домена, необходимо изменить политику **Разрешить вход в систему через службы удаленных рабочих столов (Allow Log On Through RDS)**, чтобы разрешить доступ к приложениям RemoteApp.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ RemoteApp

Подробнее о RemoteApp см. по адресу <http://technet.microsoft.com/ru-ru/library/cc755055.aspx>.

---

#### Проверьте себя

- Какой способ развертывания следует использовать, чтобы связать приложение RemoteApp с определенным расширением имени файла?

#### Ответы

- Связывать расширения файлов с приложениями RemoteApp позволяют пакеты установщика Windows.

## App-V

App-V позволяет запускать приложения без установки на локальных компьютерах. App-V создает для каждого приложения отдельный раздел дискового пространства, так называемый бункер, в котором это приложение работает. Преимущество данного подхода состоит в том, что приложения, которые не могут выполняться на компьютере из-за проблем совместимости с основной операционной системой, могут работать при помощи App-V. App-V входит в состав пакета MDOP (Microsoft Desktop Optimization Pack).

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ MDOP

Подробнее о MDOP см. по адресу <http://www.microsoft.com/windows/enterprise/products/mdop/default.aspx>.

---

App-V использует потоковую технологию для передачи только тех частей приложения, которые используются клиентом в сети. Так как клиенту требуются различные части приложения, эти части передаются потоком по сети.

Поскольку приложение виртуализуется в бункере, App-V позволяет выполнять следующее:

- Развертывать несколько версий одного приложения с одного сервера. Можно даже запускать несколько версий одного приложения на локальном клиенте в виде бункеров, и эти версии не будут конфликтовать. Это особенно полезно для сред разработки приложений, в которых одновременно тестируются разные версии одного приложения.
- Развертывать с одного сервера приложения, которые при обычных условиях будут конфликтовать. При развертывании с использованием RemoteApp на

одном сервере узла сеансов удаленных рабочих столов можно устанавливать только не конфликтующие друг с другом приложения.

- Развертывать приложения, несовместимые с сервером узла сеансов удаленных рабочих столов. Из-за конфликтов с архитектурой сервера узла сеансов не все приложения работают через него. App-V позволяет развертывать эти приложения на клиенты аналогично тому, как это делается при помощи сервера узла сеансов удаленных рабочих столов.
- Развертывать приложения App-V как пакеты установщика Windows.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ App-V

Подробнее об App-V см. по адресу <http://technet.microsoft.com/ru-ru/appvirtualization/default.aspx>.

---

## Резюме

- Для развертывания приложений можно использовать AD DS, при условии, что эти приложения представлены в виде пакетов установщика Windows.
- Пакеты установщика Windows имеют расширение файла *.msi*.
- Развертывание веб-приложений подразумевает копирование файлов на сервер IIS. Для безопасного развертывания веб-приложений можно использовать FTP 7.5 или WebDAV.
- Приложения RemoteApp — способ виртуализации представлений, в котором по сети передается только изображение окна приложения.
- Если требуется связать определенные типы файлов с приложением RemoteApp, развертывайте приложения RemoteApp в формате установщика Windows.
- App-V позволяет приложениям, которые могут конфликтовать друг с другом, работать в бункерах на одном клиенте.
- App-V использует потоковую передачу необходимых клиенту данных приложения.
- Приложения App-V можно развертывать с помощью пакетов установщика Windows.

## Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных на занятии 2. Эти вопросы предоставлены также в электронном виде на прилагаемом к книге компакт-диске.

---

### ПРИМЕЧАНИЕ Ответы

Ответы на вопросы и пояснения к их вариантам размещены в разделе «Ответы» в конце книги.

---

1. Какими из перечисленных способов можно развернуть приложение удаленного рабочего стола RemoteApp? (Выберите все подходящие варианты.)
  - a. Развернуть ссылку на веб-доступ к удаленным рабочим столам с помощью групповой политики.

- b. Использовать пакет установщика Windows, развернутый с помощью групповой политики.
  - c. Поместить ярлык на файл RDP в общей папке.
  - d. Установить приложение в общей папке.
2. Вы работаете системным администратором в компании, занимающейся разработкой ПО. На этапе разработки приложения потребовалось развернуть несколько версий одной программы с одного сервера узла сеансов удаленных рабочих столов. При попытке установить оба приложения возникает конфликт. Как решить проблему?
- a. Развернуть приложения с помощью как приложения RemoteApp служб терминалов.
  - b. Развернуть сервер шлюза удаленного рабочего стола.
  - c. Развернуть App-V.
  - d. Развернуть приложения с помощью веб-доступа к удаленным рабочим столам.
3. Клиентские компьютеры с Windows XP не могут подключаться к приложениям RemoteApp с помощью страницы веб-доступа к удаленным рабочим столам. Клиентские компьютеры с Windows Vista подключаются без проблем. Как решить эту проблему?
- a. Установить Internet Explorer 6.0 на клиенты с Windows XP.
  - b. Отключить брандмауэр Windows XP.
  - c. Установить на клиенты с Windows XP пакет обновлений SP3.
  - d. Установить на клиенты с Windows XP Защитник Windows.
4. Ваша организация имеет сервер Windows Server 2008 R2, расположенный на периметре сети, на котором с помощью роли веб-сервера установлены службы IIS 7.5. Вы хотите, чтобы разработчики, развертывающие веб-приложения на сервере IIS, не передавали свои учетные данные по сети незащищенным способом. Сервер не входит в домен, и вы не хотите открывать порты, относящиеся к протоколу Server Message Block (SMB), на брандмауэре между внутренней сетью и периметром сети. Что следует выполнить, чтобы можно было развернуть веб-приложения на сервере в сети периметра? (Каждый ответ является готовым решением. Выберите все подходящие.)
- a. Установить DFS на сервер, расположенный на периметре сети.
  - b. Установить службу роли FTP.
  - c. Настроить общую папку на сервере, расположенном на периметре сети.
  - d. Установить средства публикации WebDAV.

## Практикум. Установка и настройка служб удаленных рабочих столов и RemoteApp

На этом практикуме вы установите и настроите службы удаленных рабочих столов, после чего развернете приложения с помощью веб-доступа к удаленным рабочим столам и RemoteApp.

## Упражнение 1. Подготовка сервера и установка служб удаленных рабочих столов

В этом упражнении вы установите и настроите службы удаленных рабочих столов на сервере VAN-SRV1.

1. Убедитесь, что серверы VAN-DC1 и VAN-SRV1 включены.
2. Зайдите на сервер VAN-SRV1 под учетной записью пользователя Kim\_Akers. Убедитесь, что на сервер не установлены компоненты роли веб-сервера и удаленных рабочих столов, выполнив следующие команды из оболочки Windows PowerShell с повышенными привилегиями:

```
Import-Module ServerManager
```

```
Remove-WindowsFeature Web-Server
```

```
Remove-WindowsFeature Remote-Desktop-Services
```

3. При необходимости перезагрузите сервер и войдите под учетной записью пользователя Kim\_Akers.
4. Откройте Проводник и создайте на диске C: общую папку **RemoteApp**.
5. Откройте диспетчер сервера и щелкните узел **Роли (Roles)**. На панели справа щелкните **Добавить роли (Add Roles)**. Откроется мастер добавления ролей. Щелкните **Далее (Next)**.
6. На странице **Роли сервера (Server Roles)** выберите **Службы удаленных рабочих столов (Remote Desktop Services)**. Щелкните **Далее (Next)** два раза.
7. На странице выбора служб ролей установите флажки **Узел сеансов удаленных рабочих столов (Remote Desktop Session Host)** и **Веб-доступ к удаленным рабочим столам (Remote Desktop Web Access)**. Получив предложение добавить дополнительные функции роли, щелкните **Добавить требуемые службы роли (Add Required Role Services)**. Щелкните **Далее (Next)** два раза.
8. На странице **Укажите метод проверки подлинности для узла сеансов удаленных рабочих столов (Specify Authentication Method for Remote Desktop Session Host)** установите переключатель **Требовать проверки подлинности на уровне сети (Require Network Level Authentication)** и щелкните **Далее (Next)**.
9. На странице **Укажите режим лицензирования (Licensing Mode and User Groups)** щелкните **Далее (Next)**.
10. На странице **Настройка взаимодействия с пользователем (Configure Client Experience)** установите все флажки, а затем щелкните **Далее (Next)** три раза. Щелкните **Установить (Install)**.
11. Щелкните **Закрыть (Close)**. Когда будет предложено перезагрузить сервер, щелкните **Да (Yes)**.

## Упражнение 2. Настройка веб-доступа к удаленным рабочим столам

В этом упражнении вы настроите веб-доступ к удаленным рабочим столам.

1. Зайдите на сервер VAN-SRV1 под учетной записью пользователя Kim\_Akers. Закройте окно **Возобновить работу мастера настройки** (Resume Configuration Wizard).
2. В меню **Администрирование | Службы удаленных рабочих столов** (Administrative Tools | Remote Desktop Services) щелкните **Настройка веб-доступа к удаленным рабочим столам** (Remote Desktop Web Access Configuration).
3. На странице с предупреждением о проблеме с безопасностью сертификата сайта, щелкните **Продолжить открытие этого веб-узла (не рекомендуется)** [Continue To This Website (Not Recommended)].
4. На странице **Подключение к службам удаленных рабочих столов по умолчанию** (Remote Desktop Services Default Connection) введите учетные данные adatum\Kim\_Akers и пароль Pa\$\$w0rd. Установите переключатель **Это личный компьютер** (This Is A Private Computer) и щелкните **Войти** (Sign In). Щелкните **Удаленные приложения RemoteApp** (RemoteApp Programs) и убедитесь, что в списке нет программ. Оставьте Internet Explorer открытым.
5. В меню **Администрирование | Службы удаленных рабочих столов**, щелкните **Диспетчер удаленных приложений RemoteApp** (RemoteApp Manager). Откроется консоль диспетчера.
6. На панели **Действия** (Actions) щелкните **Добавить удаленные приложения RemoteApp** (Add RemoteApp Programs). Откроется мастер удаленных приложений RemoteApp. Щелкните **Далее**. На странице **Выберите программы для добавления в список удаленных приложений RemoteApp** (Choose Programs To Add To The RemoteApp Programs List) выберите Калькулятор, щелкните **Далее**, после чего щелкните **Готово**.
7. Вернитесь в Internet Explorer и обновите страницу. Проверьте, отображается ли Калькулятор в списке. Щелкните на значке Калькулятора в списке. В окне предупреждения RemoteApp щелкните **Подключить** (Connect). На странице **Введите учетные данные** (Enter Your Credentials) введите пароль Pa\$\$w0rd и щелкните **ОК**. Проверьте, отображается ли калькулятор.
8. Откройте диспетчер задач. Имя программы Калькулятор на вкладке **Приложения** (Applications) будет содержать полное доменное имя (FQDN) сервера узла сеансов удаленных рабочих столов. Закройте Калькулятор.

## Упражнение 3. Настройка RemoteApp и установщика Windows

В этом упражнении вы настроите установщик приложений RemoteApp для программы WordPad.

1. Выполнив вход на компьютер VAN-SRV1 под учетной записью Kim\_Akers, откройте диспетчер удаленных приложений RemoteApp из меню **Администрирование | Службы удаленных рабочих столов** (Administrative Tools | Remote Desktop Services).

2. На панели **Действия** (Actions) щелкните **Добавить удаленные приложения RemoteApp** (Add RemoteApp Programs). В окне мастера щелкните **Далее**. На странице выбора приложений выберите WordPad, щелкните **Далее**, а затем щелкните **Готово**.
3. В диспетчере удаленных приложений RemoteApp в списке **Удаленные приложения RemoteApp** (RemoteApp Programs) выберите WordPad. На панели **Действия** (Actions) щелкните **Создать пакет установщика Windows** (Create Windows Installer Package). Откроется мастер удаленных приложений RemoteApp. Щелкните **Далее**.
4. На странице **Задание параметров пакета** (Specify Package Settings) введите путь к каталогу C:\RemoteApp, который вы создали на шаге 4 упражнения 1, и щелкните **Далее**.
5. На странице **Настройка пакета распространения** (Configure Distribution Package) установите флажки **Рабочий стол** (Desktop) и **Папка меню «Пуск»** (Start Menu Folder). Щелкните **Далее**, а затем щелкните **Готово**.
6. Зайдите на сервер VAN-DC1 под учетной записью пользователя Kim\_Akers. Перейдите в сетевую папку \\VAN-SRV1\RemoteApp. Дважды щелкните файл WordPad.msi. В диалоговом окне с предупреждением щелкните **Выполнить** (Run).
7. В диалоговом окне службы контроля учетных записей щелкните **Да** (Yes). После установки приложения RemoteApp посмотрите на рабочий стол. Дважды щелкните ярлык WordPad на рабочем столе. В окне с предупреждением щелкните **Подключить** (Connect). Введите пароль Pa\$\$w0rd и щелкните **ОК**. Убедитесь, что открылось приложение WordPad.
8. Откройте диспетчер задач. Убедитесь, что на вкладке **Приложения** (Applications) программа отображается как **Документ – WordPad (удаленный)** [Document - WordPad (Remote)]. Закройте приложение RemoteApp.

## Закрепление материала главы

Чтобы попрактиковаться и закрепить знания, полученные при изучении этой главы, выполните следующее:

- прочитайте резюме главы;
- выполните задания лабораторной работы, моделирующей реальные ситуации, требующие применения полученных знаний;
- выполните рекомендуемые упражнения;
- пройдите пробный тест.

## Резюме главы

- Виртуализация представлений подразумевает запуск приложения на одном компьютере и его отображение на другом. Преимущество виртуализации представлений состоит в том, что можно обновить приложение один раз на сервере вместо многократного обновления на всех клиентах.



- App-V использует потоковую передачу приложения с сервера, так что оно выполняется на клиенте, но не устанавливается на нем. App-V позволяет запускать два конфликтующих приложения на одном компьютере. App-V требует наличия MDOP.
- Можно безопасно публиковать веб-приложения на веб-серверах с помощью FTP 7.5 или WebDAV.

## Лабораторная работа

Для выполнения заданий лабораторной работы используйте знания о планировании установки и обновления серверов, полученные из этой главы. Ответы можно найти в разделе «Ответы» в конце книги.

### Задание 1. Планирование стратегии служб виртуальных рабочих столов для Wingtip Toys

Вы планируете развертывание служб виртуальных рабочих столов для компании Wingtip Toys. Компания имеет офисы во всех штатах Австралии. Из-за децентрализованной структуры компании каждый офис имеет собственный домен в лесу WingtipToys.internal. Все клиенты в организации работают под управлением Windows XP SP2 и Windows Vista без пакетов обновлений. Принимая это во внимание, решите следующие технические задачи.

- Каждый офис должен отвечать за приобретение клиентских лицензий удаленного рабочего стола и управление ими. Как следует спланировать развертывание серверов лицензирования удаленных рабочих столов?
- Сервер узла сеансов удаленных рабочих столов в офисе Квинсленда не справляется с нагрузкой, и скоро будет заменен. Как можно будет продолжить обслуживание клиентов в этом офисе и повторно подключить прерванные сеансы?
- Что следует предпринять, чтобы клиенты имели доступ к приложениям RemoteApp через веб-доступ к удаленным рабочим столам?

### Задание 2. App-V в компании Contoso

Компания Contoso разрабатывает пользовательские приложения для компьютеров под управлением Windows 7. Ежегодно выпускается новая версия определенного приложения, и пока пользователи выполняют обновление, вы должны предоставить персоналу техподдержки Contoso возможность запускать текущую и предыдущую версии приложения. Техническая проблема состоит в том, что эти две версии не могут одновременно устанавливаться на один компьютер под управлением Windows 7. Также вы развернули в Contoso службы удаленных рабочих столов для поддержки ряда важных приложений. Вы хотите, чтобы приложение, расположенное на сервере узла сеансов удаленных рабочих столов, запускалось каждый раз, когда пользователи щелкают файлы во вложениях, полученных по электронной почте. Вы развернули сервер шлюза удаленного рабочего стола на периметре сети компании. Учитывая все это, ответьте на вопросы:

1. Какая технология даст отделу тестирования возможность запускать разные версии одного приложения?
2. Как следует развернуть приложения RemoteApp, чтобы требуемое приложение открывалось, когда пользователь открывает файл определенного типа?
3. Как предоставить пользователям из Интернета доступ к приложениям RemoteApp?

## Рекомендуемые упражнения

Чтобы успешно справиться с экзаменационными заданиями по темам этой главы, выполните следующие упражнения.

### Предоставление приложений

- **Упражнение 1:** С помощью диспетчера удаленных приложений RemoteApp создайте пакет установщика Windows для Блокнота.
- **Упражнение 2:** Установите службу роли Лицензирование удаленных рабочих столов. Активируйте компьютер через веб-страницу, используя другой компьютер, подключенный к Интернету.

### Планирование сервера приложений и служб

- **Упражнение 1:** Установите службы ролей веб-сервера и FTP 7.5. Используйте FTP для передачи содержимого на сайт, размещенный на веб-сервере.
- **Упражнение 2:** Установите и настройте службу роли WebDAV и используйте ее для передачи содержимого на сайт, размещенный на веб-сервере.

## Пробный экзамен

Тренировочные тесты на прилагаемом к книге компакт-диске позволяют проверить знания только по одной или сразу по всем темам сертификационного экзамена 70-646. Тестирование можно организовать так, чтобы оно проводилось как настоящий экзамен, а можно проходить в режиме обучения, просматривая правильные ответы и объяснения после каждого ответа.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Пробный экзамен

Подробнее о пробном экзамене рассказано во Введении.

---

# Файловые серверы и серверы печати

|                                                           |            |
|-----------------------------------------------------------|------------|
| <b>Занятие 1. Планирование управления службами печати</b> | <b>288</b> |
| <b>Занятие 2. Планирование файловых серверов</b>          | <b>307</b> |

В этой главе рассматриваются роли файловых служб и служб печати и документов с точки зрения планирования их использования для организации печати, хранения файлов и обеспечения безопасности доступа. Мы обсудим публикацию и доступность принтеров, разрешения на доступ к файлам и принтерам, файловые квоты и обеспечение доступности данных, а также планирование развертывания компонента BranchCache для сетевых файлов в режимах распределенного и размещенного кэша.

## Темы экзамена

Планирование ролей файлового сервера и сервера печати.

## Прежде всего

Для выполнения упражнений этой главы потребуется:

- Сервер с именем VAN-DC1, работающий под управлением Windows Server 2008 R2 Enterprise, настроенный как контроллер домена Adatum.com, как описано в Приложении.
- Дополнительный сервер VAN-SRV1, работающий под управлением Windows Server 2008 R2 Enterprise, настроенный как рядовой сервер в домене Adatum.com, как описано в Приложении. Этот сервер не требуется для выполнения практических упражнений этой главы, но его можно использовать для изучения BranchCache для сетевых файлов.
- Учетная запись пользователя Kim Akers с паролем Pa\$\$w0rd в домене adatum.com, включенная в группы администраторов домена, администраторов предприятия и администраторов схемы. Процедура создания этой учетной записи описана в Приложении.
- Для выполнения практических упражнений рекомендуем использовать изолированную сеть, не входящую в рабочую сеть. Доступ к Интернету не

требуется, как и настройка шлюза по умолчанию. Для экономии времени и затрат на настройку физических компьютеров используйте виртуальные машины, например, созданные с использованием роли сервера Hyper-V.

### Реальный мир

*Йен Маклин*

В июле 1993 г. Microsoft представила новую файловую систему NTFS. Это было значительное достижение в то время. Появилась возможность защищать файлы и папки от интерактивных и сетевых пользователей, и защиту можно было применять на уровне отдельных файлов, а не только папок. Не буду рассказывать обо всех новшествах, представленных в NTFS, — наша книга не по истории, — но замечу, что на дисках с NTFS я терял файлы гораздо реже, чем на дисках с FAT.

Однако NTFS принесла не только хорошие новости, особенно для сетевого инженера, который готовился к сдаче первых экзаменов MCSE (для меня). Вычисление разрешений пользователей в NTFS оказалось связано с определенными сложностями, которые почти гарантированно вели к провалу на экзамене тех, кто не вполне понимал, как взаимодействуют разрешения, особенно с учетом замены старого разрешения Нет доступа (No-Access) более подробным Запретить (Deny).

Для определения результирующих разрешений создавались специальные программы, но их нельзя было взять с собой на экзамен. Мое решение было гораздо проще: я рисовал три прямоугольных поля в ряд. Правое я подписывал «Файл», среднее — «Папка», левое — «Общая папка».

Затем я записывал разрешения NTFS, которые пользователь имел на доступ к файлу, и разрешения того же пользователя на доступ к папке, содержащей этот файл. Разрешения файла переопределяли разрешения папки, и я получал результирующие разрешения NTFS. Если вход выполнялся локально, это и были действующие разрешения на доступ к файлу. Разрешения на доступ к общей папки я записывал в третье поле и учитывал их при удаленном доступе.

Я использовал этот прием при сдаче экзаменов и во время работы. Получив статус МСТ, я учил этому студентов, рисуя прямоугольники на доске в аудитории. Это простой прием. Кто-то даже назвал его тупым.

Но он работает. Попробуйте.

## Занятие 1. Планирование управления службами печати

Если смотреть на сеть организации с точки зрения пользователей, одной из ее самых востребованных функций будет возможность печатать файлы быстро и без проблем. Чтобы пользователи могли печатать, вы должны опубликовать принтеры, но при этом контролировать использование дорогих расходных материалов для печати. Инфраструктуру печати следует спланировать таким образом, чтобы срочные задания печати выполнялись сразу, а крупные и несроч-

ные — в нерабочее время. На этом занятии мы обсудим роль сервера служб печати и документов, способы обеспечения их доступности, публикацию принтеров и настройку разрешений доступа.

---

**Изучив материал этого занятия, вы сможете:**

- ✓ Устанавливать роль служб печати и документов, устанавливать и управлять принтерами и драйверами принтеров.
- ✓ Управлять разрешениями на доступ к принтеру и доступностью принтера.

**Продолжительность занятия — примерно 35 мин.**

---

## Планирование служб печати и документов

Опытным администраторам наверняка приходилось администрировать принтеры и устройства печати. В Windows Server 2008 R2 службы печати, появившиеся в Windows Server 2008, получили название служб печати и документов. Эту роль сервера необходимо установить на сервер, который будет сервером печати. Вы установите эту роль на практикуме этого занятия. В Windows Server 2008 R2 улучшена консоль **Управление печатью** (Print Management), рассматриваемая на этом занятии.

Роль сервера **Службы печати и документов** (Print and Document Services) позволяет управлять серверами печати и принтерами. Если настроить сервер под управлением Windows Server 2008 R2 как сервер печати, можно уменьшить объем работы по администрированию и управлению, выполняя все задачи по управлению принтерами из консоли **Управление печатью** (Print Management).

По умолчанию роль сервера **Службы печати и документов** устанавливает роль службы **Сервер печати** (Print Server), которая позволяет совместно использовать принтеры в сети и публиковать их в службе каталогов Active Directory (AD DS). При желании можно установить также службу LPD (Line Printer Daemon), позволяющую печатать на принтерах, подключенных к серверам UNIX; службу роли распределенного сканирования (впервые появилась в Windows Server 2008 R2), позволяющую запускать процессы сканирования, передавать по сети отсканированные документы и вести журнал событий, относящихся к сканированию; а также службу роли печати через Интернет, позволяющую подключаться к принтерам и управлять ими через веб-интерфейс.

---

**ПРИМЕЧАНИЕ Принтеры и устройства печати**

Устройство печати — это физическое устройство, печатающее твердые копии документов. Принтер управляет устройством печати. Можно установить несколько принтеров, подключенных к одному устройству печати, установить разные разрешения на доступ к ним и назначить разные расписания для разных пользователей. Например, если у вас есть дорогое цветное устройство печати, вы можете разрешить доступ к нему обычных пользователей только в нерабочие часы, а менеджерам — в любое время. Для этого нужно создать два принтера, подключенных к одному устройству печати.

---

Планирование роли служб печати и документов включает анализ текущих и будущих требований к печати, настройку расписания принтера и разрешений

доступа. Если из какого-то отдела постоянно отправляют на устройство печати очень большие, но не срочные задания, то принтер, печатающий эти задания, следует настроить на печать в нерабочие часы.

Всем ли пользователям требуется цветная печать? Если дать людям возможность, они будут печатать в цвете, независимо от того, нужно им это или нет. Одни пользователи имеют привычку несколько раз нажимать кнопку **Печать**, когда хотят распечатать документ, другие — распечатывать все свои сообщения электронной почты. В таких случаях можно настроить аудит принтера для выявления частого использования принтера и пользователей, которые за это ответственны. В книге мы еще не раз отметим, что администраторам приходится решать не только технические проблемы, но и проблемы с людьми.

Некоторые решения должны быть практичными и прагматичными. Приобретение устройства печати с несколькими лотками для разного типа бумаги может быть хорошей идеей, но вряд ли целесообразно использовать это устройство для обычной печати. Не лучшим выбором будет и устройство, выдающее сообщение об ошибке и приостанавливающее работу, блокируя остальные задания в очереди печати, когда пользователь указывает неверный размер бумаги (а такое может случаться часто). Кроме того, следует учитывать возможность использования пула принтеров, в котором один принтер управляет несколькими устройствами печати, когда требуется обеспечить высокую доступность печати.

## Управление сущностями принтеров

Если на сервер установлена роль служб печати и документов, можно управлять следующими сущностями:

- **Очередь печати.** Это представление устройства печати. В очереди печати отображаются активные задания печати и их состояние. Если первое задание в очереди не обрабатывается (например, из-за указания неверного размера бумаги), можно удалить его, чтобы продолжить обработку очереди.
- **Служба диспетчера очереди печати.** Сервер печати имеет одну службу диспетчера очереди печати. Эта служба управляет всеми заданиями и очередями печати на сервере. Обычно служба диспетчера очереди печати запускается автоматически. Если она по какой-то причине остановилась, необходимо запустить ее повторно. Симптом остановки — первое задание в очереди не обрабатывается, но не может быть удалено.
- **Драйвер принтера.** Для печати заданий на устройстве печати требуется драйвер принтера. Администратор должен убедиться, что на сервере печати установлен и корректно работает соответствующий драйвер принтера.
- **Порт сетевого принтера.** Драйвер принтера использует порт сетевого принтера для взаимодействия с физическим устройством по сети. Это может быть порт принтера TCP/IP, порт LPR, стандартный порт COM или LPT.
- **Кластер серверов печати.** Обычно печать является важной операцией, и для обеспечения высокой доступности и отказоустойчивости серверы печати можно объединить в кластер. Администрирование кластеров рассматривается в гл. 11.

## Публикация принтеров

Если открыть общий доступ к принтеру, но не опубликовать этот принтер в Active Directory, пользователи должны узнать сетевой путь к нему, чтобы использовать. Опубликованный в Active Directory принтер проще найти, а если вы решите перенести принтер на другой сервер печати, не придется изменять параметры на клиентах, достаточно изменить соответствующую запись в Active Directory.

Если к принтеру открыт общий доступ, его можно опубликовать, установив флажок **Внести Active Directory** (List In The Directory) на вкладке **Доступ** (Sharing) диалогового окна свойств принтера (рис. 7-1).

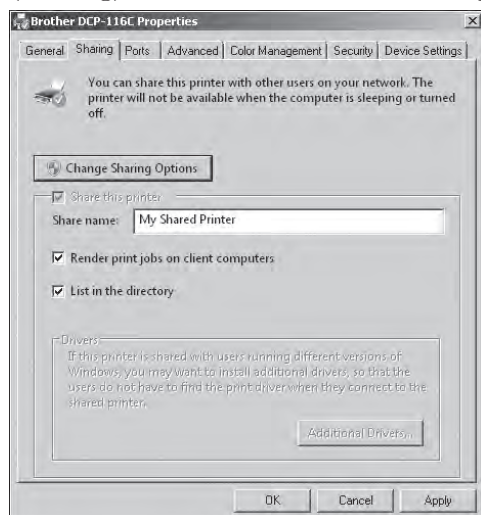


Рис. 7-1. Публикация принтера

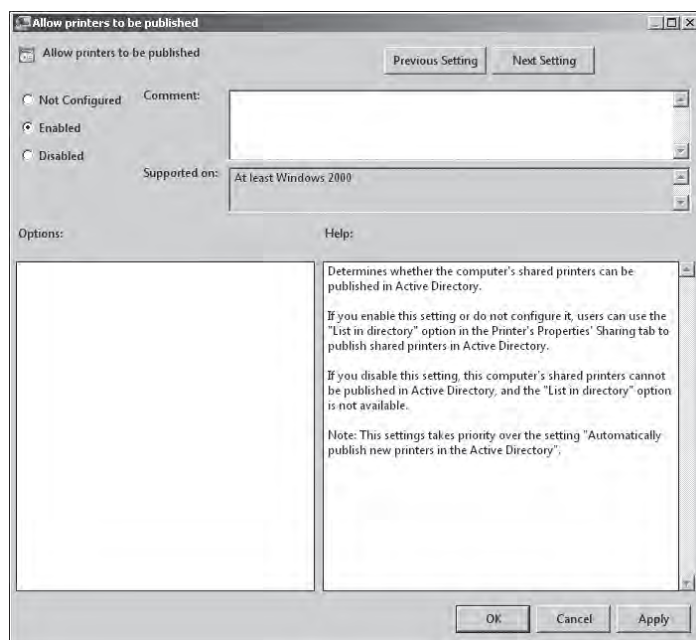


Рис. 7-2. Разрешение публикации принтеров



Если добавить принтер на сервер печати, работающий под управлением Windows Server 2008 R2, и открыть к нему общий доступ, он будет опубликован автоматически, если включены параметры групповой политики **Автоматическая публикация новых принтеров в Active Directory** (Automatically Publish New Printers In Active Directory) и **Разрешить публикацию принтеров** (Allow Printers To Be Published). На рис. 7-2 показана установка параметра **Разрешить публикацию принтеров**. К опубликованному принтеру должен быть открыт общий доступ. Если запретить общий доступ к принтеру, он перестает быть опубликованным.

## Улучшения служб печати в Windows Sever 2008 R2

В Windows Server 2008 R2 включена роль сервера **Службы печати и документов**, производительность которой улучшена за счет использования документов XPS, путей печати и драйверов принтеров. Эта роль предоставляет усовершенствованные инструменты управления печатью и, в частности, расширенную консоль **Управление печатью** (Print Management). Также предоставляется встроенная поддержка WSD, повышающая эффективность и уменьшающая нагрузку на службы печати и документов за счет выполнения обработки заданий печати на клиентах.

### Документы XPS

В Windows Server 2008 R2 формат XPS интегрирован в подсистему печати. Это обеспечивает повышение эффективности, совместимости и качества документов. Формат XPS основан на технологии создания документов с фиксированной структурой. Этот формат определен спецификациями Microsoft XPS и OPC, созданными на основе стандартов XML и ZIP.

Формат документов XPS поддерживает широкий ряд платформ и является стандартом в Windows Vista. Также он поддерживается .NET Framework 3.0 в Windows XP, Windows Vista, Windows 7 и Windows Server 2003. Открытые спецификации сделали возможными межплатформенные решения. Многие производители продуктов для печати и сканирования разрабатывают решения на основе технологий XPS, позволяющие повышать производительность и улучшать качество в приложениях .NET Framework 3.0 и Win32.

Драйверы принтеров XPSDrv используют модульную архитектуру, позволяющую более эффективно обрабатывать документы из очереди печати. Драйверы принтера XPSDrv в Windows Server 2008 R2 используют архитектуру, расширяющую существующую инфраструктуру драйверов и добавляющую новые возможности, сохраняя совместимость с существующими принтерами и приложениями. Архитектура драйверов принтеров XPSDrv имеет следующие характеристики:

- поддерживает WPF и совместима с приложениями Win32;

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Подробнее о WPF см. по адресу <http://msdn.microsoft.com/ru-ru/library/ms754130.aspx>. Учитывайте, однако, что на экзамене вряд ли встретятся подробные вопросы по этой теме.

---

- позволяет включать настраиваемые фильтры, выполняющие такие функции, как добавление корпоративного водяного знака, управление квотами и учет заданий печати;
- позволяет независимым производителям оборудования использовать общие функции для аналогичных моделей драйверов. Это может повысить надежность компонентов драйверов и улучшить работу драйвера сервера печати, благодаря поддержке повторного использования общих компонентов драйвера принтера.

Архитектура печати дает существующим приложениям возможность использовать функции, присущие только драйверам принтеров XPSDrv. Новые приложения на основе .NET Framework 3.0 и 3.5 могут использовать все эти функции, предоставляемые в пути печати.

---

### **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ .NET Framework 3.0 и 3.5**

Подробнее о .NET Framework 3.0 и 3.5, включая ссылки для загрузки, см. по адресам <http://www.microsoft.com/ru-ru/download/details.aspx?id=22444> и <http://www.microsoft.com/ru-ru/download/details.aspx?id=21>, соответственно.

---

Драйверы принтеров XPS обеспечивают более высокое качество печати. Они не ограничены использованием только функций обработки интерфейса графических устройств (GDI). Это позволяет им обрабатывать графику в альтернативных цветовых пространствах и использовать высокопроизводительные графические библиотеки, недоступные старым драйверам принтеров на основе GDI.

### **Пути печати**

Windows Server 2008 R2 поддерживает пути печати XPS, использующие формат документов XPS на всем пути от приложения до принтера. Это позволяет получать результат, в полной мере соответствующий принципу WYSIWYG («что видите, то и получите»). Пути печати в Windows Server 2008 R2 предоставляют следующие преимущества:

- избавляют от преобразования форматов файлов, часто выполняющегося при использовании драйверов на основе GDI. Это повышает производительность и качество результатов печати, а также уменьшает общий размер буферных файлов;
- обеспечивают поддержку дополнительных цветовых пространств и технологий для компонентов драйвера принтера;
- используют 32 бита на канал цвета и цветовое пространство CMYK, в котором для цветной печати используются чернила четырех цветов: голубого, пурпурного, желтого и черного;
- обеспечивают непосредственную поддержку прозрачности и градиентов;
- используют пути преобразования для поддержки существующих приложений и драйверов принтеров.

### **Оснастка Управление печатью**

Службы печати и документов в Windows Server 2008 R2 позволяют совместно использовать принтеры в сети и централизованно управлять серверами печати

и сетевыми принтерами при помощи оснастки **Управление печатью** (Print Management). Эта оснастка (рис. 7-3) позволяет наблюдать за очередями печати и получать уведомления, когда останавливается обработка заданий печати. Также ее можно использовать для переноса серверов печати и развертывания подключений к принтерам при помощи групповой политики. Чтобы открыть эту оснастку, выберите **Управление печатью** (Print Management) в меню **Администрирование** (Administrative Tools). Заметьте, что эта оснастка не будет доступна, если не установить средства удаленного администрирования (RSAT) или роль сервера Службы печати и документов. Вы установите эту роль сервера на практикуме этой главы.

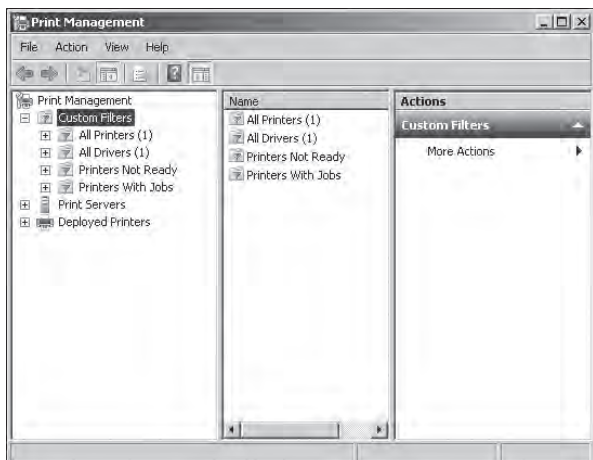


Рис. 7-3. Оснастка Управление печатью

Улучшенная оснастка **Управление печатью** в Windows Server 2008 R2 поддерживает перенос серверов печати из Windows 2000 Server и Windows Server 2003 в Windows Server 2008 R2. Также она включает улучшенный мастер установки сетевых принтеров, уменьшающий объем работы при добавлении сетевых принтеров. Этот мастер автоматически находит принтеры и устанавливает соответствующие драйверы принтера, если они доступны.

### Проверьте себя

- Какие три функции предоставляет архитектура драйверов принтеров XPSDrv в Windows Server 2008 R2?

### Ответ

- Поддерживает WPF.
- Позволяет включать настраиваемые фильтры, выполняющие такие функции, как добавление корпоративного водяного знака, управление квотами и учет заданий печати.
- Позволяет независимым производителям оборудования использовать общие функции для аналогичных моделей драйверов.

## Веб-службы для устройств (WSD)

Windows Server 2008 R2 имеет встроенную поддержку веб-служб для устройств, которые являются набором протоколов для доступа и управления службами на подключенных к сети устройствах. Эти веб-службы облегчают подключение, установку и использование принтеров. Microsoft сотрудничает с некоторыми производителями принтеров, обеспечивающими поддержку этого протокола своими устройствами.

## Улучшенная масштабируемость

Для уменьшения нагрузки на компьютер, на котором установлена роль служб печати и документов, подготовка печати выполняется на клиенте (в частности, на клиентах под управлением Windows Vista). В некоторых случаях это значительно снижает сетевой трафик, в зависимости от содержимого задания печати и использования языка описания страниц (PDL).

Диспетчер очереди печати в Windows Server 2008 R2 для организации взаимодействия клиента с сервером использует вызовы удаленных процедур (RPC). В Windows Server 2008 R2 намного уменьшено число отдельных потоков обработки, требуемых для RPC. Это может значительно улучшить производительность в крупных и средних сетях.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Управление печатью

Подробнее об оснастке **Управление печатью** в Windows Server 2008 R2, Windows Vista и Windows 7 см. по адресу <http://technet.microsoft.com/ru-ru/library/cc766474.aspx>.

---

## Управление принтерами с помощью оснастки

### Управление печатью

В Windows Server 2008 R2 оснастка **Управление печатью** (Print Management) устанавливается в составе роли служб печати и документов. Можно также установить ее отдельно. Для этого откройте Диспетчер сервера, щелкните **Компоненты** (Features), а затем **Добавить компоненты** (Add Features). Раскройте узел **Средства удаленного администрирования сервера** (Remote Server Administration Tools), раскройте **Средства администрирования ролей** (Role Administration Tools) и установите флажок **Средства компонента Службы печати и документов** (Print And Document Services Tools). Щелкните **Далее**, а затем **Установить**. По завершении установки щелкните **Заккрыть**.

Оснастка **Управление печатью** позволяет организовать централизованное администрирование в крупной сети с несколькими серверами печати (часто с большим числом). Если эта оснастка установлена как часть RSAT (она также устанавливается по умолчанию при установке роли служб печати и документов), ее можно открыть из меню **Администрирование** или из диспетчера сервера. После установки оснастку следует настроить, указав принтеры и серверы печати, которыми она должна управлять. Принтеры можно добавлять вручную или выполнить сканирование сети, чтобы найти их автоматически, щелкнув **Принтеры** (Printers) в дереве консоли (рис. 7-4).

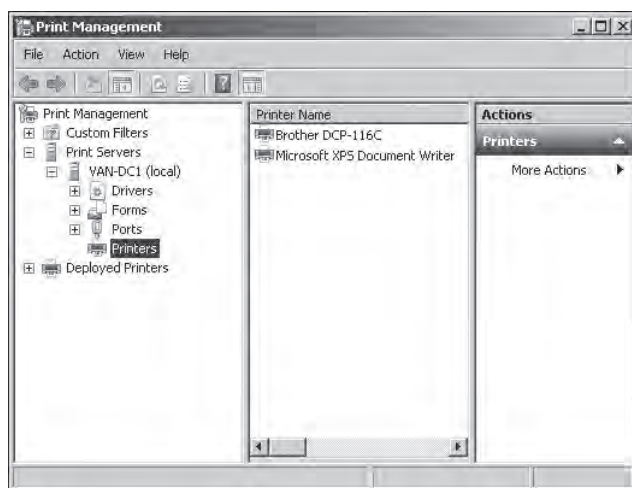


Рис. 7-4. Автоматический поиск принтеров в оснастке Управление печатью

Чтобы добавить в оснастку сервер печати, щелкните правой кнопкой узел **Серверы печати (Print Servers)** и выберите команду **Добавление и удаление серверов (Add/Remove Servers)**. Добавлять принтеры в сеть Windows Server 2008 R2 можно при помощи мастера добавления принтеров, доступного в предыдущих версиях Windows, который в Windows Server 2008 R2 называется мастером установки сетевых принтеров. Оснастка **Управление печатью** позволяет запускать этот мастер на удаленных серверах печати, работающих под управлением Windows Server 2008 и 2008 R2; раньше его необходимо было запускать локально.

Чтобы запустить мастер установки сетевых принтеров из оснастки **Управление печатью**, раскройте узел **Серверы печати (Print Servers)** и щелкните правой кнопкой сервер печати, на котором хотите разместить принтер, и выберите команду **Добавить принтер (Add Printer)** (рис. 7-5). Этот мастер позволяет установить принтер, расположенный на удаленном сервере печати.

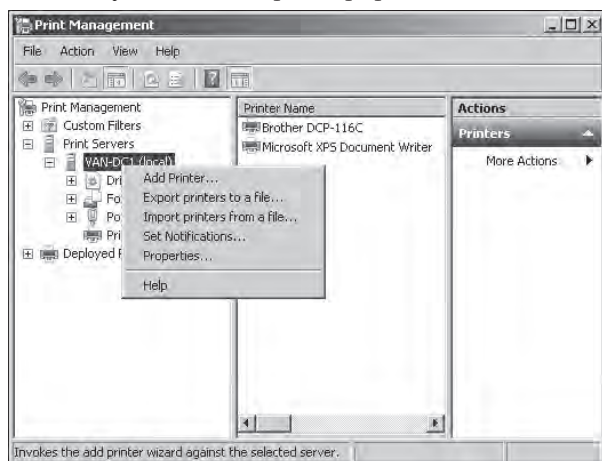


Рис. 7-5. Запуск мастера установки сетевых принтеров

Добавив в оснастку **Управление печатью** удаленные серверы печати и настроив на них принтеры, можно просматривать и администрировать их централизованно. Эта оснастка позволяет удаленно выполнять задачи, которые раньше выполнялись только локально на сервере печати, например, изменять порты принтера, просматривать состояние принтеров, добавлять и изменять формы. Есть и новые задачи, такие как создание настраиваемых фильтров принтеров, позволяющих просматривать и управлять принтерами, выбранными по принадлежности к узлу, правам и ролям. Процедура создания фильтра принтеров описана в следующем разделе.

## Создание фильтра принтеров и фильтра драйверов печати

Фильтры принтеров позволяют отображать только принтеры, соответствующие указанным критериям. Можно создавать настраиваемые фильтры для фильтрации по типу принтера (лазерный, цветной лазерный, плоттер и т.д.), производителю, модели, расположению или конфигурации. Например, можно настроить фильтр для отображения всех принтеров, расположенных в одном здании, независимо от того, какой сервер печати они используют.

Оснастка **Управление печатью** по умолчанию предоставляет два фильтра: **В состоянии «Не готов»** (Printers Not Ready) и **С заданиями печати** (Printers With Jobs). Создавая новый фильтр, можно настроить уведомление по электронной почте или запуск сценария при выполнении условий фильтра. Опишем процедуру создания настраиваемого фильтра принтеров.

1. Откройте оснастку **Управление печатью** (Print Management).
2. В дереве «Управление печатью» щелкните правой кнопкой папку **Настраиваемые фильтры принтеров** (Custom Filters) и выберите команду **Добавить новый фильтр принтеров** (Add New Printer Filter). Запустится мастер создания фильтра принтеров.
3. На странице **Имя и описание фильтра принтеров** (Printer Name And Description) введите имя фильтра принтера. Это имя появится в папке **Настраиваемые фильтры принтеров** (Custom Printer Filters) в дереве консоли.
4. Если хотите, добавьте описание.
5. Если хотите отображать число принтеров, удовлетворяющих условиям фильтра, установите флажок **Показывать общее число принтеров после имени фильтра принтеров** (Display The Total Number Of Items Next To The Name Of The Filter).
6. Страница **Имя и описание фильтра принтеров** (Filter Name And Description) должна выглядеть аналогично рис. 7-6. Щелкните **Далее**.
7. На странице **Определить фильтр принтеров** (Define A Printer Filter) в списке **Поле** (Field) выберите очередь печати или характеристику состояния принтера. Выберите состояние (Condition) и значение (Value), как показано на рис. 7-7, и щелкните **Далее**.

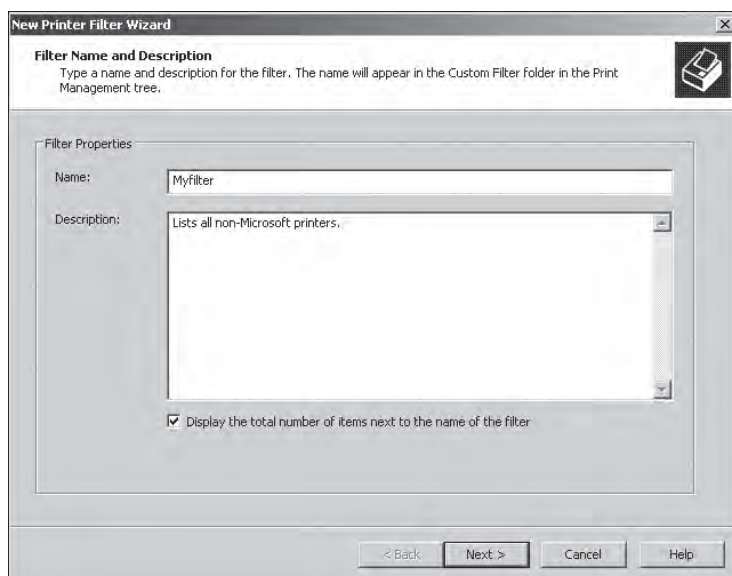


Рис. 7-6. Страница Имя и описание фильтра принтеров

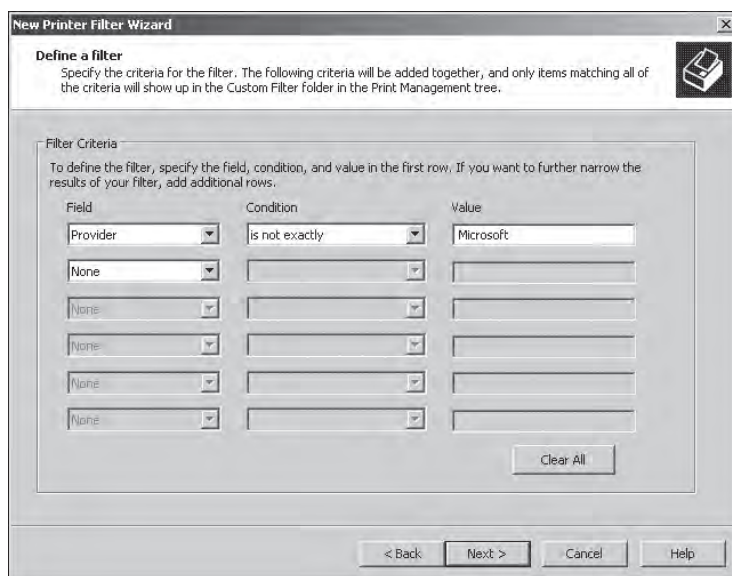


Рис. 7-7. Определение фильтра

8. Если требуется, на странице **Настроить уведомления (не обязательно)** [Set Notifications (Optional)] настройте почтовые уведомления и/или запуск сценария. Щелкните **Готово**.
9. Щелкните имя созданного фильтра в контейнере **Настраиваемые фильтры** (Custom Filters) (рис. 7-8). Просмотрите список принтеров в средней части окна.



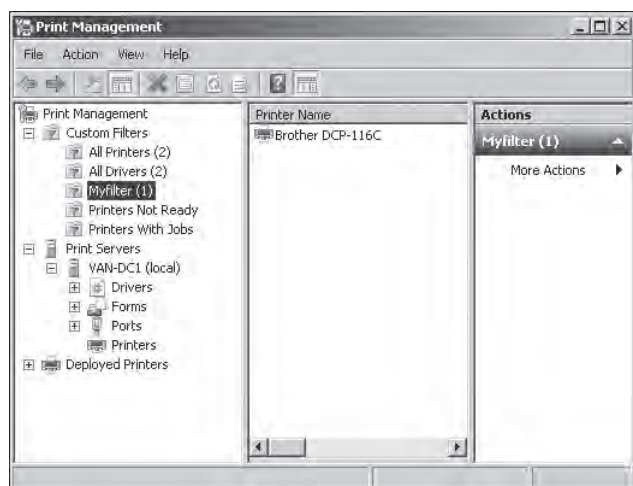


Рис. 7-8. Просмотр принтеров, соответствующих условиям фильтра принтеров

Аналогичным образом в оснастке **Управление печатью** можно создавать настраиваемые фильтры драйверов принтера, которые будут отображать только драйверы, соответствующие определенным критериям. Процедура создания фильтра драйверов почти идентична процедуре создания фильтра принтеров за исключением того, что на шаге 2 нужно щелкнуть правой кнопкой папку **Настраиваемые фильтры** (Custom Filters) и выбрать команду **Добавить новый фильтр драйверов** (Add New Driver Filter). Далее следует ввести имя и (если требуется) описание и указать, нужно ли отображать число элементов рядом с именем фильтра.

Для настройки фильтра драйверов, как и фильтра принтеров, следует указать поле, условие и значение и можно настроить почтовое уведомление и/или запуск сценария.

---

### СОВЕТ Подготовка к экзамену

Настраиваемые фильтры — новая возможность, доступная только на серверах печати под управлением Windows Server 2008 и 2008 R2.

---

#### Проверьте себя

- Какие два фильтра по умолчанию предлагает оснастка **Управление печатью** в Windows Server 2008 R2?

#### Ответ

- В состоянии **«Не готов»** (Printers Not Ready) и **С заданиями печати** (Printers With Jobs).

### Управление драйверами, портами, формами и принтерами

В оснастке **Управление печатью** можно раскрыть любой сервер печати, представленный в дереве консоли, и управлять его драйверами, портами, формами и принтерами. Можно также добавить драйвер, порт или принтер.

Щелкните правой кнопкой узел **Драйверы** (Drivers) и выберите команду **Управление драйверами** (Manage Drivers). Откроется диалоговое окно свойств сервера печати с выбранной вкладкой **Драйверы** (Drivers) (рис. 7-9). Здесь можно добавить новый драйвер, удалить имеющийся или просмотреть свойства любого драйвера из списка.

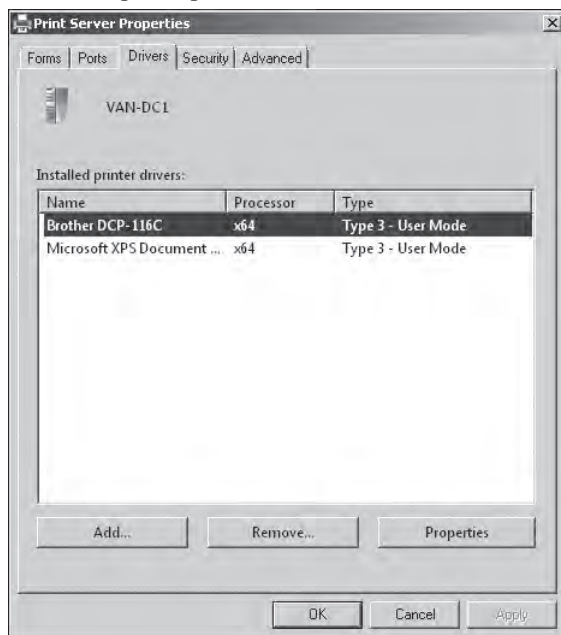


Рис. 7-9. Вкладка Драйверы диалогового окна свойств сервера печати

Если щелкнуть правой кнопкой узел **Порты** (Ports) и выбрать команду **Управление портами** (Manage Ports), откроется диалоговое окно свойств сервера печати с выбранной вкладкой **Порты** (Ports). На этой вкладке можно удалить существующий порт, добавить новый и настроить выбранный. Чтобы настроить порт, щелкните **Настройка порта** (Configure Port), введите значение интервала последующих попыток передачи в секундах и щелкните **ОК**.

Если щелкнуть правой кнопкой узел **Формы** (Forms) и выбрать команду **Управление формами** (Manage Forms), откроется диалоговое окно свойств сервера печати с выбранной вкладкой **Формы** (Forms). Установив флажок **Создать новую форму** (Create A New Form), можно дать форме имя, указать размер бумаги и полей печати (рис. 7-11). После этого можно нажать кнопку **Сохранить форму** (Save Form), чтобы создать форму. Кнопка **Удалить** (Delete) становится активной, если уже есть созданные формы, одна из которых выбрана на вкладке **Формы** (Forms). С помощью этой вкладки нельзя удалить стандартные формы.

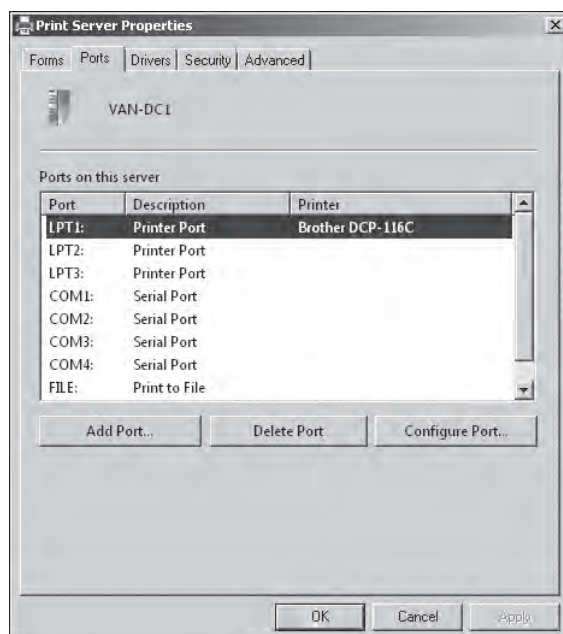


Рис. 7-10. Вкладка «Порты» диалогового окна свойств сервера печати

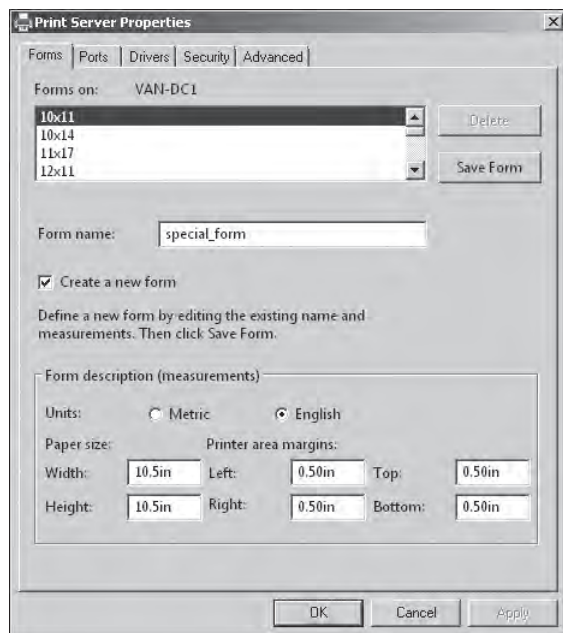


Рис. 7-11. Вкладка «Формы» диалогового окна свойств сервера печати

Если щелкнуть правой кнопкой узел **Принтеры** (Printers), можно добавить принтер, показать или скрыть расширенное представление возможностей принтера (рис. 7-12). Если выбрать расширенное представление, будет показано больше параметров для любого принтера, выбранного в оснастке **Управление**

**печатью.** В этом представлении можно просмотреть текущие задания печати и обратиться к веб-странице принтера (если таковая существует).

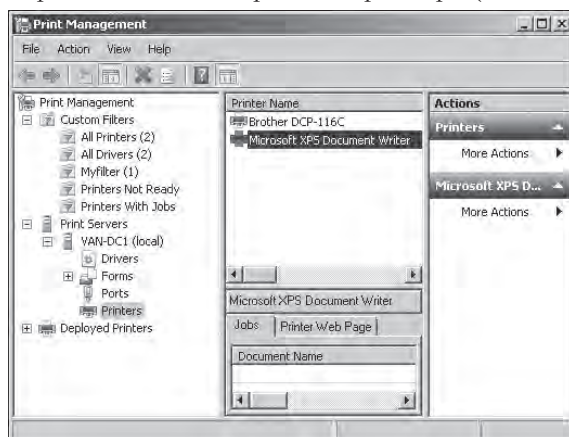


**Рис. 7-12.** Расширенное представление возможностей принтера

Можно также открыть диалоговое окно свойств сервера печати, щелкнув на узле сервера в дереве консоли **Управление печатью** и выбрав команду **Свойства** (Properties). По умолчанию при этом открывается вкладка **Дополнительно** (Advanced) (рис. 7-13), на которой можно изменить расположение папки очереди печати, включить звуковое оповещение о найденных в удаленном документе ошибках и отображение уведомлений для локальных и/или удаленных принтеров.

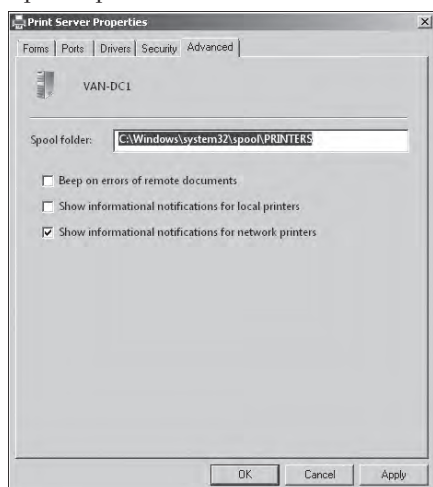


**Рис. 7-13.** Дополнительные свойства сервера печати

## Планирование и управление безопасностью и разрешениями доступа

Для обеспечения безопасности сервера печати и управления доступом к принтерам необходимо определить, какие права должны иметь пользователи и группы. Возможно, вы уже имеете опыт настройки разрешений для файлов и принтеров.

Помните, что разрешения следует выдавать группам, а не отдельным пользователям, а явные запрещающие разрешения следует назначать как можно реже.

Возможно, вы сталкивались с ситуациями, когда пользователь, который должен иметь доступ к принтеру, его не имеет, или (что сложнее диагностировать) когда пользователь, который не должен иметь доступа к принтеру, имеет его. Назначение разрешений и отладка их конфигурации — обычные административные задачи.

Планирование разрешений — более сложная работа. Надо ли настроить два драйвера принтера для дорогого устройства печати, чтобы члены группы менеджеров имели постоянный доступ к нему, а все остальные — только в часы с наименьшей загруженностью? Как планировать доступ к цветным принтерам или принтерам формата А3? Как настроить аудит и мониторинг, чтобы выявлять пользователей с «плохими привычками» (например, отправляющих по несколько раз одни и те же задания, если печать не началась немедленно)? Следует ли использовать пулы принтеров, чтобы лучше справляться с высокой нагрузкой?

---

### **СОВЕТ Подготовка к экзамену**

Помните, что можно настроить несколько принтеров для одного устройства печати и предоставить разным группам разные разрешения и время доступа. Можно также настроить несколько устройств печати так, чтобы они контролировались одним принтером, создав пул принтеров.

---

Параметры доступа ко всем принтерам сервера печати и к самому серверу печати настраиваются на вкладке **Безопасность** (Security) диалогового окна свойств сервера печати. Возможно, вы знакомы с разрешениями печати, но опишем их для напоминания:

- **Печать** (Print). По умолчанию назначается группе **Все** (Everyone). Пользователи могут подключаться к принтеру и отправлять документы. Члены групп администраторов, операторов печати и операторов сервера также имеют явное разрешение **Печать**.
- **Управление документами** (Manage Documents). Явно назначается группе создателей-владельцев и является единственным разрешением, назначенным этой группе. Группы администраторов, операторов печати и операторов сервера тоже имеют это разрешение, но им также назначается разрешение **Управление принтерами**. Пользователь может приостанавливать, возобновлять, перезапускать, отменять и изменять порядок документов, отправленных другими пользователями. Однако если пользователь имеет только разрешение **Управление документами**, он не может отправлять документы на печать и управлять состоянием принтера.
- **Управление принтерами** (Manage Printers). Назначается группам администраторов, операторов печати и операторов сервера. Предоставляется возможность выполнять задачи, связанные с разрешением **Печать**, и полный административный контроль над принтером: приостановка и возобновление работы принтера, изменение параметров очереди печати, предоставление общего доступа к принтеру, настройка разрешений принтера и изменение свойств принтера.

Разрешения на доступ к самому серверу печати можно настраивать в диалоговом окне его свойств. Разрешение **Просмотр сервера** (View Server) дает возможность просматривать сервер печати. Без этого разрешения пользователь не может видеть принтеры, которыми управляет сервер, поэтому оно предоставляется членам группы **Все** (Everyone).

Разрешение **Управление сервером** (Manage Server) дает пользователям возможность создавать и удалять очереди печати (с уже установленными драйверами), добавлять и удалять порты и формы. По умолчанию это разрешение имеют администраторы, операторы сервера и операторы печати. Обычного пользователя, получившего это разрешение, называют администратором делегированной печати.

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Делегированное администрирование

Подробнее о делегировании управления сервером печати см. по адресу [http://msdn.microsoft.com/ru-ru/library/ee524015\(WS.10\).aspx](http://msdn.microsoft.com/ru-ru/library/ee524015(WS.10).aspx).

На рис. 7-14 показана вкладка **Безопасность** (Security) диалогового окна свойств сервера печати с разрешениями для группы **Все** (Everyone). Разрешения можно назначать группам и отдельным пользователям, хотя последнее не рекомендуется; пользователям следует давать разрешения посредством членства в группах.

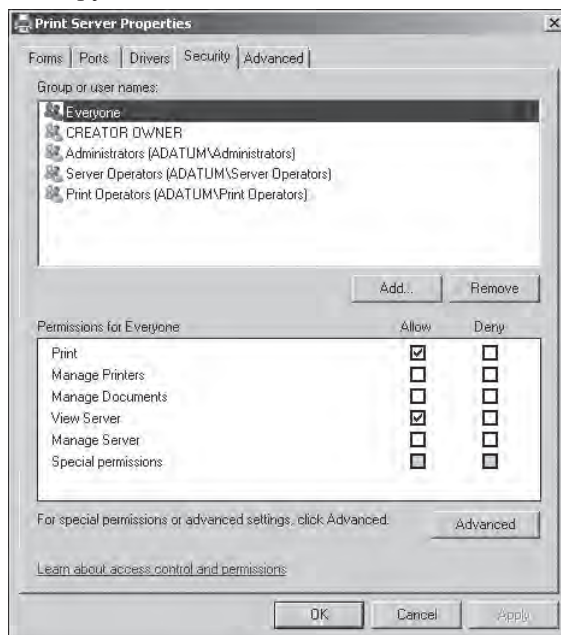


**Рис. 7-14.** Вкладка **Безопасность** диалогового окна свойств сервера печати

Пользователю или группе можно явно запретить любое разрешение. Пользователю, которому явно запрещено разрешение, или который состоит в группе, которой явно запрещено разрешение, нельзя предоставить это разрешение посредством членства в других группах. Поэтому явный запрет следует использовать как можно реже и документировать каждый такой случай.

Если требуется, пользователю или группе можно предоставить нестандартный набор разрешений. Для этого выберите пользователя или группу на вкладке **Безопасность** (Security) и щелкните кнопку **Дополнительно** (Advanced). Откроется диалоговое окно **Дополнительные параметры безопасности** (Advanced Security Settings) (рис. 7-15), в котором можно настроить разрешения, выбрав пользователя или группу и щелкнув **Изменить** (Edit). Можно также добавлять пользователей или группы и изменять их разрешения.

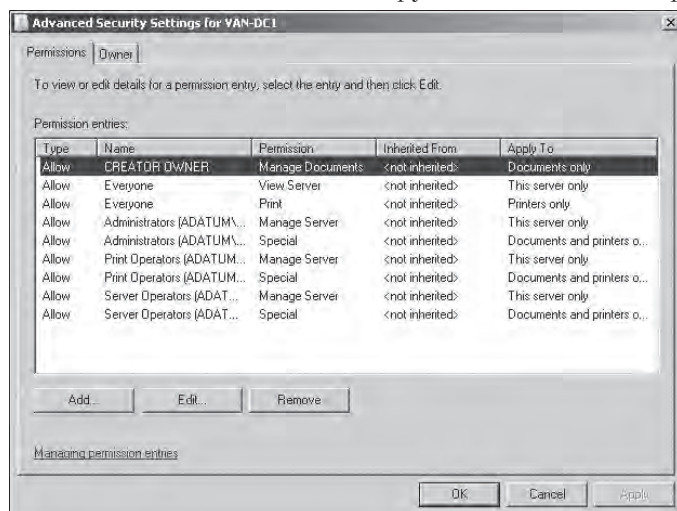


Рис. 7-15. Диалоговое окно дополнительных параметров безопасности

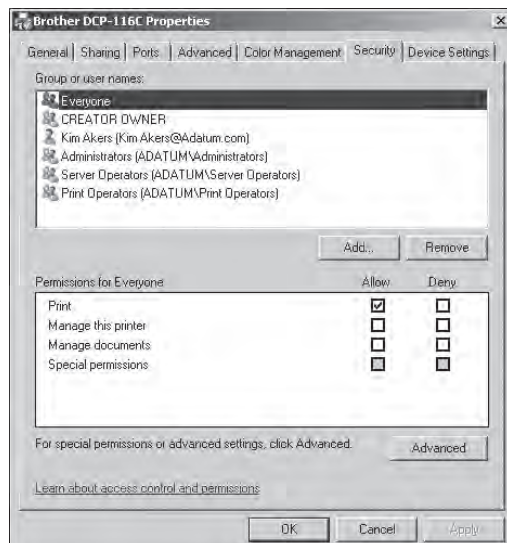


Рис. 7-16. Вкладка Безопасность диалогового окна принтера

Кроме предоставления разрешений на доступ к серверу печати, можно настраивать разрешения на доступ к отдельному принтеру. Разрешения, явно назначенные на уровне принтера, переопределяют разрешения, унаследованные от сервера печати. Можно назначать разрешения **Печать**, **Управление докумен-**



тами и **Управление принтерами** пользователям и группам, а также настраивать и назначать особые разрешения. Как и всегда, рекомендуется назначать разрешения группам, а не отдельным пользователям, и не злоупотреблять явным запретом разрешений и назначением особых разрешений. На рис. 7-16 показана вкладка **Безопасность** диалогового окна свойств принтера.

## Резюме

- Установив роль сервера **Службы печати и документов** (Print and Document Services), можно устанавливать и настраивать принтеры и драйверы принтеров, добавлять порты и управлять ими, а также настраивать формы.
- Оснастка **Управление печатью** (Print Management) позволяет централизованно управлять принтерами на удаленных серверах печати.
- Разрешения на доступ к принтерам и серверам печати можно настраивать в диалоговом окне свойств сервера печати. Разрешения на доступ к отдельному принтеру можно настраивать в диалоговом окне свойств этого принтера.

## Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных на занятии 1. Эти вопросы предоставлены также в электронном виде на прилагаемом к книге компакт-диске.

---

### ПРИМЕЧАНИЕ Ответы

Ответы на вопросы и пояснения к их вариантам размещены в разделе «Ответы» в конце книги.

---

1. Установив роль служб печати и документов, можно использовать оснастку **Управление печатью** для выполнения на удаленных серверах задач, которые раньше приходилось выполнять локально на том сервере, где находился принтер. Также эта оснастка предоставляет возможности, которых не было до выхода Windows Server 2008. Что из перечисленного является новой возможностью оснастки **Управление печатью**?
  - a. Изменение портов принтера.
  - b. Просмотр состояния принтера.
  - c. Добавление и изменение форм.
  - d. Создание настраиваемых фильтров принтеров.
2. Какое разрешение, по умолчанию назначаемое группе создателей-владельцев, позволяет изменять порядок документов, перезапускать, приостанавливать и возобновлять печать, начатую другими пользователями, но не дает возможность отправлять документы на принтер и управлять его состоянием?
  - a. **Печать** (Print).
  - b. **Управление документами** (Manage Documents).
  - c. **Управление принтерами** (Manage Printers).
  - d. **Управление сервером** (Manage Server).
3. Вы хотите делегировать обычному пользователю возможность администрировать сервер печати DEN-PRS1. Какое разрешение вы предоставите этому пользователю?

- a. **Управление сервером** (Manage Server).
  - b. **Просмотр сервера** (View Server).
  - c. **Управление документами** (Manage Documents).
  - d. **Управление принтерами** (Manage Printers).
4. Если добавить принтер на сервер печати, работающий под управлением Windows Server 2008 R2, и открыть к нему общий доступ, этот принтер будет автоматически опубликован, если включены два параметра групповой политики. Какие это параметры? (Каждый ответ является частью решения. Выберите два.)
- a. **Запретить установку принтеров, использующих работающие в режиме ядра драйверы** (Disallow Installation Of Printers Using Kernel Mode Drivers).
  - b. **Всегда обрабатывать задания печати на сервере** (Always Render Print Jobs On The Server).
  - c. **Автоматическая публикация новых принтеров в Active Directory** (Automatically Publish New Printers In Active Directory).
  - d. **Заполнение строки поиска принтера** (Pre-Populate Printer Search Location Text).
  - e. **Разрешить публикацию принтеров** (Allow Printers To Be Published).

## Занятие 2. Планирование файловых серверов

Пользователям требуется возможность создавать файлы и сохранять их там, откуда их легко извлечь. При этом администратор не должен допустить чтение конфиденциальных файлов пользователями, которым это не разрешено. Администратор должен следить за тем, чтобы пользователи не засоряли сеть множеством файлов большого размера. На этом занятии рассказывается о настройке файлового сервера, разрешений доступа, квот, доступности хранилищ и нового компонента BranchCache для сетевых файлов, появившегося в Windows Sever 2008 R2.

---

### Изучив материал этого занятия, вы сможете:

- ✓ Планировать инфраструктуру файлов и папок и устанавливать службы ролей, необходимые для реализации этого плана.
- ✓ Управлять разрешениями на доступ и обеспечивать доступность хранилищ.
- ✓ Планировать и применять файловые квоты.
- ✓ Использовать компонент BranchCache для сетевых файлов.

**Продолжительность занятия — примерно 45 мин.**

---

## Настройка файлового сервера

Файловый сервер обеспечивает место в сети, где пользователи могут хранить файлы и предоставлять их другим пользователям. Если какой-то файл, напри-

мер, документ с описанием политики компании, нужен многим пользователям, следует обеспечить удаленный доступ к нему. В целях централизации администрирования, резервного копирования, восстановления и использования теневых копий, следует хранить пользовательские файлы на файловом сервере, а не на отдельных компьютерах, хотя пользователям обычно требуется также возможность работать со своими файлами в автономном режиме.

Чтобы настроить сервер под управлением Windows Server 2008 R2 как файловый сервер, добавьте роль файловых служб, включающую несколько служб ролей. Роль файлового сервера устанавливается автоматически при открытии общего доступа к папке на этом сервере. На рис. 7-17 показан список служб ролей, устанавливаемых в составе роли файловых служб.

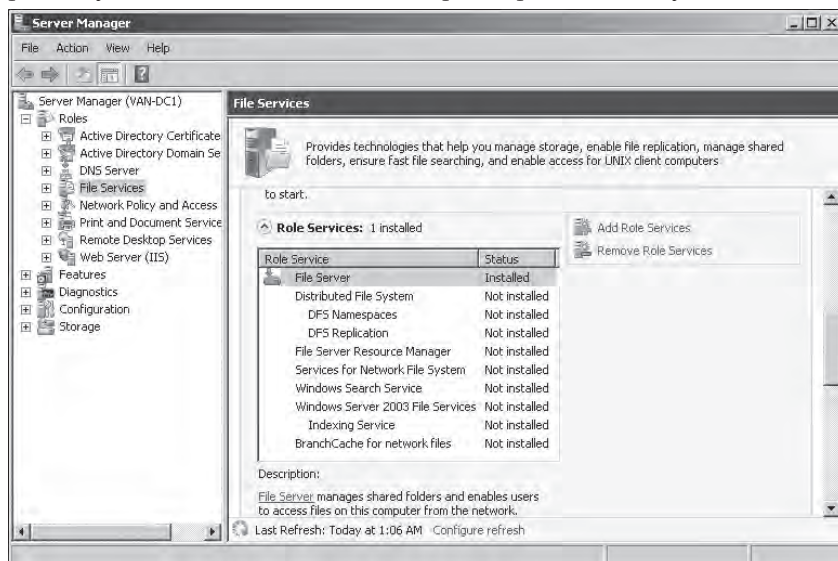


Рис. 7-17. Службы ролей, входящие в состав файловых служб

На этапе планирования необходимо определить, какие службы ролей требуются, и как они должны быть настроены. Всегда есть искушение установить все службы на случай, если они когда-нибудь понадобятся. Не делайте этого. Чем больше служб установлено на сервере, тем выше нагрузка на ограниченные ресурсы и больше возможностей для атаки.

Роль файловых служб включает следующие компоненты:

- средство управления общими ресурсами и хранилищами (предоставляется файловым сервером), включающее оснастку **Управление дисками**, позволяющую настраивать теневые копии;
- распределенная файловая система (DFS), включающая пространства имен DFS и репликацию DFS;
- диспетчер ресурсов файлового сервера;
- службы для сетевой файловой системы;
- служба поиска Windows;
- файловые службы Windows Server 2003, включающие устаревшую службу индексации;

- BranchCache для сетевых файлов, новый компонент Windows Server 2008 R2.

### ПРИМЕЧАНИЕ Дополнительные компоненты

Часто одновременно с файловыми службами устанавливаются такие компоненты, как модуль архивации сервера Windows, диспетчер хранилища для сетей SAN, средство отказоустойчивости кластера и многопутевой ввод-вывод. Эти компоненты рассматриваются в главах 10 и 13.

## Управление общими ресурсами и хранилищами

Оснастка **Управление общими ресурсами и хранилищами** (Share And Storage Management) по умолчанию устанавливается совместно с ролью файлового сервера. Открыть эту оснастку можно из диспетчера сервера или из меню **Администрирование**. Для совместного доступа к содержимому папок и управления общими папками она использует протокол SMB 2.0.

На рис. 7-18 показана оснастка **Управление общими ресурсами и хранилищами** (открытая из меню **Администрирование**, а не из диспетчера сервера) со списком общих папок на контроллере домена VAN-DC1. Ваш контроллер домена может иметь дополнительные общие ресурсы, если вы создавали их, экспериментируя с сетью.

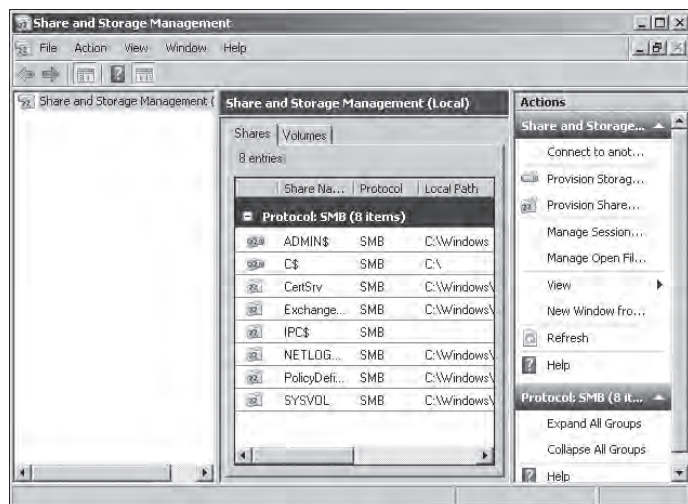


Рис. 7-18. Оснастка Управление общими ресурсами и хранилищами

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Протокол SMB

Подробнее о протоколе SMB и его разновидности — протоколе CIFS, см. по адресу <http://msdn.microsoft.com/en-us/library/aa365233.aspx> (на английском языке). Однако на экзамене вряд ли будет подробно спрашиваться об этом протоколе.

При помощи оснастки **Управление общими ресурсами и хранилищами** можно управлять томами и дисками (рис. 7-19; тома на вашем контроллере домена могут отличаться от показанных на рисунке).

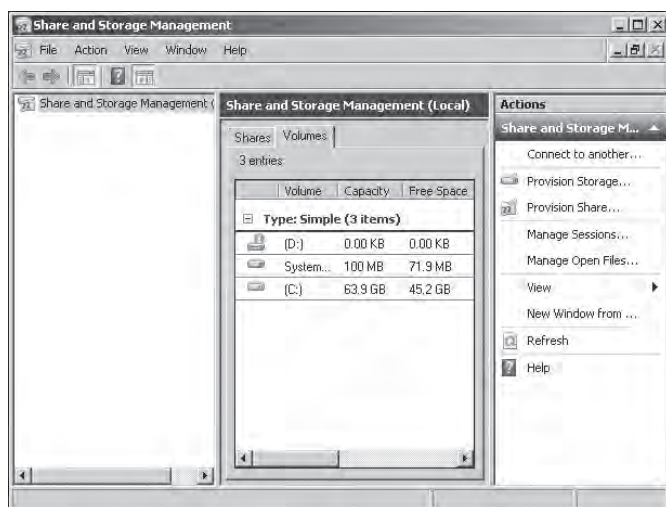


Рис. 7-19. Управление томами

Если открыть оснастку **Управление общими ресурсами и хранилищами** из диспетчера сервера, можно обращаться к консоли **Управление дисками** (рис. 7-20; диски на вашем контроллере домена могут отличаться от показанных на рисунке).

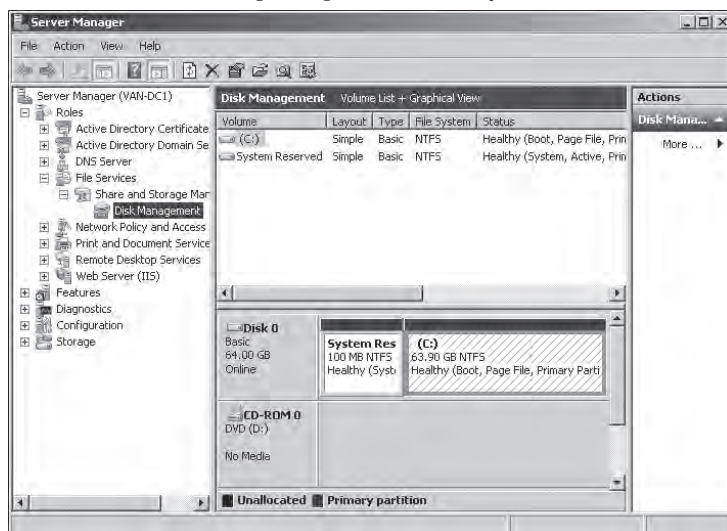


Рис. 7-20. Управление дисками

К содержимому папок и томов на сервере под управлением Windows Server 2008 и 2008 R2 можно организовать общий доступ, используя мастер подготовки общих папок, который запускается командой **Подготовить общий ресурс** (Provision Share) из области Действия (Actions) оснастки **Управление общими ресурсами и хранилищами**. Этот мастер (рис. 7-21) помогает выполнить действия, необходимые для предоставления общего доступа к папке или тому и настройки их параметров.

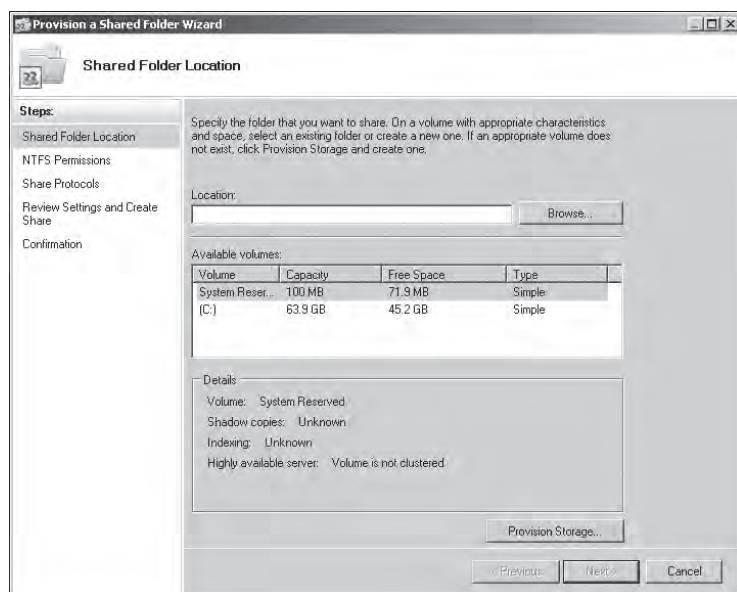


Рис. 7-21. Мастер подготовки общих папок

Мастер подготовки общих папок позволяет выполнять следующее:

- выбрать существующую папку или том или создать новую папку для организации общего доступа;
- выбрать сетевой протокол для доступа к общим ресурсам;
- изменить локальные разрешения NTFS для папки или тома, предоставляемого в общий доступ;
- настроить разрешения общего ресурса, ограничения пользователей и параметры автономного доступа к файлам из общего ресурса;
- опубликовать общий ресурс в пространстве имен DFS.

Если установлена роль сервера служб для NFS, можно указать для общего ресурса разрешения, совместимые с сетевой файловой системой (NFS). Если установлена служба роли диспетчера ресурсов файлового сервера, для общего ресурса можно настраивать квоты хранилища и ограничивать типы файлов, которые можно там хранить.

При помощи оснастки **Управление общими ресурсами и хранилищами** можно прекратить общий доступ к ресурсу, выбрав его на вкладке **Общие ресурсы** (Shares) (см. рис. 7-18) и нажав кнопку **Прекратить общий доступ** (Stop Sharing) на панели **Действия** (Actions). Если к папке или тому открыт общий доступ по протоколам SMB и NFS, нужно прекратить общий доступ для каждого протокола в отдельности. Предварительно следует убедиться, что общий ресурс не используется. Это можно сделать при помощи функций **Управление сеансами** (Manage Sessions) и **Управление открытыми файлами** (Manage Open Files) оснастки **Управление общими ресурсами и хранилищами** (см. далее в этом разделе).

Оснастка **Управление общими ресурсами и хранилищами** позволяет также просматривать и изменять свойства общей папки или тома, включая локальные



разрешения NTFS и разрешения сетевого доступа. Для этого выберите общий ресурс на вкладке **Общие ресурсы (Shares)**, а затем выберите команду **Свойства (Properties)** на панели **Действия (Actions)** или щелкните правой кнопкой ресурс и выберите команду **Свойства (Properties)**. На рис. 7-22 показано диалоговое окно свойств для общей папки Public. Кнопка **Дополнительно (Advanced)** на вкладке **Доступ (Sharing)** позволяет настроить ограничения на число пользователей и параметры кэша, а также отключить или включить перечисление на основе доступа (ABE). Перечисление на основе доступа включено по умолчанию; оно позволяет скрывать файлы и папки от пользователей, не имеющих к ним доступа. На вкладке **Разрешения (Permissions)** указываются разрешения NTFS и разрешения общего ресурса.

#### ПРИМЕЧАНИЕ Административные ресурсы

Нельзя изменить разрешения на доступ к стандартным административным общим ресурсам, таким как C\$ и ADMIN\$.

Если требуется просмотреть или закрыть открытые сеансы и открытые файлы (например, перед прекращением общего доступа к ресурсу), щелкните **Управление сеансами (Manage Sessions)** или **Управление открытыми файлами (Manage Open Files)** на панели **Действия (Actions)** в оснастке **Управление общими ресурсами и хранилищами**. На рис. 7-23 показано диалоговое окно **Управление сеансами**.

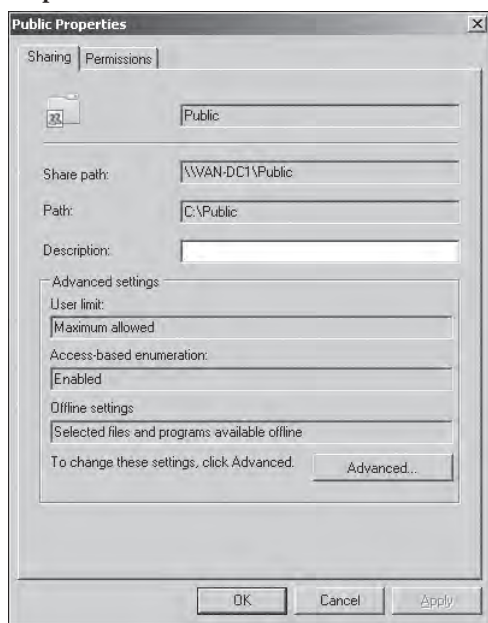


Рис. 7-22. Диалоговое окно свойств общего ресурса

Оснастка **Управление общими ресурсами и хранилищами** позволяет подготавливать хранилище на дисках сервера под управлением Windows Server 2008/2008 R2 или в подсистемах хранилищ, поддерживающих службу виртуальных дисков (VDS). Мастер подготовки хранилища (рис. 7-24) помогает создать том на существующем диске или в подсистеме хранилища, такого как



SAN, подключенного к серверу. Чтобы запустить этот мастер, щелкните **Подготовить хранилище (Provision Storage)** на панели **Действия (Actions)** в области **Управление общими ресурсами и хранилищами**.

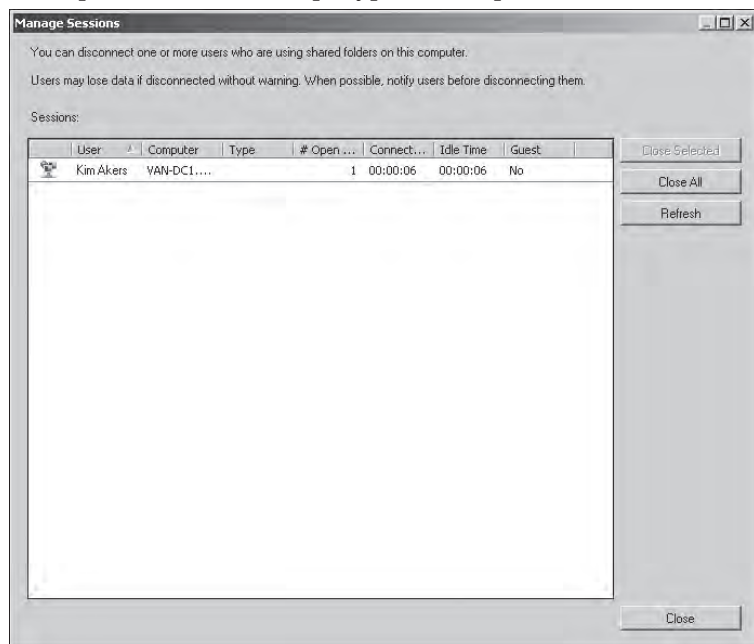


Рис. 7-23. Диалоговое окно Управление сеансами

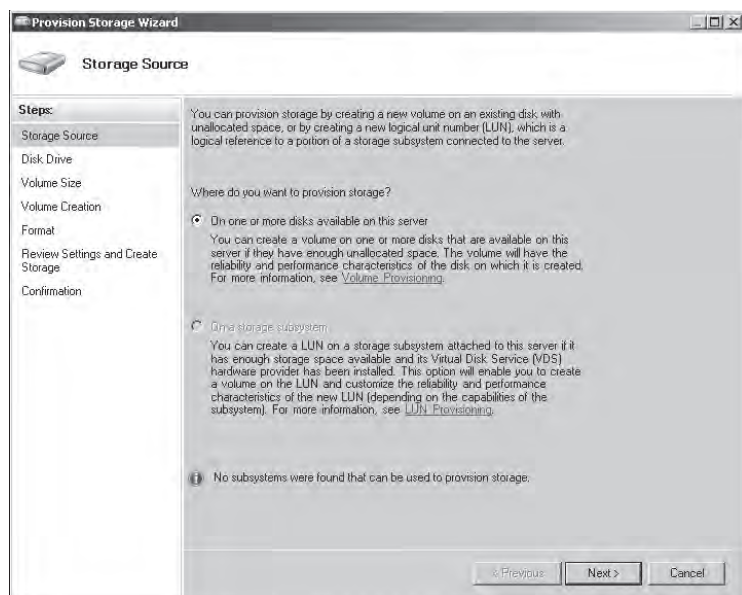


Рис. 7-24. Мастер подготовки хранилища

Если том создается в подсистеме хранилища, с помощью мастера можно создать логический номер устройства (logical unit number, LUN) для размеще-

ния этого тома. Можно также создать LUN при помощи мастера, а позже использовать оснастку **Управление дисками** (см. рис. 7-20) для создания тома.

#### **ПРИМЕЧАНИЕ** Запуск мастера подготовки хранилища

Мастер подготовки хранилища можно запустить только в том случае, если сервер имеет доступ к дискам с нераспределенным пространством или подсистемам хранилища с доступным пространством, для которых установлен поставщик оборудования VDS. Кроме того, том можно создать только на подключенном диске. Подробнее о подготовке хранилищ рассказывается в гл. 10.

Если достаточно места на диске или ресурсов в подсистеме хранилища, мастер подготовки хранилища может выполнить следующее:

- выбрать диск, на котором создается том;
- указать размер тома;
- назначить букву диска или точку подключения;
- форматировать том (это можно сделать также из оснастки **Управление дисками**).

Оснастку **Управление общими ресурсами и хранилищами** можно использовать для мониторинга и управления томами на сервере. Она позволяет выполнять следующее:

- увеличить размер тома;
- форматировать том;
- удалить том;
- изменить свойства тома, включая параметры сжатия, безопасности, доступности в автономном режиме и индексирования;
- обращаться к сервисным инструментам для проверки на ошибки, дефрагментации и резервного копирования.

#### **Логические номера устройств**

Логический номер устройства (LUN) ссылается на часть подсистемы хранилища. Это может быть диск, часть диска, дисковый массив целиком или его часть. Номера LUN упрощают управление хранилищем, предоставляя логические идентификаторы, через которые можно назначать привилегии для доступа и управления.

Мастер подготовки хранилища из оснастки **Управление общими ресурсами и хранилищами** позволяет создавать номера LUN для дисковых подсистем Fibre Channel и iSCSI, подключенных к серверу. После этого можно назначить LUN своему серверу или другим серверам в сети. В процессе создания LUN можно создать том с этим LUN и отформатировать его; кроме того, можно сначала создать LUN, а том позже.

Для создания LUN в подсистеме хранилища необходимо выполнение следующих условий:

- подсистема хранилища поддерживает VDS;
- на сервере установлен поставщик оборудования VDS для подсистемы хранилища;

- в подсистеме есть свободное место;
- подсистема хранилища подключена напрямую к серверу или доступна по сети.

Если требуется назначить LUN другому серверу или кластеру, в который не входит сервер, на котором запущен мастер подготовки хранилища, необходимо настроить подключения к серверам, используя диспетчер хранилища для сетей SAN (подробнее об этом см. в гл. 10). Если требуется назначить LUN кластеру, убедитесь, что каждый сервер кластера является членом только одного кластера и настроен посредством установки средства отказоустойчивости кластеров. Если включено несколько портов Fibre Channel или адаптеров инициатора iSCSI для доступа LUN, убедитесь, что сервер поддерживает многопутевой ввод-вывод.

---

**ПРИМЕЧАНИЕ Диспетчер хранилища для сетей SAN**

Диспетчер хранилища для сетей SAN не устанавливается по умолчанию. Чтобы установить его, щелкните **Добавить компоненты** (Add Features) под узлом **Компоненты** (Features) в диспетчере сервера.

---

---

**ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ iSCSI**

Подробнее о iSCSI можно узнать из руководства, доступного по адресу <http://download.microsoft.com/download/a/e/9/ae91dea1-66d9-417c-ade4-92d824b871af/uguide.doc> (на английском языке). Однако на экзамене вряд ли будет подробно спрашиваться о iSCSI.

---

---

**ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Многопутевой ввод-вывод**

Подробнее о многопутевом вводе-выводе см. по адресу [http://technet.microsoft.com/en-us/library/ee619734\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/ee619734(Ws.10).aspx) (на английском языке).

---

---

**ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Управление общими ресурсами и хранилищами**

Подробнее об оснастке **Управление общими ресурсами и хранилищами** можно узнать, выполнив в командной строке команду `hh storagemgmt.chm`.

---

**Распределенная файловая система**

Распределенная файловая система (DFS) в Windows Server 2008 и 2008 R2 значительно улучшена и устанавливается как служба роли в составе файловых служб. Подробнее эта тема рассматривается в гл. 10, здесь же приводится только краткое описание. DFS включает две технологии: DFSN (пространства имен DFS) и DFSR (репликация DFS), которые можно использовать (совместно или по отдельности) для обеспечения отказоустойчивости и повышения гибкости служб репликации и совместного использования файлов.

DFSN позволяет группировать общие папки с разных серверов (и из разных сайтов) в одно или несколько логически структурированных пространств имен. Пользователи просматривают каждое пространство имен как одну папку, содержащую подпапки. Лежащая в основе структура общих папок скрыта от пользователей, и эта структура обеспечивает отказоустойчивость и возможность автоматически подключать пользователей к локальным общим папкам, когда таковые доступны, вместо перенаправления по WAN-подключениям.

DFSR предоставляет механизм репликации с несколькими хозяевами, который позволяет синхронизировать папки с нескольких серверов по локальной сети или WAN-подключениям. Используется протокол RDC, позволяющий обновлять только те файлы, которые были изменены с момента последней репликации. DFSN и DFSR можно использовать совместно или по отдельности.

## Диспетчер ресурсов файлового сервера

Диспетчер ресурсов файлового сервера (File Server Resource Manager, FSRM) — служба роли, которую можно установить в составе файловых служб Windows Server 2008 R2. Установка этой службы роли предоставляет доступ к инструментам, с помощью которых можно определять и контролировать объем и тип данных, хранящихся на серверах. С помощью FSRM можно устанавливать квоты для папок и томов, активно отслеживать файлы и генерировать отчеты хранилища. Подробнее о возможностях FSRM рассказывается далее на этом занятии. Роль сервера FSRM вы установите на практикуме этой главы.

## Службы для NFS

Службы для NFS (сетевой файловой системы) можно установить в составе файловых служб. NFS предоставляет решение для совместного использования файлов, подходящее для организаций со смешанными сетями Windows и UNIX. Службы для NFS позволяют передавать файлы между компьютерами, работающими под управлением Windows Sever 2008/2008 R2 и UNIX, по протоколу NFS. Службы для NFS в Windows Sever 2008 и 2008 R2 имеют следующие улучшения:

- **Поиск в Active Directory.** Управление удостоверениями для UNIX расширяет схему Active Directory, добавляя поля идентификатора пользователя UNIX (UID) и идентификатора группы (GID). Это позволяет серверу для NFS и клиенту для NFS обращаться к сопоставлениям учетных записей пользователей Windows с UNIX непосредственно из AD DS. Управление удостоверениями для UNIX упрощает сопоставление учетных записей пользователей Windows с UNIX в AD DS.
- **Поддержка 64-разрядных систем.** Службы для NFS можно устанавливать во всех версиях Windows Server 2008, включая 64-разрядные, и во всех версиях Windows Server 2008 R2.
- **Повышенная производительность сервера.** Службы для NFS включают драйвер фильтра файлов, который значительно уменьшает задержки при обращении к файловому серверу.
- **Поддержка специальных устройств UNIX.** Поставщики служб для NFS поддерживают специальные устройства UNIX, используя функцию *mknod* (создание каталога, специального или обычного файла).

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ MKNOD

Подробнее о функции *mknod* см. по адресу <http://www.opengroup.org/onlinepubs/009695399/functions/mknod.html> (на английском языке). Однако на экзамене вряд ли будут вопросы о функциях UNIX.

---

- **Расширенная поддержка UNIX.** Службы для NFS поддерживают следующие версии UNIX: Sun Microsystems Solaris версии 9, Red Hat Linux версии 9, IBM AIX версии 5L 5.2 и Hewlett Packard HP-UX версии 11i.

---

**ПРИМЕЧАНИЕ Улучшения в Windows Server 2008 R2**

Службы для NFS в Windows Server 2008 R2 усовершенствованы и поддерживают сетевые группы, используемые для поддержки именованных групп хостов в сети. Также поддерживается протокол удаленного вызова процедур служб безопасности Security\_Generic (RPCSEC\_GSS), позволяющий приложениям использовать интерфейс GSS\_API для проверки подлинности и целостности. Это позволяет использовать инструментарий WMI для удаленного управления NFS и делает возможным доступ несопоставленных пользователей UNIX к общим ресурсам NFS.

---

**ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Службы для NFS**

Чтобы подробнее узнать о службах для NFS, в том числе о появившихся в Windows Server 2008 R2 улучшениях, откройте командную строку и введите `hh nfs__lh.chm`.

**Проверьте себя**

- Какие три основные задачи можно выполнять при помощи диспетчера ресурсов файлового сервера?

**Ответ**

- Устанавливать квоты для папок и томов, активно отслеживать файлы, генерировать отчеты хранилища.

**Служба поиска Windows**

Служба поиска Windows позволяет клиентам, совместимым с этой службой, быстро выполнять поиск файлов на сервере. Она создает указатель наиболее распространенных типов данных на сервере, таких как сообщения электронной почты, контакты, события в календаре, документы, фотографии и мультимедиа. Файлы указателя и типы данных позволяют выполнять быстрый поиск файлов на сервере Windows Server 2008/2008 R2 с клиентов под управлением Windows Vista или Windows 7, а также Windows XP с установленной панелью поиска Windows.

Служба поиска Windows заменяет службу индексирования, имевшуюся в Windows Server 2003. В составе роли **Файловые службы** в Windows Server 2008 и 2008 R2 можно установить роль файловых служб Windows Server 2003, включая службу индексирования. Однако службу индексирования нельзя установить, если установлена служба поиска Windows.

В процессе установки службы поиска Windows можно выбрать тома или папки, которые требуется индексировать. Microsoft рекомендует выбирать том, а не папку, только в том случае, если этот том используется исключительно для размещения общих папок.

## Файловые службы Windows Server 2003

Роль файловых служб в Windows Server 2008 и 2008 R2 включает службы ролей, совместимые с Windows Server 2003. Если требуется, можно включить устаревшую службу индексирования, которая каталогизирует содержимое и свойства файлов на локальном и удаленных компьютерах. Заметьте, что если установить службу поиска Windows, то службу индексирования установить нельзя.

В Windows Server 2008 можно установить также службу репликации файлов (FRS), которая позволяет синхронизировать папки с файловыми серверами, использующими FRS. Однако Microsoft рекомендует использовать службу DFSR, когда это возможно. В Windows Server 2008 R2 для репликации папок DFS и SYSVOL вместо FRS используется DFSR. В Windows Server 2008 R2 нет возможности установить службу роли FRS.

## BranchCache для сетевых файлов

Служба роли BranchCache для сетевых файлов помогает уменьшить использование WAN и повысить скорость ответа сетевых приложений при обращении из офисов филиалов к содержимому, хранящемуся в центральном офисе. Это новая для Windows Server 2008 R2 роль, и мы подробнее обсудим ее далее.

## Дополнительные компоненты

При необходимости можно установить следующие компоненты в дополнение к службам ролей, входящим в состав роли файловых служб:

- **Система архивации данных Windows** предоставляет надежный способ резервного копирования и восстановления операционной системы, приложений, файлов и папок, хранящихся на сервере.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Система архивации данных Windows

Для получения подробной информации откройте командную строку и введите `hh backup.chm`.

- **Диспетчер хранилища для сетей SAN** позволяет подготавливать хранилище в одной или нескольких подсистемах хранилища Fibre Channel или iSCSI в сети SAN.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Диспетчер хранилища для сетей SAN

Для получения подробной информации откройте командную строку и введите `hh sanmgr.chm`.

- **Отказоустойчивость кластеров.** Этот компонент позволяет объединять несколько серверов в кластер для повышения доступности служб и приложений. Если один из узлов (серверов) кластера выходит из строя, другие узлы продолжают работать, обеспечивая отказоустойчивость.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Отказоустойчивость кластеров в Windows Server 2008 R2

Подробнее об отказоустойчивости кластеров, в том числе об улучшениях в Windows Server 2008 R2, см. по адресу [http://technet.microsoft.com/ru-ru/library/ff182338\(WS.10\).aspx](http://technet.microsoft.com/ru-ru/library/ff182338(WS.10).aspx).

---

- **Многопутевой ввод-вывод (МPIO)**, о котором уже упоминалось выше, обеспечивает поддержку нескольких путей к данным между файловым сервером и устройством хранилища. Многопутевой ввод-вывод можно использовать для повышения доступности данных, предоставляя избыточные подключения к подсистемам хранилища, а также для балансировки нагрузки на устройства ввода-вывода и повышения производительности системы и приложений.

## Улучшения в файловых службах Windows Server 2008 R2

В Windows Server 2008 R2 управление данными выполняется более эффективно и рационально. Предоставляемые инструменты помогают понять, как организуется работа с данными, и уменьшить затраты на хранение, обслуживание и контроль данных. Теперь стало проще применять политику компании и снижать риск утечки данных.

### Инфраструктура классификации файлов

Инфраструктура классификации файлов (FCI) в Windows Server 2008 R2 помогает более эффективно управлять данными, снизить затраты и риски. Она предоставляет встроенное решение для классификации файлов, позволяющее автоматизировать ранее выполнявшиеся вручную процессы обработки, используя заранее определенные политики, основанные на ценности данных для предприятия.

Файловые системы на серверах, работающих под управлением предыдущих операционных систем, хранят файлы и предоставляют доступ на основе разрешений. Однако они не классифицируют файлы в соответствии с их ценностью для организации. Если нет никаких указаний относительно ценности данных, хранящихся в файле, сложно принимать решения насчет срока хранения старых файлов или определять, какие файлы требуют более высокого уровня защиты. Возможность вручную и автоматически классифицировать файлы в соответствии с установленными правилами позволяет управлять организационными данными более эффективно и определять, какие данные и где требуется сохранить.

Диспетчер ресурсов файлового сервера позволяет обращаться к свойствам и правилам классификации и использовать встроенную функциональность Windows Server 2008 R2, чтобы классифицировать файлы на основе их содержимого и расположения. Это обеспечивает более эффективную защиту и управление на основе ценности для организации. Классификация файлов позволяет выполнять следующее:

- идентифицировать чувствительные данные на серверах, находящихся в открытом доступе;
- автоматически настраивать срок хранения старых файлов;
- использовать собственные сценарии; например, можно использовать сценарий для перемещения файлов с низкой ценностью на более дешевые запоминающие устройства;
- производить интеграцию с ПО сторонних производителей.



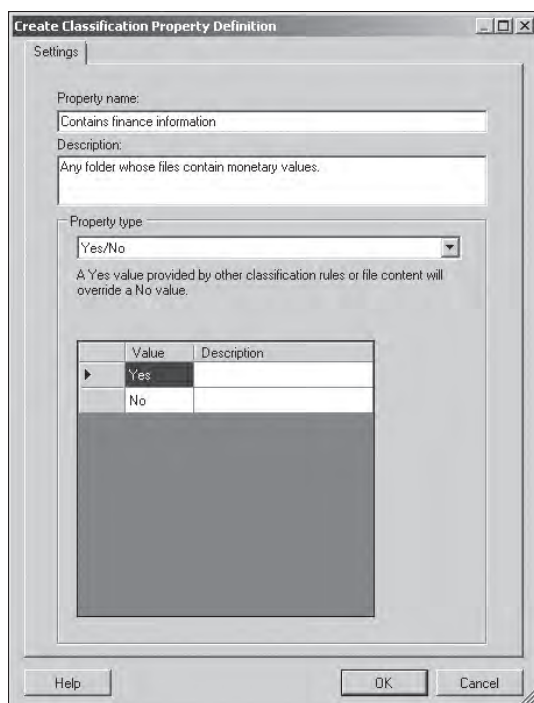


Рис. 7-25. Диалоговое окно Создание определения свойства классификации

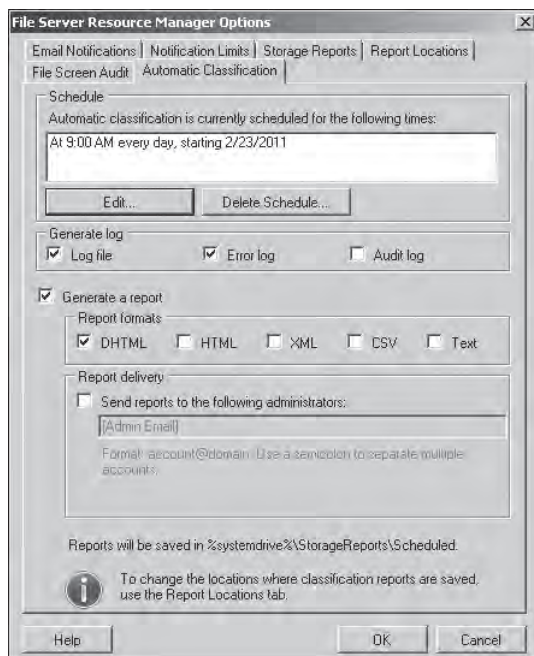


Рис. 7-26. Настройка расписания классификации

На рис. 7-25 показано диалоговое окно **Создание определения свойства классификации** (Create Classification Property Definition). Щелкнув **Правила**

**классификации** (Classification Rules), можно создать новое правило классификации или настроить расписание классификации. На рис. 7-26 показано настроенное расписание классификации на вкладке **Автоматическая классификация** (Automatic Classification) диалогового окна **Параметры диспетчера ресурсов файлового сервера** (File Server Resource Manager Options). Чтобы открыть это окно, щелкните **Правила классификации** (Classification Rules) под узлом **Свойства классификации** (Classification Properties) в оснастке диспетчера ресурсов файлового сервера, а затем щелкните **Настроить расписание классификации** (Configure Classifications Schedule) на панели **Действия** (Actions).

---

#### **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ** Классификация файлов

Подробнее о работе с классификацией файлов см. по адресу [http://technet.microsoft.com/ru-ru/library/dd758765\(v=ws.10\).aspx](http://technet.microsoft.com/ru-ru/library/dd758765(v=ws.10).aspx).

---

### **Управление распределенными файлами**

Файловые службы Windows Server 2008 R2 включают службы DFSR и DFSN, о которых уже говорилось на этом занятии. Эти службы облегчают доступ к файлам и общим ресурсам в инфраструктуре сети. DFSR обеспечивает эффективную двустороннюю репликацию изменений в файлах, выполняя синхронизацию нескольких копий одного файла. DFSN облегчает поиск общих ресурсов и позволяет пользователям обращаться к данным, не обращая внимания на то, на каких физических серверах находятся эти файлы. Прозрачное перенаправление и реплицированные копии повышают продуктивность работы, приближая данные к пользователям и обеспечивая их высокую доступность.

Подробнее DFS обсуждается в гл. 10. Коротко говоря, технологии DFS используются для выполнения репликации по WAN-каналам, упрощают доступ к географически распределенным файлам и повышают их доступность. В Windows Server 2008 R2 DFS улучшена, работает более эффективно и предоставляет следующие преимущества:

- более эффективный доступ к данным;
- упрощенный доступ к файлам;
- повышенная продуктивность и доступность данных;
- поддержка отказоустойчивых кластеров;
- репликация папок, доступных только для чтения.

---

#### **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ** Управление DFS в Windows Server 2008 R2

Подробнее о возможностях управления DFS в Windows Server 2008 R2 см. по адресу <http://technet.microsoft.com/ru-ru/library/cc732006.aspx>.

---

### **Управление дисками**

Оснастка **Управление дисками** (Disk Management), о которой мы уже говорили, используется для управления жесткими дисками и томами или разделами на них. Можно инициализировать диски, создавать тома и форматировать их в FAT, FAT32 и NTFS. Эта оснастка позволяет выполнять большинство задач по работе с дисками, не перезагружая систему и не прерывая работу пользователей. Большинство изменений вступает в силу незамедлительно.

В Windows Server 2008 R2 оснастка **Управление дисками** предоставляет следующие возможности:

- **Упрощенное создание разделов дисков.** Щелкнув том правой кнопкой мыши, можно выбрать из контекстного меню, какой раздел следует создать: простой, составной или чередующийся.
- **Возможности преобразования диска.** Если добавить более четырех разделов на простой диск, будет предложено преобразовать диск в динамический или в таблицу разделов GUI (GPT).
- **Возможность расширять и сжимать разделы.** Расширять и сжимать разделы можно непосредственно из оснастки **Управление дисками**.

---

#### **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ** Управление дисками

Подробнее об управлении дисками в Windows Server 2008 R2 см. по адресу <http://technet.microsoft.com/ru-ru/library/cc771097.aspx>.

---

### **Диспетчер ресурсов файлового сервера**

Как уже говорилось, в составе службы роли диспетчера ресурсов файлового сервера (FSRM) устанавливается оснастка **Управление классификацией** (Classification Management). В Windows Server 2008 R2 диспетчер ресурсов предоставляет улучшенные службы управления файлами по протоколам CIFS/SMB и NFS. FSRM объединяет несколько утилит файловых служб, доступных в предыдущих версиях серверных ОС Windows, и предоставляет единый интерфейс для управления всеми параметрами распределения файлов, квот и общего доступа. В Windows Server 2008 R2 FSRM имеет встроенные средства создания отчетов, позволяющие определять, как можно использовать для управления, аудита и планирования доступные ресурсы, и предоставляет следующие преимущества:

- улучшенные файловые службы;
- улучшенный контроль и соответствие файлов;
- понимание того, как используются файловые серверы.

О том, как использовать FSRM для настройки квот и политики фильтра блокировки файлов, рассказывается далее на этом занятии.

---

#### **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ** Диспетчер ресурсов файлового сервера

Подробнее о возможностях диспетчера ресурсов файлового сервера в Windows Server 2008 R2 см. по адресу <http://technet.microsoft.com/ru-ru/library/cc732431.aspx>.

---

### **Съемные ЗУ**

Оснастка **Съемные ЗУ** (Removable Storage) позволяет отслеживать съемные запоминающие устройства и управлять библиотеками, которые содержат их. Эта оснастка помечает, каталогизирует и отслеживает носители, управляет библиотеками, гнездами и дверцами и выполняет очистку устройств. Она работает совместно с программами управления данными, которые работают с данными, хранящимися на съемных носителях. Оснастка **Съемные ЗУ** позволяет нескольким программам совместно использовать одни и те же ресурсы

съемных ЗУ и собирает все носители из библиотек в различные пулы. Также она перемещает носители между пулами, предоставляя приложениям требуемый объем хранилища.

Microsoft убрала из Windows Server 2008 R2 диспетчер съемных носителей, заменив его новой технологией архивации. Недоступна также утилита Ntbackup, и невозможно восстанавливать файлы и папки или целые тома из старых архивов, созданных при помощи Ntbackup в Windows Server 2008 и предыдущих версиях Windows. Однако это возможно, если установить утилиту восстановления архивов Windows NT для Windows 7 и Windows Server 2008 R2, доступную по адресу <http://support.microsoft.com/kb/974674>.

---

#### **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Съемные ЗУ в Windows Server 2008 R2**

Подробнее об оснастке **Съемные ЗУ** в Windows Server 2008 R2 см. по адресу <http://technet.microsoft.com/ru-ru/library/cc772263.aspx>.

---

## **Службы для NFS**

Как уже говорилось, службы для NFS можно установить в составе роли сервера Файловые службы. Они включают сервер для NFS и клиент для NFS и предоставляют организациям со смешанными сетями Windows и UNIX решение для общего доступа к файлам. Службы для NFS позволяют передавать файлы между серверами, работающими под управлением Windows Server 2008 R2 и UNIX, по протоколу NFS. Версия служб для NFS, входящая в состав Windows Server 2008 R2, имеет следующие улучшения:

- **Упрощенное администрирование.** Для упрощения настройки клиентов NFS представлена функция доступа несопоставленных пользователей UNIX.
- **Поиск Active Directory.** Расширение схемы Active Directory для управления удостоверениями UNIX включает поля UNIX UID и GID. Это позволяет серверу для NFS и клиенту для NFS выполнять поиск сопоставлений учетных записей Windows с UNIX напрямую в AD DS.
- **Повышенная производительность сервера.** Службы для NFS включают драйвер фильтра файлов, который значительно уменьшает задержки доступа при обращении к файлам на сервере.
- **Поддержка особых устройств UNIX.** Службы для NFS поддерживают особые устройства UNIX.
- **Улучшенная поддержка UNIX.** Службы для NFS поддерживают Sun Microsystems Solaris версии 9, Red Hat Linux версии 9, IBM AIX версии 5L 5. и Hewlett Packard HP-UX версии 11i. Безопасность NFS повышается при помощи протокола Kerberos.

---

#### **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Службы для NFS**

Подробнее о службах для NFS в Windows Server 2008 R2 см. по адресу <http://technet.microsoft.com/ru-ru/library/cc753495.aspx>.

---

## **Теневые копии общих папок**

Теневые копии общих папок предоставляют копии файлов, хранящихся в общих ресурсах, в том состоянии, в котором они находились в определенный момент

времени. Доступ к предыдущим версиям файлов (теневым копиям) дает пользователям возможность восстанавливать случайно удаленные или перезаписанные файлы и сравнивать разные версии файлов.

Ниже приведены характеристики теневых копий общих папок в Windows Server 2008 R2:

- **Целостность драйвера снимков тома.** Для создания теневых копий общих папок используется драйвер снимков тома (Volsnap.sys). Этот драйвер использует пространство хранилища, выделенное для хранения снимка содержимого общих папок. Это пространство называется областью копирования или разностной областью.
- **Целостность области копирования.** Снимок — это блочный набор данных, представляющих разницу между текущим содержимым и содержимым в определенный момент времени. На томе выделяется область копирования, в которой хранятся снимки содержимого общих папок. Целостность существующих и новых снимков зависит от целостности области копирования.
- **Откат тома.** Теневые копии общих папок позволяют возвращать том в то состояние, в котором он был при создании теневой копии.

---

**ПРИМЕЧАНИЕ Откат тома**

После отката тома все изменения, произошедшие в файлах и папках на этом томе со времени создания теневой копии, будут потеряны.

---

---

**ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Теневые копии в Windows Server 2008 R2**

Подробнее о теневых копиях общих папок в Windows Server 2008 R2 см. по адресу [http://technet.microsoft.com/en-us/library/dd364797\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/dd364797(Ws.10).aspx) (на английском языке).

---

**Управление общими ресурсами и хранилищами**

Оснастка **Управление общими ресурсами и хранилищами** (Share And Storage Management), о которой мы уже говорили на этом занятии, позволяет централизованно управлять файлами и томами, к которым открыт общий доступ, а также томами на дисках и в подсистемах хранилищ. Мастер подготовки общих папок позволяет организовать общий доступ к содержимому папок и томов на серверах в сети. Оснастка позволяет подготавливать хранилища на доступных серверу дисках или подсистемах хранилищ, поддерживающих VDS.

Мастер помогает пройти процесс создания тома на существующем диске или в подсистеме хранилища, подключенной к серверу. Если том создается в подсистеме хранилища, мастер также поможет создать LUN для размещения этого тома. Кроме того, можно сначала создать LUN, а затем использовать оснастку **Управление дисками** (Disk Management) для создания тома. Оснастку **Управление общими ресурсами и хранилищами** можно использовать для мониторинга и управления созданными и любыми имеющимися томами, доступными серверу.

---

**ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Управление общими ресурсами и хранилищами**

Подробнее об оснастке **Управление общими ресурсами и хранилищами** в Windows Server 2008 R2 см. по адресу <http://technet.microsoft.com/ru-ru/library/cc731574.aspx>.

---

## Общие папки

В Windows Server 2008 R2 доступна оснастка **Общие папки** (Shared Folders) (рис. 7-27), позволяющая централизованно управлять общими ресурсами. С помощью этой оснастки можно создавать общие ресурсы, задавать разрешения, просматривать и управлять открытыми файлами и пользователями, подключенными к общим ресурсам компьютера.

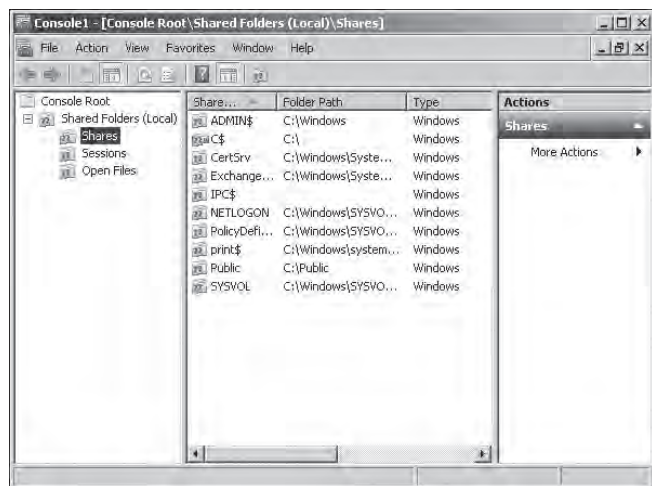


Рис. 7-27. Оснастка Общие папки

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Общие папки

Подробнее об оснастке **Общие папки** в Windows Server 2008 R2 см. по адресу <http://technet.microsoft.com/ru-ru/library/cc770406.aspx>.

---

## Проводник хранилищ

Коммутирующая матрица (fabric) — сетевая топология, в которой устройства подключены друг к другу через один или несколько высокоэффективных путей данных. В коммутирующей матрице Fibre Channel сеть включает один или несколько коммутаторов Fibre Channel, позволяющих серверам и устройствам хранения подключаться друг к другу через виртуальные соединения точка-точка. В коммутирующей матрице iSCSI сеть включает один или несколько серверов iSNS, обеспечивающих возможность поиска и разделения ресурсов. Проводник хранилищ позволяет просматривать и управлять коммутирующими матрицами Fibre Channel и iSCSI, доступными в сети SAN.

Оснастка **Проводник хранилищ** (Storage Explorer) (рис. 7-28) позволяет просматривать подробную информацию о серверах, подключенных к сети SAN, и о компонентах коммутирующей матрицы, таких как адаптеры главной шины (host bus adapter, HBA), коммутаторы Fibre Channel, инициаторы и конечные объекты iSCSI. Можно также выполнять административные задачи в коммутирующей матрице iSCSI; например, можно заходить на конечные объекты iSCSI, настраивать безопасность iSCSI, добавлять конечные порталы iSCSI, добавлять iSNS-серверы, управлять доменами обнаружения и наборами доменов обнаружения.

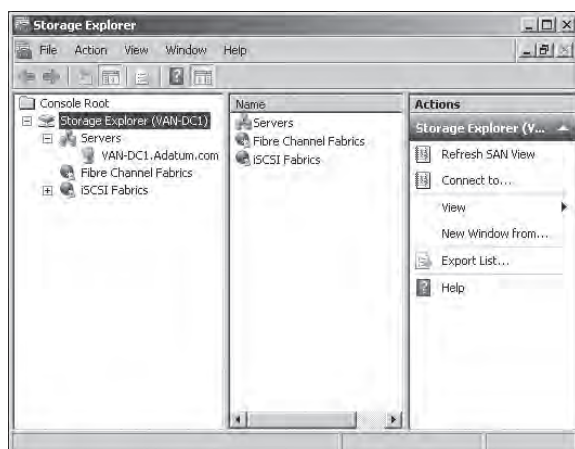


Рис. 7-28. Оснастка Проводник хранилищ

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Домены обнаружения и наборы доменов обнаружения

Подробнее о доменах обнаружения и наборах доменов обнаружения см. по адресу <http://technet.microsoft.com/ru-ru/library/cc753442.aspx>.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Проводник хранилищ

Подробнее об оснастке **Проводник хранилищ** в Windows Server 2008 R2 см. по адресу <http://technet.microsoft.com/library/cc731884.aspx>.

---

## Диспетчер хранилища для сетей SAN

Оснастка **Диспетчер хранилища для сетей SAN** (Storage Manager for SANs) позволяет создавать логические номера устройств (LUN) и управлять ими в дисковых подсистемах хранения Fibre Channel и iSCSI, поддерживающих виртуальную дисковую службу (VDS) в сети хранения данных (SAN). Использование LUN упрощает управление ресурсами хранилищ в сети SAN, поскольку LUN служат логическими идентификаторами, через которые можно назначать привилегии доступа и управления.

Как уже говорилось, LUN представляет собой логическую ссылку на часть подсистемы хранения. LUN может указывать на диск, часть диска, целый дисковый массив или раздел дискового массива в подсистеме.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Диспетчер хранилища для сетей SAN

Подробнее об оснастке **Диспетчер хранилища для сетей SAN** в Windows Server 2008 R2 см. по адресу <http://technet.microsoft.com/ru-ru/library/cc771378.aspx>.

---

#### Проверьте себя

- Какой инструмент позволяет просматривать коммутирующие матрицы Fibre Channel и iSCSI, доступные в сети SAN, и управлять ими?

#### Ответ

- Проводник хранилищ.



## Перенаправление папок

Перенаправление папок позволяет перенаправить путь к папке в новое расположение, такое как каталог в общем ресурсе в сети. Пользователи могут продолжать работать с файлами на файловом сервере, как если бы эти файлы хранились на локальном диске клиентской станции. Документы в папке доступны в сети со всех клиентских станций. Перенаправление папок — это параметр групповой политики, который можно настроить для любого объекта групповой политики (GPO) с включенным разделом **Конфигурация пользователя**. Можно щелкнуть правой кнопкой любую папку, выбрать команду **Свойства** и настроить параметры перенаправления. На рис. 7-29 показаны параметры перенаправления, доступные для папки **Start Menu** (Главное меню).

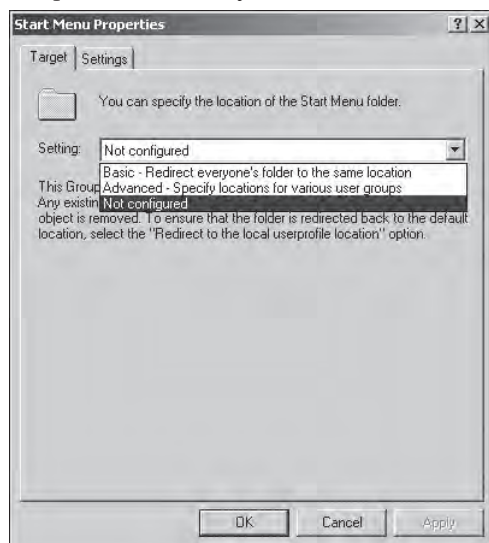


Рис. 7-29. Параметры перенаправления папки Start Menu

Перенаправление папок — не новая возможность, но в Windows Server 2008 R2 появились улучшения:

- возможность перенаправлять больше папок из профиля пользователя, чем в предыдущих версиях Windows; к таким папкам относятся **Контакты**, **Загрузка**, **Избранное**, **Ссылки**, **Музыка**, **Сохраненные игры**, **Поиски** и **Видео**;
- возможность применять параметры для перенаправленных папок к компьютерам, работающим под управлением предыдущих версий Windows;
- возможность перенаправления папок **Музыка**, **Изображения** и **Видео** совместно с папкой **Документы**;
- возможность перенаправления папки **Главное меню** в определенное расположение для всех пользователей.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Перенаправление папок

Подробнее о перенаправлении папок, в том числе об улучшениях в Windows Server 2008 R2, см. по адресу <http://technet.microsoft.com/ru-ru/library/cc732275.aspx>.

---

## Автономные файлы

Автономные файлы дают мобильным и удаленным пользователям возможность обращаться к файлам из общих ресурсов и продолжать работать с ними, когда компьютер не подключен к сети.

Компонент **Автономные файлы** (Offline Files) создает локальный кэш удаленных файлов и папок, делая их доступными пользователю при отсутствии подключения к сети. Пользователи могут работать с этими файлами таким же образом, как при подключении к сети, так как сохраняются пути к сетевым ресурсам и пространства имен. Кроме того, кэш ускоряет доступ к этим файлам и папкам при низкой скорости подключения.

Когда подключение к сети восстанавливается, все изменения, внесенные пользователем при работе в автономном режиме, автоматически передаются в сеть. Изменения, внесенные при работе через медленное подключение, автоматически синхронизируются с версией на сервере в качестве фоновой задачи, выполняемой с регулярными интервалами.

Главное изменение в компоненте **Автономные файлы** в Windows Server 2008 R2 — значительное улучшение доступа к файлам через WAN-подключения, благодаря которому удаленным пользователям стало удобнее работать с сетевыми файлами. Есть и другие улучшения:

- быстрый первый вход в систему;
- фоновая синхронизация;
- список исключений;
- прозрачное кэширование.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Автономные файлы

Подробнее об улучшениях компонента **Автономные файлы** в Windows Server 2008 R2 см. по адресу [http://technet.microsoft.com/ru-ru/library/ff183315\(Ws.10\).aspx](http://technet.microsoft.com/ru-ru/library/ff183315(Ws.10).aspx) (на английском языке).

---

## BranchCache для сетевых файлов

Как уже говорилось на этом занятии, BranchCache для сетевых файлов — служба роли, которую в Windows Server 2008 R2 можно установить в составе роли сервера **Файловые службы**. Эта роль службы недоступна в предыдущих версиях Windows Server. Она уменьшает нагрузку на WAN-каналы и повышает скорость ответа сетевых приложений, когда удаленные пользователи обращаются к данным, хранящимся в центральном офисе.

Эта служба роли кэширует на удаленных компьютерах копию данных, полученных от веб-сервера или файлового сервера, расположенного в центральном офисе. Если другой клиент из того же удаленного офиса запрашивает эти данные, он может получить их из своей локальной сети, а не через WAN-подключение. На практикуме этой главы вы установите службу роли BranchCache для сетевых файлов.

Удаленные пользователи могут столкнуться с проблемами производительности при использовании сетевых приложений, подключающихся к серверам по WAN-каналам. Открытие большого файла из общей папки, расположенной на сервере в центральном офисе, может потребовать много времени, и это при том, что современным пользователям задержка даже в несколько секунд кажется

ся долгой. Например, пользователь, просматривающий видео через веб-обозреватель, вынужден ждать, пока загрузится видео.

Если используется BranchCache для сетевых файлов, пользователи из удаленного офиса получают тот же уровень обслуживания, что и пользователи в центральном офисе. Первый клиент из удаленного офиса, загрузивший данные с веб-сервера или файлового сервера (*сервера содержимого*), создает копию в локальной сети этого офиса. Другие клиенты загружают локальную кэшированную копию после прохождения проверки подлинности и авторизации на сервере содержимого.

Служба роли BranchCache для сетевых файлов предназначена для работы с существующей сетевой инфраструктурой и инфраструктурой безопасности. Она поддерживает IPv4, IPv6 и методы шифрования типа «узел-узел», такие как SSL и IPSec. Клиенты получают самую свежую версию содержимого из своей локальной сети, предварительно пройдя авторизацию на сервере содержимого. Клиенты должны работать под управлением Windows 7 с включенной функцией BranchCache, а файловые и веб-серверы — под управлением Windows Server 2008 R2 с установленной службой роли BranchCache для сетевых файлов. Чтобы включить использование BranchCache для общей папки, откройте диалоговое окно свойств этой папки и щелкните **Параметры автономного режима** (Offline Settings) на вкладке **Общие** (General). На рис. 7-30 показано диалоговое окно **Параметры автономного режима** (Offline Settings) с установленным флажком **Включить BranchCache** (Enable BranchCache).

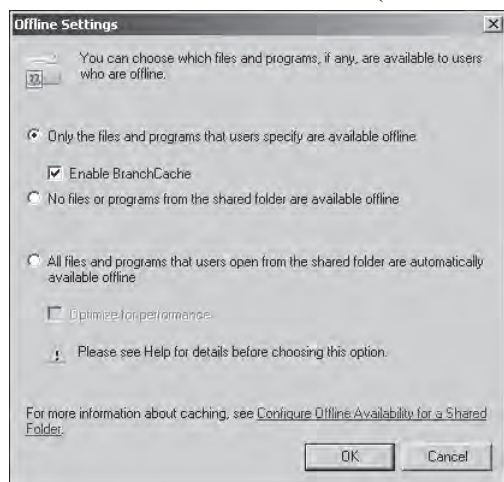


**Рис. 7-30.** Включение BranchCache для сетевых файлов

В зависимости от размещения кэша, BranchCache может работать в одном из двух режимов:

- **Размещенный кэш.** В удаленном офисе один компьютер под управлением Windows Server 2008 R2 назначается хостом. Клиентам указывается полное доменное имя хоста, с которого они могут получать содержимое размещенного кэша. Если в размещенном кэше нет нужных данных, они загружаются с сервера содержимого по WAN-каналу и сохраняются в кэше для следующих клиентов.

- **Распределенный кэш.** Обычно используется в филиалах, где пользователей меньше 50. В этом режиме локальный клиент под управлением Windows 7 хранит копию содержимого и делает ее доступной другим авторизованным клиентам. Это избавляет от необходимости развертывания сервера в филиале. Однако этот режим работает только в одной подсети (в отличие от размещенного кэша), а значит, содержимое приходится получать по WAN-каналу для каждой подсети в филиале. Кроме того, клиенты, отключающиеся от сети (например, отправляемые в режим гибернации), не могут предоставлять запрашиваемое содержимое.

Для уменьшения трафика BranchCache отправляет метаданные содержимого клиентам, которые затем получают содержимое из своей локальной сети. Метаданные содержимого значительно меньше, чем само содержимое. Перед отправкой метаданных сервер авторизует клиента. Сервер содержимого должен отправлять метаданные каждому клиенту, чтобы гарантировать, что клиент всегда получает хеши актуального содержимого.

Содержимое разбивается на блоки. Для каждого блока вычисляется хеш. Кроме того, для набора блоков вычисляются хеши сегментов. Метаданные содержимого состоят, в основном, из хешей блоков и хешей сегментов. В качестве алгоритма хеширования используется SHA 256. Достигается коэффициент сжатия примерно 2000:1, т.е. размер метаданных примерно в 2000 раз меньше размера исходных данных.

---

#### **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ SHA 256**

Если у вас есть профессиональный интерес к алгоритмам хеширования, изучите документ [http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchange\\_notice.pdf](http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchange_notice.pdf). Однако на экзамене не будет вопросов по алгоритмам хеширования, описанным в этом документе.

---

Хеши сегментов помогают уменьшить общее число операций поиска определенного содержимого (в сравнении с поиском каждого блока). Когда клиенту требуется получить данные из размещенного кэша или с другого клиента, он загружает содержимое частями, которые определяются хешами блоков.

---

#### **ПРИМЕЧАНИЕ Минимальный размер кэшируемого содержимого**

Минимальный размер содержимого, кэшируемого BranchCache — 64 КБ. Данные меньшего размера загружаются напрямую с сервера содержимого по WAN-каналу.

---

## **Windows Storage Server 2008 R2**

Windows Storage Server 2008 R2 предоставляет те же файловые службы, что и Windows Storage Server 2008, но с некоторыми дополнениями и улучшениями. Это сервер хранилища в составе Windows Server 2008 R2, предоставляющий платформу для NAS-устройств. Семейство Windows Storage Server 2008 R2, включающее версии Enterprise, Standard и Workgroup, предоставляет решения для организации хранилищ организациям любого размера, используя такие технологии, как дедупликация файлов (удаление дубликатов файлов и данных) и программные конечные объекты iSCSI для унифицированных файловых служб и хранилища блоков ввода-вывода.

---

**ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Инициатор iSCSI в Windows Server 2008 R2**

Подробнее об инициаторе iSCSI в Windows Server 2008 R2 см. по адресу [http://technet.microsoft.com/ru-ru/library/dd878522\(WS.10\).aspx](http://technet.microsoft.com/ru-ru/library/dd878522(WS.10).aspx).

---

Windows Storage Server 2008 R2 обеспечивает упрощенное развертывание и управление отдельными устройствами и кластерами хранилищ с двойными узлами. Версия Enterprise включает мастера, позволяющие автоматизировать установку отказоустойчивого кластера с двумя узлами.

Хранилище единственных копий (Single Instance Storage, SIS) уменьшает объем хранилища, используемый данными, заменяя несколько идентичных копий логическими ссылками на единственную копию, выполняя таким образом дедупликацию. Теперь SIS поддерживает 128 томов на одном сервере. Windows Storage Server 2008 R2 включает командлеты Windows PowerShell для управления SIS, такие как Install-SisVolume, Enable-SisVolume и Get-SisVolume.

---

**ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Командлеты PowerShell для управления SIS**

Подробнее о командлетах PowerShell, используемых для управления SIS в Windows Storage Server 2008 R2, см. по адресу <http://technet.microsoft.com/en-us/library/gg278036.aspx> (на английском языке).

---

Windows Storage Server 2008 R2 обеспечивает сетевой доступ к файлам по протоколам SMB и NFS. При помощи DFS и DFSR организуется унифицированное пространство имен и репликация файлов, публикуемых в дополнительных офисах. Windows Storage Server 2008 R2 можно удаленно администрировать из Internet Explorer при помощи элемента управления ActiveX и из других обозревателей посредством элементов управления Java RDP. Windows Storage Server 2008 R2 предоставляет рентабельное, надежное и масштабируемое решение для предоставления доступа к данным и управления ими. Доступны следующие возможности:

- **Распределенный доступ к файловым службам.** Файловые службы Windows Storage Server 2008 R2 позволяют более эффективно предоставлять доступ к файлам, которые обычно распределены по всей сети организации. Распределенный доступ повышает эффективность управления хранилищем. Доступ производится быстрее, а управление облегчается, независимо от платформы и расположения данных.
- **Централизованное управление файловыми службами.** Средства централизованного управления включают элементы управления для исключения ненужных данных и утилиты, облегчающие управление нужными данными. Эти инструменты уменьшают затраты на администрирование и предоставляют информацию об инфраструктурах, помогающую более эффективно обеспечивать соответствие и доступность файловых служб.
- **Рентабельная масштабируемость и повышенная продуктивность.** Файловые службы Windows Storage Server 2008 R2 позволяют расширять спектр ИТ-услуг и обеспечивают эффективную и недорогую поддержку роста числа пользователей.

Эти улучшенные возможности реализованы посредством следующих компонентов файловых служб Windows Storage Server 2008 R2 (и Windows 7):

- **SMB версии 2.1.** Это более эффективная версия протокола SMB, оптимизированная для работы по медленным каналам связи и обеспечивающая большую гибкость и совместимость для клиентов под управлением Windows 7.
- **NFS.** Этот протокол позволяет организациям с гетерогенным окружением объединять общие ресурсы в Windows Storage Server 2008 R2 и облегчает предоставление общего доступа к ресурсам на компьютерах, работающих под управлением Windows и других операционных систем.
- **DFS.** DFSR и DFSN более эффективно предоставляют доступ к данным и упрощают доступ к файлам и общим ресурсам в сетевой инфраструктуре. Кроме того, DFS расширяет традиционные файловые службы, облегчая поиск общих ресурсов.
- **FSRM.** Эта роль сервера предоставляет единый интерфейс, позволяющий управлять файловыми службами по протоколам CIFS/SMB и NFS и улучшающий контроль и соответствие файлов.
- **FCI.** Этот компонент автоматизирует процессы классификации, помогающие управлять данными более эффективно. Организация может сэкономить деньги и снизить риски, храня файлы на основе их ценности. FCI предоставляет средства для определения срока действия файлов, выполнения настраиваемых задач и создания отчетов.

### Пакет средств переноса файлового сервера

При переходе на Windows Server 2008 R2 с предыдущих версий Windows Server необходимо обеспечить правильное назначение разрешений и сохранить прежние способы работы пользователей и соглашения насчет имен файлов. Пакет средств переноса файлового сервера (File Server Migration Toolkit, FSMT) можно загрузить по адресу <http://www.microsoft.com/downloads/en/details.aspx?FamilyID=d00e3eae-930a-42b0-b595-66f462f5d87b&displaylang=en>. Пакет включает два пошаговых мастера, помогающих перенести существующие файловые серверы в Windows Server 2008 R2.

## Управление доступом

Управление доступом — процесс предоставления пользователям, группам и компьютерам доступа к объектам в сети или на компьютере с учетом разрешений, наследования разрешений, владения объектом, аудита и прав пользователей.

Разрешения определяют тип доступа к объекту, предоставляемый пользователю или группе. Если к папке или тому открыт общий доступ, и пользователи удаленно обращаются к содержимому (например, файлам на файловом сервере), для этих пользователей действуют разрешения, настроенные для общего ресурса. Папки и файлы на томе NTFS имеют также разрешения NTFS, действующие как при локальном доступе, так и при доступе по сети. Разрешения на доступ к файлам на файловом сервере обычно определяются комбинацией разрешений NTFS и разрешений общего ресурса, назначенных для папки или иерархии папок, содержащей файлы. Объектам принтера назначаются разрешения печати.



Каждый контейнер и объект в сети имеет связанную (или прикрепленную) информацию об управлении доступом, определенную в дескрипторе безопасности. Эта информация определяет тип доступа, разрешенный пользователям и группам безопасности. Разрешения, определенные в дескрипторе безопасности объекта, связаны с конкретными пользователями и группами безопасности (назначены им). Каждое назначение разрешений пользователю или группе представлено в системе в виде записи ACE (access control entry). Полный набор таких записей в дескрипторе безопасности называется набором разрешений или списком управления доступом (access control list, ACL).

Разрешения NTFS можно назначать файлам, объектам Active Directory, объектам реестра и системным объектам, таким как процессы. Это выполняется на вкладке **Безопасность** (Security) диалогового окна свойств объекта, которую иногда называют интерфейсом управления доступом пользователям. Разрешения можно предоставлять отдельным пользователям, группам безопасности, компьютерам и другим объектам, имеющим идентификаторы безопасности в домене. Рекомендуется назначать разрешения группам безопасности, а не отдельным пользователям.

Разрешения, назначенные на доступ объекту, зависят от типа объекта. Например, разрешения на доступ к файлу, отличаются от разрешений на доступ к принтеру или разделу реестра. Назначая разрешения, вы указываете уровень доступа пользователей и групп. Например, можно позволить одному пользователю читать содержимое файла, другому вносить изменения в файл, а всем остальным запретить доступ.

Microsoft утверждает, что наследование разрешений облегчает администраторам назначение и управление разрешениями и обеспечивает согласованность разрешений для всех объектов в определенном контейнере. Наследование приводит к автоматическому получению объектами, находящимися в контейнере, всех наследуемых разрешений этого контейнера. Например, дочерние папки по умолчанию наследуют разрешение родительской папки, а файлы в папке автоматически получают разрешения, настроенные для папки.

Несомненно, наследование удобно для настройки разрешений. Можно блокировать наследование разрешений папки и явно назначать разрешения дочерним объектам. Можно изменить разрешения на доступ к файлам так, что разные файлы в папке будут иметь разные разрешения. Это дает большую гибкость, но может и усложнять ситуацию, так что наследование затрудняет, а не облегчает управление разрешениями. Как и в случае с остальными административными задачами, главное — тщательно все планировать и избегать исключений. Следует также ограничить использование явного запрета разрешений. Если пользователю явно запрещено разрешение, или он входит в группу, имеющую разрешение **Запретить**, это разрешение ему будет запрещено, независимо от того, в какие еще группы он входит.

При создании объекту назначается владелец. Обычно это тот пользователь, который создал объект. Так, владельцем файлов, сохраненных в папке **Документы** в профиле пользователя, является этот пользователь. Владелец объекта всегда может изменить разрешения на доступ к этому объекту.



---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Владение объектами

Подробнее о владении объектами см. по адресу <http://technet.microsoft.com/ru-ru/library/cc732983%28WS.10%29.aspx>.

---

Права дают пользователям и группам безопасности определенные привилегии и возможности. Их можно назначать группам и отдельным пользователям. Права авторизуют пользователей на выполнение определенных действий, таких как интерактивный вход в систему или резервное копирование файлов и каталогов.

Права пользователей отличаются от разрешений, так как права применяются к учетным записям пользователей, а разрешения прикрепляются к объектам. Хотя права можно применять к отдельным учетным записям пользователей, рекомендуется применять их к группам безопасности. Для администрирования прав пользователей используется оснастка **Локальные параметры безопасности** (Local Security Settings).

Можно выполнять аудит успешных и неудачных попыток доступа для каждого пользователя. Объекты для аудита выбираются при помощи интерфейса управления доступом, но сначала необходимо включить политику аудита, выбрав **Аудит доступа к объектам** (Audit Object Access) в разделе **Локальные политики** (Local Policies) оснастки **Локальные параметры безопасности**. После этого можно просматривать события в журнале безопасности, используя средство просмотра событий.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Аудит безопасности

Подробнее о аудите безопасности см. по адресу <http://technet.microsoft.com/ru-ru/library/cc771475%28WS.10%29.aspx>.

---

## Настройка разрешений на доступ

По умолчанию в Windows Server 2008 и 2008 R2 включен общий доступ к файлам и отключен доступ к общим папкам. Эти функции можно отключать и включать, щелкнув **Изменить дополнительные параметры общего доступа** (Change Advanced Sharing Settings) в Центре управления сетями и общим доступом, который запускается из Панели управления. На рис. 7-31 показано диалоговое окно **Дополнительные параметры безопасности** (Advanced Sharing Settings).

Можно также открыть консоль MMC и добавить оснастку **Общие папки** (Shared Folders), после чего щелкнуть правой кнопкой узел **Общие ресурсы** (Shares) и выбрать команду **Новый общий ресурс** (New Share), чтобы запустить мастер создания общих ресурсов. Этот мастер позволяет указать путь к папке, к которой требуется организовать общий доступ, и разрешения на доступ к ней.

На странице **Разрешения для общей папки** (Shared Folder Permissions) (рис. 7-32) можно выбрать стандартные разрешения для общей папки, например, **У всех пользователей доступ только для чтения** (All users have read-only access) или **Администраторы имеют полный доступ, остальные — доступ только для чтения** (Administrators have full access; other users have read-only access). Можно также установить переключатель **Настройка разрешений доступа** (Customize Permissions) и щелкнуть **Другой** (Custom), чтобы выбрать собственный

вариант разрешений. На рис. 7-33 показано диалоговое окно **Настройка разрешений доступа** (Customize Permissions). Мастер позволяет также настраивать параметры автономного доступа. Общий доступ можно открыть для папки или тома.

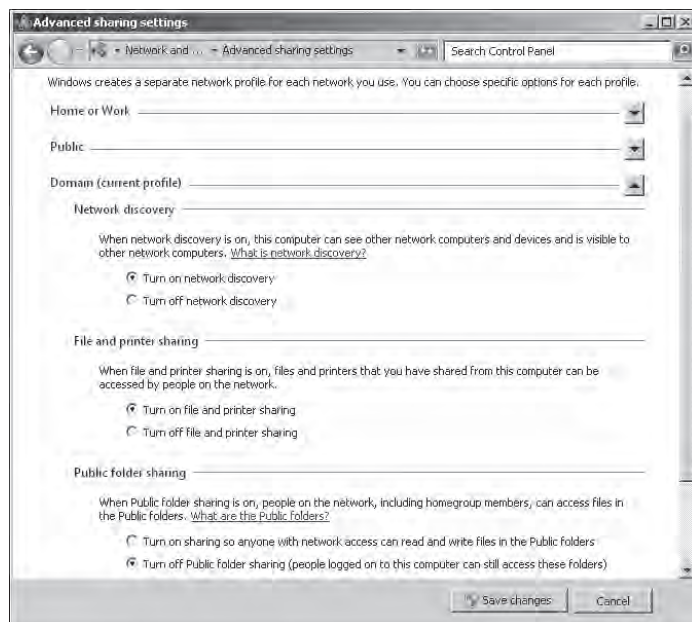


Рис. 7-31. Диалоговое окно дополнительных параметров общего доступа

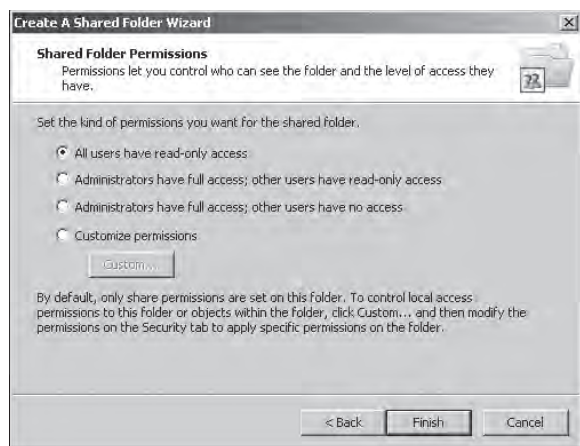


Рис. 7-32. Страница Разрешения для общей папки

### СОВЕТ Подготовка к экзамену

По умолчанию в Windows Server 2008 R2 для общей папки устанавливается разрешение **Все пользователи имеют доступ только для чтения** (All users have read-only access). В Windows Server 2008 по умолчанию предоставлялся полный доступ администраторам, а остальные пользователи имели доступ только для чтения.

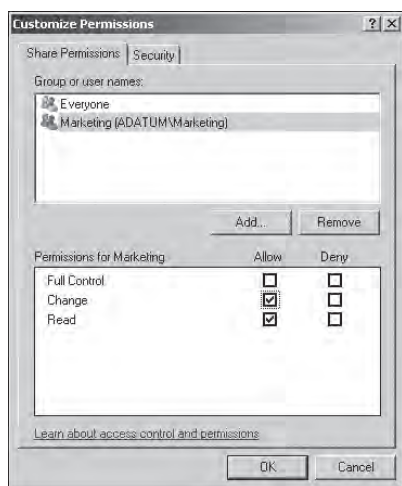


Рис. 7-33. Диалоговое окно Настройка разрешений

Если выбрать настройку разрешений, можно открыть вкладку **Безопасность** (Security), на которой можно настроить разрешения NTFS, выбрав группу или пользователя и щелкнув **Изменить** (Edit) (рис. 7-34). Для пользователей, обращающихся по сети к папкам на сервере (а это почти все пользователи), разрешения доступа будут складываться из разрешений для общей папки и разрешений NTFS.

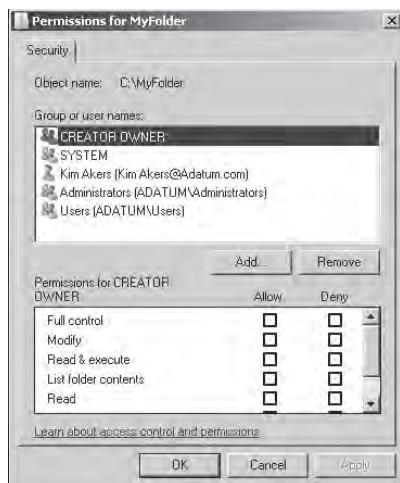


Рис. 7-34. Настройка разрешений NTFS

Создать и подготовить общую папку можно также при помощи оснастки **Управление общими ресурсами и хранилищами** (Share And Storage Management). В области **Действие** (Action) щелкните **Подготовка общего ресурса** (Provision Share) и укажите путь к папке. Запустится мастер подготовки общих папок, позволяющий изменить назначенные по умолчанию разрешения NTFS. Затем можно выбрать протокол, по которому пользователи смогут обращаться к общей папке: SMB и/или NFS. Заметьте, что NFS можно выбрать только в том случае, если установлены службы для NFS.

Нажав кнопку **Дополнительно** (Advanced), можно ограничить число пользователей, включить или отключить перечисление на основе доступа и настроить параметры кэширования. На рис. 7-35 показаны доступные параметры кэширования для работы в автономном режиме.

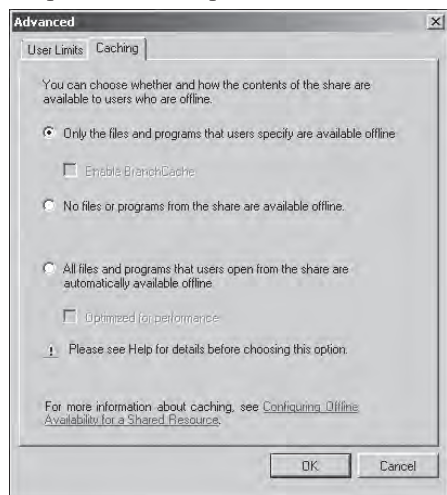


Рис. 7-35. Параметры кэширования

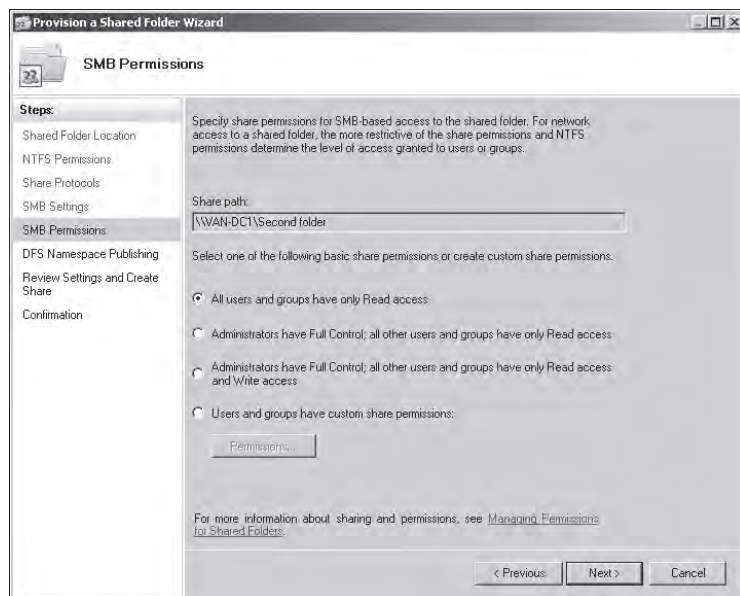


Рис. 7-36. Страница Разрешения SMB

Если настраиваются разрешения SMB (они используются чаще всего), можно выбрать одну из трех стандартных конфигураций разрешений для общих папок или настроить собственный набор разрешений. На рис. 7-36 показана страница **Разрешения SMB** (SMB Permissions). Если вы решите настроить разрешения, мастер откроет диалоговое окно, аналогичное окну **Настройка разрешений** (Customize Permissions), которое показано выше на рис. 7-33.

**ПРИМЕЧАНИЕ Разрешения SMB и NTFS**

Если разрешения SMB отличаются от разрешений NTFS для той же папки, применяться будет наиболее ограничивающий набор разрешений.

Далее мастер предложит опубликовать общий ресурс в пространстве имен DFS. Заметьте, что это нельзя сделать, если не установлены соответствующие службы ролей. Наконец, мастер покажет сводку параметров. Щелкните **Создать** (Create), чтобы создать общий ресурс.

Можно также вручную открыть общий доступ к папке и настроить разрешения для общей папки и разрешения NTFS, щелкнув правой кнопкой папку или том в Проводнике Windows и выбрав команду **Свойства** (Properties). Если использовать этот способ, откроется диалоговое окно, аналогичное показанному на рис. 7-37. На вкладке **Безопасность** (Security) диалогового окна свойств можно настроить разрешения NTFS.

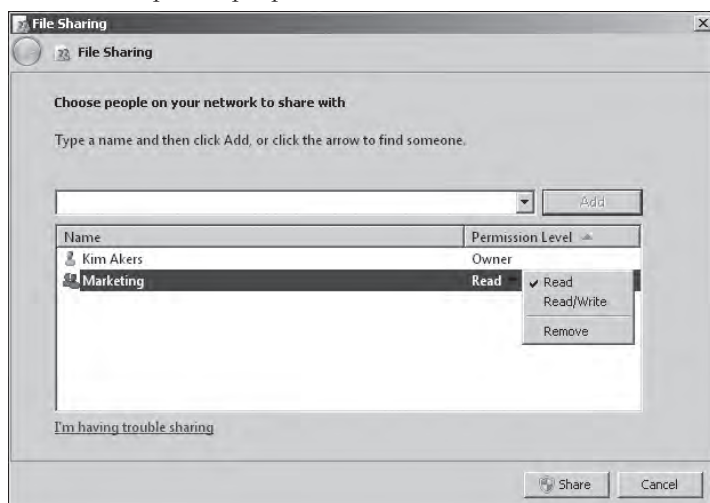


Рис. 7-37. Открытие общего доступа к папке вручную

**Комбинирование разрешений общих папок и NTFS**

К файлам, папкам и другим объектам пользователи обычно обращаются по сети; например, когда те расположены на файловом сервере. Однако элементы ACE применяются и на уровне общего ресурса (разрешения для общей папки), и на уровне файловой системы (разрешения NTFS). Это значит, что разрешения требуется изменять в двух местах.

Например, если члены группы безопасности Managers должны иметь возможность добавлять, изменять и удалять файлы в папке Reports, тогда как в текущий момент они могут только просматривать их, следует изменить разрешения NTFS для этой группы, добавив разрешение **Изменение** (Modify). Однако, если для общей папки установлено разрешение **Чтение** (Read), и вы забудете изменить его, члены группы по-прежнему смогут только просматривать содержимое файлов.

Одно из возможных решений этой проблемы — предоставить всем полный доступ на уровне общего ресурса и ограничивать доступ при помощи разреше-

ний NTFS. Действовать будут разрешения NTFS, как более ограничивающие. Однако многим администраторам не нравится идея предоставления неограниченных разрешений на уровне общей папки. С точки зрения безопасности лучше назначать разрешения **Изменение** (Change).

Чтобы выяснить, какие разрешения на доступ к файлу имеет группа, сначала нужно определить действующие разрешения NTFS, помня о том, что любые разрешения, явно установленные на уровне файла, переопределяют разрешения на уровне папки. Затем нужно сравнить разрешения NTFS с разрешениями для общего ресурса; действующими будут самые ограничивающие разрешения. Если пользователь входит в несколько групп, определить разрешения гораздо сложнее.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Действующие разрешения пользователя можно определить вручную. Это уточнительно, но с опытом становится проще. Во время написания книги в Windows Server 2008 и 2008 R2 не было средств для автоматизации этого процесса, но можно использовать утилиту Server Share Check из пакета Windows Server 2003 Resource Kit. Загрузить этот пакет можно по адресу <http://www.microsoft.com/downloads/details.aspx?familyid=9d467a69-57ff-4ae7-96ee-b18c4790cffd&displaylang=en>.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Server Share Check

Подробнее об утилите Server Share Check см. по адресу <http://searchwindowsserver.techtarget.com/tip/Checking-access-permissions-with-Server-Share-Check> (на английском языке). Для просмотра необходимо зарегистрироваться в сообществе SearchWindowsServer.com (бесплатно). Если не можете обратиться по этому адресу или не хотите регистрироваться на сайте, поищите в Интернете «Server Share Check».

---

## Настройка квот, политики блокирования файлов и отчетов хранилищ

В Windows Server 2008 и 2008 R2 расширены возможности по управлению квотами. Квоты можно назначать для папок и томов и настраивать шаблоны квот, позволяющие быстро создавать квоты. Можно создавать собственные квоты или брать за основу существующие шаблоны.

Microsoft рекомендует создавать квоты на основе шаблонов. Это упрощает управление квотами, так как можно автоматически обновлять все квоты, основанные на определенном шаблоне. Изменив такой шаблон, можно обновить параметры всех квот, созданных на его основе. Также можно исключить выбранные квоты из обновления. Например, если вы создали квоту на основе шаблона, а затем вручную изменили некоторые ее параметры, можете исключить ее из обновления, чтобы не потерять эти параметры.

Можно создать автоматически применяющуюся квоту и назначить шаблон квоты родительскому тому или папке. Квоты, созданные на основе этого шаблона, автоматически генерируются и применяются ко всем существующим подпапкам и подпапкам, которые будут созданы в будущем.



## Создание квот

Если установлена служба роли диспетчера ресурсов файлового сервера (File Server Resource Manager, FSRM), можно создавать квоты при помощи оснастки **Диспетчер ресурсов файлового сервера** (File Server Resource Manager). На рис. 7-38 показано диалоговое окно **Создание квоты** (Create Quota). Это окно не будет доступно, если не установлена соответствующая роль сервера (ее вы установите на практикуме этой главы). Здесь можно выбрать шаблон, на основе которого будет создана квота (это вы тоже сделаете на практикуме).

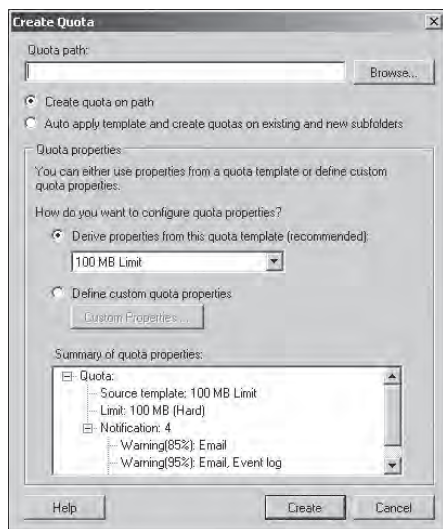


Рис. 7-38. Диалоговое окно Создание квоты

Следует ввести путь к тому или папке, для которой требуется создать квоту, и указать, будет ли квота создана только для этого пути, или будет автоматически применяться как шаблон для существующих и новых вложенных папок.

Обычно достаточно установить переключатель **Наследовать свойства из следующего шаблона квоты (рекомендуется)** [Derive Properties From This Quota Template (Recommended)] и выбрать шаблон. Если требуется, можно задать настраиваемые свойства квоты, но это не рекомендуется. Можно выбрать шаблоны, определяющие размер квоты, выделенной каждому пользователю, и указать, какой будет квота: жесткой или мягкой. Жесткая квота не может быть превышена. Пользователь может превысить мягкую квоту, но при этом обычно создается отчет, отправляется уведомление по электронной почте, а в журнал записывается событие. Мягкие квоты используются для мониторинга. Доступны следующие шаблоны квот:

- **Предел 100 МБ (100 MB Limit)** — жесткая квота; если достигнут предел квоты, пользователю и указанным администраторам по электронной почте отправляются уведомления, а в журнал событий записывается соответствующее событие;
- **Предел 200 МБ с уведомлением пользователя (200 MB Limit Reports To User)** — жесткая квота; при достижении предела квоты создается отчет, отправляются уведомления по электронной почте и создается запись в журнале событий;



- **Предел 200 МБ с расширением 50 МБ** (200 MB Limit With 50 MB Extension) — технически это жесткая квота, поскольку при попытке пользователя превысить предел квоты выполняется действие, а не просто ведется мониторинг. В качестве действия запускается программа, применяющая шаблон **Расширенный предел 250 МБ**, тем самым предоставляя пользователю дополнительно 50 МБ. Если предел превышен, по электронной почте отправляются уведомления, а в журнале событий создается запись;
- **Расширенный предел 250 МБ** (250 MB Extended Limit) — предел в 250 МБ, который не может быть превышен; если предел достигнут, по электронной почте отправляются уведомления, а в журнале событий создается запись;
- **Наблюдение за томом 200 ГБ** (Monitor 200 GB Volume Usage) — мягкая квота, применяемая только к томам; используется для мониторинга;
- **Наблюдение за общим ресурсом размером 500 МБ** (Monitor 500 MB Share) — мягкая квота, применяемая только к общим ресурсам; используется для мониторинга.

Шаблоны можно настроить так, чтобы они отправляли уведомления и создавали записи в журнале событий при достижении определенного процента квоты. На рис. 7-39 показаны свойства шаблона **Предел 200 МБ с уведомлением пользователя**.

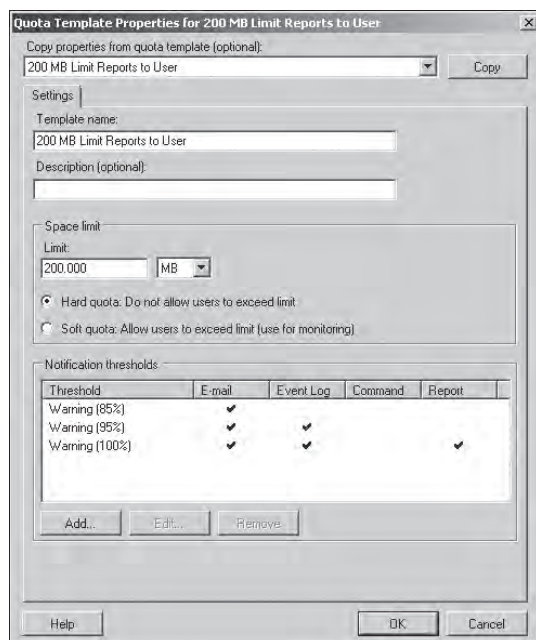


**Рис. 7-39.** Свойства шаблона Предел 200 МБ с уведомлением пользователя

Если создать обычную или автоматически применяющуюся квоту, ее можно редактировать. На рис. 7-40 показано диалоговое окно **Свойства квоты** (Quota Properties). Здесь можно добавить описание и изменить шаблон квоты, предел используемого пространства и пороговые значения для уведомлений. Можно добавить новые пороговые значения для уведомлений и указать, какое действие будет

выполняться, если достигнут предел. Например, можно указать, будет ли отправляться предупреждение по электронной почте пользователю и администраторам. Также можно ввести команду, создать отчет и указать, будет ли записываться событие в журнал. Если изменить параметры квоты или создать настраиваемую квоту, эту квоту можно использовать для создания нового шаблона.

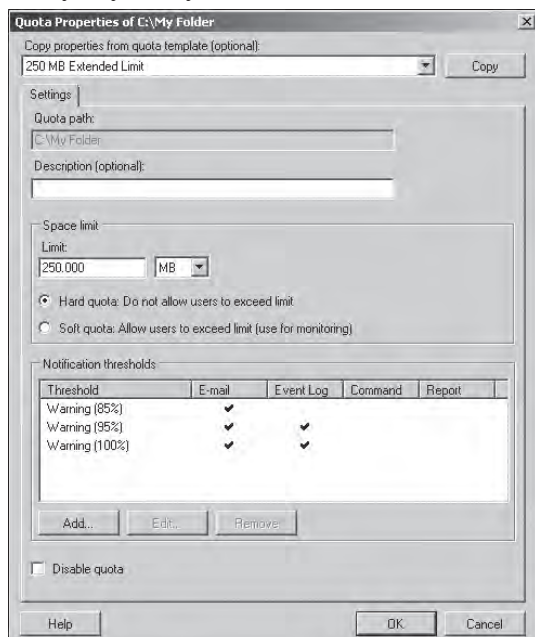


Рис. 7-40. Свойства квоты

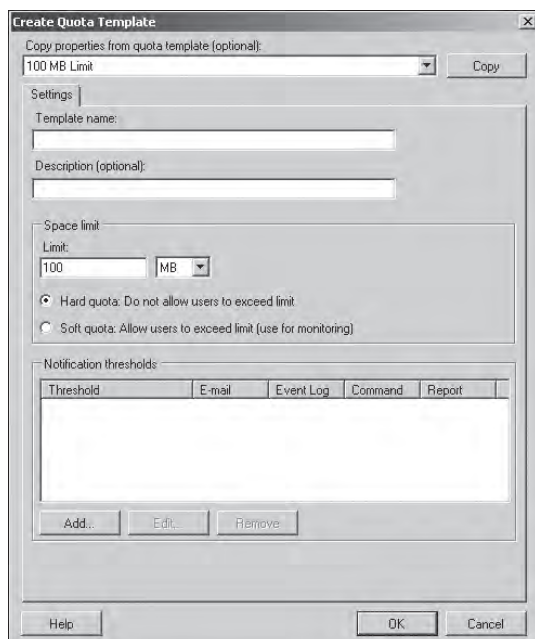


Рис. 7-41. Создание шаблона квоты

## Создание шаблонов

Если ни один из предлагаемых шаблонов вам не подходит, можете создать новый. Можно скопировать параметры из существующего шаблона и изменить их, а можно указать новые. На рис. 7-41 показано диалоговое окно **Создание шаблона квоты** (Create Quota Template). Многие из представленных здесь параметров аналогичны параметрам, настраиваемым при изменении квоты.

## Управление фильтрами блокировки файлов

Диспетчер ресурсов файлового сервера позволяет создавать фильтры блокировки файлов, позволяющие контролировать типы файлов, которые пользователям разрешено сохранять, и генерировать уведомления, когда пользователи пытаются сохранить неавторизованные файлы. Можно также определять шаблоны фильтров блокировки файлов и применять их к новым томам и папкам в сети организации.

Диспетчер позволяет также создавать исключения фильтров блокировки файлов, повышающие гибкость правил блокировки. Например, можно запретить пользователям хранить музыкальные файлы в личных папках, но разрешить хранение медиа-файлов определенного типа, таких как учебные материалы, согласующиеся с политикой компании. Можно также создать исключение, разрешающее членам группы руководителей сохранять файлы любого типа (если это не противоречит законодательству).

Процедуру блокировки можно настроить так, чтобы администратор получал по электронной почте уведомление, когда в общей папке сохраняется исполняемый файл. В уведомление можно включить имя пользователя, сохранившего файл, и точное расположение этого файла.

---

### СОВЕТ Подготовка к экзамену

Фильтры блокировки файлов не включены в темы экзамена. Вы должны знать, что это, для чего они используются, и как ими управлять из диспетчера ресурсов файлового сервера. Но подробные вопросы о настройке фильтров блокировки файлов вам вряд ли встретятся.

---

## Управление ресурсами хранилища

Диспетчер ресурсов файлового сервера включает узел **Управление ресурсами хранилища** (Storage Reports Management), позволяющий генерировать отчеты о ресурсах хранилища, например, о дубликатах файлов, о самых больших файлах, о файлах с наибольшим или наименьшим числом обращений. Можно настроить периодическое создание отчетов, что помогает определять тенденции использования дисков и отслеживать попытки сохранения неавторизованных файлов.

Например, можно настроить расписание, согласно которому каждое воскресенье в полночь будут создаваться отчеты, информирующие о том, к каким файлам обращались пользователи за два предыдущих дня. Это позволит отслеживать активность хранилища за выходные дни и планировать время простоя сервера так, чтобы это не влияло на работу пользователей, подключающихся из дома в выходные.

Данные из отчета можно использовать для выявления файлов-дубликатов, которые можно удалить, чтобы освободить дисковое пространство, или для анализа использования ресурсов хранилища отдельными пользователями.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Диспетчер ресурсов файлового хранилища

Для получения дополнительной информации о диспетчере ресурсов файлового хранилища откройте командную строку и введите `hh fsm.chm`.

---

## Резюме

- Служба роли файлового сервера, входящая в состав роли сервера **Файловые службы** (File Services), устанавливается по умолчанию и предоставляет доступ к оснастке **Управление общими ресурсами и хранилищами** (Share And Storage Management). Эта оснастка, в свою очередь, предоставляет доступ к мастеру подготовки общих папок и позволяет контролировать доступ и управлять общими папками, томами, открытыми сеансами и файлами. Предоставить общий доступ к папке и настроить разрешения можно также с помощью оснастки **Общие папки** (Shared Folders).
- При необходимости можно установить DFS, диспетчер ресурсов файлового хранилища, службы для NFS, службу поиска Windows и BranchCache для сетевых файлов. DFS включает DFSN и DFSR. Также можно установить роль файловых служб Windows Server 2003 для обеспечения совместимости с предыдущими версиями Windows.
- Диспетчер ресурсов файлового хранилища позволяет настраивать квоты и фильтры блокировки файлов и создавать отчеты хранилища. Квоты можно настраивать для общих папок и томов.
- BranchCache для сетевых файлов кэширует файлы, загруженные из центрального расположения, создавая копию на компьютере в филиале. Другие компьютеры из этого филиала, обращающиеся к тому же файлу, могут получать его из локальной сети.

## Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных на занятии 2. Эти вопросы предоставлены также в электронном виде на прилагаемом к книге компакт-диске.

---

### ПРИМЕЧАНИЕ Ответы

Ответы на вопросы и пояснения к их вариантам размещены в разделе «Ответы» в конце книги.

---

1. Какой из перечисленных мастеров можно запустить из оснастки **Управление общими ресурсами и хранилищами**?
  - a. Мастер подготовки общих папок.
  - b. Мастер создания нового пространства имен.
  - c. Мастер создания квоты.
  - d. Мастер создания фильтра блокировки файлов.

2. Вы не устанавливали дополнительных служб ролей для роли сервера **Файловые службы**. Установлена только служба роли файлового сервера. Вы запустили мастер подготовки общих папок. Все тома отформатированы в NTFS. Какие задачи позволит выполнить этот мастер? (Каждый ответ является законченным решением. Выберите три.)
  - a. Указать папку для общего доступа.
  - b. Создать новую папку для общего доступа.
  - c. Указать сетевой протокол, используемый для доступа к общему ресурсу.
  - d. Изменить локальные разрешения NTFS для папки или тома, предоставляемого в общий доступ.
  - e. Опубликовать общий ресурс в пространстве DFS.
3. Какой из доступных по умолчанию шаблонов квот создает мягкую квоту, которую можно применять только к томам?
  - a. Предел 100 МБ.
  - b. Предел 200 МБ с уведомлением пользователя.
  - c. Наблюдение за томом 200 ГБ.
  - d. Наблюдение за общим ресурсом размером 500 МБ.
4. В каком режиме какой роли сервера в филиале развертывается компьютер под управлением Windows Server 2008 R2? Хост хранит файлы, загруженные из центрального расположения по WAN-каналу, так что другие клиенты в филиале могут получать эти файлы из локальной сети.
  - a. Диспетчер ресурсов файлового сервера в режиме размещенного кэша.
  - b. Диспетчер ресурсов файлового сервера в режиме распределенного кэша.
  - c. BranchCache для сетевых файлов в режиме распределенного кэша.
  - d. BranchCache для сетевых файлов в режиме размещенного кэша.

## Практикум. Добавление роли сервера Службы печати и документов

На этом практикуме вы добавите роль сервера **Службы печати и документов** и службу роли **Печать через Интернет**. Это позволит предоставлять общий доступ к принтерам (публиковать их).

1. Зайдите на сервер VAN-DC1 под учетной записью Kim Akers и откройте Диспетчер сервера.
2. В дереве консоли раскройте узел **Диспетчер сервера (Server Manager)**. Найдите раздел **Сводка по ролям (Roles Summary)** в правой части окна (см. рис. 7-42). Убедитесь, что роль **Службы печати и документов (Print and Document Services)** не указана в списке. Если роль есть в списке, значит, она установлена, и выполнять это упражнение не требуется.

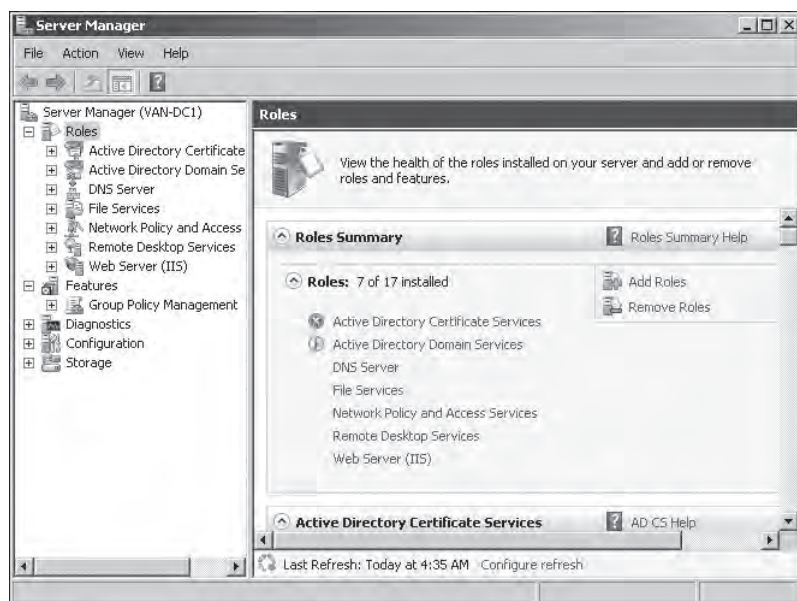


Рис. 7-42. Список установленных ролей в разделе Сводка по ролям

- Щелкните **Добавить роли** (Add Roles). Если откроется страница **Перед началом работы** (Before You Begin), щелкните **Далее** (Next).
- На странице **Выбор ролей сервера** (Select Server Roles) выберите роль **Службы печати и документов** (Print And Document Services) (рис. 7-43). Щелкните **Далее**.

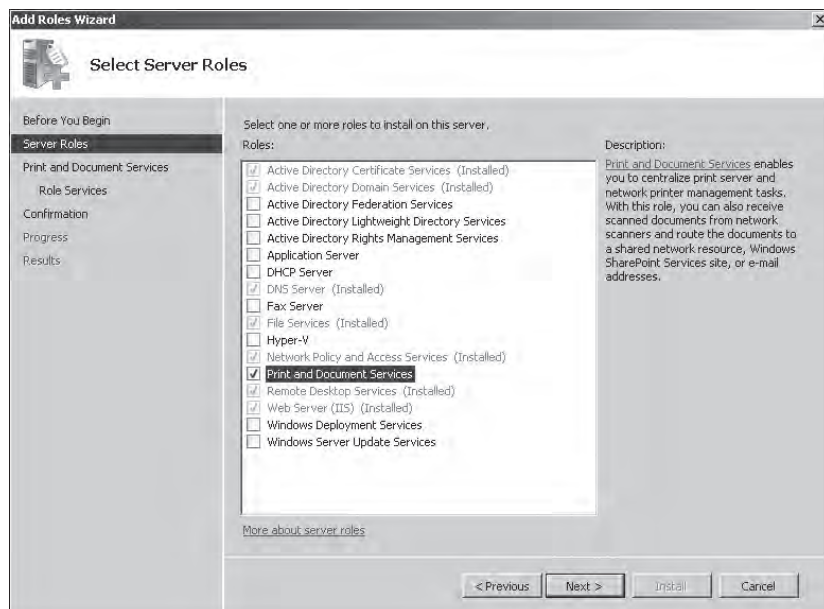


Рис. 7-43. Выбор роли Службы печати и документов

5. Прочитайте информацию под заголовками **Общие сведения о службах печати и документов** (Introduction to Print and Document Services) и **На что обратить внимание** (Things To Note). Если хотите, можете перейти по ссылкам на файлы справки. Щелкните **Далее**.
6. На странице **Выбор служб ролей** (Select Role Services) (рис. 7-44) по умолчанию должна быть выбрана служба роли **Сервер печати** (Print Server). Выберите также **Печать через Интернет** (Internet Printing). Если появится окно с предложением добавить дополнительные службы ролей, щелкните **Добавить требуемые службы ролей** (Add Required Role Services). На странице **Выбор служб ролей** щелкните **Далее**.

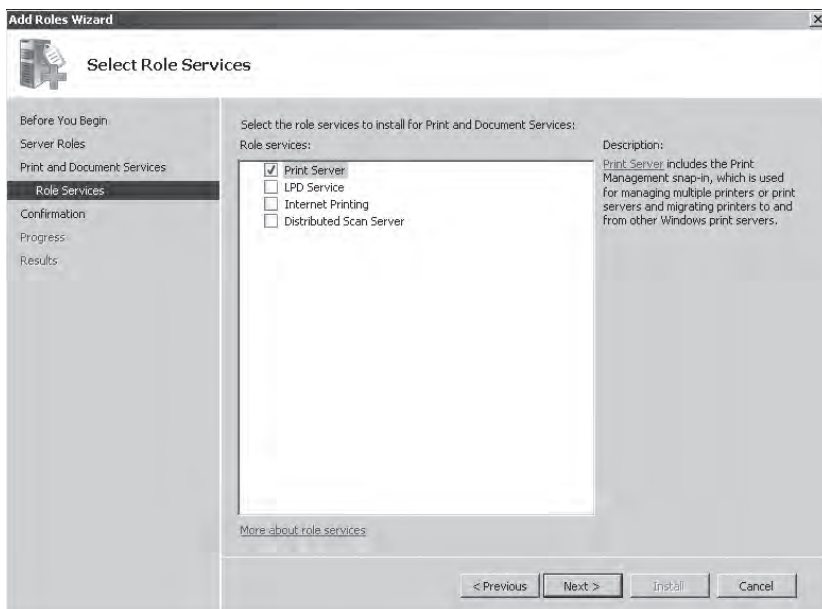


**Рис. 7-44.** По умолчанию выбрана служба роли Сервер печати

7. Если откроется страница **Веб-сервер (IIS)** [Web Server (IIS)], прочитайте информацию и щелкните **Далее**.
8. Страница **Выбор служб ролей** (Select Role Services) должна выглядеть аналогично рис. 7-45. На ней должно быть указано, что служба роли веб-сервера уже установлена. Если эта роль сервера не установлена, выберите **Веб-сервер** (Web Server). Щелкните **Далее**.
9. Прочитайте информацию на странице подтверждения (рис. 7-46). Заметьте, что по завершении установки может потребоваться перезагрузка сервера. Щелкните **Установить**.



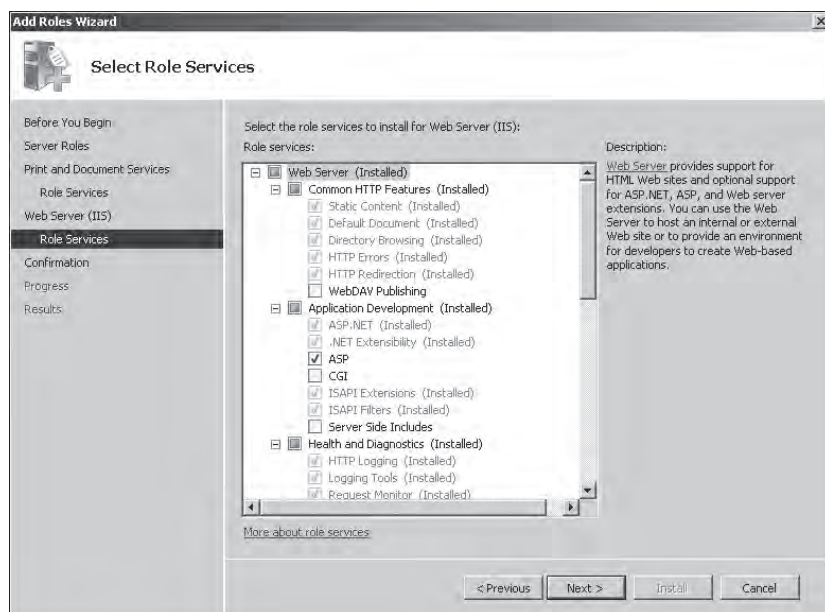


Рис. 7-45. Служба роли веб-сервера уже установлена

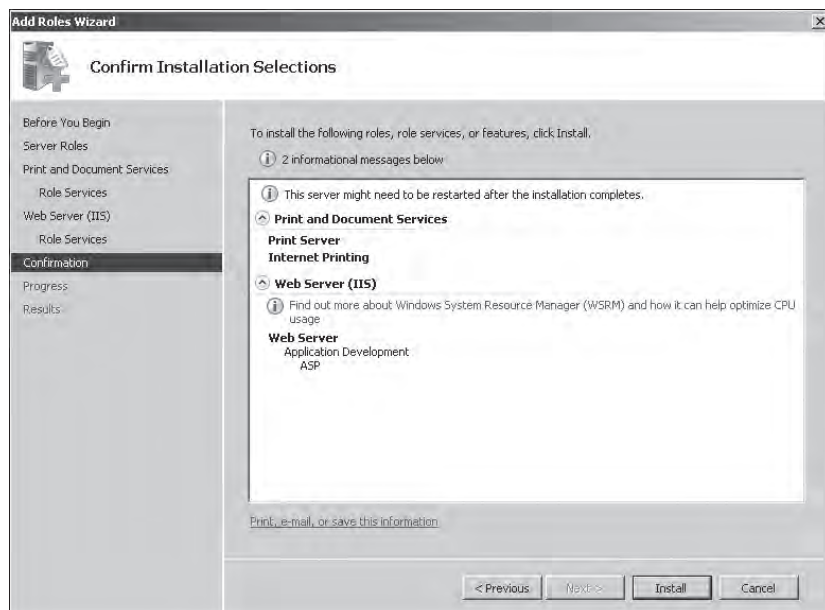


Рис. 7-46. Страница подтверждения выбранных элементов для установки

10. Когда установка завершится, щелкните **Заккрыть**. Убедитесь, что службы печати и документов указаны в списке ролей в диспетчере сервера.
11. Сохраните все несохраненные файлы, закройте все окна и перезагрузите VAN-DC1, если требуется.

## Практикум. Добавление служб ролей для роли сервера Файловые службы и настройка квоты

На этом практикуме вы добавите выбранные службы ролей для роли сервера **Файловые службы** на контроллере домена VAN-DC1. Затем вы создадите на этом контроллере домена общую папку и настроите для нее квоту. Как и раньше, вы зайдете на VAN-DC1 интерактивно. В производственной сети вход на контроллеры домена обычно выполняется удаленно.

### Упражнение 1. Добавление служб ролей для роли сервера Файловые службы

В этом упражнении вы откроете Диспетчер сервера и добавите выбранные службы ролей для роли сервера Файловые службы. Вы не будете добавлять дополнительные компоненты, связанные с этой ролью. Папка C:\Public должна существовать на контроллере домена по умолчанию. Если этой папки нет, создайте ее, прежде чем приступить к упражнению.

1. Если требуется, зайдите на VAN-DC1 под учетной записью Kim Akers, откройте общий доступ к папке C:\Public с разрешениями по умолчанию и откройте Диспетчер сервера.
2. Раскройте узел **Роли (Roles)** и щелкните узел **Файловые службы (File Services)**. В правой части окна найдите список служб ролей (рис. 7-47).

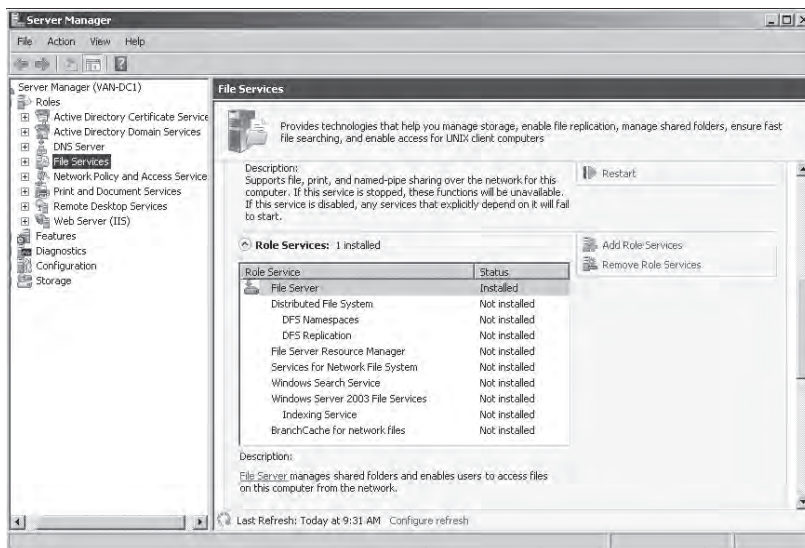


Рис. 7-47. Службы ролей, которые можно добавить для роли Файловые службы

3. Щелкните **Добавить службы ролей (Add Role Services)**.
4. В открывшемся окне выберите все не установленные службы ролей, кроме файловых служб Windows Server 2003 и службы индексирования, как показано на рис. 7-48.

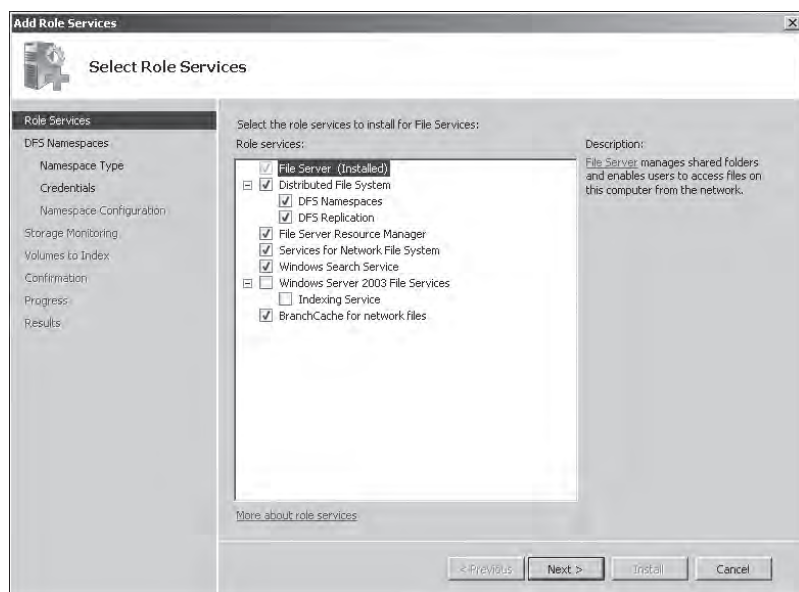


Рис. 7-48. Выбор служб ролей

5. Щелкните **Далее**.
6. Введите для пространства имен DFS имя **MyNameSpace** (рис. 7-49) и щелкните **Далее**.

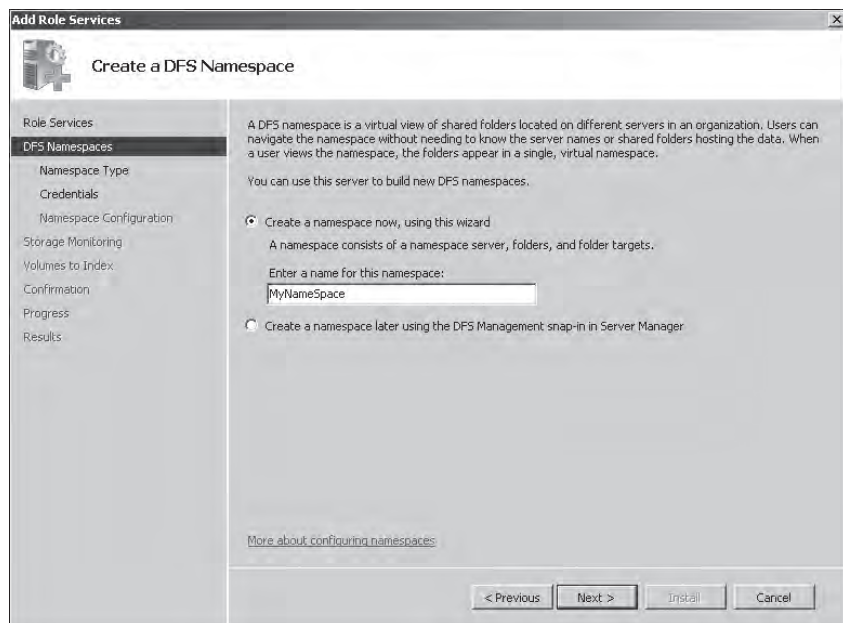


Рис. 7-49. Создание пространства имен DFS

7. Оставьте выбранный по умолчанию вариант **Пространство имен на основе домена (Domain-based namespace)** (рис. 7-50). Щелкните **Далее**.

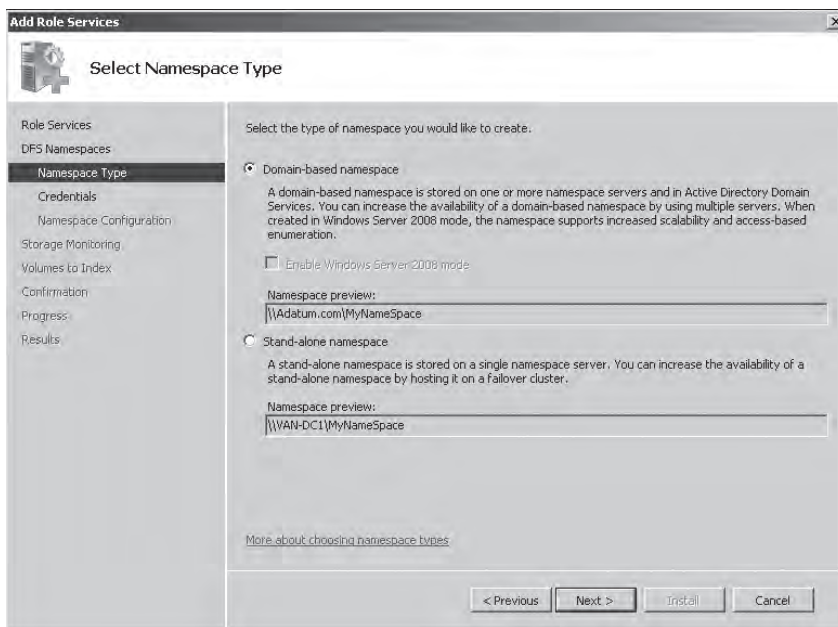


Рис. 7-50. Определение типа пространства имен DNS

#### ПРИМЕЧАНИЕ Пространства имен

О пространствах имен на основе домена и изолированных пространствах имен рассказывается в гл. 10.

8. На странице **Предоставьте учетные данные для создания пространства имен** (Provide Credentials To Create A Namespace) щелкните **Выбрать** (Select). Укажите имя и пароль пользователя Kim Akers и щелкните **ОК**. Щелкните **Далее**.
9. В окне **Настройка пространства имен** (Configure Namespace) щелкните **Добавить** (Add). В диалоговом окне **Добавление папки в пространство имен** (Add Folder To Namespace) щелкните **Обзор** (Browse).
10. В диалоговом окне **Обзор общих папок** (Browse For Shared Folders) щелкните **Показать общие папки** (Show Shared Folders). Убедитесь, что выбрана папка Public (рис. 7-51), и щелкните **ОК**.
11. По умолчанию соответствующая папка в пространстве имен получит такое же имя, как у выбранной общей папки. Щелкните **ОК**, чтобы принять параметры по умолчанию.
12. Страница **Настройка пространства имен** (Configure Namespace) должна выглядеть, как показано на рис. 7-52. Щелкните **Далее**.
13. На странице **Настроить наблюдение за использованием хранилища** (Configure Storage Usage Monitoring) выберите том C: (рис. 7-53). На вашем компьютере размер и объем свободного пространства будет отличаться от показанного на рисунке. Не изменяйте параметры по умолчанию. Щелкните **Далее**.

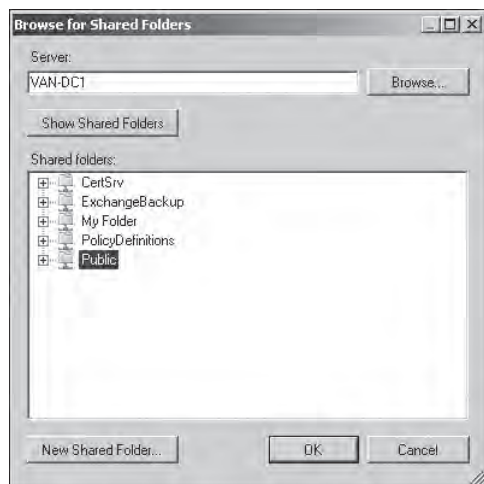


Рис. 7-51. Выбор общей папки

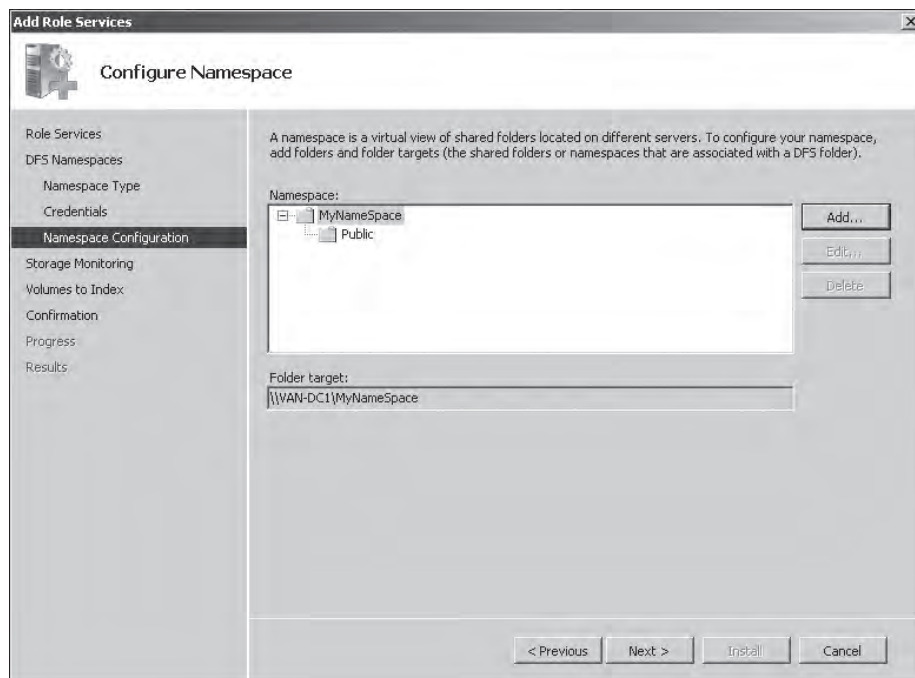


Рис. 7-52. Настройка пространства имен

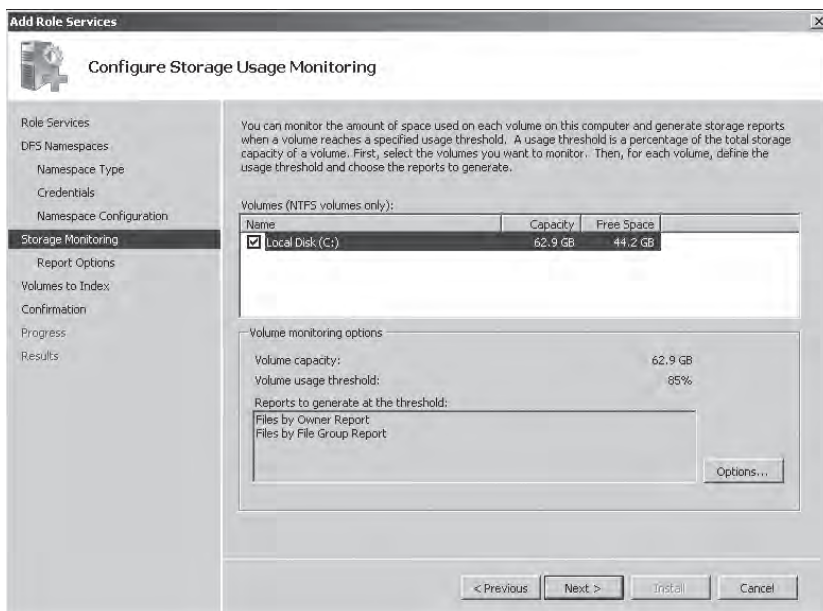


Рис. 7-53. Настройка наблюдения за использованием хранилища

14. Страница **Настроить параметры отчета** (Set Report Options) должна выглядеть, как показано на рис. 7-54. Щелкните **Далее**, чтобы принять параметры по умолчанию.

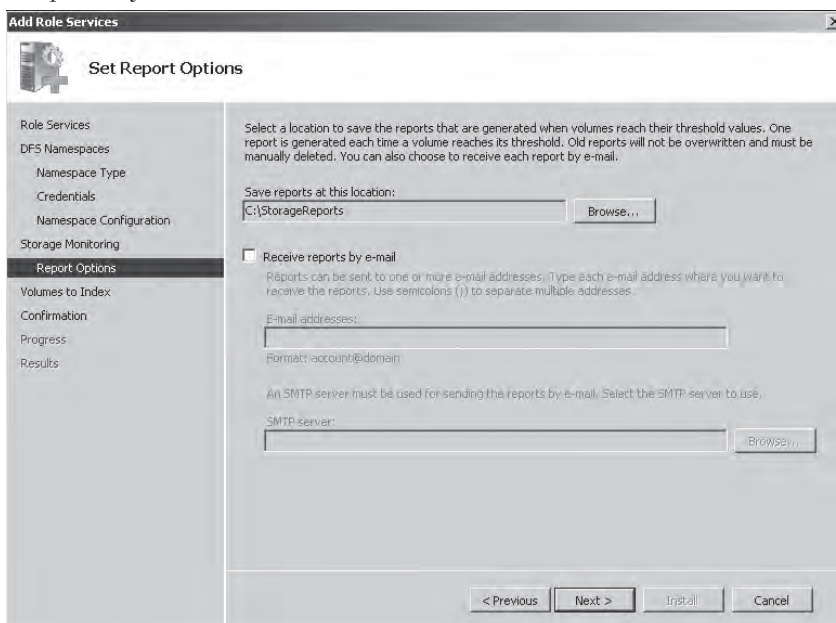


Рис. 7-54. Настройка параметров отчета

15. Включите индексацию тома, не содержащего операционную систему. Если на вашем сервере только один том C:, не индексируйте его. Щелкните **Далее**.



16. Проверьте выбранные элементы для установки. Если вас все устраивает, щелкните **Установить**.
17. Когда установка завершится, щелкните **Заккрыть**.

## Упражнение 2. Настройка квоты

В этом упражнении вы создадите общую папку на контроллере домена VAN-DC1 и настроите для нее квоту. Если хотите, можете открыть диспетчер ресурсов файлового сервера из меню **Администрирование**, а не добавлять оснастку в консоль MMC.

1. Если требуется, зайдите на VAN-DC1 под учетной записью Kim Akers.
2. В корневом каталоге диска C: создайте папку **My Folder** и откройте к ней общий доступ, предоставив группе **Все** (Everyone) разрешение на чтение. Если не знаете, как сделать это, обратитесь к занятию 2.
3. В меню **Пуск** щелкните **Выполнить**. Введите **mmc**.
4. Если требуется, щелкните **Да** в окне службы контроля учетных записей.
5. В консоли MMC в меню **Файл** выберите команду **Добавить или удалить оснастку** (Add/Remove Snap In).
6. Выберите **Диспетчер ресурсов файлового сервера** (File Server Resource Manager) (рис. 7-55). Щелкните **Добавить** (Add), а затем **ОК**.

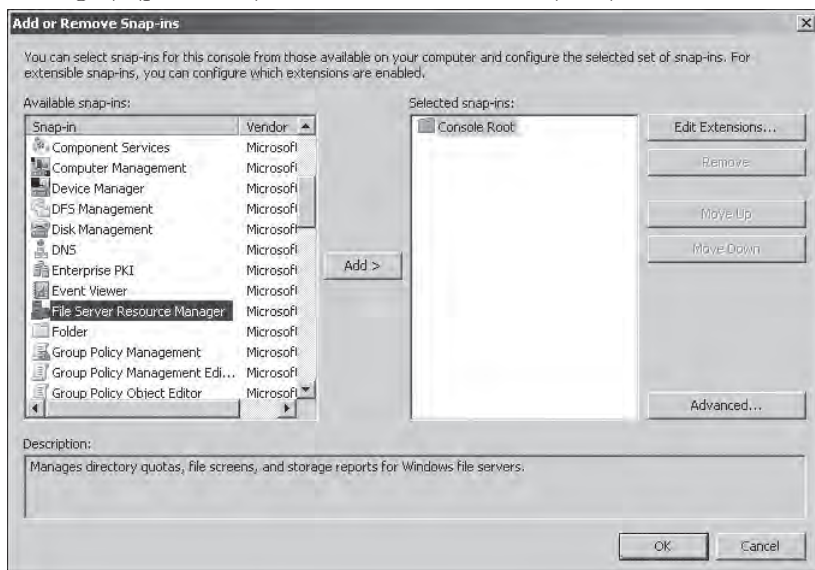


Рис. 7-55. Добавление оснастки Диспетчер ресурсов файлового сервера

7. Раскройте узел диспетчера ресурсов файлового сервера, раскройте узел **Управление квотами** (Quota Management) и выберите узел **Шаблоны квот** (Quota Management) (рис. 7-56).



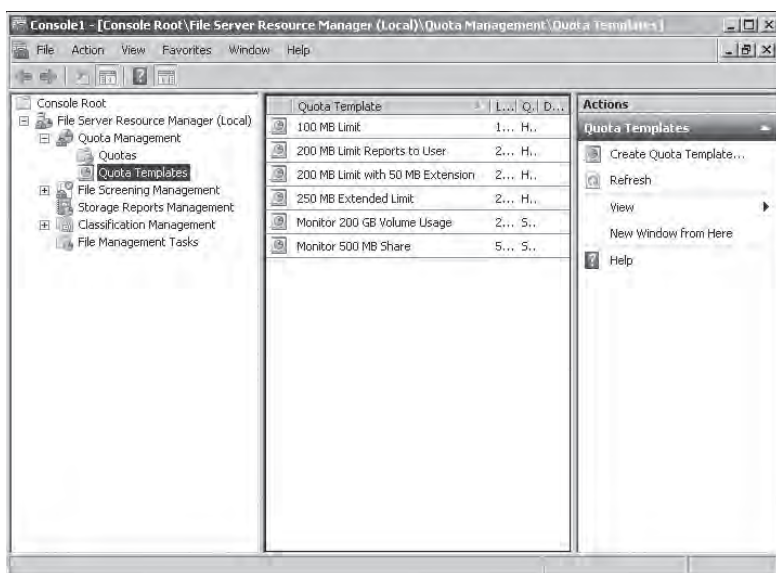


Рис. 7-56. Шаблоны квоты

8. Выберите шаблон **Расширенный предел 250 МБ** (250 MB Extended Limit). В области **Действия** (Actions) щелкните **Создать квоту на основе шаблона** (Create Quota From Template).
9. В диалоговом окне **Создание квоты** (Create Quota) щелкните **Обзор** (Browse) и перейдите в папку C:\My Folder. Щелкните **ОК**. Диалоговое окно будет выглядеть, как показано на рис. 7-57.

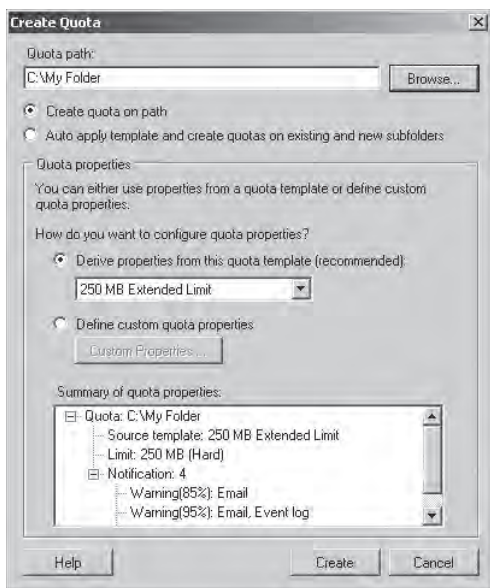


Рис. 7-57. Выбор общей папки для применения квоты

10. Щелкните **Создать** (Create).

## Закрепление материала главы

Чтобы попрактиковаться и закрепить знания, полученные при изучении этой главы, выполните следующее:

- прочитайте резюме главы;
- просмотрите список основных терминов, представленных в этой главе;
- выполните задания лабораторной работы, моделирующей реальные ситуации, требующие применения полученных знаний;
- выполните рекомендуемые упражнения;
- пройдите пробный тест.

## Резюме главы

- Роль сервера **Службы печати и документов** позволяет управлять принтерами, драйверами принтеров, очередями печати и разрешениями принтеров, как для локально установленных принтеров, так и для принтеров, установленных на серверах печати в сети.
- Службы ролей, входящие в состав роли сервера **Файловые службы**, позволяют настраивать параметры доступа, управлять общими папками, томами, открытыми сеансами и файлами, управлять DFS, DFSN и DFSR, настраивать квоты и фильтры блокировки файлов, настраивать параметры работы с файлами вне сети, создавать отчеты хранилища, настраивать индексацию и организовать кэширование файлов в филиалах.

## Основные термины

Проверьте, знаете ли вы, что означают перечисленные ниже термины из этой главы:

- ACE;
- список управления доступом (ACL);
- управление доступом;
- кэширование;
- пространство имен DFS (DFSN);
- репликация DFS (DFSR);
- распределенная файловая система (DFS);
- автономный файл;
- квота.

## Лабораторная работа

Для выполнения заданий лабораторной работы используйте знания о планировании служб каталогов и служб сертификации, полученные из этой главы. Ответы можно найти в разделе «Ответы» в конце книги.

## Задание 1. Планирование обновления Windows Server 2008 R2

Вы главный администратор компании Blue Yonder Airlines. Все серверы компании работают под управлением Windows Server 2008, а все клиенты под управлением Windows 7. Инфраструктура сети компании включает центральный офис и несколько удаленных филиалов, обращающихся к файлам из центрального офиса по WAN-связи. Иногда большие файлы загружаются неприемлемо долго. Все филиалы небольшие (10-15 клиентов), и все компьютеры филиалов находятся в одной подсети. Компания планирует обновить в центральном офисе все контроллеры домена и некоторые рядовые серверы до Windows Server 2008 R2. Ответьте на следующие вопросы:

1. Технический директор недоволен медленной передачей фалов в филиалы. Он хочет знать, поможет ли решить эту проблему установка Windows Server 2008 R2. Что вы ответите?
2. Для обновления серверов в филиалах нет средств. Как это повлияет на кэширование файлов в филиалах?
3. Финансовый директор обеспокоен тем, что в настоящий момент файлы можно классифицировать по размеру, папкам, в которых они хранятся, и времени обновления. Он спрашивает, помогут ли затраты на обновление классифицировать файлы по другим критериям, таким как ценность содержимого для организации. Что вы ответите?
4. Технический директор недоволен также временем и числом действий, необходимых для установки сетевых принтеров. Он хочет знать, стоит ли устанавливать Windows Server 2008 R2 на компьютер, где установлена роль сервера Службы печати. Что вы ответите?

## Рекомендуемые упражнения

Чтобы успешно справиться с экзаменационными заданиями по темам этой главы, выполните следующие упражнения.

### Используйте улучшенную оснастку Управление печатью

- Овладеть инструментом можно только на практике. Используйте улучшенную оснастку **Управление печатью**, входящую в состав Windows Server 2008 R2, и ознакомьтесь с различными мастерами, которые предоставляет эта оснастка. Если вы имеете доступ к компьютеру под управлением Windows Server 2008, сравните возможности, предоставляемые для печати этими операционными системами, и найдите различия.

### Используйте диспетчер ресурсов файлового сервера

- Возможно, вы знакомы с возможностями, которые предоставляет оснастка **Диспетчер ресурсов файлового сервера** в Windows Server 2008. Эти возможности сохранились в Windows Server 2008 R2. Эта служба роли не претерпела значительных изменений, но остается важной, и на экзамене веро-

ятны вопросы о квотах, фильтрах блокировки файлов и создании отчетов. Вы должны быть знакомы с этими темами.

- Наверно, самая значимая возможность роли службы диспетчера ресурсов файлового сервера — возможность применять квоты. Вы должны уметь настраивать квоты, знать, чем различаются доступные стандартные шаблоны квот, и понимать разницу между жесткими и мягкими квотами.

## **Узнайте подробнее о Windows Storage Server 2008 R2**

- В основе Windows Storage Server 2008 R2 лежат технологии Windows Server 2008 R2, и вы должны быть знакомы с этим компонентом. В этой главе мы описали его лишь вкратце. Поищите подробную информацию в специализированных изданиях и на сайте TechNet.

## **Узнайте подробнее о BranchCache для сетевых файлов**

- BranchCache для сетевых файлов — новый компонент Windows Server 2008 R2. Прочитайте любую информацию о нем, которую найдете, включая статьи TechNet.

## **Пробный экзамен**

Тренировочные тесты на прилагаемом к книге компакт-диске позволяют проверить знания только по одной или сразу по всем темам сертификационного экзамена 70-646. Тестирование можно организовать так, чтобы оно проводилось как настоящий экзамен, а можно проходить в режиме обучения, просматривая правильные ответы и объяснения после каждого ответа.

---

### **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Пробный экзамен**

Подробнее о пробном экзамене рассказано во Введении.

---

## Планирование политик безопасности

|                                                    |            |
|----------------------------------------------------|------------|
| <b>Занятие 1. Разработка политик безопасности</b>  | <b>361</b> |
| <b>Занятие 2. Управление безопасностью сервера</b> | <b>383</b> |

В этой главе рассказывается, как настраивать систему безопасности сервера, управлять ей и выполнять ее мониторинг. Мы поговорим также о том, как планировать защиту, чтобы она была адекватной, но не чрезмерной, и своевременно обновлялась. Для планирования системы безопасности необходимо знать, как использовать различные политики аудита для слежения за важными объектами и данными, как выполняется проверка подлинности и авторизация, как обезопасить данные и как выполнять аудит политик безопасности.

Своевременное обновление операционной системы и приложений — важный аспект обеспечения защиты сервера, поскольку обновления часто выпускаются для решения проблем безопасности. В процессе планирования системы безопасности следует учитывать возможность централизованного развертывания обновлений через службы обновления серверов Windows (WSUS). Администратор должен организовать управление обновлениями операционной системы и приложений и спланировать расписание обновлений. Необходимо также проверить, работает ли централизованное развертывание исправлений, как ожидается.

### Темы экзамена

- Мониторинг и поддержка безопасности и политик.
- Реализация стратегии управления обновлениями.

### Прежде всего

Для выполнения упражнений этой главы потребуется:

- Сервер с именем VAN-DC1, работающий под управлением Windows Server 2008 R2 Enterprise, настроенный как контроллер домена adatum.com, как описано в Приложении.
- Учетная запись пользователя Kim Akers с паролем Pa\$\$w0rd в домене adatum.com, включенная в группы администраторов домена, администрато-

ров предприятия и администраторов схемы. Процедура создания этой учетной записи описана в Приложении.

- Учетная запись пользователя Don Hall с паролем Pa\$\$w0rd в домене adatum.com. Ранее вы добавили эту учетную запись в группу операторов архива. Для выполнения упражнений этой главы членство в этой группе не требуется, но его можно оставить. Однако важно, чтобы пользователь Don Hall входил в стандартную группу безопасности **Пользователи домена**.
- Убедиться, что в домене adatum.com не существует учетная запись Jim Hance и группа безопасности DonGroup. Если они существуют, удалите их.
- Для выполнения практических упражнений рекомендуем использовать изолированную сеть, не входящую в рабочую сеть. Для выполнения упражнений доступ к Интернету обычно не требуется, но он потребуется для выполнения второго практикума этой главы. Поэтому второй практикум выполнять не обязательно; подробнее см. в описании практикума. Для экономии времени и затрат на настройку физических компьютеров используйте виртуальные машины, например, созданные с использованием роли сервера Hyper-V.

## Реальный мир

*Йен Маклин*

Цель опытного администратора — применить тщательно спланированную адекватную политику безопасности и регулярно проверять систему безопасности. Ключевые слова здесь — «спланированная» и «адекватная». Нет идеальной системы безопасности, и если слишком стараться максимально все защитить, может получиться совсем не то, что предполагалось. Строгая политика безопасности бесполезна, если пользователи записывают слишком сложные пароли на бумажках, которые прикрепляют к мониторам.

Как ни старайтесь, вы не сможете предусмотреть все последствия небрежности пользователей. Неопытность или самонадеянность администратора может стать причиной всевозможных проблем в сети. Злонамеренный пользователь обычно более опасен, чем любая внешняя атака. Вы можете делать все возможное, чтобы нейтрализовать угрозы, исходящие от пользователей и администраторов, но вы всегда будете проигрывать, если подавляющее большинство пользователей не будет соглашаться с тем, что вы делаете.

Обычно пользователи хотят, чтобы им не мешали работать. Если они будут считать, что процедуры обеспечения безопасности создают им проблемы и замедляют работу, они всегда найдут способ обойти грамотно спланированную политику безопасности. Вы должны объяснить людям, использующим серверы, которые вы обслуживаете, почему важна политика безопасности, и рассказать, как убрать неудобства, которые может причинить политика безопасности. Пользователи должны быть на вашей стороне.

Всегда помните, что обеспечение безопасности серверов — это не только технический процесс планирования и настройки политик безопасно-

сти. Это еще и обучение людей, использующих серверы, тому, как работать после применения этих политик безопасности. Администрирование системы безопасности, как и администрирование в целом, требует уделять людям не меньше внимания, чем технической стороне.

## Занятие 1. Разработка политик безопасности

Обеспечение безопасности — непрерывный процесс. Сначала требуется спланировать систему безопасности и определить, какая модель разрешений будет использоваться, какие события подлежат мониторингу и как настроить брандмауэр Windows (см. гл. 9). Затем следует спланировать стратегию, обеспечивающую эффективную защиту сервера. Необходимо не только спланировать и реализовать защиту сервера, но и выполнять мониторинг событий безопасности, чтобы убедиться, что защита работает должным образом. На этом занятии мы поговорим о планировании защиты, политиках безопасности, защите данных и аудите.

---

### Изучив материал этого занятия, вы сможете:

- ✓ Планировать политики безопасности сервера.
- ✓ Развертывать политики безопасности и управлять ими.
- ✓ Выполнять мониторинг безопасности сервера.
- ✓ Выполнять мониторинг проверки подлинности и аутентификации.
- ✓ Выполнять мониторинг безопасности данных.
- ✓ Настраивать аудит.

**Продолжительность занятия — примерно 50 мин.**

---

## Планирование системы безопасности сервера

Прежде чем применять политику безопасности и развертывать на серверах антивирусы и другие специализированные программы, необходимо спланировать стратегию защиты. Невозможно наблюдать за всем, поэтому следует определить, какие серверы больше всего подвержены внешним атакам или попыткам несанкционированного входа, и как предотвратить ошибки администраторов, связанные с неправильной настройкой разрешений и предоставлением пользователям доступа к тем ресурсам, к которым доступа быть не должно. Невозможно выполнять мониторинг и аудит всей информации, предоставляемой даже одним сервером, не говоря уже о ферме серверов, а значит, необходимо спланировать мониторинг и аудит так, чтобы максимально эффективно использовать ценное рабочее время администратора.

### Определение требований к безопасности

Для обеспечения эффективной защиты сети необходимо решить несколько задач:

- **Защита информации.** Требуется определить, какая информация должна быть защищена, насколько важна эта информация для организации, и какой уровень защиты необходим.



- **Уровни авторизации.** Требуется определить уровни авторизации и разрешений для пользователей и администраторов.
- **Мониторинг безопасности.** Требуется применить работоспособную политику мониторинга, предоставляющую максимум необходимой информации об определенных событиях безопасности.

Область развертывания защиты, мониторинга и аудита следует соотносить с диапазоном известных потенциальных угроз. Так, если администратор изменяет параметр политики, который прописан в политике компании, это нарушение политики. Если пользователь обнаруживает, что имеет доступ к конфиденциальной информации, которая должна быть доступна только старшим менеджерам, это тоже нарушение политики. Подробнее о нарушениях политики см. ниже в разделе «Выявление и устранение нарушений политики».

Серверы редко используются для просмотра страниц в Интернете, поэтому некоторые типы внешних атак (например, фишинговые) маловероятны. Однако серверу обычно требуется подключение к Интернету для загрузки различных данных (например, программы Process Explorer, описанной в гл. 12). Кроме того, злоумышленники прилагают много усилий, пытаясь установить троянские программы (сокращенно их называют просто «троянами») на файловые серверы и контроллеры домена. Веб-серверы обычно располагаются в периферийных сетях и могут подвергаться атакам типа «отказ в обслуживании» (DoS). Следовательно, вы должны определить наиболее вероятные типы внешних атак и серверы, на которые эти атаки могут быть направлены.

Если произошла внешняя атака или нарушение политики, следует разработать процедуры анализа, позволяющие выявить причины нарушения и определить, почему атака прошла успешно или неудачно. Необходимо также настроить аудит, чтобы можно было принять соответствующие меры.

## Планирование мониторинга безопасности

Средство просмотра событий (Event Viewer) подробно описано в гл. 12. В этой главе нас интересует только журнал безопасности, мониторинг которого можно выполнять с помощью этого средства. Можно связать задачу с событием или создать настраиваемое представление, отображающее только те события, которые удовлетворяют определенным критериям. Кроме того, можно назначить разные уровни аудита безопасности для разных пользователей. Учитывайте это, когда планируете ведение журналов безопасности.

В журнал безопасности (рис. 8-1) записываются события двух типов: аудит успехов и аудит отказов. Событие аудита успеха указывает на то, что операция, выполненная пользователем, службой или программой, завершилась успешно. Аудит отказа указывает на то, что такая операция не завершилась успешно. Например, если включить аудит отказов входа в систему, в журнал безопасности будут записываться неудачные попытки входа в систему.

Чтобы просмотреть категории аудита событий безопасности, в редакторе управления групповой политикой раскройте узел **Конфигурация компьютера | Политики | Параметры Windows | Параметры безопасности | Конфигурация расширенной политики аудита | Политики аудита системы** (Computer Configuration | Policies | Windows Settings | Advanced Audit Policy Configuration | Audit Policies). В табл. 8-1 перечислены эти категории и относящиеся в них события, записываемые в журнал в Windows Server 2008 R2.

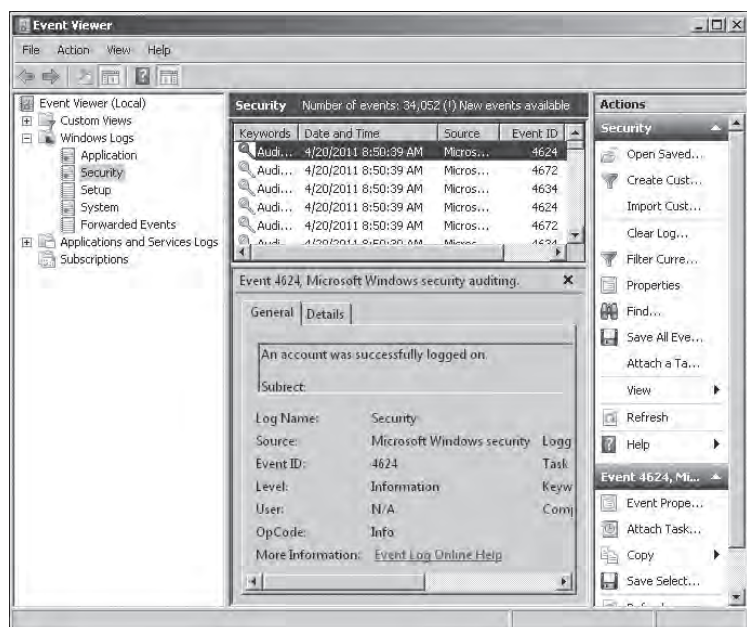


Рис. 8-1. Мониторинг журнала безопасности

Табл. 8-1. Категории аудита событий безопасности

| Категория                                         | Описание                                                                                                                                                                                                                                |
|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Вход в систему<br>(Account Logon)                 | Запись попыток входа в систему с использованием локальной учетной записи. Если используется доменная учетная запись, это событие также появляется на контроллере домена                                                                 |
| Управление учетными записями (Account Management) | Запись сведений о создании, изменении и удалении учетных записей пользователей и групп, а также об изменении и сбросе паролей                                                                                                           |
| Подробное отслеживание (Detailed Tracking)        | Запись событий, сгенерированных при создании запросов на шифрование или дешифровку для событий DPAI, сгенерированных при создании, запуске или завершении процесса. Также записываются события, сгенерированные входящими событиями RPC |
| Доступ к службе каталогов (DS) [DS Access]        | Запись событий доступа к объектам службы каталогов Active Directory                                                                                                                                                                     |
| Вход/выход (Logon/Logoff)                         | Запись попыток входа на рабочие станции и рядовые серверы, сведения о выходе из системы и блокировке учетной записи, а также событий IPSec                                                                                              |
| Доступ к объекту (Object Access)                  | Запись попыток доступа к объектам (файлам, папкам, разделам реестра и принтерам), для которых в списках SACL определены параметры аудита                                                                                                |
| Изменение политики (Policy Change)                | Запись любых изменений в политиках назначения прав пользователей, аудита, учетных записей и доверия                                                                                                                                     |

Табл. 8-1. (окончание)

| Категория                                                           | Описание                                                                                                                                   |
|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Использование прав (Privilege Use)                                  | Запись каждого случая применения указанных прав пользователей, например, изменения системного времени                                      |
| Отслеживание процессов (Process Tracking)                           | Запись сведений о поведении приложений, например, о запуске или завершении программы                                                       |
| Система (System)                                                    | Запись системных событий, таких как запуск и завершение работы, а также событий, относящихся к безопасности системы и журналу безопасности |
| Аудит доступа к глобальным объектам (Global Object Access Auditing) | Позволяет настроить глобальный SACL для файловой системы и реестра, относящийся к компьютеру целиком                                       |

На рис. 8-2 показан контейнер групповой политики **Политики аудита системы** (Audit Policy), определяющий, какие события создают записи в журналах безопасности. Параметры политики аудита системы можно настроить при помощи консоли управления локальными параметрами безопасности или на уровне сайта, домена или подразделения через групповую политику и AD DS.

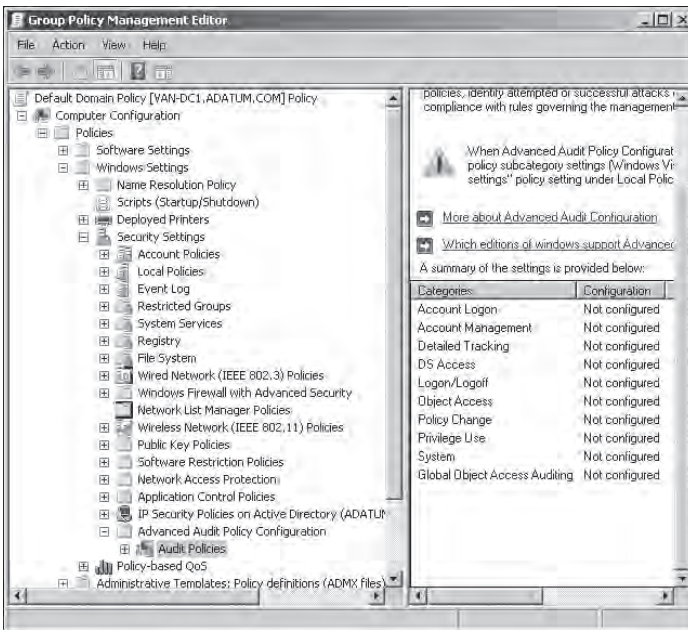


Рис. 8-2. Контейнер Политики аудита системы

Журналы безопасности предоставляют хорошую базу, на основе которой можно планировать подробную политику мониторинга безопасности. Параметры групповой политики позволяют централизованно настраивать уровни аудита журналов безопасности, а параметры безопасности, назначенные по умолчанию, позволяют обращаться к журналам безопасности только администраторам. Однако для мониторинга распределенных атак и выполнения последующего анализа требуется система мониторинга, позволяющая централизованно

анализировать события аудита. Пересылка событий (см. также гл. 12) позволяет собирать события с серверов (и клиентов, если требуется выполнять мониторинг всей сети) на одном компьютере. Однако для полного анализа собранных событий может потребоваться установка специализированного ПО, такого как Microsoft System Center Operations Manager 2007 R2.

---

**ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ System Center Operations Manager 2007 R2**

Подробнее о System Center Operations Manager 2007 R2 см. по адресу <http://technet.microsoft.com/ru-ru/library/bb310604.aspx>. Пробную версию можно получить по адресу <http://technet.microsoft.com/ru-ru/evalcenter/bb738014.aspx>.

---

**ПРИМЕЧАНИЕ Компьютеры на периметре сети**

Поскольку компьютеры, расположенные на периметре сети (например, веб-серверы), обычно являются членами рабочей группы, а не домена, нельзя настроить для них параметры групповой политики. Вместо этого следует использовать локальные политики и файлы шаблонов.

---

**Выявление и устранение нарушений политики**

Нарушения политики обычно составляют самую большую категорию проблем с безопасностью, возникающих в сети организации. Нарушения могут быть следующими:

- создание учетных записей пользователей в обход установленной процедуры;
- использование административных привилегий без надлежащей авторизации;
- использование учетных записей служб для интерактивного входа в систему;
- удаление файлов, на доступ к которым пользователи имеют разрешения;
- запуск неразрешенных программ;
- попытки обращения к файлам, на доступ к которым пользователи не имеют разрешений.

Наиболее распространенный тип нарушения политики — непреднамеренные попытки доступа. Пример — попытки пользователя открыть папку, доступную только членам группы безопасности, в которую этот пользователь не входит. Однако ограничение доступа и ограниченные права не дают пользователям нанести какой-либо значимый ущерб. Гораздо опаснее нарушения политики, совершенные администраторами, случайные или преднамеренные.

Ошибки сетевых администраторов представляют серьезную угрозу для организаций. Администраторам для работы требуется более высокий уровень прав и привилегий. Они могут создавать учетные записи, сбрасывать пароли и изменять владельцев файлов и папок. Однако если администратор может выполнить какую-то задачу, это не значит, что он авторизован для ее выполнения. Права администраторов могут позволять им просматривать сетевые ресурсы, которые они не должны просматривать, например, финансовые отчеты или базы данных отдела кадров.

Вероятность нарушения политики высока, как и возможный ущерб. Планируя политику безопасности, следует сделать выявление нарушений политики приоритетной задачей. Старший администратор может иметь голос при под-

боре персонала в штат администраторов. Убедитесь, что проверка кандидатов выполняется достаточно строго, и регулярно выполняйте проверки в дальнейшем. Однако эта книга посвящена техническим аспектам, а не работе с персоналом. В техническом плане следует выполнять следующее:

- независимые проверки действий администраторов, относящихся к безопасности;
- регулярные проверки системы мониторинга безопасности, позволяющие быстро обнаружить бреши в системе безопасности;
- проверка серьезности бреши в безопасности для ограничения возможного ущерба.

Убедитесь, что внутренние пользователи, не являющиеся постоянными сотрудниками организации, подписывают документ, определяющий условия соблюдения безопасности и описывающий требования к обеспечению безопасности сети. Люди должны понимать, что если они попытаются открыть файл или сетевой ресурс, на доступ к которому не имеют разрешений, в журналах безопасности будет зафиксирована эта попытка. Внутренние пользователи, работающие с файлами, имеющими высокую ценность, должны знать, что в журналы безопасности записываются все случаи обращения к этим файлам. Администратор не всегда имеет полномочия для применения такой политики. Обратитесь к руководству и постарайтесь добиться ее применения.

В организации должны строго распределяться обязанности, чтобы за проверку действий администраторов отвечали разные люди или группы. Члены таких групп инспекторов могут не иметь прав на выполнение административных задач.

При планировании следует предусмотреть регулярную проверку функций мониторинга. Например, необходимо убедиться в нормальной работе оповещений. Выполняйте такие проверки с разными интервалами, чтобы злоумышленник не смог подготовиться к ним.

План должен позволять быстро выявлять бреши в безопасности. Необходимо разработать подробные процедуры, определяющие способы выполнения различных сетевых операций. Например, администраторы имеют возможность создавать учетные записи пользователей напрямую, но политика организации может запрещать это, и если система мониторинга безопасности показывает, что произошло соответствующее событие (код события 624 — создание учетной записи пользователя), следует проверить, не связано ли это событие с учетной записью администратора.

Для уменьшения ущерба, который может причинить появление бреши в безопасности, план должен определять действия, выполняемые в случае происшествий. Скорость и эффективность этих действий может значительно повысить безопасность организации. Если пользователи и администраторы знают, что за любым инцидентом последует тщательное расследование, они будут более серьезно относиться к соблюдению политики безопасности.

Обычно вероятность потери или компрометации данных из-за внешних атак гораздо ниже, чем из-за неправильных действий сетевых администраторов. Не следует пренебрегать угрозой внешних атак. Приобрести средства для борьбы с внешними атаками нетрудно, гораздо сложнее предотвратить ошибки, совершаемые администраторами.

## Выявление внешних атак и защита от них

Внешние атаки могут совершаться человеком непосредственно или посредством установки вредоносных программ, таких как трояны. Разные типы атак имеют разные характеристики и представляют различные угрозы. Люди могут получить информацию о целевой сети и изменить соответствующим образом способы атаки; вредоносные программы могут влиять на работу многих компьютеров и создавать возможности для атаки.

К вредоносным приложениям относятся вирусы, черви и трояны. Хотя эти приложения могут приводить к значительным нарушениям в работе, такие атаки легче предотвратить, чем проводящиеся людьми.

Особое внимание выявлению вредоносных приложений следует уделять организациям, работающим в финансовом или любом другом секторе, регулирующемся законодательством. О шпионских приложениях, которые могут устанавливаться на серверы или рабочие станции и передавать конфиденциальную информацию злоумышленникам, помнить следует всегда, но в таких организациях — особенно.

Не всегда легко определить наличие вредоносных приложений в сети. Например, если вредоносный компонент является руткитом, он может получить полный контроль над компьютером и успешно скрывать этот факт. Сложно быть уверенным в том, что на сервере не работают такие приложения.

Выявлять вредоносные приложения следует путем отслеживания процессов. Это позволит найти каждую программу, которая запускается или останавливается на рабочей станции или сервере. Недостаток такого подхода в том, что генерируется очень много событий, большинство из которых никакого интереса не представляет.

Анализ отслеживаемых процессов может быть затруднительным в следующих случаях:

- веб-серверы используют интерфейс CGI, в котором каждый переход к странице создает новый процесс;
- приложения на рабочих станциях, используемых для разработки ПО, создают много процессов за короткий период времени.

Если при мониторинге создается очень много событий постоянно или в течение короткого периода времени, требуются эффективные фильтры, позволяющие отделить обычные события от событий, имеющих отношения к атакам.

Существует много методов проникновения с использованием внешних атак:

- подбор паролей;
- попытки изменить или сбросить пароли;
- попытки заставить пользователей запустить вредоносное приложение;
- атаки с использованием уязвимостей;
- повышение привилегий для компрометации дополнительных компьютеров (это называется *прыжками по островам*);
- установка вредоносных программ под видом обычных приложений;
- установка трояна;
- фишинговые атаки, в которых рассылаются электронные письма со ссылками на вредоносные веб-сайты (в случае с серверами такие атаки проходят реже).



Наверно, лучший способ выявления злоумышленников и вредоносных программ — отслеживание процессов. Его следует использовать совместно с политиками ограничения приложений, применяемыми через групповую политику. В частности, следует разработать очень строгие политики, определяющие, какие программы можно запускать на компьютерах в сетях периметра.

План для выявления внешних атак, скорее всего, будет пересекаться с планом для выявления внутренних угроз. Он должен включать следующее:

- эффективные журналы аудита безопасности;
- автоматизированный анализ журналов безопасности для выявления признаков атак;
- централизованный сбор журналов безопасности, например, с помощью пере-сылки событий.

Решение для выявления вредоносных приложений должно включать следующее:

- эффективные процедуры для выявления любых неавторизованных приложений в сети;
- журналы аудита безопасности, настроенные должным образом;
- надежный способ централизованного сбора и фильтрации журналов безопасности;
- автоматизированный анализ журналов безопасности с целью выявления подозрительного поведения.

## Планирование криминалистического анализа

Криминалистический анализ позволяет определить время, серьезность и последствия появления бреши в системе безопасности и понять, какие системы были скомпрометированы. При таком анализе записывается следующее:

- время атаки;
- длительность атаки;
- атакованные компьютеры;
- изменения, внесенные в сеть вследствие атаки.

Криминалистический анализ используется для расследования инцидентов после того, как они произошли, а не во время проведения атаки. Следовательно, необходим список всех событий, имеющих отношение к инциденту, произошедших на одном или нескольких компьютерах. Администратор должен спланировать систему анализа, способную обрабатывать и архивировать большие объемы данных, используя пригодную для работы базу данных.

Следует определить, как долго должны храниться криминалистические данные. Установите максимальный срок хранения этих данных, после которого их можно удалить. В табл. 8-2 приведено типичное время хранения криминалистических данных.



Табл. 8-2. Сроки хранения данных для криминалистического анализа

| Особенности хранилища                   | Срок хранения | Примечание                                                                 |
|-----------------------------------------|---------------|----------------------------------------------------------------------------|
| Онлайновые хранилища (базы данных)      | 21 день       | Быстрый доступ к данным о последних событиях                               |
| Хранение вне сети (резервные копии)     | 180 дней      | Достаточный срок для большинства организаций                               |
| Системы, регулируемые законодательством | 7 лет         | Обычно закон требует хранения данных в течение 7 лет                       |
| Разведывательные службы                 | Бессрочное    | Если данные имеют отношение к национальной безопасности, их нельзя удалять |

Можно использовать онлайновые базы данных для хранения событий за последние три недели, после чего архивировать старые данные для дальнейшего хранения. Если потребуется, эти данные можно будет импортировать обратно в базу данных для анализа.

Используемая система должна позволять быстро расследовать недавние события и при необходимости восстанавливать старые события. Сроки хранения информации в онлайновых базах данных и в резервных копиях определяются опытным путем. Применение мониторинга безопасности для криминалистического анализа требует сбора и хранения очень большого числа событий. План должен предусматривать следующее:

- надежное и безопасное онлайновое хранилище данных;
- надежная система резервного копирования старых событий с автоматическим переносом старых резервных копий в хранилища архивов;
- возможность восстановления информации из старых резервных копий;
- наличие больших объемов дискового пространства на высокопроизводительных устройствах для онлайн-хранения.

Обычно объем данных, собранных для криминалистического анализа, непрерывно растет. Сотруднику, отвечающему за работу с этими данными (обычно это администратор системы безопасности предприятия, и никто другой), доступ к этой информации может требоваться очень редко. В целях безопасности такой доступ должен иметь один, максимум два очень надежных человека.

## Развертывание политик безопасности для реализации решения

Следующим этапом после планирования системы мониторинга безопасности и выявления атак будет проектирование решения, удовлетворяющего предъявленным требованиям. Это решение должно соответствовать задачам трех определенных ранее уровней:

- выявление нарушений политики;
- выявление внешних атак;
- выполнение криминалистического анализа.

Конкретные варианты такого решения будут различаться в зависимости от топологии сети организации, но каждое решение должно использовать базовые

компоненты для всех трех уровней, хотя криминалистический анализ может потребовать дополнительных ресурсов для хранения информации в онлайн-базах данных, в резервных копиях и в архиве. Прежде чем приступить к реализации решения, необходимо выполнить следующее:

- **Просмотреть текущие параметры безопасности.** Просмотрите текущие параметры аудита безопасности и файла журнала безопасности, чтобы создать основу для запланированных изменений. Нужно знать текущие действующие параметры аудита безопасности, уровень применения этих параметров (локальный, компьютер, сайт, домен или подразделение) и текущие параметры файла журнала (такие как максимальный размер журнала и действия, выполняемые при достижении журналом максимального размера). Необходимо учитывать и все дополнительные параметры аудита безопасности (например, в производственной сети), которые могут быть настроены в текущий момент, чтобы выполнять аудит прав на резервное копирование и восстановление.
- **Выявить уязвимые компьютеры.** Необходимо определить, какие серверы с наибольшей вероятностью будут атакованы первыми. Обычно это компьютеры из сети периметра, такие как веб-серверы. Тщательно проверьте все уязвимые компьютеры и убедитесь, что на них установлены все пакеты обновлений и исправления, отключены ненужные службы и учетные записи, службы работают с использованием учетных записей локальной или сетевой службы, а не пользователей, если это возможно, и применены шаблоны политики безопасности, обеспечивающие надежную защиту компьютера. Определенные меры предосторожности следует принять на всех серверах, но для уязвимых компьютеров это особенно важно.
- **Определить ценные ресурсы.** Вероятно, вы уже определили, какие ресурсы важны для организации, и обеспечили их защиту при помощи списков управления доступом (ACL) и шифрования. Важно также перечислить эти защищенные файлы в письменной политике организации и указать, что неавторизованные пользователи и администраторы не должны пытаться получить доступ к ним. Администраторы и пользователи должны знать об этих ограничениях. Следует наблюдать за всеми изменениями в ACL этих защищенных файлов. Особенно важно отслеживать изменение владельца, так как это указывает на попытки злоумышленника (или неопытного администратора) получить доступ к файлам без соответствующей авторизации.
- **Оценить роли администраторов и задачи пользователей.** Убедитесь, что знаете, какие роли и обязанности выполняет каждый человек из штата администраторов. Например, все администраторы домена могут создавать учетные записи пользователей домена, однако в политике организации может быть указано, что это разрешено только определенным сотрудникам. В таком случае при создании учетной записи администратором должно генерироваться предупреждение. Пользователи имеют значительно меньше прав доступа к сетевым ресурсам, чем администраторы. Например, пользователи обычно не имеют доступа к файловой системе серверов в сети периметра, и выполнять мониторинг таких действий на этих серверах вряд ли требуется.

- **Просмотреть политики и процедуры, определенные в организации.** Просмотр политик и процедур следует соотнести с оценкой ролей и задач администраторов. Например, определите, кто может и не может добавлять пользователей в группы безопасности. В отделах организации должны быть разработаны процедуры для запроса изменений и методы для выполнения этих запросов. Например, если пользователь добавляется в обход установленных процедур, это требует расследования.
- **Выявить важные и подозрительные учетные записи.** Необходимо проверить все важные учетные записи и определить, какие из них требуют более высокого уровня аудита. Это относится к встроенной учетной записи администратора, всем членам групп администраторов предприятия, схемы и домена и всем учетным записям, используемым службами для входа в систему. Если замечена подозрительная активность какого-либо пользователя, политика безопасности должна требовать для него применения более высоких уровней аудита.
- **Определить авторизованные программы.** Злоумышленники могут запускать различные программы для сбора информации о сети. Ограничение списка программ, запуск которых разрешен, позволит значительно уменьшить угрозу внешних атак. Следует выполнять аудит всех авторизованных программ и считать любую неопознанную программу подозрительной.
- **Проверить брандмауэры и антивирусы.** Для борьбы с вирусами и прочими вредоносными программами можно использовать продукты Microsoft или других компаний. Иногда такие программы изменяют параметры брандмауэра (см. гл. 9). Антивирусные базы должны постоянно обновляться. Если сервер постоянно подключен к Интернету, обновление должно происходить автоматически. Использование WSUS (см. занятие 2) позволяет некоторым серверам работать без подключения к Интернету большую часть времени, что делает их менее уязвимыми к внешним атакам. Однако при подключении такого сервера к Интернету в первую очередь следует обновить антивирусные базы.

Выполнение этих задач должно делать серверы максимально защищенными с учетом текущих параметров безопасности. Проведение различных проверок поможет определить требуемые изменения в системе безопасности и убедиться в надежности плана обеспечения защиты. Исходя из собранной информации, можно выполнять дополнительную настройку в соответствии с планом.

## Развертывание политик аудита

План по обеспечению безопасности обычно предусматривает включение политик аудита в разделе **Конфигурация расширенной политики аудита** (Advanced Audit Policy Configuration) параметров GPO по умолчанию или GPO, созданного специально для этого. Если хотите применять на разных серверах разные политики аудита, можете группировать серверы в подразделениях и применять к ним разные GPO.

Если в редакторе управления групповой политикой выбрать узел **Политики аудита системы** (Audit Policies) (см. рис. 8-2), в области результатов будет показан список категорий политик аудита. Узел **Политики аудита системы** мож-

но раскрыть, чтобы эти категории отображались в виде дерева, а затем выбрать любую категорию, чтобы просмотреть доступные параметры. Общая информация о категориях приведена в табл. 8-1 выше; для удобства перечислим их здесь, а далее опишем более подробно:

- Вход в систему;
- Управление учетными записями;
- Подробное отслеживание;
- Доступ к службе каталогов (DS);
- Вход/выход;
- Доступ к объекту;
- Изменение политики;
- Использование прав;
- Отслеживание процессов;
- Система;
- Аудит доступа к глобальным объектам.

На рис. 8-3 показаны подкатегории категории **Вход в систему** (Account Logon). Для каждой подкатегории можно выполнять аудит успехов и/или аудит отказов.

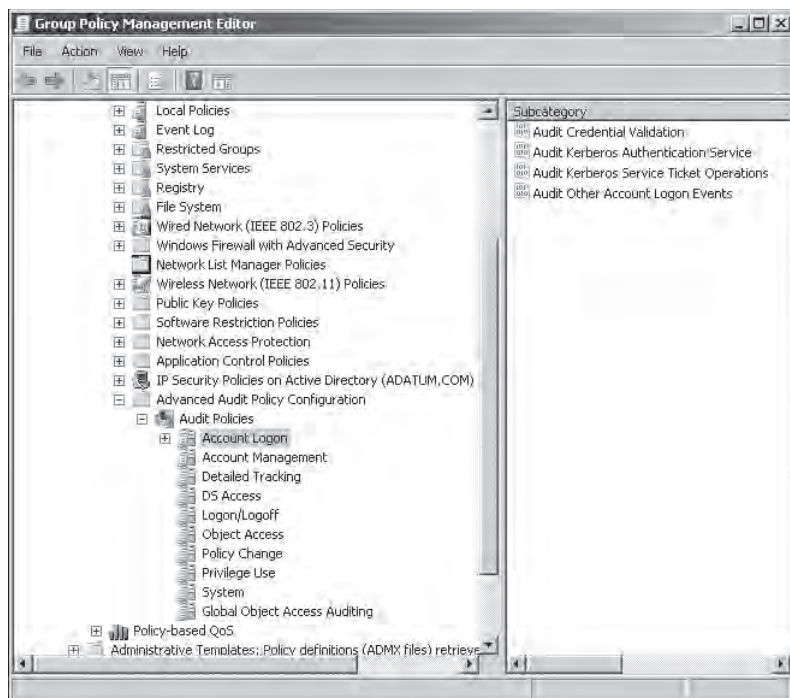


Рис. 8-3. Подкатегории категории Вход в систему

Дважды щелкнув категорию, можно настраивать ее на вкладке **Политика** (Policy) диалогового окна свойств. Прежде чем делать это, убедитесь, что точно знаете, аудит чего выполняется, прочитав информацию на вкладке **Объяснение** (Explain). На рис. 8-4 показано объяснение для подкатегории **Аудит проверки**

**учетных данных** (Audit Credential Validation). Место не позволяет описать все параметры подкатегорий, поэтому мы опишем только самые важные. Однако вы можете изучить объяснения всех этих параметров самостоятельно.

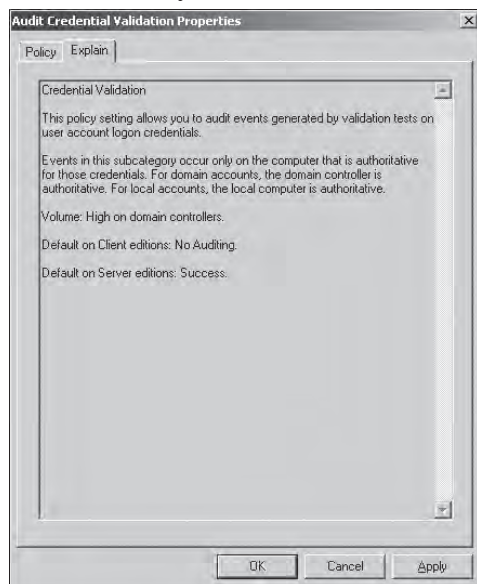


**Рис. 8-4.** Объяснение подкатегории Аудит проверки учетных данных

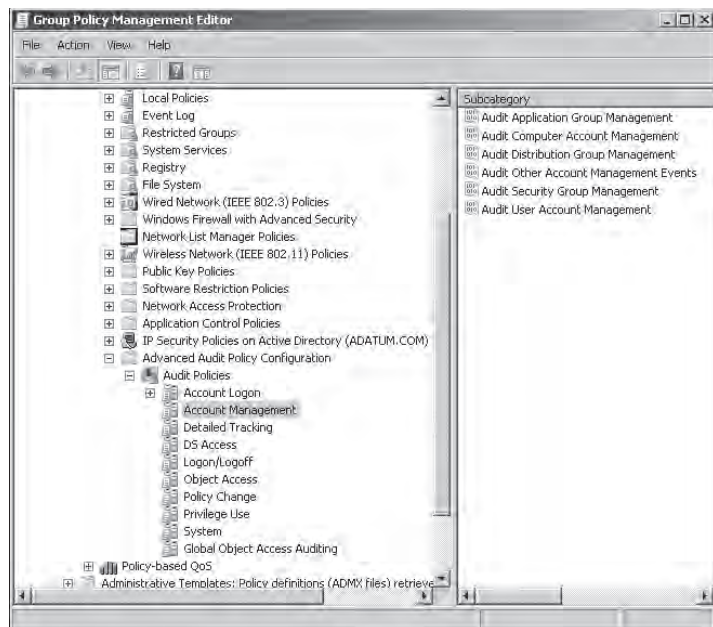


**Рис. 8-5.** Подкатегории категории Управление учетными записями

Категория **Управление учетными записями** (Account Management) позволяет выполнять аудит создания, удаления и изменения групп приложений, рассылки

и безопасности, учетных записей компьютеров и пользователей. Подкатегория **Другие события управления учетными записями** (Audit Other Account Management Events) позволяет настраивать аудит более редких событий, таких как доступ к хешу учетной записи пользователя во время переноса учетных записей. На рис. 8-5 показаны подкатегории категории **Управление учетными записями**. На практикуме этой главы вы выполните аудит создания учетных записей пользователей и добавления пользователей в группы безопасности.

Категория **Подробное отслеживание** (Detailed Tracking) позволяет выполнять аудит событий, которые генерируются при отправке запросов на шифрование или дешифрование DAPI, при создании, запуске и завершении процесса и при установке входящего подключения RPC.

Категория **Доступ к службе каталогов (DS)** [Directory Service (DS) Access] позволяет выполнять аудит событий, относящихся к доступу к DS, репликации DS и изменению объектов AD DS.

Категория **Вход/выход** (Logon/Logoff) позволяет выполнять аудит событий, относящихся к успешным и неудачным попыткам входа в систему и входам в систему с использованием явно указанных учетных данных (например, при запуске приложений от имени другого пользователя). Можно также выполнять аудит событий, относящихся к завершению сеанса входа и блокировке учетных записей. Можно настроить аудит событий, относящихся к сеансам служб терминалов, повышению привилегий, защите доступа к сети (NAP) и IPsec.

Категория **Доступ к объектам** (Object Access) позволяет выполнять аудит широкого диапазона событий доступа и событий, относящихся к операциям. События доступа включают доступ к реестру, к сетевым общим ресурсам и содержащимся в них файлам и папкам, к объектам файловой системы, к объектам COM+, к объектам SAM и объектам ядра. Кроме этого, можно выполнять аудит операций служб сертификации Active Directory, подключений, разрешенных или запрещенных платформой фильтрации Windows (WFP), и событий, сгенерированных при открытии или закрытии дескриптора объекта.

Категория **Изменение политики** (Policy Change) позволяет выполнять аудит изменений параметров политики, аутентификации и авторизации. Можно настроить аудит изменений в WFP и включить аудит событий, сгенерированных изменениями в правилах политики, примененных к службе защиты Microsoft (MPSSVC), используемой брандмауэром Windows.

Категория **Использование прав** (Privilege Use) позволяет определить, надлежащим ли образом используют свои права члены групп администраторов. Например, добавляют ли они рабочие станции в домен, изменяют ли квоты памяти, запрещают ли локальный вход в систему другим пользователям? Можно также выполнять аудит использования более важных привилегий. Пытается ли административный пользователь использовать привилегии, которые должны использоваться только операционной системой? Пытается ли такой пользователь изменить параметры аудита и журнала безопасности? На рис. 8-6 показаны подкатегории категории **Использование прав** (Privilege Use). Заметьте, что в подкатегории **Другие события использования прав** (Audit Other Privilege Use Events) пока нет параметров.



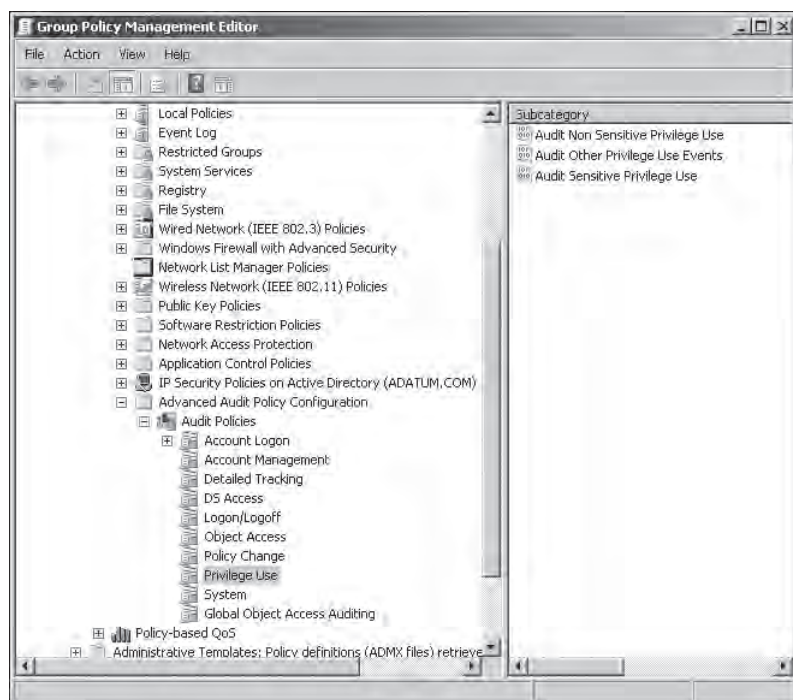


Рис. 8-6. Подкатегории категории Использование прав

Категория **Система** (System) позволяет выполнять аудит событий, относящихся к драйверу IPsec и системе безопасности. Категория **Аудит доступа к глобальным объектам** (Global Object Access Auditing) позволяет настраивать глобальные списки SACL для файловой системы и реестра всего компьютера.

## Защита уязвимых компьютеров

Обычно веб-серверы, находящиеся в периферийных зонах — наиболее вероятные цели для атак. Такие серверы не входят в домен и не могут быть защищены при помощи параметров групповой политики. Необходимо организовать мониторинг таких серверов, чтобы, например, быстро выявлять активность, указывающую на DoS-атаку, и принимать соответствующие меры. Следует применять IP-фильтрацию, чтобы блокировать трафик с закрытых или подозрительных IP-адресов.

Контроллерам домена доступ к Интернету обычно требуется гораздо реже, чем веб-серверам, если вообще требуется, поэтому они менее уязвимы к внешним атакам. Однако атака, проводимая внутренним пользователем, или небрежная настройка неопытным администратором может быть серьезной угрозой. Например, следует выполнять мониторинг неудачных и успешных попыток входа. Множественные неудачные попытки входа могут указывать на попытку подобрать пароль администратора. Успешный вход пользователя, не имеющего права на вход, может указывать на то, что администратор превысил свои полномочия и предоставил такую возможность.



## Мониторинг безопасности сервера

Аудит — основной метод мониторинга безопасности компьютера под управлением Windows Server 2008 R2. В первой части этого занятия говорилось о том, как планировать использование различных категорий аудита, применяемых к компьютерам под управлением Windows Server 2008 R2. В этом разделе мы подробнее рассмотрим ситуации, в которых следует использовать мониторинг каждой политики аудита.

## Мониторинг журнала безопасности

События аудита записываются в журнал безопасности, который можно просматривать средством просмотра событий (Event Viewer). В гл. 12 будет рассказано, как использовать средство просмотра событий для привязки задач к определенным событиям и выполнения других действий. Привязка задач позволяет получать оповещения, когда происходят определенные события. Кроме того, привязанные задачи можно настроить для запуска групп сборщиков данных, которые позволяют получать более подробную информацию. При соответствующей настройке группы сборщиков данных позволяют получать подробные сведения о событиях, произошедших на компьютере под управлением Windows Server 2008 R2, таких как запуск определенных приложений или процессов.

Другая возможность, о которой будет рассказано в гл. 12 — использование пересылки событий и подписок. Если отслеживается информация о входе пользователей, особенно когда пользователи могут проходить проверку подлинности на одном из многих контроллеров домена в сайте, настройка подписок журналов событий дает значительные преимущества, позволяя просматривать все данные централизованно. Серверы, настроенные как сборщики, должны иметь достаточно дискового пространства для хранения больших файлов журналов, генерируемых при пересылке событий безопасности со всех серверов организации, работающих под управлением Windows Server 2008 R2.

Наконец, в гл. 12 рассматриваются настраиваемые представления. При аудите окружения Windows Server 2008 R2 можно получать огромные объемы данных. Создание набора пользовательских представлений позволит сфокусироваться на событиях, представляющих какой-либо интерес. Если просматривать каждую строку журнала безопасности, можно быстро утомиться и не заметить важную информацию. Обнаружив интересное событие, создайте настраиваемое представление, чтобы в следующий раз можно было быстро найти похожие события.

## Аудит событий входа в систему и событий входа учетной записи

Есть два типа аудита событий входа, и даже опытные системные администраторы могут путать их и обращаться к документации, чтобы убедиться, что используется нужная категория аудита:

- аудит событий входа учетной записи;
- аудит событий входа.

События входа учетной записи генерируются, когда учетная запись пользователя домена проходит проверку подлинности на контроллере домена. События записываются в журналы на контроллере домена, и для их централизован-

ного аудита следует настроить пересылку событий на этом контроллере домена. Если пересылка событий не используется, необходимо проверять журналы событий на каждом контроллере домена в сайте, поскольку любой из них может выполнять проверку подлинности входа учетных записей.

При аудите событий входа записываются локальные входы в систему. Если включен аудит обеих категорий, то при входе пользователя на рядовой сервер, включенный в домен, в журнал событий на этом сервере будет записано событие входа, а в журнал событий на контроллере домена — событие входа учетной записи.

### **Аудит управления учетными записями**

Если включена политика **Аудит управления учетными записями** (Audit Account Management), в журнал записываются события, относящиеся к управлению учетными записями на контроллере домена или локальном компьютере. События управления учетными записями включают:

- создание, удаление и изменение учетных записей пользователей;
- создание, удаление и изменение групп безопасности и рассылки;
- изменение паролей пользователей.

Политика аудита чаще всего используется для ведения независимых записей о действиях сотрудников службы поддержки и отдела кадров, выполняющих управление учетными записями пользователей. Тщательный аудит событий управления учетными записями позволит выявить случаи несанкционированного изменения учетных записей; например, когда сотрудник службы поддержки изменяет пароль директора, чтобы получить доступ к важным данным на файловом сервере.

### **Аудит доступа к службе каталогов**

Аудит доступа к службе каталогов позволяет записывать события доступа к объектам из службы каталогов Active Directory, для которых настроены списки SACL. Эта политика аудита полезна, когда требуется следить за изменениями в важных объектах Active Directory, например, подразделениях.

### **Аудит доступа к объектам**

Политика **Доступ к объектам** (Object Access) используется для аудита доступа ко всем объектам, кроме хранящихся в AD DS. Эту политику можно использовать для записи информации о доступе к определенным файлам, папкам, разделам реестра и принтерам. Обеспечивая защиту важных данных, следует настроить эту политику так, чтобы можно было выполнять аудит попыток доступа к этим данным. Следует записывать не только имена пользователей, успешно получивших доступ к данным, но и имена пользователей, пытавшихся получить доступ неудачно. Это позволит обнаружить пользователей, которые не должны иметь доступа к данным, но имеют его или пытаются получить.

### **Аудит изменения политики**

Политика **Аудит изменения политики** (Audit policy change) позволяет следить за изменениями прав пользователей, политик аудита и политик доверия. Эта политика часто используется для отслеживания изменений в учетных записях

сотрудников ИТ-отделов. В сетях со строгой политикой безопасности необходимо следить, каким пользователям делегированы определенные права. Иногда бывает сложно следить за правами, делегированными какой-либо учетной записи или группе. Аудит активности такого типа позволяет убедиться, что учетным записям не делегированы ненадлежащие права. Вряд ли вы захотите, вернувшись из недельного отпуска, обнаружить, что какой-то сотрудник делегировал себе привилегии администратора предприятия, не добавляя свою учетную запись в соответствующую группу.

### **Аудит использования привилегий**

Включение политики **Аудит использования привилегий** (Audit privilege use) позволяет следить за использованием прав пользователей. В окружениях с высоким уровнем защиты полезно записывать, как используются учетные записи административного уровня, и следить за тем, чтобы администраторы не превышали своих полномочий, изменяя что-то только потому, что могут это изменять, но не имея официального разрешения на это.

### **Аудит системных событий и отслеживания процессов**

Политики **Аудит системных событий** (Audit system events) и **Аудит отслеживания процессов** (Audit process tracking) позволяют выполнять мониторинг событий, относящихся к компьютеру, а не пользователю. Политику аудита отслеживания процессов можно использовать для слежения за активацией программ, за использованием программами объектов и завершением приложений. Политика аудита системных событий позволяет записывать информацию о запуске и выключении компьютера. Ее можно использовать также для записи данных о событиях, изменяющих журнал безопасности.

---

#### **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ    Аудит AD DS**

Подробнее об аудите AD DS в Windows Server 2008 и 2008 R2 см. по адресу <http://technet.microsoft.com/ru-ru/library/cc731607.aspx>.

---

### **Использование шифрованной файловой системы**

Шифрованная файловая система (EFS) позволяет обеспечить целостность данных. Можно шифровать отдельные файлы и папки при помощи открытого ключа шифрования, привязанного к определенной учетной записи пользователя. Зашифрованный файл можно расшифровать только при помощи закрытого ключа шифрования, имеющегося только у пользователя. Можно также шифровать документы с использованием открытых сертификатов EFS других пользователей. Документ, зашифрованный таким сертификатом, может быть расшифрован только при помощи закрытого сертификата этого пользователя.

Группы безопасности не могут иметь сертификаты шифрования, поэтому число пользователей, имеющих возможность обращаться к зашифрованному документу, всегда ограничено индивидуальными сертификатами EFS, назначенными документу. Добавить для зашифрованного файла сертификат другого пользователя может только тот пользователь, который зашифровал этот файл. С использованием EFS исчезает вероятность того, что зашифрованный файл, хранящийся в общей папке, может быть прочитан кем-то, кто не должен иметь

доступа к этому файлу, из-за неверно настроенных разрешений общей папки или NTFS. Как известно многим администраторам, научить пользователей настраивать разрешения NTFS может быть сложно. Это становится еще сложнее, если учесть разрешения общих папок. Научить людей использовать EFS для ограничения доступа к документам значительно проще, чем объяснять принципы работы ACL в NTFS.

Рассматривая возможность развертывания EFS в своей организации, помните, что конфигурация EFS по умолчанию использует самоподписанные сертификаты. Эти сертификаты создаются на компьютере пользователя, а не в центре сертификации (ЦС), и могут вызывать проблемы при совместном доступе к документам, так как они не обязательно доступны с других компьютеров, где пользователь не имеет зашифрованных документов. Более надежное решение — изменить используемый по умолчанию шаблон сертификатов EFS, предоставляемый ЦС предприятия Windows Server 2008 R2, чтобы включить автоматическую регистрацию. Сертификаты EFS, автоматически выданные ЦС предприятия, могут храниться в AD DS и применяться к файлам, которые должны совместно использоваться разными пользователями. Другая возможность развертывания EFS — использование смарт-карт. В этом случае закрытые сертификаты EFS пользователей могут храниться на смарт-картах, а открытые сертификаты — в AD DS.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ EFS

Подробнее о EFS см. по адресу [http://technet.microsoft.com/ru-ru/library/cc749610\(WS.10\).aspx](http://technet.microsoft.com/ru-ru/library/cc749610(WS.10).aspx).

---

#### Шифрование диска BitLocker

BitLocker — альтернативный способ защиты файлов, хранящихся на томе с операционной системой Windows Server 2008 R2 и других фиксированных томах данных на внутренних жестких дисках. Для защиты данных на съемных дисках используется технология BitLocker To Go. BitLocker используется для шифрования целых томов; EFS позволяет шифровать отдельные файлы.

Если файлы зашифрованы с использованием BitLocker, можно войти в систему и работать с ними как обычно, но злоумышленники не смогут получить доступ к системным файлам и определить пароль пользователя. BitLocker предотвратит получение доступа к диску, даже если снять этот диск и подключить к другому компьютеру.

Новые файлы, добавляемые на диск, зашифрованный с использованием BitLocker, автоматически шифруются. Файлы, копируемые с зашифрованного тома на другой том или компьютер, дешифруются. Если открыть общий доступ к файлам, они будут зашифрованы, но авторизованные пользователи смогут получить к ним доступ.

Если зашифрован том операционной системы Windows Server 2008 R2, BitLocker во время загрузки проверяет сервер на наличие условий, представляющих угрозу для безопасности, таких как изменение загрузочных файлов. Если обнаружена потенциальная угроза, BitLocker блокирует том

операционной системы, и для его разблокирования требуется ключ восстановления BitLocker. Этот ключ создается при первом включении BitLocker.

Шифрование BitLocker наиболее эффективно при использовании совместно с доверенным платформенным модулем (TPM) версии 1.2. TPM — аппаратный компонент, устанавливаемый производителем компьютера. Если компьютер имеет чип TPM, BitLocker использует его для записи ключей, применяемых для разблокирования шифрованного тома операционной системы. При запуске компьютера BitLocker запрашивает у TPM ключи для разблокирования тома.

BitLocker можно использовать и на компьютерах без чипа TPM. Для запуска компьютера потребуется вставить загрузочный USB-ключ, и при этом предзагрузочная проверка целостности системы, как при использовании TPM, выполняться не будет.

Загрузочный USB-ключ необходимо хранить в надежном месте. Если потерять его, том операционной системы будет заблокирован, и доступ к файлам, хранящимся на этом диске, будет навсегда утрачен.

Если шифруются фиксированные или съемные диски данных, их можно разблокировать паролем или смарт-картой. Можно настроить автоматическую разблокировку при входе в систему. BitLocker можно в любой момент отключить — временно, приостановив шифрование, или постоянно, выполнив дешифрование тома.

## ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Подробнее об использовании BitLocker на компьютерах под управлением Windows Server 2008 R2 см. по адресу <http://technet.microsoft.com/ru-ru/library/cc732774.aspx>.

## СОВЕТ Подготовка к экзамену

В темы экзамена использование BitLocker не входит, и вряд ли вам встретятся подробные вопросы об этом. Однако вы должны знать, что шифрование BitLocker работает с целыми томами, и его (в отличие от EFS) нельзя использовать для ограничения доступа отдельных пользователей.

### Проверьте себя

- Какую политику аудита следует использовать для отслеживания доступа к важным файлам?

### Ответ

- Аудит доступа к объекту.

## Резюме

- Во время планирования системы безопасности следует проверить текущие параметры безопасности, определить уязвимые компьютеры и важные ре-

судсы, просмотреть политики и процедуры, установленные в организации, оценить роли и задачи пользователей и администраторов. Необходимо выявить важные или подозрительные учетные записи и авторизованные программы, настроить брандмауэр и антивирусные программы.

- В процессе планирования системы безопасности, скорее всего, потребуется настроить политики аудита безопасности, позволяющие выявлять угрозы, представляемые злонамеренными или неосторожными внутренними пользователями и неправильными действиями неопытных администраторов.
- EFS позволяет шифровать отдельные файлы и папки при помощи открытых ключей шифрования, связанных с определенными учетными записями пользователей.

## Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных на занятии 1. Эти вопросы предоставлены также в электронном виде на прилагаемом к книге компакт-диске.

---

### ПРИМЕЧАНИЕ Ответы

Ответы на вопросы и пояснения к их вариантам размещены в разделе «Ответы» в конце книги.

---

1. В главном офисе организации находится три контроллера домена. Вы хотите настроить рядовой сервер с именем SRV-Records для получения записей обо всех событиях входа и выхода с использованием учетных записей домена, происходящих в главном офисе. Как это сделать?
  - a. Настроить на контроллерах домена пересылку событий. Пересылать на сервер SRV-Records события, генерируемые политикой **Аудит событий входа учетной записи** (Audit Account Logon Events).
  - b. Настроить на контроллерах домена пересылку событий. Пересылать на сервер SRV-Records события, генерируемые политикой **Аудит управления учетными записями** (Audit Account Management).
  - c. Настроить на контроллерах домена пересылку событий. Пересылать на сервер SRV-Records события, генерируемые политикой **Аудит событий входа** (Audit Logon Events).
  - d. Настроить на контроллерах домена пересылку событий. Пересылать на сервер SRV-Records события, генерируемые политикой **Аудит доступа к службе каталогов** (Audit Directory Service Access).
2. Пять бухгалтеров хотят использовать общую папку **Accounting** для временного совместного использования конфиденциальной клиентской информации. Доступ к этой папке имеют тридцать бухгалтеров, и опыт показывает, что пользователи почти всегда неправильно настраивают разрешения на доступ к файлам и папкам. Какой из следующих методов можно использовать, чтобы обеспечить безопасность конфиденциальных данных, размещенных в общей папке **Accounting**?
  - a. Использовать BitLocker для шифрования конфиденциальных данных.

- b. Использовать EFS для шифрования конфиденциальных данных, используя учетную запись особой группы.
  - c. Использовать EFS для шифрования конфиденциальных данных с использованием сертификатов EFS каждого из пяти бухгалтеров.
  - d. Использовать BitLocker для шифрования конфиденциальных данных с использованием сертификатов шифрования каждого из пяти бухгалтеров.
3. Вы планируете использовать криминалистический анализ для выявления брешей в системе безопасности сети. Вы собираетесь использовать полученную при анализе информацию для создания плана, указывающего угрозы и позволяющего повысить безопасность. Какую информацию следует записывать при криминалистическом анализе? (Каждый ответ составляет часть решения; выберите четыре.)
- a. Идентификационные данные злоумышленника.
  - b. Время проведения атаки.
  - c. Длительность атаки.
  - d. Идентификационные данные компьютера, с которого произведена атака.
  - e. Атакованные компьютеры.
  - f. Изменения, произведенные злоумышленником в сети.
4. Во время плановой проверки конфигурации AD DS в администрируемом вами домене вы заметили, что было добавлено несколько групп безопасности, не предусмотренных планом обеспечения безопасности домена, и удалено несколько групп, которые должны существовать. Вы подозреваете, что недавно назначенный системный администратор превысил свои полномочия. Какую категорию политик аудита следует настроить, чтобы отслеживать создание и удаление групп безопасности?
- a. Доступ к службе каталогов.
  - b. Подробное отслеживание.
  - c. Доступ к объектам.
  - d. Управление учетными записями.
5. Вы планируете использовать криминалистический анализ данных, имеющих отношение к безопасности организации, работающей в регулируемом законодательством секторе. Требуется определить срок хранения криминалистических данных. Как долго должны храниться такие данные с учетом законодательства?
- a. 21 день.
  - b. 180 дней.
  - c. 7 лет.
  - d. Бессрочно.



## Занятие 2. Управление безопасностью сервера

Службы обновления сервера Windows (WSUS) — дополнительный компонент Windows Server 2008 R2, функционирующий как локальный сервер обновлений. Чтобы каждый компьютер в организации не загружал мегабайты обновлений из Интернета, можно настроить сервер WSUS, чтобы только он получал обновления, а все остальные компьютеры настроить на использование этого сервера в качестве источника обновлений. На этом занятии вы узнаете, как использовать WSUS в качестве основного метода управления обновлениями в среде Windows Server 2008 R2. Мы также расскажем о более сложных программных решениях, таких как System Center Essentials 2010 и System Center 2012 Configuration Manager, которые позволяют выполнять обновления и обеспечивать соответствие компьютеров установленным правилам и предписаниям.

---

### Изучив материал этого занятия, вы сможете:

- ✓ Управлять обновлениями операционной системы.
- ✓ Управлять обновлениями приложений.
- ✓ Управлять WSUS.

**Продолжительность занятия — примерно 40 мин.**

---

## Развертывание обновлений при помощи WSUS

WSUS 3.0 со вторым пакетом обновлений (SP2) — бесплатный компонент, который можно установить в Windows Server 2008 R2, позволяющий централизованно развертывать обновления приложений и операционной системы в сети организации. WSUS 3.0 SP2 можно загрузить с сайта Microsoft и установить на компьютере под управлением Windows Server 2008 R2, если выполняются требования к установке. WSUS 3.0 SP2 нельзя установить на сервер, работающий в режиме Server Core, хотя такая возможность может появиться в следующих версиях.

### Требования к установке

Перед установкой WSUS 3.0 SP2 необходимо установить следующее ПО:

- IIS 6.0 или выше;
- .NET Framework 2.0 или выше;
- консоль управления (MMC) 3.0;
- дистрибутивный пакет Microsoft Report Viewer 2008 или выше.

На сервере под управлением Windows Server 2008 R2 по умолчанию должно быть установлено все перечисленное ПО, кроме Report Viewer (последняя версия — дистрибутивный пакет Report Viewer 2010). Report Viewer нельзя установить как дополнительный компонент или роль; его можно загрузить из центра загрузок Microsoft. Установочный файл WSUS 3.0 SP2 работает с дистрибутивным пакетом Report Viewer 2008, но не с версией 2008 SP1 или 2010. Со времени написания книги ситуация могла измениться, но практикум этой главы написан с учетом имеющихся условий.

Для создания отчетов WSUS необходимы средства для работы с базами данных. WSUS 3.0 SP2 может взаимодействовать со следующими СУБД:

- Microsoft SQL Server 2008 Standard или Enterprise;
- Microsoft SQL Server 2005 SP3 или выше.

Если поддерживаемая версия SQL Server не установлена, мастер установки WSUS 3.0 SP2 установит внутреннюю базу данных Windows (Windows Internal Database).

Установка WSUS 3.0 SP2 может быть выполнена только в том случае, если включены следующие компоненты Windows Server 2008 R2:

- Проверка подлинности Windows;
- Статическое содержимое;
- Совместимость управления IIS 6.0 (или выше);
- Совместимость метабазы IIS 6.0 (или выше).

Включив все перечисленные компоненты и установив Report Viewer, можно установить WSUS 3.0 SP2.

При установке WSUS 3.0 SP2 на компьютере под управлением Windows Server 2008 R2 создаются две локальные группы. Эти группы функционируют как административные роли WSUS, и вы можете назначать пользователям роли, добавляя их учетные записи в соответствующие группы.

- **Администраторы WSUS (WSUS Administrators).** Пользователи, входящие в эту локальную группу, могут администрировать сервер WSUS, выполняя задачи от одобрения обновлений и настройки групп компьютеров до настройки автоматического одобрения и источника обновлений сервера WSUS. Пользователи, входящие в эту группу, могут удаленно управлять WSUS, подключаясь с помощью консоли служб обновления.
- **Создатели отчетов WSUS (WSUS Reporters).** Пользователи, входящие в эту локальную группу, могут создавать отчеты на сервере WSUS и удаленно подключаться через консоль служб обновления для работы с отчетами.

Как уже говорилось, для хранения конфигурации и информации об отчетах WSUS можно использовать базы данных SQL Server 2005 SP3 и выше (последняя версия — SQL Server 2012). Организации, которым требуются настраиваемые отчеты, вместо стандартных возможностей, предоставляемых консолью служб обновления, могут использовать этот вариант и создавать собственные приложения для взаимодействия с базой данных SQL Server. Например, разработчики могут создать приложение, извлекающее информацию из базы данных и ежедневно пересылающее ее администраторам по электронной почте. Организациям, выбравшим такой тип развертывания, следует обратить внимание на System Center Essentials 2010 (см. ниже) в качестве решения для управления обновлениями, которое предоставляет больше возможностей по работе с отчетами.

## Варианты развертывания

Способ развертывания WSUS зависит от архитектуры сети организации. Ниже описаны четыре распространенных варианта развертывания WSUS и сетевые окружения, для которых они лучше всего подходят.

### Один сервер WSUS

В этом варианте в защищенной сети разворачивается один сервер WSUS, синхронизирующий содержимое непосредственно со службой обновлений Microsoft, после чего обновления распространяются среди клиентов (рис. 8-7).

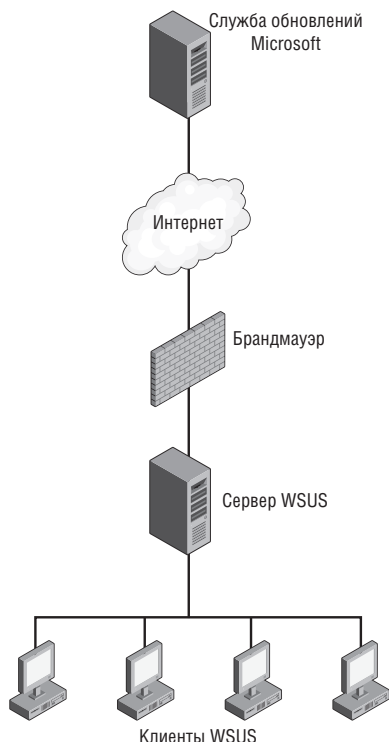


**Рис. 8-7.** Вариант с одним сервером WSUS

### Несколько независимых серверов WSUS

В организациях, имеющих удаленные филиалы, часто используется несколько независимых серверов WSUS. Каждый сервер WSUS действует как вышестоящий сервер (выступает в роли источника обновлений). Настройка и одобрение данных выполняется для каждого сервера в отдельности, обычно администраторами на местах. На рис. 8-8 показан такой вариант разворачивания.

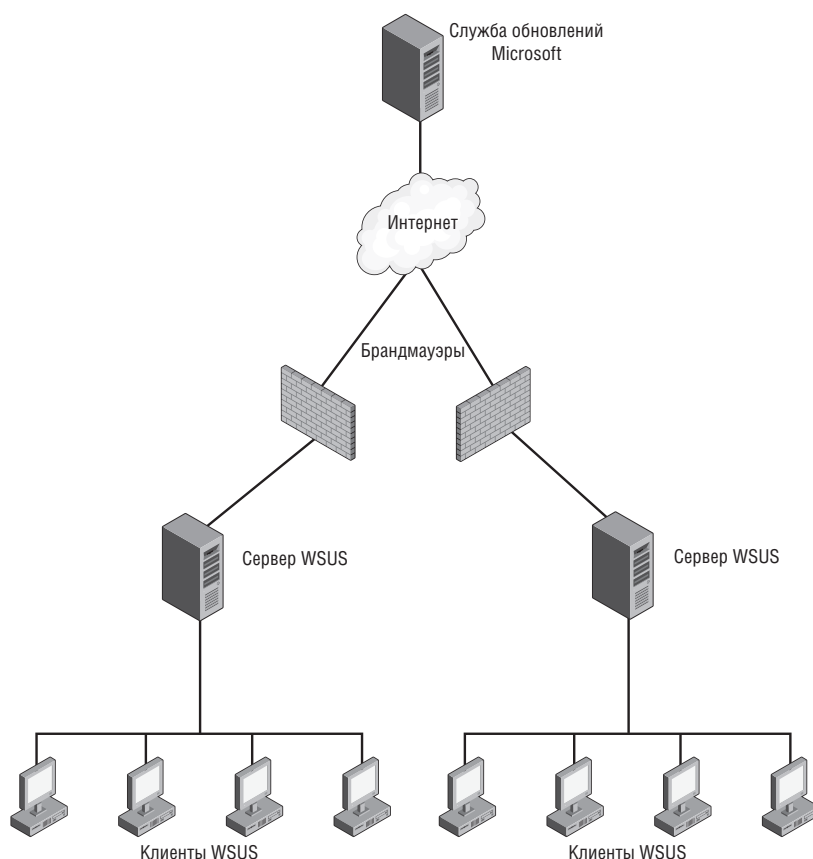


Рис. 8-8. Несколько независимых серверов WSUS

### Несколько серверов WSUS с внутренней синхронизацией

В этом варианте развертывания сервер WSUS, получающий обновления от службы обновлений Microsoft, назначается вышестоящим сервером. Сервер WSUS получающий обновления от другого сервера WSUS, назначается подчиненным сервером. Такой тип развертывания выходит из употребления, поскольку WSUS 3.0 SP2 поддерживает до 25000 клиентов, а одноранговое кэширование BITS (фоновой интеллектуальной службы передачи) позволяет передавать обновления от клиента к клиенту по локальной сети. При использовании однорангового кэширования BITS один клиент может получить обновления от сервера WSUS, затем передать их остальным клиентам из той же подсети.

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ BITS

Подробнее о BITS и одноранговом кэшировании см. по адресу [http://msdn.microsoft.com/en-us/library/aa362708\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa362708(VS.85).aspx) (на английском языке). Однако на экзамене вряд ли будут вопросы, касающиеся BITS.

При проверке в сети Microsoft применение однорангового кэширования снизило нагрузку на серверы WSUS настолько, что 70% процентов обновлений было получено от других компьютеров из локальной сети, а не от сервера WSUS

непосредственно. Это значит, что один сервер WSUS может справиться с нагрузкой почти всегда, кроме самых крупных сайтов. Модель развертывания нескольких серверов с внутренней синхронизацией показана на рис. 8-9.

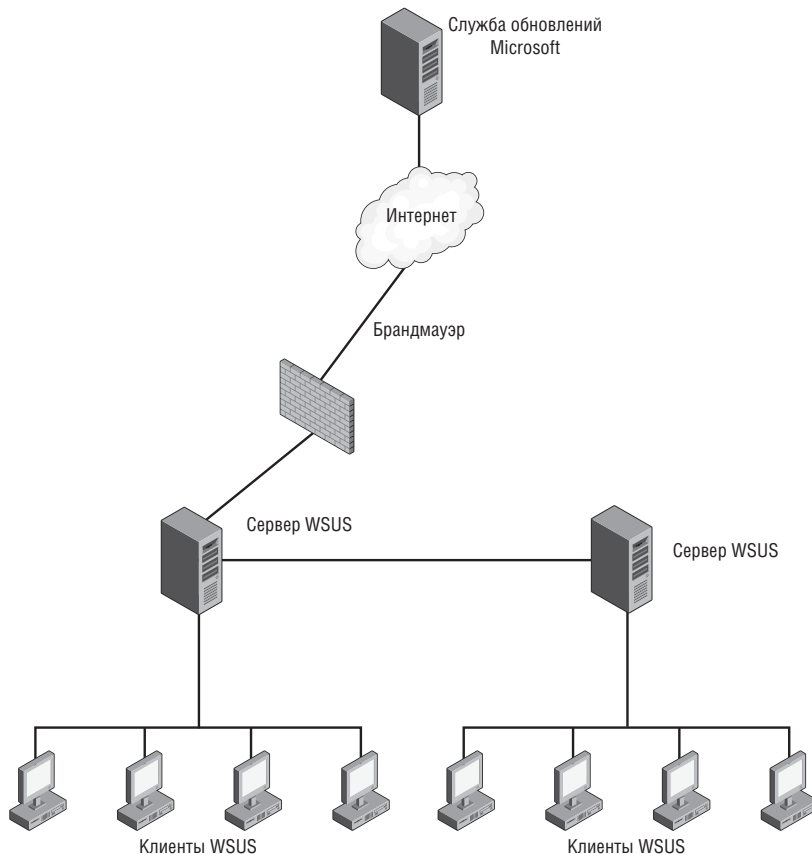


**Рис. 8-9.** Несколько серверов WSUS с внутренней синхронизацией

### Отключенные серверы WSUS

В модели с отключенными серверами один сервер получает обновления из Интернета, после чего эти обновления распространяются на других носителях (на записываемых DVD или съемных USB-носителях) и устанавливаются на остальных серверах, которые развертывают их на клиентах. Многие администраторы используют такую модель для работы с удаленными филиалами. Вместо того чтобы передавать гигабайты обновлений по медленным WAN-каналам на новый сервер WSUS, расположенный в удаленном филиале, данные физически транспортируются и добавляются локально. На рис. 8-10 показана модель с использованием отключенных серверов.

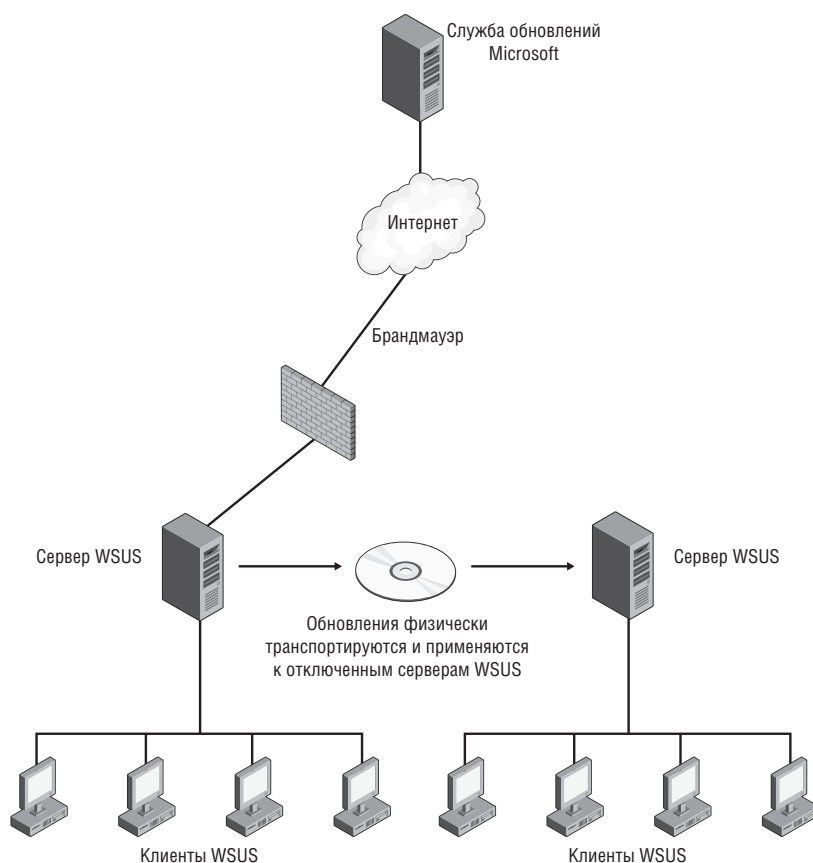


Рис. 8-10. Отключенные серверы WSUS

## Новые возможности WSUS 3.0 SP2

WSUS 3.0 SP2 — обновление WSUS 3.0 с пакетом обновлений 1 (SP1), а не новый выпуск. Тем не менее, эта версия имеет значительные изменения и новые функции, о которых необходимо знать. Сервер WSUS, работающий под управлением Windows Server 2008 R2, требует установки WSUS 3.0 SP2 (хотя сервер WSUS 3.0 SP2 будет работать и в другой серверной ОС, например, Windows Server 2008 SP1). В документации Microsoft особо отмечается, что не следует устанавливать WSUS 3.0 SP1 на сервер под управлением Windows Server 2008 R2.

### ПРИМЕЧАНИЕ Обновление в правильном порядке

Если на компьютер под управлением Windows Server 2008 установить WSUS 3.0 SP2, а затем попытаться обновить операционную систему до Windows Server 2008 R2, обновление завершится неудачно.

WSUS 3.0 SP2 в Windows Server 2008 R2 можно установить как роль сервера. Наверно, самые значимые новые возможности WSUS 3.0 SP2 — поддержка клиентов под управлением Windows 7 и поддержка BranchCache (см. гл. 7).

Кроме того, в WSUS 3.0 SP2 значительно улучшен агент клиента обновления Windows (WUA). Время сканирования клиента сокращено, и серверы WSUS могут проводить выборочное сканирование клиентов вместо полного. Это значительно ускоряет выполнение сканирования приложениями, использующими API обновления Microsoft, такими как Защитник Windows.

Правила автоматического одобрения WSUS 3.0 SP2 позволяют указывать дату и время крайнего срока одобрения обновлений для всех компьютеров или отдельных групп компьютеров. Выбор языка для подчиненных серверов теперь имеет новое диалоговое окно предупреждения, отображающееся в случае загрузки обновлений только на заданных языках. Можно выполнять отчеты о состоянии компьютеров и обновлений из консоли WSUS или использовать программный интерфейс (API) для включения этих функций в собственные отчеты. Отчеты о состоянии обновлений позволяют фильтровать обновления, одобренные для установки.

Изменились также требования к установке WSUS 3.0 SP2 (см. выше). Возможно, самое значительное изменение заключается в необходимости установки дистрибутивного пакета Report Viewer 2008 или более поздней версии. Для WSUS 3.0 SP1 требовалась установка Report Viewer 2005 или выше.

---

### **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ   Заметки о выпуске WSUS 3.0 SP2**

Подробнее о новых возможностях и требованиях к установке см. в заметках о выпуске, доступных по адресу <http://technet.microsoft.com/ru-ru/library/dd939886.aspx>.

---

## **Автономный режим и режим реплики**

При настройке подчиненных серверов WSUS есть несколько вариантов. Первый вариант — настроить подчиненный сервер WSUS как реплику вышестоящего сервера. Чтобы открыть диалоговое окно, показанное на рис. 8-11, щелкните **Обновления** (Updates) в консоли управления WSUS, а затем щелкните **Источник обновления и прокси-сервер** (Update Source and Proxy Server). Это можно сделать, только установив WSUS 3.0 SP2, как описано на практикуме этого занятия.

Если настроить сервер WSUS таким образом, на нем будут использоваться все одобрения, параметры, компьютеры и группы с вышестоящего сервера. Подчиненный сервер в режиме реплики не может использоваться для одобрения обновлений, хотя можно переключить его в автономный режим, если требуется срочно развернуть обновление. Второй вариант — *автономный режим*. Этот режим позволяет локальным администраторам WSUS настраивать отдельные параметры одобрения, но продолжать получать обновления от вышестоящего сервера WSUS.



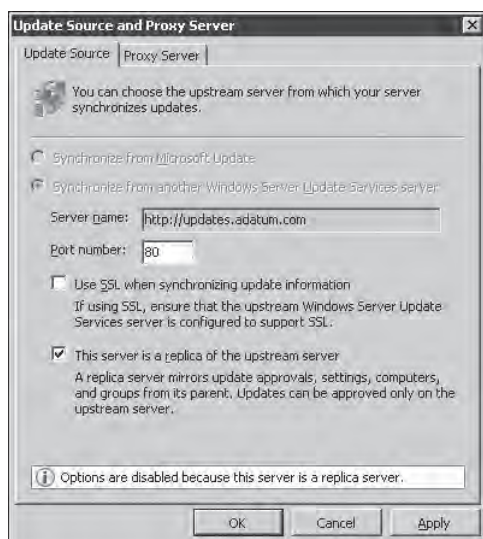


Рис. 8-11. Настройка подчиненного сервера в режиме реплики

## Использование групп компьютеров

В большинстве базовых вариантов развертывания WSUS все компьютеры, являющиеся клиентами сервера WSUS, получают обновления в одно время. Хотя такой способ подходит для многих организаций, иногда требуется развертывать обновления пошагово. Пошаговое и целевое развертывание обновлений можно выполнять при помощи групп. Microsoft сделала все возможное, чтобы обновления продуктов не приводили к появлению проблем с другими приложениями. Однако если в организации развертываются собственные приложения, обновления могут вызывать конфликты. Создав тестовую группу, можно развертывать обновления на отдельных компьютерах организации. Это позволяет проверить, не будет ли конфликтовать обновление с существующей конфигурацией, прежде чем проводить полномасштабное развертывание.

Группы компьютеров WSUS имеют следующие особенности:

- по умолчанию создаются две группы: **Все компьютеры** (All Computers) и **Неназначенные компьютеры** (Unassigned Computers). Когда клиент в первый раз обращается к серверу WSUS, он добавляется в группу **Неназначенные компьютеры**, если ему не назначена группа;
- можно создавать иерархию групп. Обновление, добавляемое в группу, расположенную на верхнем уровне иерархии, будет развернуто и на компьютерах, стоящих ниже в иерархии. Группа **Неназначенные компьютеры** входит в иерархию группы **Все компьютеры**;
- компьютеры могут входить в несколько групп.

Администраторы могут назначать учетные записи в группы WSUS двумя способами. Первый — указание на стороне сервера. Чтобы выбрать этот метод, в разделе параметров консоли **Update Services** выберите элемент **Компьютеры** (Computers) и установите переключатель **Использовать консоль Update Ser-**

vices (Use the Update Services console) (рис. 8-12). Когда компьютер в первый раз обратится к серверу WSUS, он будет добавлен в группу **Неназначенные компьютеры** (Unassigned Computers). После этого пользователь с привилегиями администратора WSUS может вручную добавить этот компьютер в другую группу, используя консоль WSUS.

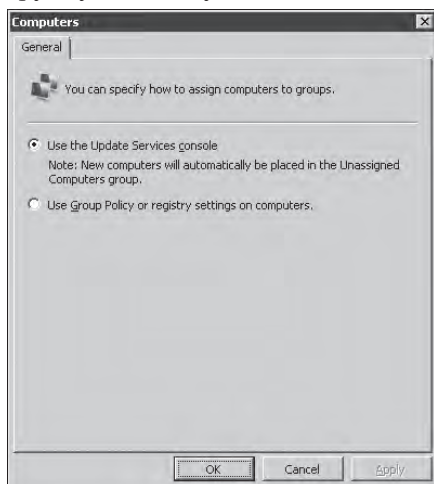


Рис. 8-12. Указание на стороне сервера

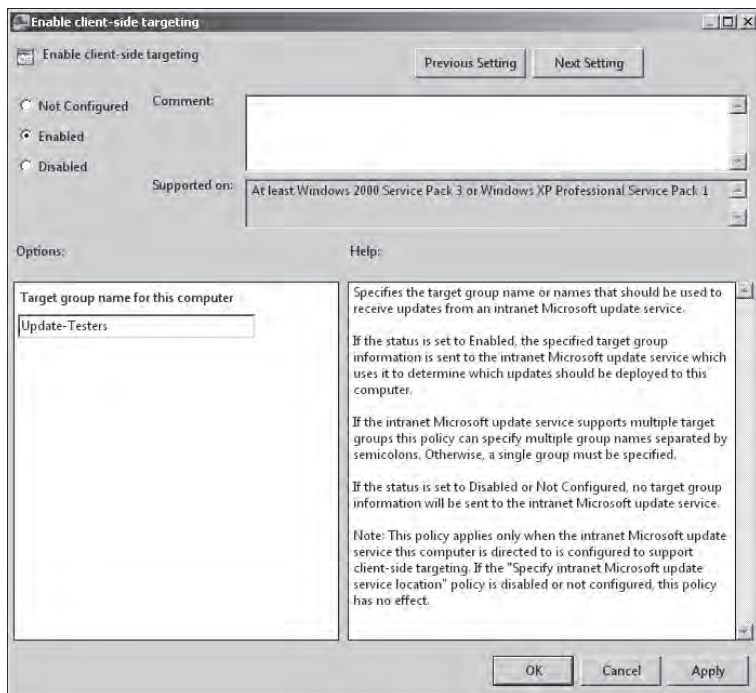


Рис. 8-13. Включение указания на стороне клиента

Второй способ назначения компьютеров в группы — использовать групповую политику или параметры реестра на клиентах WSUS. В крупных сетях этот

способ требует меньше работы и упрощает добавление компьютеров в группы. Независимо от того, какой способ используется, сначала необходимо создать группы при помощи консоли WSUS. Чтобы настроить GPO для поддержки указания на стороне клиента, выполните следующее:

- Измените GPO, который хотите использовать для назначения группы компьютера.
- В разделе **Конфигурация компьютера | Политики | Административные шаблоны | Компоненты Windows | Центр обновления Windows** (Computer Configuration | Policies | Administrative Templates | Windows Components | Windows Update) дважды щелкните элемент **Разрешить клиенту присоединение к целевой группе** (Enable Client-Site Targeting).
- Установите переключатель **Включить** (Enable) и укажите имя целевой группы (рис. 8-13).

## Настройка клиента WSUS

Хотя клиенты WSUS могут настраиваться в ручную, в большинстве крупных сетей их настраивают через групповую политику. Политики, имеющие отношение к WSUS, находятся в разделе **Конфигурация компьютера | Политики | Административные шаблоны | Компоненты Windows | Центр обновления Windows** (Computer Configuration | Policies | Administrative Templates | Windows Components | Windows Update); просмотреть их можно с помощью редактора управления групповой политикой (рис. 8-14). Если требуется, чтобы компьютер под управлением Windows Server 2008 R2, являющийся сервером WSUS, получал обновления, его нужно настроить так же, как любой другой клиент.

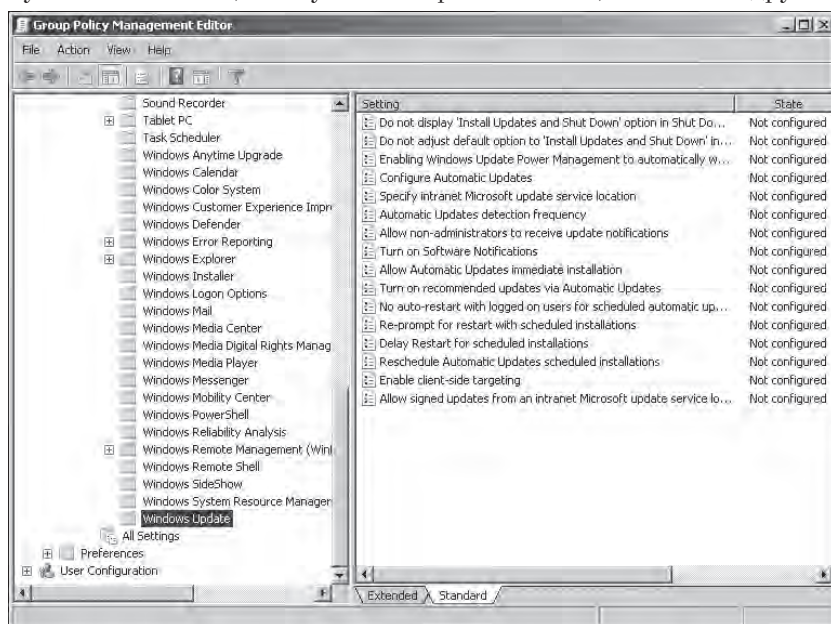


Рис. 8-14. Политики, имеющие отношение к WSUS

## Поведение установки обновлений

Кроме политик, отвечающих за включение компьютеров в группы WSUS и расположение локального сервера WSUS, важное значение имеют политики, определяющие, как и когда загружаются и устанавливаются обновления WSUS. Администратору следует избегать ситуаций, в которых обновления не устанавливаются из-за того, что пользователь вмешался и отменил установку, или расписание назначено на такое время, в которое компьютер всегда выключен. Следует найти компромисс, чтобы предотвратить вмешательство пользователей и не мешать им работать. Никто не будет рад, если потеряет несколько часов работы над важным документом из-за того, что администратор назначил установку обновлений и перезагрузку компьютера, не дав пользователю возможности как-то повлиять на этот процесс.

Планируя расписание развертывания обновлений, учитывайте следующие элементы политики:

- **Разрешить управлению электропитанием центра обновления Windows выводить систему из спящего режима для установки запланированных обновлений** (Enabling Windows Update Power Management To Automatically Wake Up The System To Install Scheduled Updates). Эта политика действует только для клиентов под управлением Windows Vista и Windows 7, имеющих совместимое оборудование и соответствующим образом настроенные параметры BIOS. Чтобы не беспокоиться о том, что работа пользователей будет прерываться из-за перезагрузок во время установки обновлений, можно включить эту политику, позволяющую выводить компьютеры из спящего режима ночью (или в другое время, когда они не используются), устанавливать обновления и снова отправлять компьютеры в спящий режим.
- **Настройка автоматического обновления** (Configure Automatic Updates). Эта политика указывает, будут ли обновления автоматически загружаться и включаться в расписание установки, или пользователь будет уведомляться о том, что доступны обновления (уже загруженные или на сервере WSUS).
- **Частота поиска автоматических обновлений** (Automatic Updates Detection Frequency). Если эта политика не включена, по умолчанию частота поиска равна 22 часам. Если требуется проверять наличие обновлений чаще, настройте эту политику.
- **Разрешить немедленную установку автоматических обновлений** (Allow Automatic Updates Immediate Installation). Если эта политика включена, все обновления, не требующие остановки служб и перезагрузки Windows, устанавливаются автоматически.
- **Не выполнять автоматическую перезагрузку при автоматической установке обновлений, если в системе работают пользователи** (No Auto-Restart With Logged On Users For Scheduled Automatic Updates Installations). Если эта политика включена, компьютер не перезагружается автоматически, а ждет, когда вошедший в систему пользователь инициирует перезагрузку. Пользователю сообщается о том, что требуется перезагрузка для установки обновлений. Если эта политика не включена, компьютер автоматически перезагружается через 5 минут после установки обновлений.

- **Задержка перезагрузки при запланированных установках** (Delay Restart For Scheduled Installations). Эта политика позволяет изменять время до автоматической перезагрузки. Как указано выше, по умолчанию перезагрузка выполняется через 5 минут. С помощью этой политики можно установить задержку до 30 минут.
- **Перенос запланированных автоматических установок обновлений** (Reschedule Automatic Updates Scheduled Installations). Если запланированная установка не выполнена (например, если компьютер был выключен или отключен от сети), эта политика обеспечивает установку обновлений через указанный промежуток времени после следующей загрузки компьютера. Если эта политика отключена, пропущенные обновления будут установлены во время следующей запланированной установки.

## Поддержка WSUS для перемещающихся клиентов

Во многих организациях есть сотрудники, постоянно находящиеся в разъездах. Такие сотрудники обычно имеют портативные компьютеры. С точки зрения развертывания обновлений это значит, что если не установлена технология вроде NAP (см. гл. 9), эти компьютеры могут не получать обновления до тех пор, пока не будут подключены в сети в главном офисе.

Чтобы перемещающиеся клиенты имели доступ к обновлениям на любом сервере WSUS в организации, с помощью групповой политики настройте все клиенты, чтобы они ссылались на одно имя сервера WSUS, а затем настройте DNS так, чтобы это имя (полное доменное имя) разрешалось в локальный IP-адрес в каждой подсети. Для этого откройте диспетчер DNS и настройте циклическое обслуживание DNS с расстановкой по адресу, используя диалоговое окно свойств компьютера (рис. 8-15). Если сделать это, DNS-сервер будет возвращать запись хоста из подсети запрашивающего компьютера. Заметьте, что для этого необходимо настроить для каждого сервера WSUS одно и то же полное доменное имя.

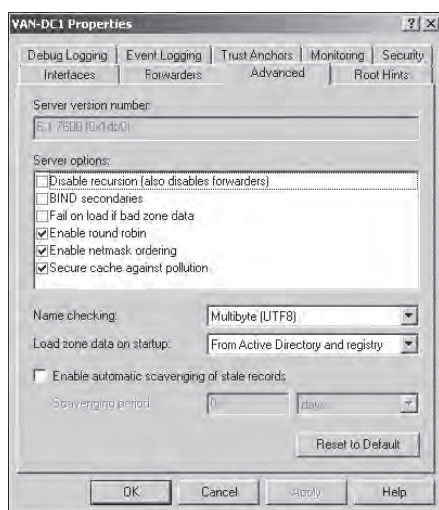


Рис. 8-15. Настройка циклического обслуживания DNS с расстановкой по адресу

## Стратегии обновления и синхронизации

Когда на сервер WSUS загружаются обновления, полученные из центра обновлений Microsoft или с вышестоящего сервера, метаданные и файлы обновлений сохраняются в разных местах. Метаданные обновления хранятся в базе данных WSUS. В зависимости от конфигурации WSUS, сами файлы обновлений хранятся на сервере WSUS или на серверах службы обновлений Microsoft. Эта конфигурация определяется во время установки WSUS. Если обновления хранятся на серверах Microsoft, одобренные обновления загружаются клиентами непосредственно из Интернета, а не с сервера WSUS.

Правила автоматического одобрения позволяют администратору автоматически одобрять определенные категории обновлений. В WSUS 3.0 SP2 правила автоматического одобрения позволяют указывать дату и время крайнего срока одобрения обновлений для всех компьютеров или отдельных групп. Обновления можно настроить для определенной классификации и определенных продуктов и применять к определенным группам компьютеров. Доступны следующие классификации: **Важные обновления** (Critical Updates), **Обновления определений** (Definition Updates), **Драйверы** (Drivers), **Пакеты дополнительных компонентов** (Feature Packs), **Обновления безопасности** (Security Updates), **Пакеты обновлений** (Service Packs), **Утилиты** (Tools), **Накопительные пакеты обновлений** (Update Rollups) и **Обновления** (Updates). Категория продуктов включает почти все текущие продукты Microsoft, которых слишком много, чтобы перечислить здесь.

Правил автоматического одобрения много, и их можно включать и отключать при необходимости. Эти правила настраиваются в диалоговом окне **Автоматическое одобрение** (Automatic Approvals) (рис. 8-16) и доступны в разделе **Параметры** (Options) в консоли **Update Services**. По умолчанию в WSUS 3.0 SP2 никакие обновления не одобряются автоматически.

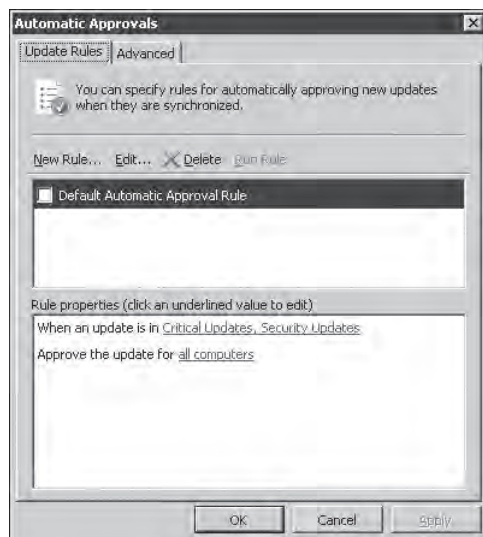


Рис. 8-16. Настройка автоматического одобрения

Чтобы одобрить обновление, выполните следующее:



1. Откройте консоль **Update Services**. Под узлом **Обновления** (Updates) щелкните **Все обновления** (All Updates).
2. В раскрывающемся списке **Одобрение** (Approval) выберите **Неодобренные** (Unapproved), а в раскрывающемся списке **Состояние** (Status) выберите **Любое** (Any).
3. Щелкните правой кнопкой обновление и выберите команду **Одобрить** (Approve). Откроется диалоговое окно **Одобрить обновления** (Approve Updates).
4. Щелкните **Подключиться ко всем компьютерам** (Connect To All Computers), а затем **Одобрено для установки** (Approved For Install).
5. Щелкните правой кнопкой новое назначенное одобрение в группе **Все компьютеры** (All Computers), щелкните **Крайний срок** (Deadline) и выберите срок 2 недели. Теперь одобренное обновление будет развертываться с установленным крайним сроком.

---

**ПРИМЕЧАНИЕ Форсирование обновлений**

Если требуется развернуть обновление незамедлительно, выберите в качестве крайнего срока прошедшую дату.

---

**Проверьте себя**

1. Какой режим следует выбрать для подчиненного сервера WSUS 3.0 SP2, чтобы использовать одобрения и конфигурацию групп компьютеров с указанного вышестоящего сервера?
2. Какое ПО, кроме WSUS 3.0 SP2, необходимо загрузить с сайта Microsoft перед установкой WSUS?

**Ответ**

1. Чтобы использовать одобрения и конфигурацию компьютеров с указанного вышестоящего сервера, подчиненный сервер должен работать в режиме реплики.
2. Перед установкой WSUS 3.0 SP2 необходимо загрузить и установить дистрибутивный пакет Report Viewer 2008 или выше.

## Управление обновлениями и соответствие условиям

Соответствие условиям означает обеспечение настройки компьютера предписанным образом. Сюда входит не только установка определенного набора обновлений, но и соответствующая настройка других параметров, таких как строгая политика паролей, конфигурация брандмауэра и антивирусного ПО.

### Отчеты WSUS

WSUS 3.0 SP2 предоставляет базовые средства для работы с отчетами. Отчеты создаются на основе информации, полученной от WSUS. WSUS не сканирует компьютеры, чтобы определить, какие обновления отсутствуют, а записывает, были ли обновления загружены на целевые компьютеры, и сообщили ли эти



компьютеры серверу WSUS об успешной установке обновлений. Чтобы получить доступ к средствам создания отчетов, щелкните узел **Отчеты** (Reports) в консоли **Update Services** (рис. 8-17).

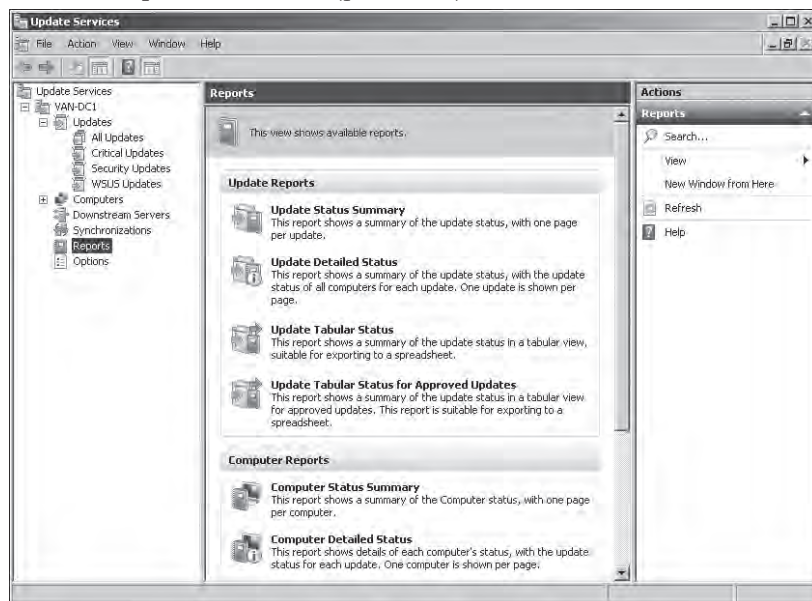


Рис. 8-17. Средства создания отчетов WSUS

Отчеты WSUS можно распечатывать или экспортировать в формат Excel или PDF. Если данные WSUS записываются в базу данных SQL Server, можно выполнять собственный анализ, используя собственные запросы. Пользователи WSUS 3.0 SP2, входящие в группы **Создатели отчетов WSUS** (WSUS Reporters) или **Администраторы WSUS** (WSUS Administrators) могут создавать следующие отчеты:

- **сводный отчет о состоянии обновлений** — предоставляет основную информацию о развертывании обновлений, включая число компьютеров, на которые обновление установлено, требуется установить или не удалось установить, и число компьютеров, о которых WSUS не имеет данных. Доступна одна страница для одного обновления;
- **детальный отчет о состоянии обновлений** — предоставляет гораздо больше информации о развертывании обновлений. Он предоставляет список компьютеров и состояние их обновлений, по одной странице на обновление. Отчет можно просматривать в виде сводки или таблицы;
- **табличный отчет о состоянии обновлений** — предоставляет данные о каждом обновлении в виде таблицы. Создав такой отчет, можно переключить его в режим сводки или режим детального отчета. Отчеты в такой форме лучше всего подходят для экспорта в Excel, так как уже представлены в виде таблицы;
- **табличный отчет о состоянии обновлений для утвержденных обновлений** — содержит сводную информацию о состоянии утвержденных обновлений,

представленную в виде таблицы. Такие отчеты можно экспортировать в электронные таблицы;

- **сводный отчет о состоянии компьютеров** — аналогичен детальному отчету о состоянии обновлений, но предоставляет информацию об обновлениях для каждого компьютера, а не для каждого обновления. Данные представлены в виде сводки;
- **детальный отчет о состоянии компьютеров** — предоставляет подробную информацию о состоянии определенных обновлений на указанном компьютере. Создав такой отчет, можно просматривать его в виде сводки или таблицы;
- **табличный отчет о состоянии компьютеров** — предоставляет данные о состоянии обновления в виде таблицы, где строки представляют отдельные компьютеры. Создав такой отчет, можно просматривать его в виде сводки или в виде детального отчета. Заметьте, что такой отчет отличается от табличного отчета о состоянии обновлений;
- **результаты синхронизации** — показывает результаты последней синхронизации сервера WSUS.

Если включить свертывание отчетов для подчиненных серверов WSUS, в отчеты, создаваемые на вышестоящих серверах, будут включаться данные об обновлениях, компьютерах и синхронизации, полученные от подчиненных серверов, работающих в режиме реплики.

## Другие средства управления обновлениями

Хотя WSUS является основным инструментом для управления обновлениями, рассматриваемым на экзамене, есть и другие средства, о которых следует знать. К таким средствам относятся Microsoft Baseline Security Analyzer, System Center Essentials 2010 и System Center 2012 Configuration Manager.

### Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer (MBSA) не используется для развертывания обновлений, но позволяет системным администраторам сканировать сеть, чтобы определить, на каких компьютерах обновления отсутствуют или неправильно настроены. MBSA можно использовать совместно с WSUS, чтобы проверять на целевых компьютерах наличие не всех обновлений из каталога, а только одобренных.

### System Center Essentials 2010

System Center Essentials 2010 — следующий уровень управления обновлениями в среде Windows Server 2008 R2 после WSUS 3.0 SP2. Этот инструмент позволяет управлять большим числом серверов (до 50) и создавать гораздо более подробные отчеты, чем WSUS. System Center Essentials 2010 позволяет развертывать обновления для продуктов сторонних производителей и предоставляет широкие возможности по управлению распространением обновлений и составлению гибкого расписания. Доступны базовые средства проверки соответствия условиям и управления ресурсами. Имеется встроенная технология работы с виртуальными машинами (Virtual Machine Manager 2008 R2), позволяющая управлять не только физическими, но и виртуальными серверами. Сюда

входит поддержка преобразования физических серверов в виртуальные машины и поддержка миграции без прекращения работы. System Center Essentials 2010 требует доступа к SQL Server 2008 Standard или Enterprise с первым пакетом обновлений.

---

**ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ System Center Essentials 2010**

Подробнее о System Center Essentials 2010 см. на странице продукта: <http://www.microsoft.com/ru-ru/server-cloud/system-center/essentials.aspx>. Подробнее об обновлении до System Center Essentials 2010 см. по адресу <http://technet.microsoft.com/ru-ru/library/cc339466.aspx>.

---

**System Center 2012 Configuration Manager**

System Center 2012 Configuration Manager — новейшая версия из линейки продуктов по управлению серверами. Этот продукт предоставляет более широкие возможности, чем System Center Essentials и может использоваться для мониторинга почти всех аспектов сетевого окружения. System Center 2012 Configuration Manager позволяет создавать подробные отчеты о соответствии и предназначен для очень крупных сетей, превышающих возможности System Center Essentials 2010 (50 серверов, см. выше).

---

**ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ System Center 2012 Configuration Manager**

Подробнее о System Center 2012 Configuration Manager см. по адресу <http://www.microsoft.com/ru-ru/server-cloud/system-center/configuration-manager-2012.aspx>.

---

**Резюме**

- Службы WSUS позволяют одному серверу получать обновления от службы обновлений Microsoft через Интернет и доставлять их клиентам в сети. При этом клиентам WSUS не требуется доступ к службе обновлений Microsoft и подключение к Интернету.
- Реплики WSUS — подчиненные серверы, наследующие конфигурацию вышестоящего сервера. Подчиненные серверы WSUS, работающие в автономном режиме, тоже получают обновления от вышестоящего сервера, но одобрения на них может настраивать локальный администратор.
- При указании на стороне сервера компьютеры включаются в группы WSUS через консоль администрирования WSUS. При указании на стороне клиента клиенты включаются в группы WSUS через групповую политику или посредством изменения параметров реестра на клиенте. Поэтапное развертывание обновлений позволяет проверить, не возникнут ли на клиентах конфликты при установке определенного обновления.
- System Center Essentials 2010 предоставляет более широкие возможности, чем WSUS, и требует доступа к базе данных под управлением SQL Server 2008 Standard или Enterprise с первым пакетом обновлений.
- System Center 2012 Configuration Manager предоставляет расширенные возможности по работе с отчетами, позволяющие проверять соответствие компьютеров предъявляемым требованиям.

## Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных на занятии 2. Эти вопросы предоставлены также в электронном виде на прилагаемом к книге компакт-диске.

---

### ПРИМЕЧАНИЕ Ответы

Ответы на вопросы и пояснения к их вариантам размещены в разделе «Ответы» в конце книги.

---

1. Ваша организация имеет 30 филиалов по всей Европе. 30% сотрудников организации используют ноутбуки с Windows 7. После изучения некоторых отчетов о соответствии вы обнаружили, что эти ноутбуки обновляются, только когда подключаются к сети филиала, в котором были первоначально развернуты. Что следует сделать, чтобы эти компьютеры всегда получали обновления от локального сервера WSUS, независимо от того, в каком филиале подключаются к сети? (Каждый вариант является частью решения; выберите два.)
  - a. На каждом сервере WSUS настроить балансировку нагрузки сети (NLB).
  - b. На каждом DNS-сервере организации настроить циклическое обслуживание с расстановкой по адресу.
  - c. Настроить для всех серверов WSUS одинаковые полные доменные имена.
  - d. Для каждого DNS-сервера организации настроить дополнительные серверы BIND.
  - e. На каждом клиенте настроить файл хостов, указав имя хоста и IP-адрес каждого сервера WSUS.
2. Вы планируете развертывание WSUS в университете с пятью факультетами, каждый из которых имеет собственный ИТ-персонал. Вы хотите минимизировать объем данных, загружаемых с серверов службы обновлений Microsoft, но персонал каждого факультета должен иметь возможность одобрять обновления. Какой из вариантов развертывания WSUS вы выберете?
  - a. Настроить один вышестоящий сервер. Настроить пять подчиненных серверов в режиме реплики.
  - b. Настроить пять серверов, работающих в режиме реплики.
  - c. Настроить один вышестоящий сервер. Настроить пять подчиненных серверов, работающих в автономном режиме.
  - d. Настроить пять автономных серверов.
3. Вы хотите выполнять развертывание обновлений с сервера WSUS 3.0 SP2 поэтапно, отдельно для каждого департамента организации. Учетные записи компьютеров каждого департамента находятся в соответствующих подразделениях. Что следует выполнить? (Каждый ответ составляет часть решения; выберите два.)
  - a. Создать группы компьютеров WSUS для каждого департамента.
  - b. Создать несколько GPO и связать их с доменом. В каждом GPO указать имя группы компьютеров WSUS, созданной для соответствующего департамента.

- c. Создать несколько GPO и связать их с подразделениями. В каждом GPO указать имя группы компьютеров WSUS, созданной для соответствующего департамента.
  - d. Создать отдельные группы безопасности для всех учетных записей компьютеров в каждом подразделении департамента.
  - e. Создать отдельные группы безопасности для всех учетных записей пользователей в каждом подразделении департамента.
4. Что следует сделать, чтобы все важные обновления и обновления безопасности развертывались на компьютерах из группы компьютеров PatchTest?
- a. Создать запланированную задачу.
  - b. Создать правило автоматического одобрения, указав в качестве целевой группы **Все компьютеры**.
  - c. Создать правило автоматического одобрения, указав в качестве целевой группы компьютеров WSUS **PatchTest**.
  - d. Создать правило автоматического одобрения, указав в качестве целевой группы безопасности **PatchTest**.
5. Вам требуется список компьютеров, на которые не установлено последнее обновление, чтобы отправить туда специалиста техподдержки. Какой отчет следует создать, чтобы быстро получить эту информацию?
- a. Сводный отчет о состоянии обновлений.
  - b. Сводный отчет о состоянии компьютеров.
  - c. Детальный отчет о состоянии обновлений.
  - d. Детальный отчет о состоянии компьютеров.

## Практикум. Мониторинг создания учетных записей неопытным администратором

Ким Акерс — старший администратор корпорации Adatum. Дон Холл недавно повышен до администратора домена, и Ким должен предоставить ему соответствующие права. Однако Ким хочет проверить, какие учетные записи пользователей и группы безопасности будет создавать Дон. На этом практикуме вы настроите аудит для записи сведений о создании пользователей и групп безопасности, повысите учетную запись Дона до администратора домена и проверите, как он использует свои права.

### Упражнение 1. Настройка аудита создания пользователей и групп безопасности и повышение пользователя до администратора домена

В этом упражнении вы настроите аудит создания пользователей и групп, прежде чем добавить пользователя Don Hall в группу администраторов домена. Всегда рекомендуется настраивать аудит безопасности перед внесением изменений, способных повлиять на безопасность организации.

1. Зайдите на контроллер домена VAN-DC1 под учетной записью Kim Akers.

- Из меню **Пуск | Администрирование** (Start | Administrative Tools) откройте оснастку **Управление групповой политикой** (Group Policy Management).
- Если требуется, раскройте лес Adatum.com, раскройте узел **Домены** (Domains) и узел Adatum.com.
- Раскройте узел **Контроллеры домена** (Domain Controllers).
- Правой кнопкой щелкните **Политика контроллеров домена по умолчанию** (Default Domain Controller Policy) и выберите команду **Изменить** (Edit). Откроется редактор управления групповой политики.
- Раскройте узел **Конфигурация компьютера | Политики | Конфигурация Windows | Параметры безопасности | Конфигурация расширенной политики аудита | Политики аудита системы** (Computer Configuration | Policies | Windows Settings | Security Settings | Advanced Audit Policy Configuration | Audit Policies) и выберите **Управление учетными записями** (Account Management) (рис. 8-18).

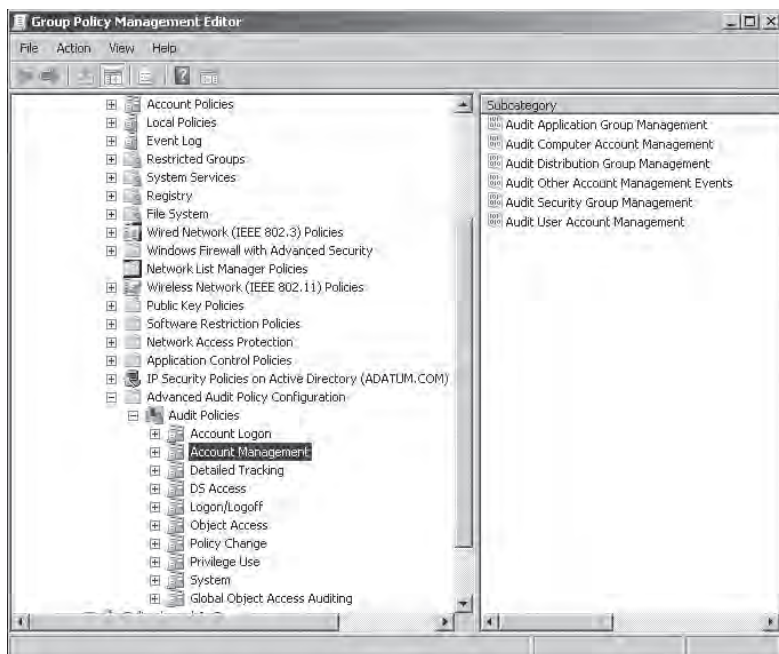


Рис. 8-18. Настройка управления учетными записями

- На панели результатов дважды щелкните **Аудит управления учетными записями пользователей** (Audit User Account Management).
- В диалоговом окне свойств аудита управления учетными записями установите флажки **Настроить следующие события аудита** (Configure the following audit events) и **Успех** (Success), как показано на рис. 8-19, и щелкните **ОК**.
- В редакторе управления групповой политикой на панели результатов дважды щелкните **Аудит управления группами безопасности** (Audit Security Group Management).

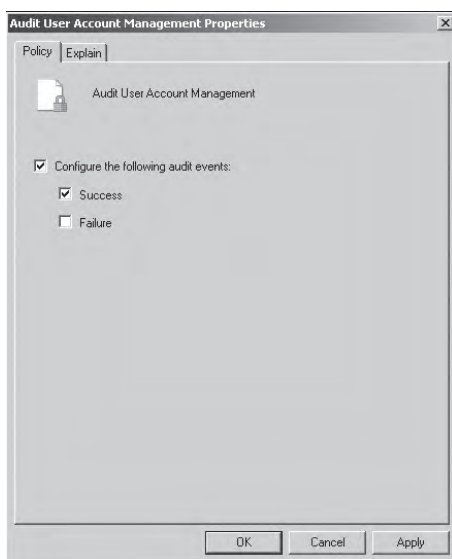


Рис. 8-19. Настройка аудита успехов

10. В открывшемся диалоговом окне установите флажок **Настроить следующие события аудита** (Configure the following audit events), установите флажок **Успех** (Success) и щелкните **ОК**.
11. Закройте редактор управления групповой политикой. Из меню **Администрирование** откройте оснастку **Active Directory — пользователи и компьютеры** (Active Directory Users And Computers).
12. Раскройте узел домена Adatum.com. Дважды щелкните **Пользователи** (Users). На панели результатов дважды щелкните **Администраторы домена** (Domain Admins). Щелкните **Добавить** (Add).
13. В открывшемся диалоговом окне ведите «Don Hall» в поле **Введите имена выбираемых объектов** (Enter the object names to select) (рис. 8-20). Щелкните **ОК**. Еще раз щелкните **ОК**, чтобы закрыть диалоговое окно свойств группы администраторов домена. Закройте оснастку **Active Directory — пользователи и компьютеры**.

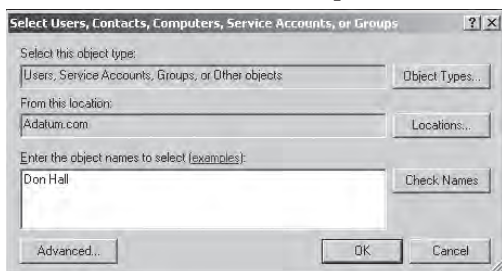


Рис. 8-20. Добавление пользователя Don Hall в группу администраторов домена

14. Откройте командную строку с повышенными привилегиями. Введите `groupdate /force` и нажмите Enter. Закройте командную строку.
15. Выйдите из системы на контроллере домена VAN-DC1.



## Упражнение 2. Вход под учетной записью Don Hall для создания пользователя и группы безопасности

В этом упражнении вы войдете в систему как новый администратор Don Hall, создадите группу безопасности и пользователя и добавите этого пользователя в группу безопасности.

1. Зайдите на контроллер домена VAN-DC1 под учетной записью Don Hall.
2. Откройте оснастку **Active Directory — пользователи и компьютеры**.
3. Раскройте узел домена Adatum.com, правой кнопкой щелкните **Пользователи (Users)** и выберите команду **Создать | Группа (Create | Group)**.
4. В открывшемся диалоговом окне введите имя группы «DonGroup». Оставьте параметры по умолчанию (рис. 8-21), чтобы создать глобальную группу безопасности, и щелкните **ОК**.
5. В оснастке **Active Directory — пользователи и компьютеры** щелкните правой кнопкой мыши узел **Пользователи (Users)** и выберите команду **Создать | Пользователь (Create | User)**.
6. Введите имя Jim Hance (рис. 8-22). Если такой пользователь уже существует, введите любое другое имя. Щелкните **Далее**.

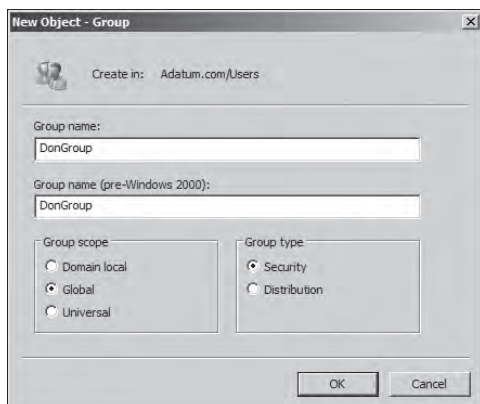


Рис. 8-21. Создание глобальной группы безопасности DonGroup

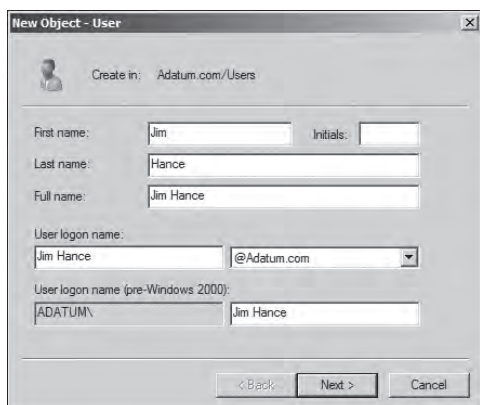


Рис. 8-22. Создание пользователя с именем Jim Hance

7. Снимите флажок **Требовать смены пароля при следующем входе в систему** (User Must Change Password At Next Logon). Установите флажок **Срок действия пароля не ограничен** (Password Never Expires). В полях **Пароль** (Password) и **Подтверждение** (Confirm Password) введите пароль **Pa\$\$w0rd**. Щелкните **Далее**.
8. Щелкните **Готово**.
9. В оснастке **Active Directory — пользователи и компьютеры** дважды щелкните **Пользователи** (Users). На панели результатов дважды щелкните **Jim Hance**.
10. Щелкните на ярлыке вкладки **Член групп** (Member of). Щелкните **Добавить** (Add).
11. В диалоговом окне выбора групп в поле **Введите имена выбираемых объектов** (Enter the object names to select) введите «DonGroup», как показано на рис. 8-23, и щелкните **ОК**.
12. Щелкните **ОК**, чтобы закрыть диалоговое окно свойств учетной записи. Закройте оснастку **Active Directory — пользователи и компьютеры**.

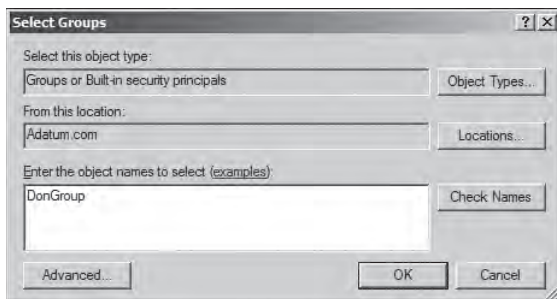


**Рис. 8-23.** Добавление пользователя Jim Hance в группу безопасности DonGroup

13. Откройте командную строку с повышенными привилегиями. Введите `groupdate /force` и нажмите Enter. Закройте командную строку.
14. Выйдите из системы на контроллере домена VAN-DC1.

### Упражнение 3. Аудит создания пользователей и групп

В этом упражнении вы войдете в систему под учетной записью Kim Akers и выполните аудит действий пользователя Don Hall.

1. Зайдите на контроллер домена VAN-DC1 под учетной записью Kim Akers.
2. В меню **Администрирование** выберите **Просмотр событий** (Event Viewer).
3. Раскройте **Журналы Windows** (Windows Logs) и дважды щелкните **Безопасность** (Security).
4. Дважды щелкните последнее событие с кодом 4720.
5. Убедитесь, что в журнал записана информация о создании пользователем Don Hall учетной записи Jim Hance (рис. 8-24).

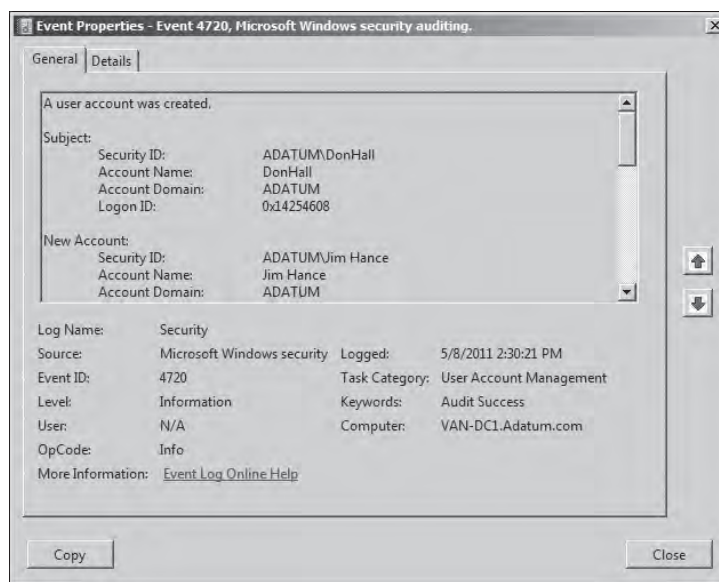


Рис. 8-24. Аудит создания учетной записи пользователем Don Hall

6. Дважды щелкните последнее событие с кодом 4728.
7. Убедитесь, что в журнал записана информация о добавлении пользователем Don Hall пользователя Jim Hance в группу безопасности DonGroup (рис. 8-25).

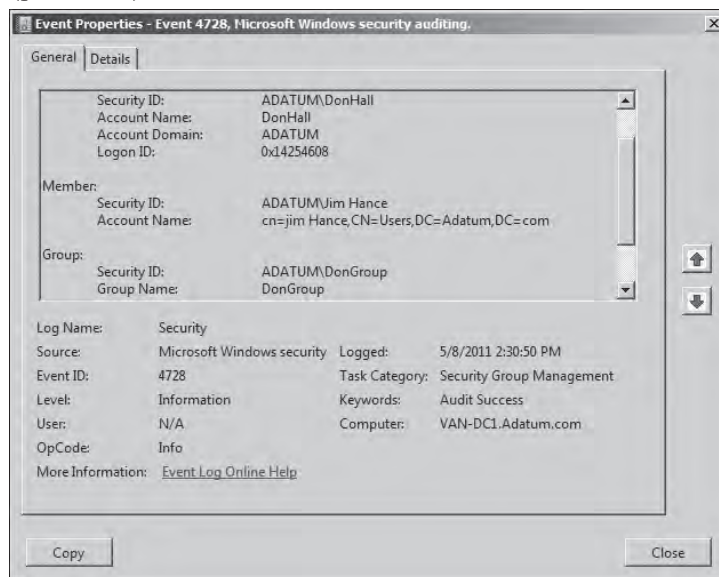


Рис. 8-25. Аудит добавления пользователя Jim Hance в группу DonGroup

8. Откройте оснастку **Active Directory — пользователи и компьютеры** и удалите пользователя Don Hall из группы администраторов домена.

## Практикум. Установка WSUS 3.0 SP2 (необязательный)

На этом практикуме вы установите WSUS 3.0 SP2 на компьютер под управлением Windows Server 2008 R2 и выполните настройку для получения обновлений с серверов Microsoft. Это необязательный практикум, так как для его выполнения требуется доступ к Интернету. Чтобы предоставить контролеру домена VAN-DC1 доступ к Интернету, можно установить вторую сетевую карту, использовать беспроводное подключение или (при использовании виртуальных машин) добавить виртуальную сетевую карту и соответствующим образом настроить параметры сети виртуальных машин. В этом практикуме предполагается, что вы не устанавливали IIS на сервер VAN-DC1. Если службы IIS установлены, используйте функцию добавления служб ролей, чтобы добавить дополнительные компоненты, перечисленные на шаге 7, и не выполняйте шаги 5 и 6.

Если не хотите подключать свою тестовую сеть к Интернету, можете загрузить установочные файлы Report Viewer и WSUS 3.0 SP2 на другой компьютер, имеющий выход в Интернет, и перенесите эти файлы на VAN-DC1 на USB-накопителе или компакт-диске. После этого установите на VAN-DC1 Report Viewer, роль сервера IIS и WSUS. Однако в этом случае вы не сможете запустить мастер настройки служб обновления, и упражнение придется прервать на шаге 15. Поскольку установка WSUS 3.0 SP2 как службы роли требует подключения к Интернету, в этом практикуме этот способ не используется; вместо этого установка WSUS выполняется из загруженных установочных файлов.

---

### ПРИМЕЧАНИЕ Расположение загрузок

Для прохождения этого практикума следует установить дистрибутивный пакет Report Viewer 2008, а не Report Viewer 2010. Установочный файл дистрибутивного пакета Report Viewer 2008 можно загрузить по адресу <http://www.microsoft.com/downloads/en/details.aspx?FamilyID=cc96c246-61e5-4d9e-bb5f-416d75a1b9ef>. Установочный файл WSUS 3.0 SP2 можно загрузить по адресу <http://www.microsoft.com/downloads/en/details.aspx?FamilyId=a206ae20-2695-436c-9578-3403a7d46e40&displaylang=en>. Чтобы не вводить эти адреса вручную, можете зайти на страницу центра загрузок (<http://www.microsoft.com/ru-ru/download/default.aspx>) и выполнить поиск продуктов.

---

## Упражнение. Установка WSUS 3.0 SP2

В этом упражнении вы установите Report Viewer, добавите роль IIS (если требуется), добавьте дополнительные компоненты для IIS, а затем установите WSUS.

1. Зайдите на контроллер домена под учетной записью Kim Akers.
2. Загрузите установочные файлы Report Viewer 2008 и WSUS 3.0 SP2 (64-разрядную версию) в папку C:\Temp. Эта папка уже должна существовать; если нет, создайте ее.
3. Запустите установочный файл Report Viewer 2008 (ReportViewer.exe) и щелкните **Выполнить** (Run), чтобы начать установку на сервер VAN-DC1. Если появится окно службы контроля учетных записей, щелкните **Да**.

4. Щелкните **Далее**. Примите условия лицензионного соглашения и щелкните **Установить** (Install). Когда процесс установки завершится, щелкните **Готово** (Finish).
5. Откройте Диспетчер сервера из меню **Администрирование**. Если появится окно службы контроля учетных записей, щелкните **Да**. В Диспетчере сервера раскройте узел **Роли** (Roles). Если роль веб-сервера (IIS) уже добавлена, щелкните **Добавить службы ролей** (Add Role Services) и перейдите к шагу 7. В противном случае правой кнопкой щелкните **Роли** (Roles) и выберите команду **Добавить роли** (Add Roles).
6. Выберите роль **Веб-сервер (IIS)** [Web Server (IIS)], как показано на рис. 8-26. Щелкните **Далее**. Прочитайте предложенную информацию и щелкните **Далее**, чтобы перейти на страницу выбора служб ролей.

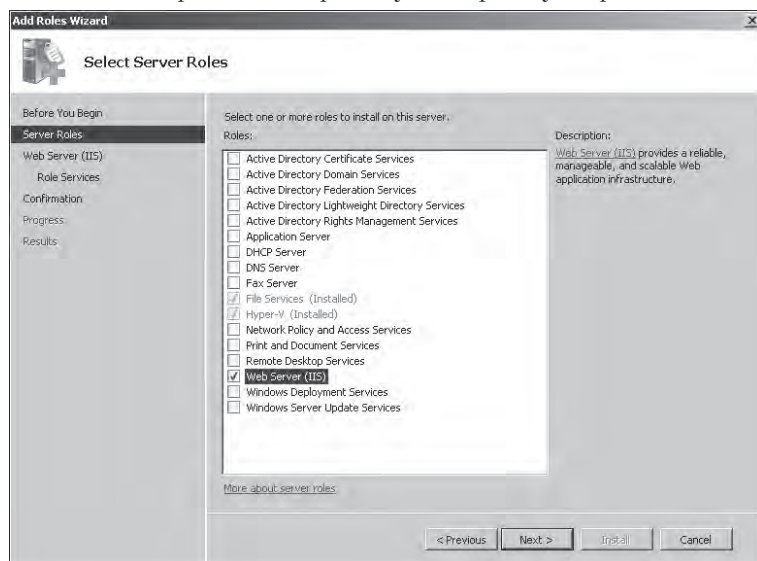


Рис. 8-26. Выбор роли веб-сервера (IIS)

7. На странице **Выбор служб ролей** (Select Role Services) выберите ASP.NET. Откроется диалоговое окно с запросом на добавление дополнительных служб ролей (рис. 8-27). Щелкните **Добавить требуемые службы ролей** (Add Required Role Services).

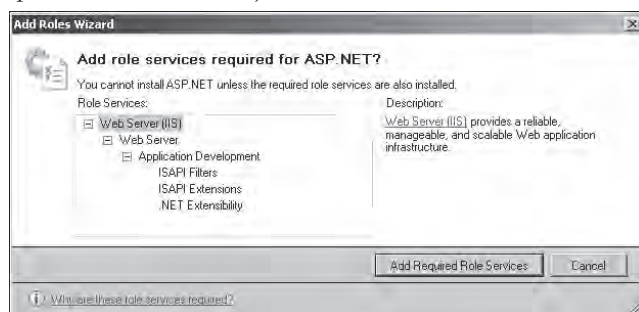


Рис. 8-27. Запрос на добавление требуемых служб ролей

8. На странице **Выбор служб ролей** (Select Role Services) под узлом **Безопасность** (Security) выберите **Windows – проверка подлинности** (Windows Authentication). Под узлом **Средства управления** (Management Tools) выберите **Совместимость метабазы IIS 6** (IIS 6 Metabase Compatibility) (рис. 8-28). Щелкните **Далее**.

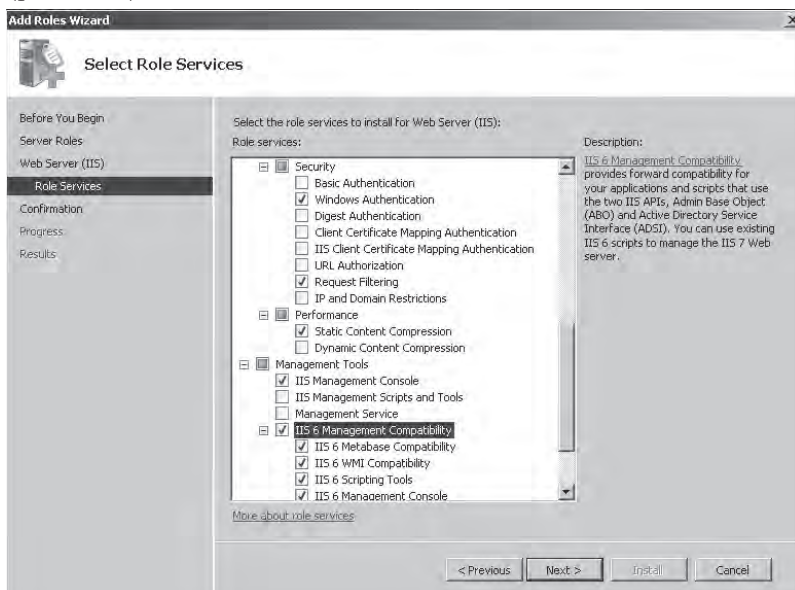


Рис. 8-28. Выбор параметров безопасности и средств управления

9. Убедитесь, что список на странице подтверждения соответствует списку на рис. 8-29, и щелкните **Установить**.

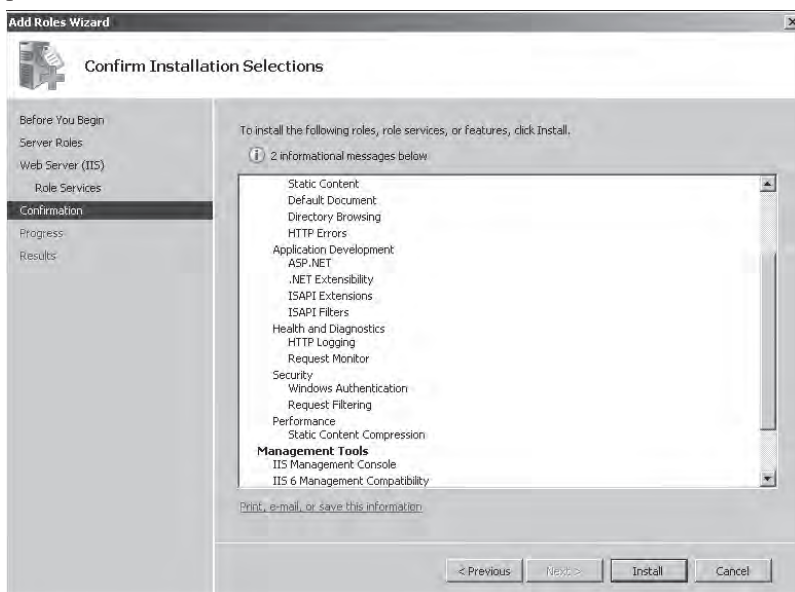


Рис. 8-29. Подготовка IIS для установки WSUS



10. Когда установка завершится, щелкните **Заккрыть**.
11. Из папки C:\Temp откройте установочный файл WSUS (во время написания книги это файл WSUS30-KZB972455-x64.exe). Если появится окно службы контроля учетных записей, щелкните **Да**, а затем **Выполнить** (Run).
12. Запустится мастер установки WSUS 3.0 SP2 (Рис. 8-30). Щелкните **Далее**.



Рис. 8-30. Мастер установки WSUS 3.0 SP2

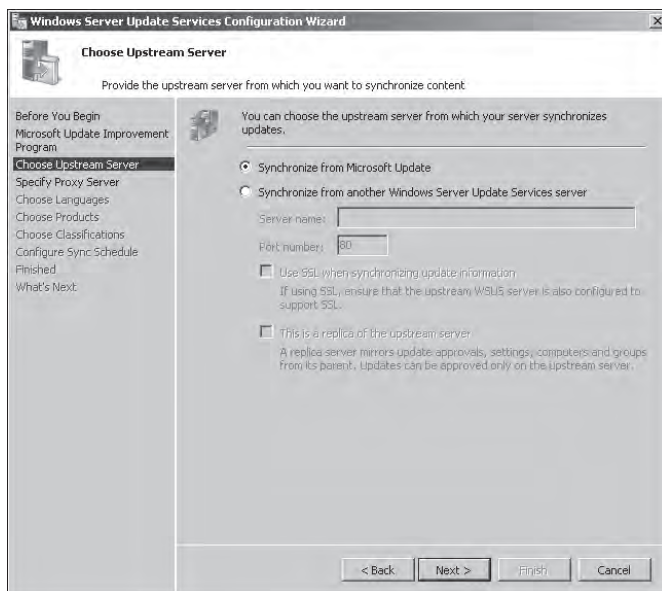


Рис. 8-31. Синхронизация с центром обновлений Microsoft

13. Установите переключатель **Полная установка сервера, включая консоль администрирования** (Full Server Installation Including Administration Console) и щелкните **Далее**.
14. Примите условия лицензионного соглашения и щелкните **Далее**. Если появится окно службы контроля учетных записей, щелкните **Да**. Когда установка завершится, щелкните **Готово**.



15. Когда установка WSUS 3.0 SP2 завершится, автоматически запустится мастер настройки Windows Server Update Services.  
Если у вас нет подключения к Интернету, щелкните **Отмена**, чтобы завершить упражнение. Если подключение есть, щелкните **Далее** два раза.
16. На странице **Выбор вышестоящего сервера** (Choose Upstream Server) установите переключатель **Синхронизировать с Центром обновления Майкрософт** (Synchronize From Microsoft Update) (рис. 8-31) и щелкните **Далее**.
17. На странице **Настройка прокси-сервера** (Specify Proxy Server) щелкните **Далее**.
18. На странице **Подключение к вышестоящему серверу** (Connect To Upstream Server) щелкните **Начать подключение** (Start Connecting). Сервер подключится к центру обновлений Microsoft, чтобы определить тип доступных обновлений, продуктов, обновление которых возможно, и доступных языков. Когда процедура подключения завершится, щелкните **Далее**.
19. На странице выбора продуктов (рис. 8-32) установите флажок **Все продукты** (All Products) и щелкните **Далее**.

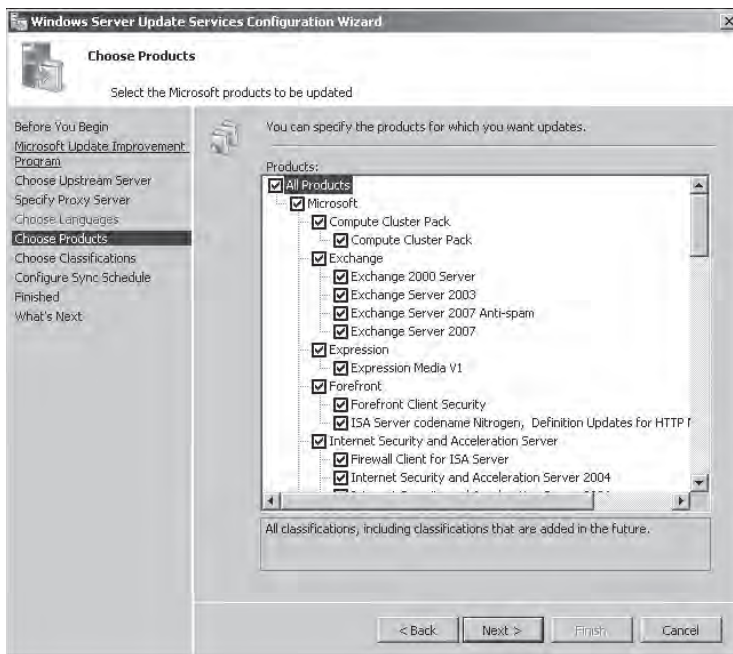


**Рис. 8-32.** Выбор продуктов, которые будут обновляться при помощи WSUS

20. На странице **Выбор классов** (Choose Classifications) выберите **Все классы** (All Classifications) и щелкните **Далее** (Next).
21. На странице **Настройка расписания синхронизации** (Set Sync Schedule) выберите **Синхронизация вручную** (Synchronize Manually) и щелкните **Далее**.
22. Убедитесь, что флажки **Запустить консоль администрирования Windows Server Update Services** (Launch The Windows Server Update Services Admin-

istration Console) и **Запустить первоначальную синхронизацию** (Begin Initial Synchronization) не установлены, и щелкните **Готово**.

23. Так как упражнения всех остальных практикумов выполняются в изолированной сети, настоятельно рекомендуем отключить VAN-DC1 от Интернета, когда закончите экспериментировать с WSUS.

## Закрепление материала главы

Чтобы попрактиковаться и закрепить знания, полученные при изучении этой главы, выполните следующее:

- прочитайте резюме главы;
- просмотрите список основных терминов, представленных в этой главе;
- выполните задания лабораторной работы, моделирующей реальные ситуации, требующие применения полученных знаний;
- выполните рекомендуемые упражнения;
- пройдите пробный тест.

## Резюме главы

- Политики аудита безопасности позволяют обнаружить угрозы для безопасности, представляемые злонамеренными или небрежными внутренними пользователями и неправильными действиями неопытных администраторов.
- Сервер WSUS можно использовать для централизованного развертывания обновлений в среде Windows Server 2008 R2.
- System Center 2012 Configuration Manager предоставляет расширенные возможности по созданию отчетов, позволяющих проверять компьютеры на соответствие предъявляемым условиям.

## Основные термины

Проверьте, знаете ли вы, что означают перечисленные ниже термины из этой главы:

- автономный режим;
- подчиненный сервер;
- шифрованная файловая система (EFS);
- режим реплики.

## Лабораторная работа

Для выполнения заданий лабораторной работы используйте знания о планировании политики безопасности, полученные из этой главы. Ответы можно найти в разделе «Ответы» в конце книги.

## **Задание 1. Реализация плана по обеспечению безопасности сети корпорации Adatum**

Вы главный администратор в корпорации Adatum. Корпорация имеет веб-сайты, некоторые из них контролируются правительственными организациями. Ваша задача — оценить безопасность сети и серверов, после чего составить план по ее повышению. Ответьте на следующие вопросы.

1. Ваш план включает выявление и устранение нарушений политики, таких как создание пользователей вне установленной процедуры, несанкционированные попытки доступа к файлам и запуск неодобренных программ. Мониторинг каких элементов следует выполнять для этого и какие инструменты для этого использовать?
2. Вы планируете использовать криминалистический анализ для получения информации о попытках доступа к сети корпорации Adatum и получения конфиденциальной информации. Некоторые защищенные данные, хранящиеся в сети корпорации, имеют отношение к национальной безопасности. Как долго должны храниться криминалистические данные об атаках и попытках доступа к этой информации?
3. Все серверы сети корпорации Adatum работают под управлением Windows Server 2008 R2. Внутренняя сеть состоит из одного домена, в который входят контроллеры домена, файловые серверы, серверы печати и серверы баз данных. Периферийная сеть включает серверы Exchange Server 2010 и веб-серверы. Вы обеспечиваете защиту от DoS-атак. Какие серверы наиболее подвержены таким атакам, а значит, требуют повышенного внимания при обеспечении безопасности?

## **Задание 2. Развертывание WSUS 3.0 SP2 в компании Fabrikam**

В компании Fabrikam несколько лет используются специализированные решения по управлению обновлениями. Технический директор решил обновить все серверы, работающие под управлением Windows 2000, до Windows Server 2008 R2. Также планируется развертывание WSUS 3.0 SP2. Компания Fabrikam расположена в штате Виктория, Австралия. Главный офис расположен в Мельбурне, и есть четыре дополнительных офиса в пригороде.

Текущий план заключается в установке сервера WSUS 3.0 SP2 на компьютере под управлением Windows Server 2008 R2 в главном офисе, после чего будут поэтапно развертываться серверы WSUS в остальных офисах. Весь ИТ-персонал работает в Мельбурне, поэтому серверы в дополнительных офисах должны использовать одобрения и группы компьютеров, настроенные в главном офисе.

Одна из причин для использования специализированного решения заключается в том, что Fabrikam использует собственное ПО, которое иногда конфликтует с обновлениями и мешает их установке. Технический директор хочет иметь возможность создавать отчеты об обновлениях со своего компьютера. Техническому директору не требуется административный доступ к серверу, и он никогда не выполняет административные задачи самостоятельно, всегда делегируя их системным администраторам.

Учитывая все это, ответьте на следующие вопросы:

1. В какие локальные группы на сервере WSUS, работающем под управлением Windows Server 2008 R2, следует включить учетную запись технического директора?
2. Как следует настроить источник обновлений подчиненных серверов WSUS в дополнительных офисах компании?
3. Отчеты какого типа должен создавать технический директор, чтобы получить подробную информацию о компьютерах, на которых не удалось установить определенные обновления?

## Рекомендуемые упражнения

Чтобы успешно справиться с экзаменационными заданиями по темам этой главы, выполните следующие упражнения.

### Мониторинг безопасности сервера

- Настройте аудит успехов и отказов использования привилегий.
- Настройте аудит событий входа учетной записи и убедитесь, что эти события записываются на сервере VAN-DC1.

### Реализация стратегии управления обновлениями

- Установите WSUS 3.0 SP2 на втором компьютере под управлением Windows Server 2008 R2. Если вы настраивали рядовой сервер VAN-SRV1 в предыдущих главах, можете использовать его.
- Настройте второй компьютер под управлением Windows Server 2008 R2 как подчиненный сервер, являющийся репликой сервера WSUS 3.0 SP2, настроенного на практикуме этой главы (VAN-DC1).
- Синхронизируйте подчиненный сервер WSUS с вышестоящим сервером.

## Пробный экзамен

Тренировочные тесты на прилагаемом к книге компакт-диске позволяют проверить знания только по одной или сразу по всем темам сертификационного экзамена 70-646. Тестирование можно организовать так, чтобы оно проводилось как настоящий экзамен, а можно проходить в режиме обучения, просматривая правильные ответы и объяснения после каждого ответа.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Пробный экзамен

Подробнее о пробном экзамене рассказано во Введении.

---

## Удаленный доступ и защита доступа к сети

|                                                       |            |
|-------------------------------------------------------|------------|
| <b>Занятие 1. Управление удаленным доступом</b>       | <b>416</b> |
| <b>Занятие 2. Брандмауэры и защита доступа к сети</b> | <b>437</b> |

Чтобы разрешить удаленным пользователям подключаться к ресурсам внутренней сети вашей организации из любой точки мира, будь то точка беспроводного доступа в курортном отеле или ADSL-подключение в столице, можно использовать виртуальные частные сети (VPN). Планируя предоставление доступа по VPN, следует принимать во внимание ряд факторов. Необходимо знать, как будет настроен внешний брандмауэр организации, какую операционную систему будет использовать клиент, и к каким типам ресурсов необходим доступ удаленным пользователям.

Защита доступа к сети (NAP) позволяет ограничивать доступ к сети в зависимости от состояния работоспособности клиента. Проще говоря, NAP позволяет установить правило, согласно которому можно ограничивать доступ к сети, если клиент не имеет последних обновлений и антивирусных баз. В этой главе рассказывается о настройке и развертывании NAP и о различных способах работы с несовместимыми компьютерами. Также вы узнаете, как планировать и развертывать службы удаленного доступа Windows Server 2008 R2, чтобы клиенты могли подключаться к внутренним ресурсам организации независимо от того, в какой точке мира они находятся.

### Темы экзамена

- Планирование ролей сервера для служб инфраструктуры.
- Мониторинг и поддержка безопасности и политик.

### Прежде всего

Для выполнения упражнений этой главы потребуется:

- выполнить задания по установке, приведенные в Приложении. Дополнительной настройки не требуется.

**Реальный мир***Орин Томас*

В традиционных моделях сетей и брандмауэров все угрозы находятся снаружи, а все безопасное — внутри. Однако в наши дни внутренняя сеть порой бывает не менее враждебной средой, чем Интернет. Раньше все компьютеры в сети были стационарными, и мало кто брал домой свою рабочую станцию. Сегодня большинство продаваемых компьютеров — это ноутбуки, и все больше людей, уходя из офиса, берет домой свои рабочие компьютеры. К сожалению, когда компьютеры покидают безопасную внутреннюю сеть, с ними может произойти все что угодно. Через домашнее ADSL-подключение можно случайно скачать вредоносную программу, которая в корпоративной сети была бы заблокирована внешним брандмауэром. Компьютеры, которые находились в полной безопасности под контролем администраторов, теперь ежедневно подвергаются всевозможным угрозам из Интернета. Хуже всего то, что эти компьютеры на следующий день возвращаются в сеть организации. Брандмауэр Windows, NAP и другие технологии в какой-то мере помогают защитить внутреннюю сеть от того, что могли принести пользователи на своих компьютерах. Тем не менее, планируя стратегию обеспечения безопасности, не надейтесь на то, что узлы с локальным IP-адресом безопаснее, чем узлы с IP-адресом в Интернете до тех пор, пока они не пройдут проверку, например, с помощью NAP, и вы не убедитесь в их безопасности.

## Занятие 1. Управление удаленным доступом

Если организация планирует разрешить работникам работать удаленно, администратор должен каким-то образом предоставить им доступ к ресурсам внутренней сети организации. На этом занятии вы узнаете, как планировать развертывание VPN-серверов для предоставления доступа извне к внутренней сети организации. Затем мы расскажем о DirectAccess, технологии, доступной в Windows 7 и Windows Server 2008 R2, которая существенно упрощает процедуру удаленного доступа с точки зрения пользователя. Также мы обсудим традиционные протоколы удаленного доступа, включая протокол туннелирования «точка-точка» (PPTP), протокол туннелирования L2TP/IPsec, протокол безопасного туннелирования сокетов (Secure Socket Tunneling Protocol, SSTP), и технологию IKEv2, появившуюся в Windows Server 2008 R2.

---

**Изучив материал этого занятия, вы сможете:**

- ✓ Планировать роли сервера инфраструктуры удаленного доступа.
- ✓ Осуществлять мониторинг и поддержку политик безопасности удаленного доступа.
- ✓ Применять технологии удаленного доступа, в том числе VPN IKEv2 и DirectAccess.

---

**Продолжительность занятия — примерно 60 мин.**

---

Служба маршрутизации и удаленного доступа (Routing and Remote Access Service, RRAS) является частью роли сервера **Службы политики сети и доступа** (Network Policy And Access Services). Компонент **Служба удаленного доступа** (Remote Access Service, RAS) службы роли RRAS необходим для использования в сети следующих ресурсов:

- VPN-сервер удаленного доступа;
- сервер удаленного доступа через коммутируемые соединения.

На этом занятии вы узнаете, как выполнять настройку и мониторинг VPN-сервера удаленного доступа под управлением Windows Server 2008 и Windows Server 2008 R2. Чтобы установить службу роли RRAS, запустите мастер добавления ролей и выберите Службы политики сети и доступа (Network Policy And Access Services). RRAS представляет собой службу роли, являющуюся частью этой роли. Можно также открыть оболочку Windows PowerShell с повышенными привилегиями на компьютере под управлением Windows Server 2008 R2 и выполнить следующие команды:

```
Import-Module ServerManager
```

```
Add-WindowsFeature NPAS-RRAS-Services
```

Чтобы полностью удалить RRAS с сервера под управлением Windows Server 2008 R2, выполните следующую команду:

```
Remove-WindowsFeature NPAS
```

---

#### **ПРИМЕЧАНИЕ** Предыдущие установки RPAS

Если ранее вы устанавливали и настраивали RRAS, может потребоваться сброс настроек, чтобы можно было выполнять другие функции. Для этого выполните следующие команды:

```
netsh ras set conf confstate=disabled and then net stop "Routing and Remote Access"
```

---

После установки RAS необходимо настроить вручную. Настраивать RAS могут только члены локальной группы **Администраторы**. В домене это следует выполнять, используя учетную запись пользователя, являющегося членом группы администраторов домена. Если ваша учетная запись пользователя не является членом группы безопасности **Администраторы домена**, попросите администратора домена, чтобы он вручную добавил учетную запись сервера RAS в доменную группу безопасности **Серверы RAS и IAS** (RAS And IAS Servers). Нет необходимости добавлять сервер RAS в эту группу, если он будет использовать локальную проверку подлинности или проверку подлинности на сервере RADIUS.

Чтобы включить удаленный доступ, откройте консоль **Маршрутизация и удаленный доступ** (Routing and Remote Access) из меню **Администрирование**, щелкните правой кнопкой мыши имя компьютера под управлением Windows Server 2008 R2, на котором хотите разместить эту роль, и выберите **Настроить и включить маршрутизацию и удаленный доступ** (Configure And Enable Routing And Remote Access). Запустится мастер настройки маршрутизации и удаленного доступа. Страница настройки, показанная на рис. 9-1, позволяет выбрать комбинацию служб, которые будет предоставлять сервер. Если требуется



предоставлять удаленный доступ клиентам, находящимся вне сети организации, установите переключатель **Удаленный доступ (VPN или модем)** [(Remote Access) (Dial-Up Or VPN)].

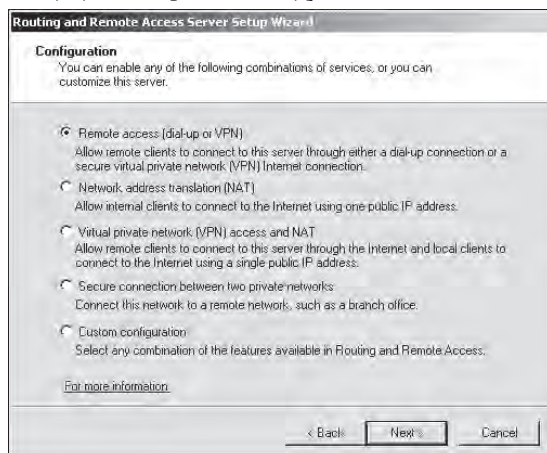


Рис. 9-1. Мастер настройки маршрутизации и удаленного доступа

Если выбрана установка VPN-сервера, на странице **VPN-подключение** (VPN Connection), (рис. 9-2) необходимо указать, какой сетевой интерфейс будет подключаться к Интернету. Это будет интерфейс с открытым, а не частным IP-адресом. Если после развертывания роли RAS на сервере будут установлены дополнительные сетевые адаптеры, их можно настроить для использования RAS с помощью консоли RRAS. Если компьютер под управлением Windows Server 2008 R2 имеет менее двух сетевых адаптеров, нельзя выполнить стандартную установку VPN-сервера, и необходимо использовать настраиваемую конфигурацию.

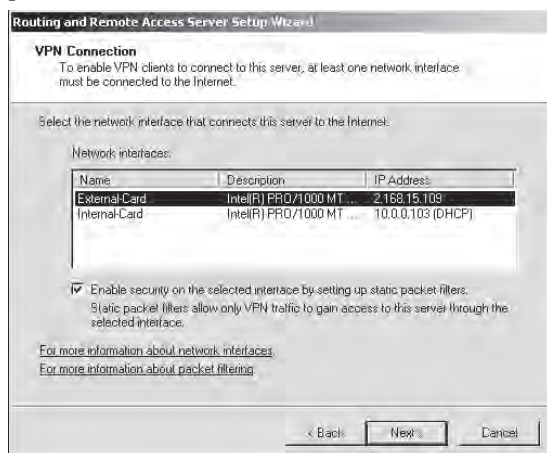


Рис. 9-2. Установка RAS

При настройке сервера удаленного доступа устанавливаются фильтры пакетов, разрешающие прохождение через подключенный к Интернету интерфейс только пакетов протоколов VPN. Это означает, что сервер может предоставлять

только VPN-доступ. Если на сервере, где будет установлена роль RAS, развернуты другие службы, потребуется настроить новые фильтры пакетов, чтобы пропускать соответствующий трафик. При планировании стратегии развертывания рекомендуется отделять сервер RAS от других служб.

После определения внешнего интерфейса следующим этапом настройки роли RAS будет определение способа назначения IP-адресов клиентам. Это можно делать несколькими способами:

- адреса клиентам может выдавать DHCP-сервер внутри организации;
- RAS-сервер может генерировать адреса самостоятельно;
- можно указать диапазон адресов для назначения подключающимся клиентам.

При использовании инфраструктуры DHCP RAS-сервер будет арендовать блоки из 10 адресов, запрашивая новые блоки, если все ранее запрошенные блоки уже используются.

DHCP-серверы под управлением Windows Server 2008 и 2008 R2 имеют предопределенный пользовательский класс — класс маршрутизации и удаленного доступа по умолчанию (Default Routing And Remote Access Class). Этот класс позволяет администраторам назначать определенные параметры только клиентам маршрутизации и удаленного доступа. Он настраивается на вкладке **Дополнительные** (Advanced) диалогового окна параметров DHCP-сервера (рис. 9-3).

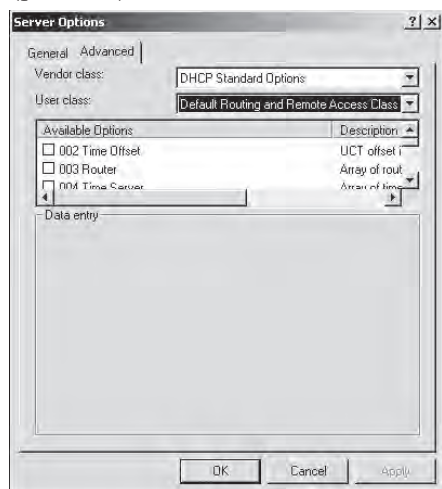


Рис. 9-3. Пользовательский класс службы RRAS

Следующий этап настройки RAS-сервера — определение способа проверки подлинности. Можно настроить RAS-сервер для прохождения проверки подлинности через доменные службы Active Directory (AD DS) или с использованием локальной базы данных учетных записей. Можно также настроить RAS-сервер как клиент RADIUS и разрешить серверу RADIUS выполнять проверку подлинности и авторизацию запросов подключений клиентов. Подробнее о параметрах RADIUS будет рассказано далее на этом занятии. После прохождения описанных этапов RAS-сервер готов к работе.

## Проверка подлинности VPN

VPN — расширение частной сети, позволяющее создавать инкапсулированные, зашифрованные и аутентифицированные каналы, проходящие через общедоступные сети. Клиент подключается к общедоступной сети, например, к Интернету, и инициирует VPN-подключение к удаленному серверу. Этот удаленный сервер обычно располагается в сети периметра организации, к которой клиент хочет подключиться. После установки соединения между клиентом и VPN-сервером создается зашифрованный туннель. Через этот зашифрованный туннель проходит трафик локальной сети между клиентом и удаленной сетью, к которой подключен клиент. Клиенты подключаются к сети так же, как если бы они находились в офисе. Вместо сетевого кабеля, подключающего их к коммутатору в офисе, для подключения к сети используется виртуальный кабель в виде VPN-туннеля.

Для проверки подлинности входящих VPN-подключений компьютер под управлением Windows Server 2008 или 2008 R2 может использовать следующие протоколы, которые перечислены в порядке от наиболее безопасных к наименее безопасным:

- **Протокол расширенной проверки подлинности безопасности транспортного уровня** (Extensible Authentication Protocol-Transport Level Security, EAP-TLS) — используется, когда клиенты VPN могут проходить проверку подлинности с помощью смарт-карт или цифровых сертификатов. EAP-TLS не поддерживается на изолированных серверах и может применяться, только если сервер, выполняющий роль RAS, является членом домена AD DS.
- **Протокол аутентификации по квитированию вызова Microsoft** (Microsoft Challenge Handshake Authentication Protocol, MS-CHAPv2) — обеспечивает взаимную аутентификацию и позволяет шифровать как данные аутентификации, так и данные подключения. Протокол MS-CHAPv2 включен по умолчанию в Windows Server 2008 и 2008 R2.
- **Протокол аутентификации по квитированию вызова** (Challenge Handshake Authentication Protocol, CHAP) — более старый протокол, шифрующий данные аутентификации с помощью хэширования MD5. Этот протокол не поддерживает шифрование данных и чаще всего используется для обеспечения совместимости с устаревшими сторонними клиентами.
- **Расширенный протокол аутентификации по квитированию вызова с помощью Message Digest 5** (Extensible Authentication Protocol-Message Digest 5 Challenge Handshake Authentication Protocol, EAP-MD5 CHAP) — версия CHAP, перенесенная на структуру EAP. Поддерживает шифрование данных аутентификации посредством хэширования MD5 и обычно используется для обеспечения совместимости со сторонними клиентами.
- **Протокол проверки пароля Shiva** (Shiva Password Authentication Protocol, SPAP) — протокол аутентификации со слабым шифрованием, не поддерживающий шифрование данных подключения.
- **Протокол проверки пароля** (Password Authentication Protocol, PAP) — данные аутентификации не шифруются, а передаются в виде простого текста. Шифрование данных не поддерживается.

Процедура проверки подлинности всегда пытается согласовать использование наиболее безопасного протокола. По умолчанию для проверки подлинности клиентов, подключающихся к VPN-серверам под управлением Windows Server 2008 и 2008 R2, используется протокол MS-CHAPv2

## Протоколы VPN

Windows Server 2008 R2 поддерживает четыре протокола VPN: PPTP, L2TP/IPsec, SSTP, и IKEv2. Выбор протокола зависит от операционной системы клиента, инфраструктуры сертификатов и способа развертывания брандмауэра в организации.

### PPTP

Проверку подлинности подключений PPTP можно выполнять только с помощью MS-CHAP, MS-CHAPv2, EAP и PEAP. PPTP-подключения для шифрования данных используют протокол MPPE. PPTP-подключения обеспечивают конфиденциальность данных, но не обеспечивают целостность данных и проверку источника данных. Можно использовать PPTP с сертификатами, если в качестве протокола проверки подлинности выбран EAP-TLS, однако преимущество PPTP над другими протоколами VPN, поддерживаемыми Windows Server 2008 и 2008 R2, заключается в том, что он не требует установки сертификатов на подключающемся клиенте. При использовании PPTP не нужно беспокоиться об общих секретах или сертификатах компьютера, равно как и о том, является ли центр сертификации (ЦС) доверенным. PPTP часто используется сторонними ОС.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ PPTP

Подробнее о настройке удаленного доступа на основе PPTP см. по адресу [http://technet.microsoft.com/en-us/library/ff687676\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/ff687676(WS.10).aspx) (на английском языке).

---

### L2TP/IPsec

Подключения L2TP используют шифрование, выполняемое протоколом IPsec. Протокол L2TP/IPsec следует использовать, если поддерживаются клиенты удаленного доступа под управлением Windows XP, так как они не могут использовать SSTP. L2TP/IPsec обеспечивает для каждого пакета проверку подлинности источника данных, проверку целостности данных, их конфиденциальность и защиту повторения.

Подключения L2TP/IPsec используют два уровня проверки подлинности. Проверка подлинности на уровне компьютера выполняется либо с помощью цифровых сертификатов, выпущенных ЦС, доверенным для клиента и VPN-сервера, либо посредством развертывания предварительных ключей. Затем при помощи протоколов PPP выполняется проверка подлинности на уровне пользователя. L2TP/IPsec поддерживает все протоколы проверки подлинности VPN, доступные в Windows Server 2008 и 2008 R2.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ L2TP/IPsec

Подробнее о L2TP/IPsec см. по адресу [http://technet.microsoft.com/en-us/library/ff687761\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/ff687761(WS.10).aspx) (на английском языке).

---

## SSTP

SSTP — технология VPN, впервые появившаяся в Windows Server 2008 и поддерживаемая Windows Server 2008 R2. Туннели VPN SSTP позволяют передавать данные через брандмауэры, блокирующие обычный VPN-трафик протоколов PPTP и L2TP/IPsec. Протокол SSTP инкапсулирует данные PPP по SSL-каналу протокола HTTPS. Точнее говоря, SSTP передает данные PPP через HTTPS. Это означает, что трафик SSTP проходит через порт TCP 443, который открыт практически у всех брандмауэров, размещаемых между Интернетом и общедоступными веб-серверами в сетях периметра.

Протокол PPP, используемый протоколом SSTP, обеспечивает поддержку методов строгой проверки подлинности, включая протокол EAP-TLS, который чаще всего используется со смарт-картами. Компонент SSL обеспечивает создание VPN-туннеля с согласованием расширенных ключей, шифрованием и проверкой целостности. Передаваемые данные шифруются, и становится возможным обнаружение попыток перехвата содержимого туннеля между исходной и конечной точками.

Планируя развертывание SSTP, необходимо учитывать следующее:

- SSTP поддерживается только в Windows Server 2008 и 2008 R2, Windows 7 и Windows Vista с первым пакетом обновлений (SP1);
- клиент должен доверять центру сертификации, издавшему сертификат SSL VPN-сервера;
- перед установкой RRAS необходимо установить сертификат SSL на VPN-сервер, иначе протокол SSTP будет недоступен;
- имена субъекта и узла в сертификате SSL, используемые внешними клиентами для подключения к VPN-серверу, должны совпадать, а клиент под управлением Windows 7 или Windows Vista SP1 должен доверять выдающему ЦС;
- SSTP не поддерживает туннелирование через сетевые прокси-серверы, требующие проверки подлинности;
- SSTP не поддерживает межсайтовые туннели (в отличие от PPTP и L2TP).

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ SSTP

Подробнее о SSTP см. по адресу [http://technet.microsoft.com/en-us/library/ff687819\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/ff687819(Ws.10).aspx) (на английском языке).

---

## IKEv2

IKEv2 — VPN-протокол, новый для Windows 7 и Windows Server 2008 R2. Этот протокол отсутствует в предыдущих версиях Windows, и клиенты под управлением Windows 7 могут использовать его, только если сервер удаленного доступа работает под управлением Windows Server 2008 R2. IKEv2 имеет следующие характеристики:

- поддерживает IPv6;
- имеет функцию повторного VPN-подключения (VPN Reconnect);
- поддерживает EAP и сертификаты компьютеров для проверки подлинности клиентов. Сюда входит возможность использования защищенного EAP, защищенного пароля EAP-MSCHAPv2, смарт-карт или сертификатов;

- не поддерживает PAP, CHAP и MS-CHAPv2 (без EAP) в качестве протокола проверки подлинности. Поддерживается проверка подлинности источника данных, защита повторения, обеспечение целостности и конфиденциальности данных;
- использует порт UDP 500;
- при настройке в Windows 7 нового VPN-подключения с параметрами по умолчанию клиент сначала попытается выполнить подключение по протоколу IKEv2;
- клиент должен работать под управлением Windows 7, а RRAS-сервер — под управлением Windows Server 2008 R2.

Преимущество IKEv2 перед другими протоколами состоит в поддержке повторного VPN-подключения. Если при подключении к VPN-серверу по протоколу PPTP, L2TP/IPsec или SSTP происходит нарушение работы сети, можно потерять VPN-подключение, после чего придется устанавливать его заново. Зачастую при этом приходится повторно вводить учетные данные. Если вы передаете файл, загружаете электронное письмо или отправляете задание печати, а подключение прерывается, приходится начинать все с начала. Повторное VPN-подключение позволяет клиентам под управлением Windows 7 автоматически повторно подключаться к прерванному сеансу VPN, даже если перерыв составлял до 8 часов.

Повторное VPN-подключение использует протокол туннелирования IKEv2 с расширением *.mobile*. Это расширение позволяет VPN-клиентам изменять свои интернет-адреса без повторного согласования проверки подлинности с VPN-сервером. Например, пользователь может использовать VPN-подключение к своей корпоративной сети во время подключения к беспроводной сети в кафе аэропорта. Когда приближается время отлета, пользователь перемещается из кафе в зал ожидания, где имеется собственная сеть Wi-Fi. Функция повторного подключения автоматически выполняет VPN-подключение, когда появляется связь с Интернетом через новую сеть. При использовании традиционного решения VPN пользователю пришлось бы вручную повторно соединяться с VPN-сервером после подключения к беспроводной сети зала ожидания, а все операции, выполняемые в тот момент через VPN, были бы потеряны. В отличие от DirectAccess, поддерживаемого только некоторыми версиями Windows 7, IKEv2 с повторным VPN-подключением поддерживается всеми версиями Windows 7.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ IKEv2

Подробнее о настройке протокола IKEv2 см. по адресу [http://technet.microsoft.com/en-us/library/ff687731\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/ff687731(WS.10).aspx) (на английском языке).

---

#### Проверьте себя

- Какие клиенты поддерживают SSTP?

#### Ответ

- SSTP поддерживают клиенты под управлением Windows Vista с пакетом обновлений 1 и Windows 7.

## DirectAccess

DirectAccess — постоянное VPN-подключение по протоколам IPv6 и IPsec. Если компьютер имеет доступ к Интернету, DirectAccess автоматически подключает его к корпоративной сети при условии соответствующей настройки. DirectAccess имеет следующие отличия от описанных выше решений VPN:

- Подключение выполняется автоматически и не требует вмешательства пользователя и входа в систему. Процесс подключения DirectAccess начинается с того момента, когда компьютер подключается к активной сети. С точки зрения пользователя, компьютер всегда имеет доступ к корпоративной интрасети независимо от того, сидит ли пользователь за своим столом или только что подключился к точке доступа Wi-Fi в кафе. Традиционное VPN-подключение приходится инициировать вручную.
- DirectAccess — двустороннее подключение, по которому серверы из интрасети могут взаимодействовать с клиентом под управлением Windows 7 так же, как если бы клиент был подключен к LAN. Во многих традиционных решениях VPN клиент имеет доступ к интрасети, однако серверы из интрасети не могут инициировать взаимодействие с клиентом.
- DirectAccess предоставляет администраторам больше гибкости в управлении доступностью ресурсов интрасети для удаленных пользователей и компьютеров. Администраторы могут интегрировать DirectAccess с NAP, чтобы у удаленных клиентов всегда были последние версии антивирусных баз и обновлений ПО. Кроме того, можно применять политики безопасности подключения для изоляции серверов и узлов.

DirectAccess работает автоматически, не требуя вмешательства пользователя, вошедшего в систему на компьютере под управлением Windows 7. Портативный компьютер, взятый домой и подключенный к Интернету, по-прежнему может получать обновления ПО и групповой политики от серверов корпоративной сети, даже если пользователь не выполнил вход. Клиенты под управлением Windows 7 используют следующую процедуру для установки подключения DirectAccess:

1. Клиент под управлением Windows 7, настроенный для использования DirectAccess, подключается к сети. Это происходит до входа пользователя в систему.
2. На этапе идентификации сети, когда компьютер обнаруживает, что подключается к новой сети или возобновляет подключение к существующей сети, клиент пытается подключиться к специально настроенному веб-сайту интрасети. Администратор указывает адрес этого веб-сайта в процессе настройки DirectAccess на сервере DirectAccess. Если клиент может связаться с этим веб-сайтом, Windows 7 считает, что установлено подключение к корпоративной сети, и в дальнейших действиях нет необходимости.
3. Если клиент не может связаться со специально настроенным веб-сайтом, он пытается определить наличие сети в основном режиме IPv6. Если такая сеть доступна, а клиенту назначен открытый адрес IPv6, DirectAccess выполняет прямое подключение к серверу DirectAccess через Интернет.



4. Если сеть в основном режиме IPv6 отсутствует, Windows 7 пытается создать туннель IPv6 поверх IPv4 сначала с помощью 6to4, а затем с помощью Teredo.
5. Если клиент не может установить подключение через Teredo или 6to4 из-за вмешательства брандмауэра или прокси-сервера, он пытается подключиться с помощью IP-HTTPS. IP-HTTPS инкапсулирует трафик IPv6 по HTTPS. Протокол IP-HTTPS, скорее всего, будет работать, так как лишь немногие брандмауэры, разрешающие подключение к Интернету, блокируют порт TCP 443.
6. Клиент и сервер DirectAccess выполняют взаимную проверку подлинности с помощью сертификатов компьютера, после чего устанавливается сеанс IPsec DirectAccess. DirectAccess поддерживает только проверку подлинности с помощью сертификатов.
7. Сервер DirectAccess проверяет соответствующую группу AD DS, чтобы убедиться, что компьютер и пользователь авторизованы для подключения с помощью DirectAccess.
8. Теперь клиент DirectAccess имеет доступ к настроенным соответствующим образом ресурсам корпоративной сети.

В табл. 9-1 приведены настройки DirectAccess и соответствующие способы взаимодействия с сервером DirectAccess по IPv6. Во время настройки сервера DirectAccess следует включить поддержку всех этих способов подключения. Это нужно сделать потому, что нельзя знать наверняка, каковы условия в удаленной сети, из которой клиент DirectAccess пытается выполнить подключение. IP-HTTPS используется в последнюю очередь, так как обладает меньшей производительностью по сравнению с другими способами подключения.

**Табл. 9-1.** Способы подключения через DirectAccess

| Подключение клиентской сети                                             | Способ подключения через DIRECTACCESS |
|-------------------------------------------------------------------------|---------------------------------------|
| Открытый адрес IPv6                                                     | Открытый адрес IPv6                   |
| Открытый адрес IPv4                                                     | 6to4                                  |
| Закрытый адрес IPv4 (NAT)                                               | Teredo                                |
| Клиент не может подключиться через брандмауэр, но подключен к Интернету | IP-HTTPS                              |

DirectAccess поддерживают только клиенты под управлением Windows 7 Enterprise и Ultimate, входящие в домен. Нельзя использовать DirectAccess с другими версиями Windows 7 или более ранними версиями Windows, например, Windows Vista или Windows XP. Во время настройки клиента для DirectAccess необходимо добавить доменную учетную запись компьютера клиента в специальную группу безопасности и указать эту группу при запуске мастера DirectAccess на сервере DirectAccess.

Клиенты получают конфигурацию DirectAccess через групповую политику. Это отличается от традиционной конфигурации VPN, где подключения выполняются вручную или распределяются через пакет администрирования диспетчера подключений (Connection Manager Administration Kit, CMAK). После добавления учетной записи клиентского компьютера в соответствующую груп-

пу безопасности необходимо установить на клиент сертификат компьютера, который будет использоваться для проверки подлинности DirectAccess. Организации необходимо развернуть службы сертификации Active Directory (AD CS), чтобы клиенты могли автоматически регистрироваться с использованием сертификатов.

Основная настройка DirectAccess происходит во время настройки сервера DirectAccess. При настройке сервера DirectAccess настраиваются и необходимые объекты групповой политики (GPO), поддерживающие DirectAccess. Прежде чем устанавливать DirectAccess, необходимо убедиться, что сервер DirectAccess отвечает следующим требованиям:

- компьютер должен работать под управлением Windows Server 2008 R2 и входить в домен;
- сервер должен иметь два сетевых адаптера;
- один из этих сетевых адаптеров должен иметь прямое подключение к Интернету; этому адаптеру нужно назначить два последовательных открытых адреса IPv4;
- второй сетевой адаптер должен иметь прямое подключение к корпоративной интрасети;
- компьютеру требуются цифровые сертификаты для поддержки проверки подлинности сервера, в том числе сертификат компьютера, соответствующий полному доменному имени (FQDN), которое назначается IP-адресам внешнего сетевого интерфейса сервера DirectAccess.

Кроме того, необходимо создать в AD DS не менее одной глобальной группы безопасности, используемой для целей DirectAccess. Этой группе можно дать любое имя, хотя за ней будет проще следить, если назначить имя, связанное с DirectAccess. При необходимости можно создать и указать несколько групп безопасности, связанных с DirectAccess. Если требуется разделить доступ к сегментам корпоративной интрасети, следует создать несколько групп.

Для установки DirectAccess на сервер под управлением Windows Server 2008 R2 добавьте функцию **Консоль управления DirectAccess** (DirectAccess Management Console) с помощью мастера добавления функций или следующей команды PowerShell:

```
Add-WindowsFeature DAMC
```

Установка консоли управления DirectAccess позволит настраивать и управлять функциями DirectAccess. Для установки консоли управления DirectAccess требуется также добавление компонента **Управление групповой политикой** (Group Policy Management). Этот компонент необходим потому, что мастер настройки DirectAccess создает объекты групповой политики, связанные с DirectAccess, которые настраивают параметры клиентов DirectAccess. Запустите мастер настройки DirectAccess, используя учетную запись пользователя, имеющего разрешение на создание и применение GPO в домене.

После установки консоли управления DirectAccess можно настроить сервер DirectAccess. Для этого необходимо выполнить следующее:

1. Откройте консоль управления DirectAccess из меню **Администрирование** на компьютере под управлением Windows Server 2008 R2. Эта консоль показана на рис. 9-4.

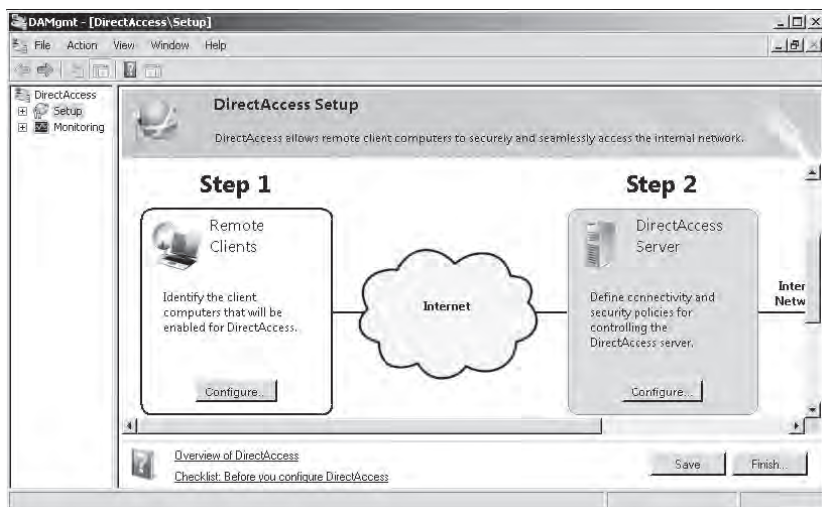


Рис. 9-4. Консоль управления DirectAccess

2. Выберите узел **Установка (Setup)**. На панели сведений в разделе **Удаленные клиенты (Remote Clients)** щелкните **Настроить (Configure)**. Откроется диалоговое окно **Настройка клиента DirectAccess (DirectAccess Client Setup)**. Щелкните **Добавить (Add)** и укажите имена групп безопасности, в которые добавляются учетные записи компьютеров, которым требуется предоставить доступ к DirectAccess. Эти группы могут иметь любые имена.
3. Используйте элемент **Настройка сервера DirectAccess (DirectAccess Server Setup)**, чтобы указать, какой интерфейс подключен к Интернету, а какой к внутренней сети. После этого на сервере DirectAccess будут активированы технологии передачи IPv6 (рис. 9-5). Используйте этот элемент, чтобы указать ЦС от которого в конечном итоге клиенты должны получать сертификаты (напрямую или через подчиненный ЦС). Также необходимо указать сертификат сервера, используемый для защиты трафика IP-HTTPS.

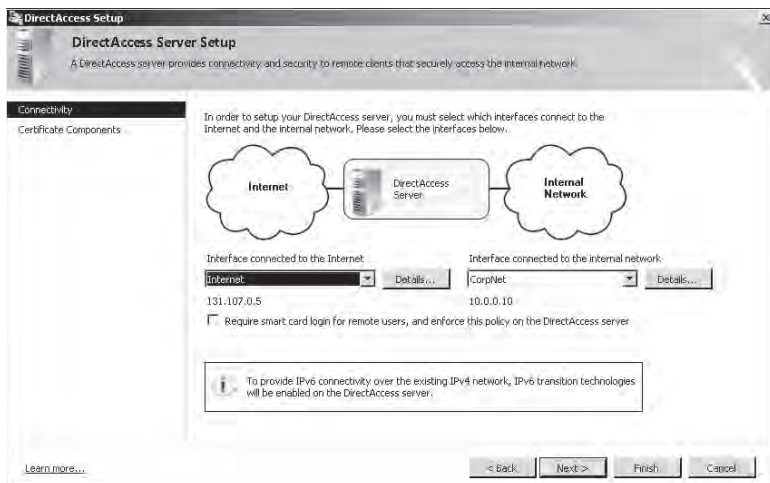


Рис. 9-5. Настройка сервера DirectAccess

4. На странице **Настройка сервера инфраструктуры** (Infrastructure Server Setup) укажите расположение внутреннего веб-сайта (называемого сервером сетевого расположения), с которым клиенты DirectAccess пытаются связаться, чтобы определить, подключены ли они к корпоративной интрасети или к удаленному расположению. Необходимо обеспечить защиту этого сайта с помощью сертификата веб-сервера. В этом диалоговом окне также указываются DNS-серверы и контроллеры домена, к которым клиенты DirectAccess могут обращаться для проверки подлинности.
5. Последний этап заключается в указании ресурсов корпоративной интрасети, которые будут доступны клиентам DirectAccess. По умолчанию разрешен доступ ко всем ресурсам. В более безопасных средах можно использовать политики изоляции, чтобы разрешать доступ отдельным группам безопасности. Например, можно создать группу безопасности и добавить в нее учетные записи некоторых файловых и почтовых серверы.
6. Если щелкнуть **Готово**, DirectAccess обратится к контроллеру домена и создаст в домене два новых GPO. Один из этих GPO предназначен для групп безопасности, содержащих учетные записи компьютеров клиентов DirectAccess. Второй объект GPO предназначен для самого сервера DirectAccess. DirectAccess опирается на несколько других компонентов сетевой инфраструктуры Windows Server 2008 R2. Домен, в котором установлен сервер DirectAccess, должен иметь следующее:

- не менее одного контроллера домена под управлением Windows Server 2008 R2 и DNS-сервер во внутренней сети;
- сервер под управлением Windows Server 2008 или более поздней версии с установленными службами AD CS, работающими как ЦС предприятия или подчиненный ЦС предприятия.

Чтобы сделать ресурсы внутренней сети доступными для удаленных клиентов DirectAccess, необходимо выполнить одно из следующих действий:

- убедиться, что все внутренние ресурсы, к которым будет иметь доступ DirectAccess, поддерживают IPv6;
- развернуть ISATAP в интрасети, чтобы обеспечить доступ к серверам и приложениям интрасети посредством туннелирования трафика IPv6 через интрасеть IPv4;
- развернуть устройство NAT-PT, чтобы обеспечить доступ к узлам, поддерживающим только адреса IPv4, для клиентов DirectAccess, использующих IPv6.

На всех серверах приложений, к которым имеют доступ клиенты DirectAccess, брандмауэр Windows с повышенной безопасностью (WFAS) должен пропускать трафик ICMPv6. Для этого можно включить указанные ниже правила брандмауэра, используя групповую политику:

- эхо-запрос — входящий трафик ICMPv6;
- эхо-запрос — исходящий трафик ICMPv6.

Для поддержки DirectAccess на внешнем брандмауэре организации должны быть открыты следующие порты:

- UDP 3544 — включает трафик Teredo;
- IPv4 41 — включает трафик 6to4;
- TCP 443 — разрешает трафик IP-HTTPS;
- ICMPv6 и IPv4 50 — требуется, когда у удаленных клиентов есть IPv6-адреса.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ DirectAccess

Подробнее о DirectAccess см. по адресу <http://technet.microsoft.com/en-us/network/dd420463.aspx> (на английском языке).

---

## Серверы NPS RADIUS

Кроме возможности предоставлять шлюзы RRAS, сервер сетевой политики (NPS) может функционировать как сервер RADIUS и как клиент RADIUS, который называется также прокси-сервером RADIUS. Если организация имеет более одного сервера удаленного доступа, администратор может настроить сервер, выполняющий роль NPS, как сервер RADIUS, а затем настроить все серверы удаленного доступа как клиенты RADIUS. Преимущество такого подхода в том, что управление сетевой политикой выполняется централизованно, а не на каждом сервере удаленного доступа в отдельности.

Если RADIUS используется в качестве поставщика проверки подлинности для RAS-серверов, запросы на подключение к серверу RADIUS отправляются в формате сообщения запроса RADIUS. Сервер RADIUS выполняет проверку подлинности и авторизацию, а затем передает информацию обратно на RAS-сервер. Сервер RADIUS должен входить в домен AD DS, однако VPN-сервер RAS, передающий запросы аутентификации серверу RADIUS, может быть изолированным компьютером.

### Клиенты RADIUS и NPS

Клиенты RADIUS представляют собой серверы доступа к сети, такие как VPN-серверы, точки беспроводного доступа и коммутаторы проверки подлинности 802.1x. Несмотря на то, что компьютеры, обращающиеся к этим серверам доступа к сети, называются *клиентами удаленного доступа*, они не считаются клиентами RADIUS. Клиенты RADIUS предоставляют доступ к сети другим узлам.

Для настройки клиентов RADIUS с помощью NPS откройте консоль **Сервер сетевых политик** (Network Policy Server) из меню **Администрирование**. Щелкните правой кнопкой мыши **Клиенты RADIUS** (RADIUS Clients) и выберите **Новый RADIUS-клиент** (New RADIUS Client). Откроется диалоговое окно, изображенное на рис. 9-6.

Настройка включает предоставление следующей информации:

- понятное имя;
- адрес (IP или DNS);
- имя поставщика (в раскрывающемся меню предлагается более 20 поставщиков);
- общий секрет (настраивается с помощью оснастки NPS на RADIUS-клиенте).

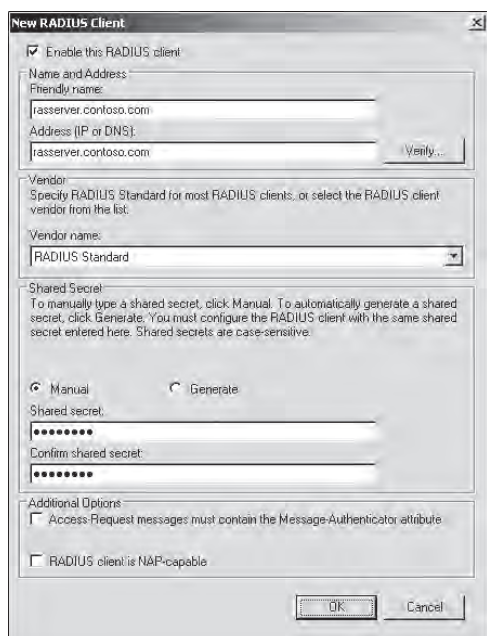


Рис. 9-6. Настройка нового клиента RADIUS

---

## ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Клиенты RADIUS

Подробнее о клиентах RADIUS см. по адресу <http://technet.microsoft.com/ru-ru/library/cc754033.aspx>.

---

## NPS как прокси-сервер RADIUS

Прокси-серверы RADIUS маршрутизируют сообщения RADIUS между серверами удаленного доступа, настроенными как клиенты и серверы RADIUS, которые выполняют проверку подлинности, авторизацию и учет. При настройке в качестве прокси-сервера RADIUS сервер NPS записывает в журнал учета информацию о сообщениях, которые он передает от RAS-клиентов серверам RADIUS. Будучи настроенным как прокси-сервер RADIUS, NPS действует как клиент RADIUS.

Если требуется обеспечить проверку подлинности и авторизацию для учетных записей из других лесов AD DS, следует развернуть NPS в качестве прокси-сервера RADIUS. Прокси-сервер RADIUS NPS использует имя сферы (которое идентифицирует расположение учетной записи пользователя), являющееся частью имени пользователя, для пересылки запроса серверу RADIUS в целевом лесу. Это позволяет проверять подлинность пользователей, обращающихся к серверу доступа к сети, расположенного в другом лесу. Использование прокси-сервера RADIUS для аутентификации между лесами не является обязательным, если оба леса имеют функциональный уровень Windows Server 2003 или выше, и между лесами установлено доверие.

Развертывать NPS как прокси-сервер RADIUS следует также в тех случаях, когда требуется выполнять проверку подлинности и авторизацию с использованием базы данных, отличной от базы данных учетных записей Windows. За-



просы на подключение, соответствующие определенному имени сферы, пересылаются на сервер RADIUS, зачастую работающий не на платформе Windows, который имеет доступ к отдельной базе данных учетных записей пользователей и данным авторизации. Следовательно, NPS следует развертывать как прокси-сервер RADIUS, когда требуется выполнять проверку подлинности и авторизацию с использованием сервера RADIUS, который использует службу каталогов Novell или работает на UNIX.

Последний довод в пользу развертывания NPS как прокси-сервера RADIUS необходимость обрабатывать большое число запросов соединения между клиентами RADIUS RAS и серверами RADIUS. Прокси-сервер RADIUS NPS может распределять трафик между несколькими серверами RADIUS, что бывает трудновыполнимо, если используются только клиенты и серверы RADIUS.

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Прокси-серверы RADIUS

Подробнее о прокси-серверах RADIUS см. по адресу <http://technet.microsoft.com/ru-ru/library/cc731320.aspx>.

## Учет удаленного доступа

Можно настроить NPS для выполнения учета RADIUS. Учет RADIUS позволяет отслеживать, кто подключается и кто не смог подключиться к инфраструктуре RADIUS. Учет NPS позволяет выполнять мониторинг следующей информации:

- запросы аутентификации пользователя;
- сообщения разрешения доступа;
- сообщения отказа доступа;
- запросы и ответы учета;
- периодические обновления состояния.

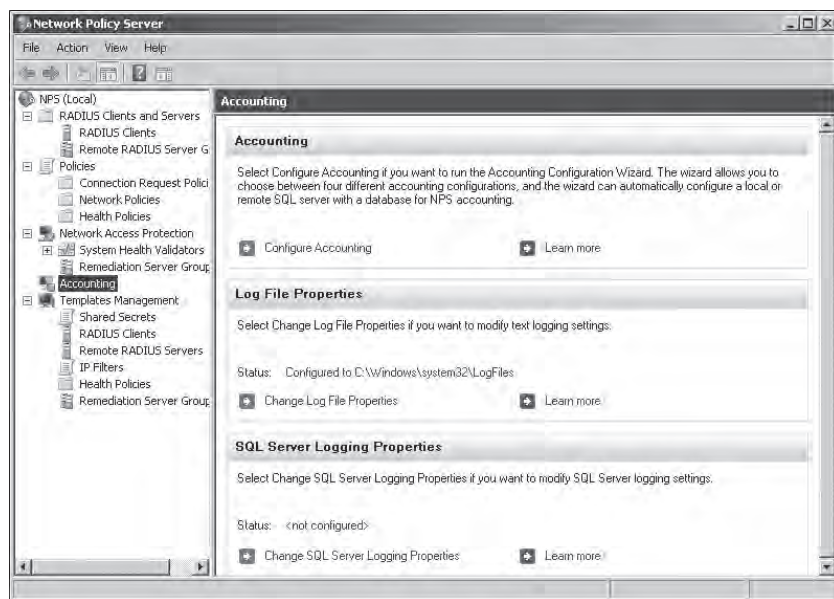


Рис. 9-7. Узел Учет консоли NPS



Как показано на рис. 9-7, есть два способа записи данных журнала. Журналы можно хранить локально или записывать в базу данных Microsoft SQL Server 2005 с пакетом обновлений 1, SQL Server 2008 или 2008 R2. Журналы, записанные локально, следует использовать, когда число клиентов удаленного доступа невелико. Если клиентов удаленного доступа много, то запись информации в базу данных SQL Server даст гораздо больше возможностей управления огромным объемом информации.

## Локальный журнал файлов

Файлы журнала NPS можно записывать в двух форматах: IAS и совместимом с базой данных. По умолчанию используется формат, совместимый с базой данных. Частоту создания новых файлов журнала следует настроить в соответствии с потребностями организации. Преимущество одного файла неограниченного размера состоит в том, что проще обнаружить отдельное событие, так как поиск приходится выполнять только в одном файле журнала. Недостаток заключается в том, что файлы журнала могут становиться огромными, что затрудняет их открытие и выполнение поиска.

Хотя по умолчанию файлы журналов записываются в папку %Systemroot%/System32/LogFiles, Microsoft рекомендует хранить их на другом разделе, отдельно от файлов операционной системы и приложений или общих файлов. При отсутствии строгого контроля файлы журнала могут заполнить все свободное дисковое пространство. Если это произойдет в системном разделе, сервер может стать недоступным. Очень важно отметить, что журналы данных учета NPS не удаляются автоматически. Можно настроить политику сохранения журналов, чтобы в случае заполнения диска старые файлы автоматически удалялись. Такой способ работает лучше всего, когда файлы журнала записываются в изолированный раздел, заполнение диска файлами журнала NPS влияло только на хранение этих файлов. Если файлы журнала NPS приходится хранить вместе с другими данными или на томе с файлами операционной системы, следует написать сценарий, который будет автоматически удалять журналы по истечении определенного времени.

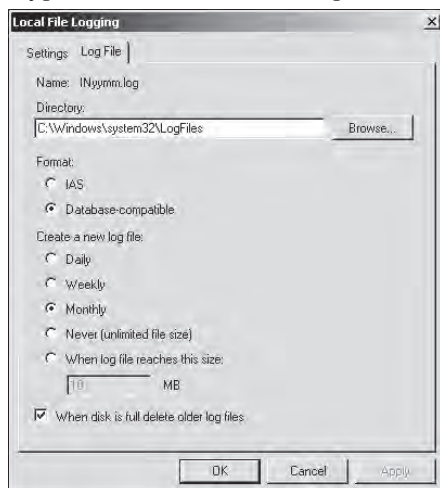


Рис. 9-8. Настройка ведения журнала NPS в локальном файле

Файлы журнала можно записывать в удаленные общие папки, если указать путь UNC общей папки. При этом необходимо настроить разрешения общей папки так, чтобы учетная запись, от имени которой записываются журналы, имела разрешение на запись данных в эту общую папку. На рис. 9-8 показана вкладка **Файл журнала (Log File)** диалогового окна **Ведение журнала в локальном файле (Local File Logging)**.

## Настройка ведения журнала SQL Server

Альтернатива локальному журналу учета NPS — запись информации в базу данных SQL Server, установленную на том же компьютере, что и NPS, или в локальной сети. NPS отправляет данные в хранимую процедуру *report\_event* на целевом компьютере с SQL Server. Эта хранимая процедура доступна в SQL Server 2000, 2005, 2008, и 2008 R2.

В диалоговом окне свойств **Ведение журнала SQL Server (SQL Server Logging)** (рис. 9-9) можно указать, какие данные учета NPS будут отправляться в базу данных SQL Server. Кнопка **Настроить (Configure)** позволяет указать свойства канала связи с компьютером, на котором работает SQL Server. Укажите имя сервера, способ проверки подлинности компьютера, на котором работает SQL Server, и базу данных SQL Server, которая будет использоваться для хранения данных учета. Аналогично записи локального журнала в отдельный раздел, рекомендуется создавать отдельную базу данных для данных учета NPS.

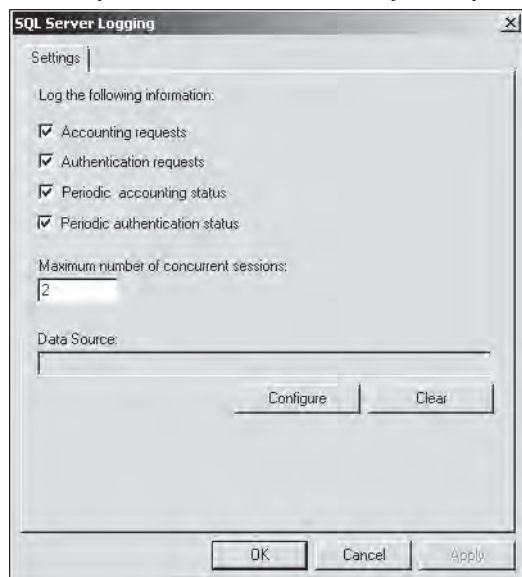


Рис. 9-9. Настройка ведения журнала SQL Server

---

## ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Изменения NPS в Windows Server 2008 R2

Подробнее об изменениях NPS в Windows Server 2008 R2 см. по адресу [http://technet.microsoft.com/en-us/library/dd365355\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd365355(WS.10).aspx) (на английском языке).

---

## Серверы шлюзов удаленных рабочих столов

Серверы шлюзов удаленных рабочих столов (RD Gateway) позволяют клиентам из Интернета подключаться к серверам RDP, расположенным в защищенных внутренних сетях, по протоколу удаленного рабочего стола (RDP) поверх HTTPS. Это дает пользователям возможность обращаться из Интернета к приложениям RemoteApp, стандартным сеансам удаленного рабочего стола и сеансам удаленного рабочего стола.

---

### ПРИМЕЧАНИЕ Изменение терминологии

В Windows Server 2008 службы удаленного рабочего стола называются службами терминалов, а шлюз удаленных рабочих столов называется шлюзом служб терминалов.

Преимущество шлюза удаленных рабочих столов состоит в том, что не нужно настраивать VPN RAS, чтобы предоставить доступ к ресурсам. Вместо того чтобы развертывать наборы клиентских подключений для всех работников организации, которым нужен доступ к ресурсам через брандмауэр со стороны Интернета, можно отправить им по электронной почте ярлык RDP и разрешить им подключаться с клиентских компьютеров под управлением Windows XP SP2, Windows Vista или Windows 7. Шлюз удаленных рабочих столов, по сути, представляет собой VPN-подключение SSL, ограниченное до RDP. Установив обычное VPN-подключение, можно иметь прямой доступ ко всем ресурсам напрямую (по крайней мере, в теории). Например, можно использовать VPN для подключения к внутренним общим папкам и общим принтерам. С помощью шлюза удаленных рабочих столов можно получить доступ к RDS-серверу или сеансу удаленного рабочего стола, а, следовательно, и к ресурсам.

Для настройки сервера шлюза удаленных рабочих столов выполните следующие действия:

1. Установите службу роли шлюза удаленных рабочих столов на компьютер под управлением Windows Server 2008 R2, находящийся в защищенной подсети. Брандмауэр периметра должен быть настроен так, чтобы сервер шлюза удаленных рабочих столов был доступен через порт 443.
2. Получите сертификат SSL. Имя сертификата должно совпадать с именем, которое клиенты используют для подключения к серверу. Установите сертификат на сервер, а затем с помощью консоли диспетчера шлюза удаленных рабочих столов выполните сопоставление сертификата сервера. Важно, выполнить сопоставление сертификата SSL именно через этот диспетчер. При использовании другого способа сервер шлюза удаленных рабочих столов не будет функционировать должным образом.
3. Настройте **Политики авторизации подключений к удаленному рабочему столу (RD-CAP)** и **Политики авторизации ресурсов удаленного рабочего стола (RD-RAP)**. О них речь пойдет в следующем разделе.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Настройка шлюза удаленных рабочих столов

Подробнее о настройке шлюзов удаленных рабочих столов см. по адресу <http://technet.microsoft.com/ru-ru/library/cc772479.aspx>.

---

## Политики авторизации подключений

Политики авторизации подключений к удаленному рабочему столу (RD-CAP) определяют, кому из пользователей разрешено подключаться через сервер шлюза удаленных рабочих столов к ресурсам, расположенным во внутренней сети организации. Обычно для этого указывается локальная группа на сервере шлюза удаленных рабочих столов или группа в AD DS. Группы могут содержать учетные записи пользователей и компьютеров. Также с помощью политик RD-CAP можно определять способ проверки подлинности (пароль или смарт-карта) удаленных клиентов для доступа к ресурсам внутренней сети через сервер шлюза удаленных рабочих столов. Политики RD-CAP можно использовать совместно с NAP; более подробно об этом будет рассказано на занятии 2.

## Политики авторизации ресурсов

Политики авторизации ресурсов удаленного рабочего стола (RD-RAP) используются для определения отдельных ресурсов во внутренней сети организации, к которым могут подключаться входящие клиенты шлюза удаленных рабочих столов. При создании RD-RAP необходимо указать группу компьютеров, к которым требуется предоставить доступ, и группу пользователей, которым этот доступ будет разрешен. Например, можно создать группу компьютеров под названием AccountsComputers, к которой будут иметь доступ члены группы Accountants. Для получения доступа к внутренним ресурсам удаленный пользователь должен соответствовать условиям как минимум одной политики RD-CAP и как минимум одной политики RD-RAP.

## Резюме

- SSTP передает данные PPP через HTTPS. Сертификат SSL, установленный на RAS-сервер, должен соответствовать имени узла, к которому подключается SSTP-клиент. SSTP могут использовать только клиенты под управлением Windows 7 и Windows Vista с пакетом обновлений 1. SSTP нельзя использовать для межсайтовых туннелей.
- VPN IKEv2 могут использовать только клиенты под управлением Windows 7, подключающиеся к VPN-серверам под управлением Windows Server 2008 R2. VPN IKEv2 поддерживает функцию повторного подключения VPN.
- DirectAccess — технология удаленного доступа по протоколу IPv6. DirectAccess поддерживается только в Windows 7 Enterprise и Ultimate и требует наличия сервера DirectAccess под управлением Windows Server 2008 R2.
- Серверы NPS можно настраивать для записи данных учета в локальные файлы журнала или в базы данных SQL Server, на которых имеется хранящая процедура *report\_event*.
- Прокси-серверы RADIUS можно использовать для балансировки нагрузки по обработке запросов от RAS-серверов к серверам RADIUS.
- Серверы шлюзов удаленных рабочих столов предоставляют еще один способ удаленного доступа, позволяя клиентам под управлением Windows Vista подключаться к RDP-серверам через порт 443.

## Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных на занятии 1. Эти вопросы предоставлены также в электронном виде на прилагаемом к книге компакт-диске.

---

### ПРИМЕЧАНИЕ Ответы

Ответы на вопросы и пояснения к их вариантам размещены в разделе «Ответы» в конце книги.

---

1. Какой из следующих протоколов VPN следует использовать, если брандмауэр блокирует весь трафик из Интернета, за исключением проходящего через порты TCP 25, 80 и 443?
  - a. L2TP/IPsec.
  - b. SSTP.
  - c. PPTP.
  - d. IKEv2.
2. Пользователи организации работают на ноутбуках под управлением Windows 7 Enterprise. Часто они переводят компьютеры в режим гибернации, и при возобновлении работы не хотят повторно проходить проверку подлинности для доступа к VPN-подключению. Какой из протоколов VPN позволяет при выходе из режима гибернации повторно подключаться к сеансу, инициированному несколько часов назад?
  - a. L2TP/IPsec.
  - b. SSTP.
  - c. PPTP.
  - d. IKEv2.
3. Какие клиенты могут подключаться к VPN-серверу под управлением Windows Server 2008 R2, если для VPN-подключений доступны только порты 25, 80 и 443? (Выберите все подходящие.)
  - a. Windows Vista с пакетом обновлений 1.
  - b. Windows 7.
  - c. Windows XP Professional с пакетом обновлений 3.
  - d. Windows 2000 Professional с пакетом обновлений 2.
4. На серверах VPN1, VPN2 и VPN3 установлена роль RAS-сервера. Они принимают входящие VPN-подключения из Интернета. Сервер NPS1 настроен как сервер RADIUS с помощью роли NPS-сервера. Серверы VPN1, VPN2 и VPN3 используют NPS1 для проверки подлинности входящих подключений. Сервер SQL1 работает под управлением Windows Server 2008 R2, и на нем установлена СУБД SQL Server 2008 R2. Вы хотите расширить возможности поиска данных учета RADIUS. Какой из следующих стратегий следует придерживаться?
  - a. Настроить VPN1, VPN2 и VPN3 так, чтобы данные учета NPS пересылались на SQL1.
  - b. Настроить VPN1, VPN2 и VPN3 так, чтобы данные учета NPS пересылались на NPS1.

- c. Настроить SQL1 так, чтобы данные учета NPS пересылались на сервер NPS1.
  - d. Настроить NPS1 так, чтобы данные учета NPS пересылались на сервер SQL1.
5. В какой из перечисленных операционных систем можно использовать Direct-Access для доступа к внутренней сети организации из Интернета?
- a. Windows XP Professional с пакетом обновлений 3.
  - b. Windows Vista Enterprise.
  - c. Windows 7 Enterprise.
  - d. Windows 7 Home Premium.

## Занятие 2. Брандмауэры и защита доступа к сети

Развертывание NAP в сети используется как способ обеспечения соответствия компьютеров, имеющих доступ к важным ресурсам, определенным критериям работоспособности. Эти критерии включают наличие последних обновлений, актуального антивирусного и антишпионского ПО и средств обеспечения безопасности, таких как брандмауэр Windows. На этом занятии вы узнаете, как планировать и настраивать инфраструктуру NAP и способ ее применения.

---

### Изучив материал этого занятия, вы сможете:

- ✓ Планировать роли сервера NAP.
- ✓ Осуществлять мониторинг и поддержку политик NAP.

**Продолжительность занятия — примерно 60 мин.**

---

## Брандмауэр Windows с повышенной безопасностью

Простейшим методом применения стандартной настройки брандмауэра в организации является использование групповой политики. Настраивать входящие и исходящие правила, включать и отключать брандмауэр Windows с повышенной безопасностью для отдельных профилей можно в разделе групповой политики **Конфигурация компьютера | Политики | Конфигурация Windows | Брандмауэр Windows с повышенной безопасностью** (Computer Configuration | Policies | Windows Settings | Windows Firewall With Advance Security).

Можно настроить новые правила на основе предопределенного правила, определенной программы или порта. Правила можно применять к входящему и исходящему трафику. Многие администраторы используют в доменах исходящие правила, чтобы запретить использование определенных программ, например, программ для обмена файлами или передачи мгновенных сообщений. Хотя лучший способ блокировки такого рода трафика состоит в том, чтобы изначально запретить установку таких программ или ограничить их использование с помощью политик AppLocker, во многих доменных средах есть пользователи с ноутбуками, которые заходят и выходят из сети. В некоторых случаях пользователи ноутбуков имеют локальные административные права на своих компьютерах. Применение правил брандмауэра к каждому компьютеру посредством

групповой политики позволяет администраторам блокировать программы, которые могут использовать SSL-туннели для обхода брандмауэра периметра.

---

### **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ    Настройка брандмауэра Windows с помощью групповой политики**

Подробнее о настройке брандмауэра Windows с повышенной безопасностью см. по адресу [http://technet.microsoft.com/en-us/library/ff602918\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/ff602918(WS.10).aspx) (на англ. языке).

---

### **Изоляция домена**

Брандмауэр Windows с повышенной безопасностью позволяет создавать правила безопасности подключения, которые защищают трафик при помощи IPsec. При изоляции домена используются параметры групповой политики брандмауэра Windows с повышенной безопасностью, домена AD DS и членства в домене, с помощью которых применяется политика, разрешающая компьютерам, входящим в домен, принимать входящие запросы только от компьютеров, входящих в тот же домен. После применения этой политики компьютеры, являющиеся членами домена, изолируются от компьютеров, не являющихся членами домена. Важно помнить, что в сценариях изоляции домена изолированные компьютеры могут инициировать коммуникацию с узлами вне домена, например, с веб-серверами в Интернете. Но когда взаимодействие инициирует узел вне домена, они не отвечают.

Политики изоляции домена применяются через элемент **Правила безопасности подключения** (Connection Security Rules) из узла GPO **Конфигурация компьютера | Политики | Конфигурация Windows | Параметры безопасности | Брандмауэр Windows | Расширенные параметры безопасности** (Computer Configuration | Policies | Windows Settings | Security Settings | Windows Firewall | Advanced Security).

---

### **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ    Изоляция домена**

Подробнее об изоляции домена см. по адресу [http://technet.microsoft.com/ru-ru/library/cc730709\(WS.10\).aspx](http://technet.microsoft.com/ru-ru/library/cc730709(WS.10).aspx).

---

### **Изоляция серверов**

Изоляция серверов аналогична изоляции доменов, с той лишь разницей, что политика изоляции серверов применяется не ко всем компьютерам внутри домена, а только к отдельной группе серверов в домене. Чтобы изолировать серверы, добавьте учетные записи компьютеров, которые должны быть изолированы, в отдельное подразделение и примените к нему объект GPO с соответствующим правилом безопасности подключения. После этого с изолированными серверами смогут взаимодействовать только компьютеры, являющиеся членами домена. Это может быть эффективным способом защиты серверов в тех случаях, когда требуется предоставить доступ к сети сторонним компьютерам. Сторонние компьютеры могут иметь доступ к некоторым сетевым ресурсам, например, к серверам интрасети, веб-серверам и DNS-серверам, но администратор может изолировать отдельные сетевые ресурсы, такие как файловые серверы и базы данных, путем настройки политик изоляции серверов.



---

**ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Изоляция серверов**

Подробнее об изоляции серверов см. по адресу [http://technet.microsoft.com/en-ca/library/cc770626\(Ws.10\).aspx](http://technet.microsoft.com/en-ca/library/cc770626(Ws.10).aspx) (на англ. языке).

---

## Forefront Threat Management Gateway

Брандмауэр Windows с повышенной безопасностью является оптимальным решением для защиты отдельных серверов, однако следует рассмотреть возможность применения более функционального брандмауэра, например, Forefront Threat Management Gateway (TMG) 2010, который будет работать между сетью периметра организации и Интернетом. Сети периметра представляют собой сети, расположенные между Интернетом и внутренней сетью организации. Некоторые ресурсы из сетей периметра должны быть доступны из Интернета. При этом можно использовать внешний брандмауэр, защищающий такие ресурсы, и брандмауэр между сетью периметра и внутренней сетью в качестве дополнительного уровня защиты. В большинстве конфигураций трафик может проходить из Интернета в сеть периметра и обратно или из внутренней сети в сеть периметра и обратно, но никогда напрямую из внутренней сети в Интернет в обход сети периметра.

Forefront TMG 2010 имеет следующие расширенные функции:

- контроль пакетов и фильтрация приложений;
- система предотвращения проникновений (IPS);
- защищенный прокси-сервер;
- веб-фильтрация на основе URL или категории URL (например, фильтрация спортивных или развлекательных сайтов);
- мониторинг сетевого трафика;
- проверка HTTPS;
- публикация в Интернете служб обратных прокси-серверов, таких как веб-сайты, сайты веб-доступа к Outlook и узлы SharePoint, имеющие функциональность моста SSL;
- создание межсайтовых VPN-соединений;
- возможность публиковать VPN-серверы в Интернете.

Forefront TMG 2010 можно устанавливать на компьютеры под управлением Windows Server 2008 с пакетом обновлений 2 или Windows Server 2008 R2. При установке Forefront TMG 2010 автоматически устанавливаются роли и службы ролей сервера сетевой политики, RRAS и служб Active Directory облегченного доступа к каталогам (AD LDS).

Обычно Forefront TMG устанавливается на компьютер с двумя сетевыми картами, один из которых подключен к Интернету, а другой — к сети периметра или внутренней сети. Можно развернуть Forefront TMG на компьютере с одним сетевым адаптером, но обычно это следует делать только в том случае, если развернут дополнительный брандмауэр в сети периметра. Forefront TMG — последняя версия продукта, ранее известного как Microsoft Internet Security and Acceleration (ISA) Server. Управление Forefront TMG выполняется с помощью консоли Forefront TMG, изображенной на рис. 9-10.

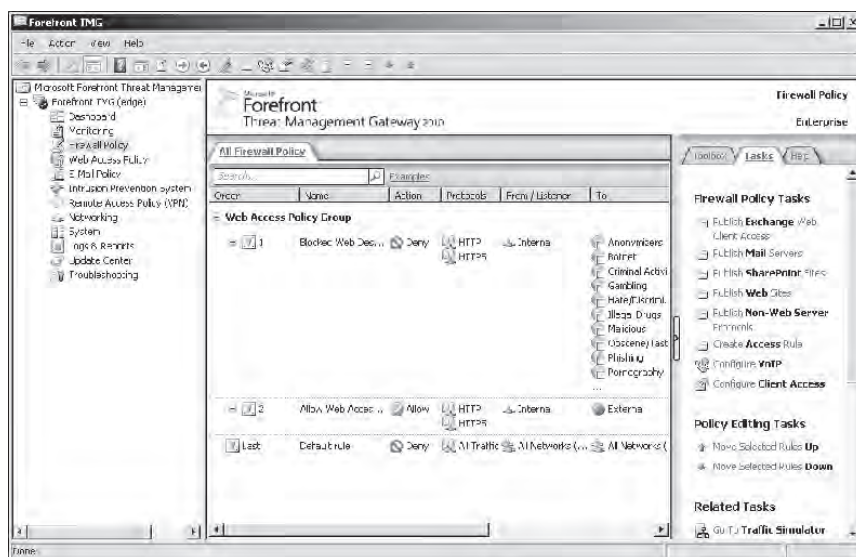


Рис. 9-10. Консоль Forefront TMG

## ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Forefront TMG 2010

Подробнее о Forefront TMG 2010 см. по адресу <http://technet.microsoft.com/ru-ru/library/ff355324.aspx>.

## Защита доступа к сети

Защита доступа к сети (NAP) — технология, позволяющая ограничивать доступ к сети в зависимости от работоспособности клиента. Агенты работоспособности системы (SHA) и средства проверки работоспособности системы (SHV) представляют собой компоненты, проверяющие работоспособность компьютера по настроенному набору показателей. SHV определяет, каким параметрам должен соответствовать клиент. SHA — компонент, с помощью которого тестируются эти показатели. Агенты работоспособности в Windows 7, Windows Vista и Windows XP можно настраивать через узел **Средства проверки работоспособности системы** (System Health Validators) под узлом NAP в NPS. На рис. 9-11 показаны параметры, которые можно настроить для SHV в Windows 7 и Windows Vista.

Сторонние организации могут предоставлять SHA и SHV для своих продуктов. При развертывании сторонних SHA и SHV компоненты SHA устанавливаются на все клиенты, а SHV — на компьютер под управлением Windows Server 2008 или 2008 R2, где установлена роль сервера NPS. После установки создается новая политика работоспособности, использующая новый компонент SHV в качестве критерия соответствия. Политика работоспособности может использовать несколько SHV. Например, можно создать политику работоспособности, требующую соответствия всем условиям SHV в Windows 7 или Windows Vista и SHV организации, прежде чем клиенту будет предоставлен доступ ко всем сетевым ресурсам.

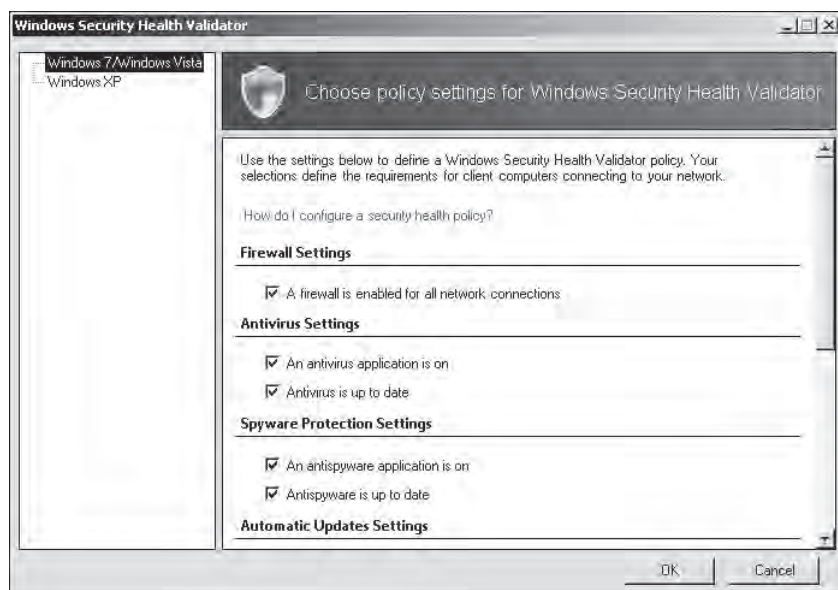


Рис. 9-11. SHV в Windows 7 и Windows Vista

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ SHV

Подробнее SHV см. по адресу [http://technet.microsoft.com/en-us/library/dd314150\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd314150(WS.10).aspx) (на английском языке).

## Способы применения NAP

Когда обнаруживается компьютер, несовместимый с применяемой политикой работоспособности, NAP принудительно ограничивает доступ к сети. Это выполняется с помощью клиента безопасности (enforcement client, EC). Windows 7, Windows Vista, Windows XP с пакетом обновлений 3, Windows Server 2008 и 2008 R2 поддерживают применение защиты доступа к сети для IPsec, IEEE 802.1X, VPN и DHCP. Windows 7, Windows Vista, Windows Server 2008 и 2008 R2 также поддерживают применение NAP для подключений через шлюз удаленных рабочих столов.

Способы применения NAP можно использовать отдельно или совместно друг с другом для ограничения доступа к сети компьютерам, которые не соответствуют настроенным политикам работоспособности. Следовательно, можно применять NAP для VPN и IPsec, чтобы внутренние клиенты и клиенты из Интернета получали доступ к ресурсам только при соответствии определенным критериям работоспособности.

### Принудительная защита доступа к сети для IPsec

Принудительная защита доступа к сети для IPsec действует посредством применения правил IPsec. Только компьютеры, соответствующие критериям работоспособности, могут взаимодействовать друг с другом. Принудительную защиту для IPsec можно применять к каждому IP-адресу, номеру порта TCP или UDP. Например, используя принудительную защиту для IPsec, можно блоки-

ровать доступ RDP к веб-серверу, чтобы только работоспособные компьютеры могли подключаться для управления этим сервером, но разрешать клиентам, не соответствующим требованиям к работоспособности, подключаться для просмотра веб-страниц на этом же веб-сервере.

Принудительная защита для IPsec применяется после получения компьютерами действительных IP-адресов от DHCP или посредством статической настройки. IPsec является наиболее эффективным способом ограничения доступа к сети через NAP. Если другие методы можно обойти с помощью статических адресов или изменения портов, сертификат IPsec, используемый для шифрования, может быть получен узлом только после прохождения проверки работоспособности. Отсутствие сертификата IPsec означает невозможность коммуникации с другими узлами, которые шифруют свои данные с помощью сертификата, выпускаемого тем же ЦС.

Для развертывания принудительной защиты IPsec в сети необходим центр регистрации работоспособности (HRA) Windows Server 2008 или 2008 R2 и центр сертификации Windows Server 2008 или 2008 R2. Клиенты должны работать под управлением ОС с клиентом безопасности IPsec: Windows 7, Windows Vista, Windows Server 2008 и 2008 R2 или Windows XP с пакетом обновления 3.

---

#### **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ   Политики применения защиты доступа к сети для IPsec**

Подробнее о применении защиты доступа для IPsec см. по адресу <http://technet.microsoft.com/ru-ru/library/cc771899.aspx>.

---

### **Принудительная защита доступа к сети для 802.1X**

Принудительная защита для 802.1X использует Ethernet-коммутаторы с проверкой подлинности или точки беспроводного доступа IEEE 802.11. Такие коммутаторы и точки доступа предоставляют неограниченный доступ к сети только компьютерам, отвечающим требованиям совместимости. Для компьютеров, не соответствующих требованиям совместимости, действует профиль ограниченного доступа. Профили ограниченного доступа применяют IP-фильтры пакетов или идентификаторы виртуальной локальной сети (VLAN). Это означает, что узлам, имеющим профиль ограниченного доступа, предоставляется только ограниченный доступ к сети. Обычно доступны только серверы обновлений. Подробнее о серверах обновлений см. ниже.

Преимущество принудительной защиты 802.1X состоит в том, что работоспособность клиентов оценивается постоянно. Подключенные клиенты, которые стали несовместимыми, автоматически получают профиль ограниченного доступа. Клиенты с профилем ограниченного доступа, которые становятся совместимыми, получают возможность взаимодействовать с другими узлами в сети без ограничений. Предположим, например, что вышло новое обновление антивируса. Клиенты, которые в последнее время не посещали сервер обновлений, получают профиль ограниченного доступа, пока не установят это обновление. После успешного прохождения проверки клиенты вновь получают неограниченный доступ к сети.

Для поддержки принудительной защиты доступа к сети для 802.1x необходим компьютер под управлением Windows Server 2008 или 2008 R2 с ролью сервера сетевых политик. Кроме того, необходим коммутатор или оборудование

беспроводной точки доступа, совместимой с 801.1X. Клиенты должны работать под управлением Windows 7, Windows Vista, Windows XP с пакетом обновлений 3, Windows Server 2008 и 2008 R2, так как только эти ОС имеют клиент безопасности EAPHost.

---

**ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Принудительная защита для 802.1X**

Подробнее о принудительной защите доступа к сети для 802.1X см. по адресу <http://technet.microsoft.com/ru-ru/library/cc770861.aspx>.

---

**Принудительная защита доступа к сети для VPN**

Принудительная защита для VPN применяется к подключающимся клиентам VPN как способ обеспечения соответствия клиентов, получающих доступ к внутренней сети, требованиям к работоспособности. Принудительная защита для VPN действует путем ограничения доступа к сети для несовместимых клиентов при помощи фильтров пакетов. Вместо получения доступа ко всей сети, несовместимые VPN-клиенты имеют доступ только к группе серверов обновлений.

Как и в случае с принудительной защитой для 802.1X, работоспособность подключенного клиента постоянно контролируется. Если клиент становится несовместимым, применяются фильтры пакетов, ограничивающие доступ к сети. Если клиент перестает быть несовместимым, фильтры, ограничивающие доступ к сети, удаляются. Принудительная защита для VPN требует наличия инфраструктуры удаленного доступа и NPS-сервера. Этот метод применения использует клиент безопасности VPN, имеющийся в Windows 7, Windows Vista, Windows XP с пакетом обновлений 3, Windows Server 2008 и 2008 R2.

---

**ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Принудительная защита VPN**

Подробнее о принудительной защите доступа к сети для VPN см. по адресу <http://technet.microsoft.com/ru-ru/library/cc753622.aspx>.

---

**Принудительная защита доступа к сети для DHCP**

Принудительная защита доступа к сети для DHCP действует путем предоставления неограниченного доступа к информации об адресах IPv4 совместимым клиентам и ограниченного доступа несовместимым клиентам. В отличие от принудительной защиты VPN и 802.1X, принудительная защита DHCP применяется только во время получения или возобновления аренды адреса клиентом. При использовании этого способа следует избегать настройки длительной аренды DHCP, так как это снижает частоту проверок на совместимость.

Для развертывания принудительной защиты DHCP необходимо использовать DHCP-сервер под управлением Windows Server 2008 или 2008 R2, поскольку эти ОС имеют службу принудительной защиты DHCP. Клиент безопасности DHCP входит в состав службы клиента DHCP в Windows 7, Windows Vista, Windows XP с пакетом обновлений 3, Windows Server 2008 и 2008 R2.

Недостаток принудительной защиты DHCP состоит в том, что его можно обойти, настроив на клиенте статический IP-адрес. Настраивать IP-адрес вручную могут только пользователи с правами локальных администраторов, и если сотрудникам организации разрешено выполнять локальное администрирование, принудительная защита DHCP может быть не самым эффективным способом ограничения доступа к сети.

---

**ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Принудительная защита DHCP**

Подробнее о принудительной защите доступа к DHCP см. по адресу <http://technet.microsoft.com/ru-ru/library/cc733020.aspx>.

---

**Проверьте себя**

1. В каком способе принудительной защиты доступа к сети используются VLAN?
2. Какие способы принудительной защиты доступа к сети можно обойти, настроив статический IP-адрес?

**Ответы**

1. VLAN используются при принудительной защите доступа к сети для 802.1X.
2. Настройкой статического IP-адреса можно обойти принудительную защиту доступа DHCP.

---

**Принудительная защита доступа к сети для шлюза удаленных рабочих столов**

Принудительная защита доступа к сети для шлюза удаленных рабочих столов проверяет соответствие клиентов под управлением Windows 7, Windows Vista, Windows Server 2008 и 2008 R2, подключающихся к шлюзу удаленных рабочих столов из Интернета, требованиям к работоспособности, прежде чем разрешить им подключение к RDP-серверам из внутренней сети. Для настройки принудительной защиты для шлюза удаленных рабочих столов выполните следующее:

1. Включите проверку политики работоспособности NAP на сервере шлюза удаленных рабочих столов, чтобы сервер требовал от клиентов отчета о работоспособности.
2. Удалите все существующие RD-CAP. Имеющиеся RD-RAP удалять необязательно.
3. Настройте SHV Windows на сервере шлюза удаленных рабочих столов, отредактировав свойства SHV Windows в консоли сервера сетевой политики на сервере шлюза удаленных рабочих столов.
4. Создайте политики NAP на сервере шлюза удаленных рабочих столов с помощью мастера настройки NAP. Требуется создать две политики работоспособности (одну для совместимых и одну для несовместимых компьютеров), политику запроса подключения и три сетевые политики (для совместимых, несовместимых и не поддерживающих NAP клиентов).

---

**ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Принудительная защита шлюза удаленных рабочих столов**

Подробнее о принудительной защите доступа к сети для шлюза удаленных рабочих столов см. по адресу <http://technet.microsoft.com/ru-ru/library/cc771213.aspx>.

---



## Принудительная защита доступа к сети для DirectAccess

Можно включить NAP в инфраструктуру DirectAccess, чтобы гарантировать, что клиенты, пытающиеся подключиться с помощью DirectAccess из удаленных сетей, смогут успешно сделать это только при условии соответствия требованиям к работоспособности. Для использования NAP совместно с DirectAccess требуется такая же инфраструктура, как для принудительной защиты доступа IPsec. В сети должен иметься минимум один центр регистрации работоспособности (HRA), центры сертификации с поддержкой NAP, серверы политик работоспособности NAP и необходимые серверы обновлений. Если серверы обновлений и центры регистрации работоспособности расположены в интрасети, необходимо выполнить следующее:

- добавить IPv6-адреса HRA и серверов обновлений в список серверов управления, используя мастер настройки DirectAccess;
- настроить правило туннеля интрасети в GPO сервера DirectAccess, чтобы требовать сертификаты работоспособности.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ DirectAccess и NAP

Подробнее об использовании NAP для DirectAccess см. по адресу [http://technet.microsoft.com/en-us/library/ff528477\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/ff528477(Ws.10).aspx) (на английском языке).

---

## Серверы обновлений

Серверы обновлений обычно содержат обновления программ, антивирусные и антишпионские базы и используются для обновления клиентов, не прошедших проверку работоспособности. Серверы обновлений доступны из ограниченных сетей, в которые направляются несовместимые клиенты, не прошедшие проверку работоспособности системы. Серверы обновлений позволяют сделать эти клиенты совместимыми, чтобы те могли получить неограниченный доступ к сети. Группы серверов обновлений добавляются через узел **Группа серверов обновлений** (Remediation Server Group) консоли сервера сетевой политики (рис. 9-12).

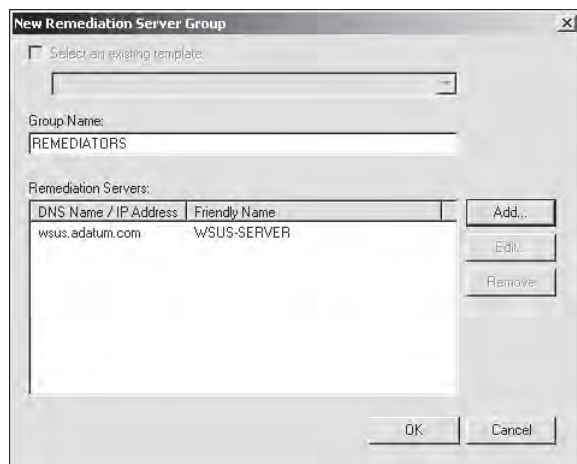


Рис. 9-12. Узел Группа серверов обновлений



## Режим мониторинга

Обычно NAR используется для ограничения доступа несовместимым клиентам, но если NAR развертывается впервые, следует использовать NAR в режиме мониторинга. Это связано с тем, что, вероятно, поначалу число несовместимых клиентов будет велико, и если сразу применить политики NAR, все они не смогут получить доступ к сети. Используя режим мониторинга, можно определить число клиентов, несовместимых с текущими политиками работоспособности. После этого можно предпринять действия для устранения проблем с клиентами, чтобы во время применения NAR, пришлось обновлять только небольшое число клиентов.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Режим мониторинга

Подробнее о настройке NAR для мониторинга, а не принудительной защиты, см. по адресу [http://technet.microsoft.com/en-us/library/dd314142\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd314142(WS.10).aspx) (на английском языке).

---

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Протокол HCAP

Протокол авторизации учетных данных узла (HCAP) позволяет интегрировать решение защиты доступа к сети с решением Cisco Network Admission Control. Протокол HCAP дает возможность NPS-серверу под управлением Windows Server 2008 или 2008 R2 выполнять авторизацию для клиентов доступа 802.1X Cisco. Подробнее о HCAP см. по адресу <http://technet.microsoft.com/ru-ru/library/cc732681.aspx>.

---

## Резюме

- Средства проверки работоспособности системы (SHV) — это набор условий, которым должен соответствовать компьютер, чтобы считаться работоспособным. Агент работоспособности системы (SHA) — инструмент, с помощью которого сервер NPS определяет, соответствует ли подключающийся клиент всем условиям SHV.
- К клиентам под управлением Windows Server 2008 и 2008 R2, Windows 7, Windows Vista и Windows XP с пакетом обновлений 3, можно применять четыре способа принудительной защиты доступа к сети: IPsec, DHCP, VPN и 802.1X. Принудительную защиту доступа к сети для шлюза удаленных рабочих столов можно использовать только в Windows 7, Windows Vista, Windows Server 2008 и 2008 R2.
- Серверы NPS устанавливаются как часть роли служб сетевой политики и доступа. Эти серверы располагаются там, где настраиваются политики работоспособности и SHV, которые определяют критерии работоспособности.
- Изоляция домена позволяет использовать IPsec для ограничения сетевого взаимодействия компьютеров, являющихся членами определенного домена.
- Forefront TMG 2010 — брандмауэр с расширенными возможностями, который можно устанавливать на серверы под управлением Windows Server 2008 и 2008 R2. Часто он устанавливается между сетью периметра и Интернетом.

## Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных на занятии 2. Эти вопросы предоставлены также в электронном виде на прилагаемом к книге компакт-диске.

---

### ПРИМЕЧАНИЕ Ответы

Ответы на вопросы и пояснения к их вариантам размещены в разделе «Ответы» в конце книги.

---

1. Вы хотите, чтобы к веб-серверу, работающему под управлением Windows Server 2008, для администрирования могли подключаться только работоспособные компьютеры, но все клиенты, независимо от работоспособности, могли получать доступ к веб-страницам на этом сервере. Какой из перечисленных способов принудительной защиты доступа к сети можно использовать, не настраивая ограничения брандмауэра или IP-адресов на этом сервере?
  - a. IPsec.
  - b. 802.1X.
  - c. DHCP.
  - d. VPN.
2. В сети имеются клиенты под управлением Windows Vista с пакетом обновлений 1 и Windows XP с пакетом обновлений 3. Вы хотите применять NAP для клиентов под управлением Windows Vista, но не Windows XP. Как это сделать? (Каждый ответ является частью решения. Выберите два.)
  - a. Создать политику сети, указывающую в качестве условия операционную систему.
  - b. Создать VLAN для всех клиентов под управлением Windows XP.
  - c. Настроить политику сети, позволяющую компьютерам под управлением Windows Vista пропускать проверку работоспособности.
  - d. Настроить политику сети, позволяющую компьютерам под управлением Windows XP пропускать проверку работоспособности.
3. Организация имеет контроллер домена с именем 2K3DC, работающий под управлением Windows Server 2003, и контроллер домена с именем 2K8DC, работающий под управлением Windows Server 2008. Домен имеет функциональный уровень Windows Server 2003. Служба DNS установлена на изолированный компьютер с именем DNS1, работающий под управлением Windows Server 2003 R2. Служба DHCP установлена на изолированный компьютер с именем DHCP1, работающий под управлением Windows Server 2003 R2. Роль NPS установлена на компьютер с именем NPS1, работающий под управлением Windows Server 2008. Какой из компьютеров необходимо обновить, чтобы можно было использовать принудительную защиту доступа к сети для DHCP?
  - a. 2K3DC.
  - b. DNS1.
  - c. DHCP1.
  - d. NPS1.

4. Какие из следующих ролей сервера должны быть доступны в сети, если вы планируете настроить правила IPsec, чтобы только работоспособные компьютеры могли взаимодействовать друг с другом? (Каждый ответ является частью решения. Выберите два.)
  - a. Центр регистрации работоспособности.
  - b. ЦС под управлением Windows Server 2008.
  - c. DHCP-сервер под управлением Windows Server 2008.
  - d. Сервер HCAP.
5. Помимо коммутаторов, совместимых с 802.1X, какие из следующих компонентов должны быть развернуты в сети для поддержки принудительной защиты доступа к сети для 802.1X? (Выберите два.)
  - a. Роль сервера NPS на компьютере под управлением Windows Server 2008.
  - b. Прокси-сервер RADIUS.
  - c. Клиент безопасности EAPHost на клиентских компьютерах.
  - d. Роль сервера HCAP на компьютере под управлением Windows Server 2008.

## Практикум. Установка и настройка NAR для DHCP

На этом практикуме вы настроите роль сервера сетевых политик для поддержки принудительной защиты доступа к сети для DHCP.

### Упражнение 1. Установка сервера сетевых политик и настройка DHCP

В этом упражнении вы установите роль сервера NPS на сервер VAN-DC1.

1. Зайдите на сервер VAN-DC1 под учетной записью пользователя Kim\_Akers.
2. Запустите оболочку PowerShell с повышенными привилегиями и введите следующие команды, чтобы убедиться, что службы ролей DHCP и NPS (если они установлены) удалены с сервера. Если эти роли установлены, необходимо перезагрузить сервер, выполнить вход, перезапустить PowerShell и вновь импортировать модуль ServerManager

```
Import-Module ServerManager
Remove-WindowsFeature DHCP, NPAS
```

3. В оболочке PowerShell с повышенными привилегиями введите следующие команды, чтобы установить роли сервера DHCP и NPS:

```
Add-WindowsFeature DHCP, NPAS
```

4. В меню **Администрирование** выберите **DHCP**. Откроется консоль DHCP. Щелкните правой кнопкой мыши узел DHCP и выберите команду **Управление авторизованными серверами** (Manage Authorized Servers). Щелкните **Авторизация** (Authorize). В диалоговом окне **Авторизация DHCP-сервера** (Authorize DHCP Server) введите имя **VAN-DC1** и щелкните **ОК**. Убедитесь, что DHCP-сервер имеет IP-адрес 10.10.0.10 и щелкните **ОК**. Выделите VAN-DC и щелкните **ОК**.

5. Откройте консоль **Службы** (Services). Настройте автоматический запуск службы DHCP-сервера. Запустите службу.
6. Перейдите в консоль **DHCP**, разверните узел **IPv4** под узлом **van-dc.adatum.com** и удалите область **Alpha Scope**.
7. Выделите и щелкните правой кнопкой мыши узел **IPv4** под узлом **van-dc.adatum.com**, после чего выберите команду **Новая область** (New Scope). Запустится мастер создания новой области. Щелкните **Далее**.
8. Введите имя области **NAP\_Scope** на странице **Имя области** (Scope Name). Щелкните **Далее**.
9. Укажите начальный IP-адрес **10.100.0.1** и конечный IP-адреса **10.100.0.254**. Установите значение **24** для параметра **Длина маски подсети** (Subnet Mask Length). Трижды щелкните **Далее**.
10. На странице **Настройка параметров DHCP** (Configure DHCP Options) установите переключатель **Настроить эти параметры позднее** (No, I Will Configure These Options Later) и щелкните **Далее**. Щелкните **Готово**.

## Упражнение 2. Настройка NPS

В этом упражнении вы настроите NPS.

1. Из меню **Администрирование** откройте оснастку **Сервер сетевых политик** (Network Policy Server).
2. На странице **Приступая к работе** (Getting Started) щелкните **Настройка NAP** (Configure NAP) (рис. 9-13).

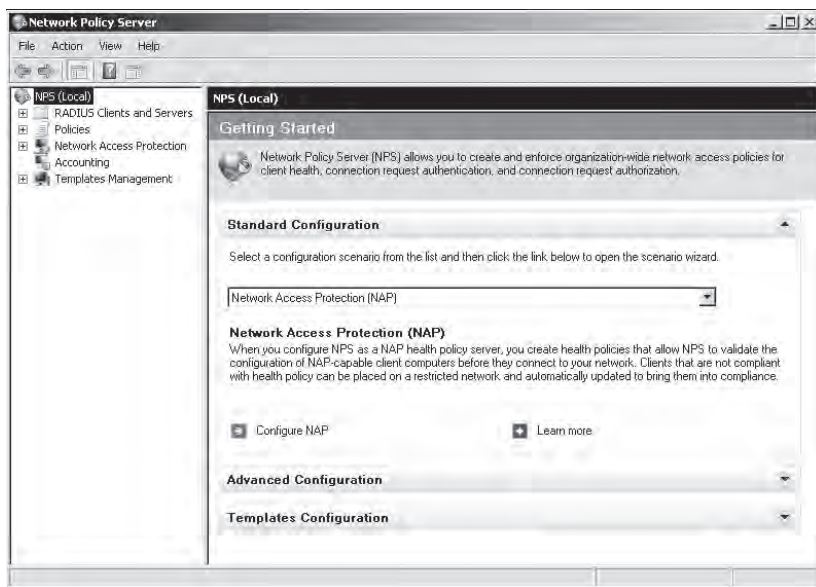


Рис. 9-13. Начало настройки NAP

3. Перейдите на страницу **Выбор способа подключения к сети для использования с NAP** (Select Network Connection Method For Use With NAP). В раскрывающемся меню выберите протокол DHCP и щелкните **Далее**.

4. На странице **Клиенты RADIUS (RADIUS Clients)** щелкните **Далее**.
5. На странице **Области DHCP (DHCP Scopes)** Щелкните **Добавить (Add)**. В поле **Укажите имя профиля, определяющего область DHCP (Specify The Profile Name That Identifies Your DHCP Scope)** введите **NAP\_Score** и щелкните **ОК**. Щелкните **Далее**.
6. На странице **Настройка групп компьютеров (Configure Machine Groups)** щелкните **Далее**.
7. На странице **Задайте группу сервера исправлений NAP и URL-адрес (Specify A NAP Remediation Server Group And URL)** щелкните **Далее**.
8. На странице **Определите политику работоспособности NAP (Define NAP Health Policy)** снимите флажок **Включить автообновление клиентских компьютеров (Enable Auto-Remediation Of Client Computers)** и установите переключатель **Разрешить полный доступ к сети для неподходящих для NAP клиентских компьютеров (Allow Full Network Access To NAP-Ineligible Client Computers)** (рис. 9-14). Щелкните **Далее**, а затем щелкните **Готово**.

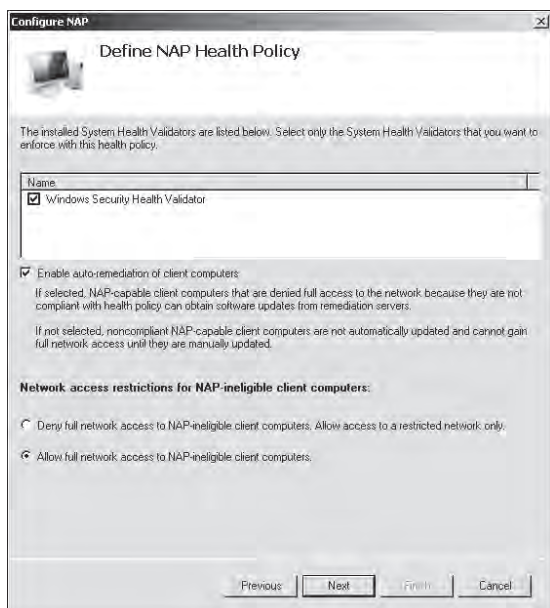


Рис. 9-14. Политика работоспособности NAP

## Упражнение 3. Настройка SHV

В этом упражнении вы настроите SHV для поддержки развертывания NAP для DHCP.

1. Откройте оснастку **Сервер сетевых политик (Network Policy Server)** и перейдите к узлу **Защита доступа к сети | Средства проверки работоспособности системы | Средства проверки работоспособности системы безопасности Windows | Параметры (Network Access Protection | System Health Validators | Windows Security Health Validator | Settings)**. На панели сведений

щелкните правой кнопкой **Настройка по умолчанию** (Default Configuration) и выберите команду **Свойства** (Properties). Откроется диалоговое окно **Средство проверки работоспособности системы безопасности Windows** (Windows Security Health Validator).

2. На панели сведений диалогового окна **Средство проверки работоспособности системы безопасности Windows** (Windows Security Health Validator), перейдите к разделу **Параметры обновлений безопасности** (Security Updates Settings). Установите флажок **Ограничить доступ для клиентов без всех установленных доступных обновлений безопасности** (Restrict Access For Clients That Do Not Have All Available Security Updates Installed) и измените уровень серьезности на **Средняя и выше** (Moderate And Above) (рис. 9-15).

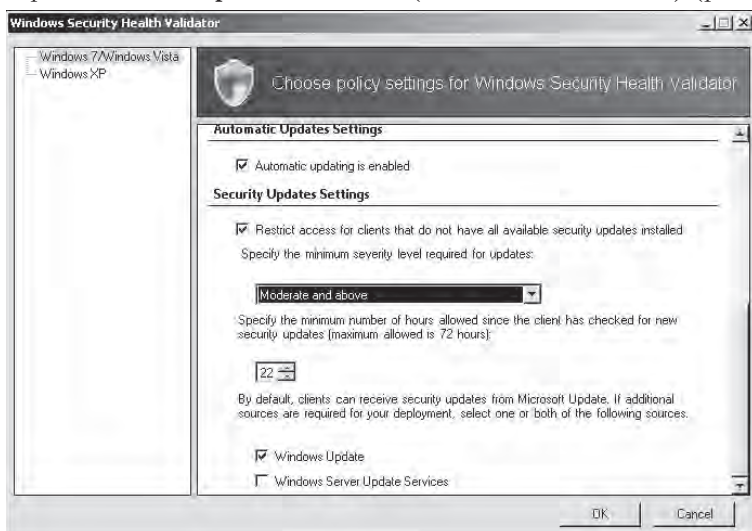


Рис. 9-15. Настройка уровня серьезности

## Закрепление материала главы

Чтобы попрактиковаться и закрепить знания, полученные при изучении этой главы, выполните следующее:

- прочитайте резюме главы;
- просмотрите список основных терминов, представленных в этой главе;
- выполните задания лабораторной работы, моделирующей реальные ситуации, требующие применения полученных знаний;
- выполните рекомендуемые упражнения;
- пройдите пробный тест.

## Резюме главы

- VPN-серверы под управлением Windows Server 2008 и 2008 R2 поддерживают протоколы PPTP, L2TP/IPsec и SSTP. Протокол SSTP могут использовать только компьютеры под управлением Windows Vista и Windows 7.

- VPN-серверы под управлением Windows Server 2008 R2 поддерживают VPN IKEv2. Подключения VPN IKEv2 поддерживают автоматическое повторное подключение, но их могут использовать только компьютеры под управлением Windows 7.
- DirectAccess — решение для постоянного удаленного доступа по протоколу IPv6. Для его использования необходим компьютер под управлением Windows Server 2008 R2 и клиенты под управлением Windows 7 Enterprise и Ultimate.
- Компьютер под управлением Windows Server 2008 или 2008 R2 можно настроить для работы в качестве сервера RADIUS, прокси-сервера RADIUS или клиента RADIUS.
- Доступно четыре способа локальной принудительной защиты доступа к сети: IPsec, DHCP, VPN и 802.1X. Можно также настроить принудительную защиту доступа к сети для шлюза удаленных рабочих столов и DirectAccess.

## Основные термины

Проверьте, знаете ли вы, что означают перечисленные ниже термины из этой главы:

- DirectAccess;
- EAP-TLS;
- IKEv2;
- L2TP/IPsec;
- PPP;
- PPTP;
- SSTP;
- RADIUS;
- VPN.

## Лабораторная работа

Для выполнения заданий лабораторной работы используйте знания о планировании установки и обновления сервера, полученные из этой главы. Ответы можно найти в разделе «Ответы» в конце книги.

### Задание 1. Удаленный доступ в Wingtip Toys

Компания Wingtip Toys имеет филиалы в Сиднее и Мельбурне (Австралия). Брандмауэры филиалов настроены таким образом, что пропускают трафик из Интернета только к узлам защищенной подсети через порты TCP 25, 80 и 443. В защищенной подсети филиала в Сиднее был установлен сервер шлюза удаленных рабочих столов. На следующей неделе в защищенной подсети филиала в Мельбурне будет развернут компьютер с несколькими сетевыми платами под управлением Windows Server 2008 R2 с установленной ролью удаленного доступа. Учитывая это, ответьте на вопросы:



1. Какой тип политики необходимо настроить, чтобы ограничить доступ в сиднейском филиале списком авторизованных пользователей?
2. Когда будет развернут сервер в Мельбурне, какой протокол VPN следует использовать для обеспечения доступа, если нельзя изменить существующие правила брандмауэра?
3. Какой метод принудительной защиты доступа к сети необходимо использовать в мельбурнском филиале?

## Задание 2. NAP в Coho Vineyard

Вы занимаетесь повышением сетевой безопасности в главном офисе компании Coho Vineyard. Компания имеет 20 серверов под управлением Windows Server 2008 R2 и 400 клиентов под управлением Windows 7 Enterprise. Вы намереваетесь развернуть NAP, однако необходимо учитывать следующие ограничения:

- Руководство компании хочет поработать полгода в тестовом режиме, прежде чем покупать новое оборудование. Пилотная программа должна позволять тестировать NAP и обеспечивать обновление несовместимых клиентов.
- Если пилотная программа окажется успешной, необходимо будет реализовать NAP таким образом, чтобы неработоспособным клиентам доступ к сети блокировался на уровне коммутатора.
- На данный момент компания не располагает необходимой аппаратной инфраструктурой для реализации ограничения доступа к сети на уровне коммутатора, однако после успешного завершения пилотной программы эта аппаратура будет куплена.
- Некоторые устаревшие сторонние системы, используемые в компании, не поддерживают протокол IPsec.

Учитывая это, ответьте на следующие вопросы:

1. Какой способ применения NAP следует использовать в Coho Vineyard во время выполнения пилотной программы?
2. Какой способ применения NAP следует использовать в Coho Vineyard после успешного выполнения пилотной программы?
3. Какие действия следует предпринять, чтобы разрешить обновление неработоспособных клиентов?

## Рекомендуемые упражнения

Чтобы успешно справиться с экзаменационными заданиями по темам этой главы, выполните следующие упражнения.

### Мониторинг и обслуживание политик безопасности

- Настройте сервер шлюза удаленных рабочих столов на изолированном компьютере под управлением Windows Server 2008 R2, у которого есть две сетевые карты, одна из которых подключена к общедоступной сети, например, к Интернету, а другая — к внутренней сети.
- Настройте и протестируйте RD-RAP и RD-CAP.

## Планирование ролей серверов служб инфраструктуры

- Создайте политику изоляции серверов с помощью брандмауэра Windows с повышенной безопасностью.
- Настройте принудительную защиту доступа к сети для IPsec, чтобы только работоспособные клиенты могли взаимодействовать друг с другом.

## Пробный экзамен

Тренировочные тесты на прилагаемом к книге компакт-диске позволяют проверить знания только по одной или сразу по всем темам сертификационного экзамена 70-646. Тестирование можно организовать так, чтобы оно проводилось как настоящий экзамен, а можно проходить в режиме обучения, просматривая правильные ответы и объяснения после каждого ответа.

---

### **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ** Пробный экзамен

Подробнее о пробном экзамене рассказано во Введении.

---

## Подготовка данных и планирование хранилищ

**Занятие 1. Подготовка данных**

**456**

**Занятие 2. Планирование хранилища Windows Server 2008 R2**

**475**

Данные — это память организации. Люди создают текстовые документы, таблицы и базы данных, чтобы когда-нибудь в будущем можно было извлечь эту сохраненную информацию. Хорошая стратегия подготовки и хранения данных должна обеспечивать их доступность для заинтересованных лиц при любых условиях, будь то сбой сети или неисправность жесткого диска. На этом занятии вы узнаете, как подготовить данные, чтобы предоставлять доступ к ним через распределенную файловую систему (DFS) или Microsoft SharePoint Foundation 2010. Вы узнаете, как подключать Windows Server 2008 R2 к iSCSI для сетей хранилищ данных (SAN) Fibre Channel, и как подготавливать логические номера устройств (LUN) для предоставления критически важным серверам централизованного хранилища данных.

### Темы экзамена

- Подготовка данных.
- Планирование хранилища.

### Прежде всего

Для выполнения упражнений этой главы потребуется:

- выполнить задания по установке, приведенные в Приложении.  
Дополнительной настройки не требуется.

#### **Реальный мир**

*Орин Томас*

Аппаратная избыточность очень важна и помогает сэкономить много времени. Я работал системным администратором на новом месте всего несколько недель, когда у сервера, за который отвечал мой коллега, вышел из строя жесткий диск. Как оказалось, на том сервере хранились почтовые

ящики руководства. Мой коллега тоже был недавно назначен на свою должность и работал лишь на пару недель дольше меня. По договоренности с поставщиком оборудования любой вышедший из строя компонент подлежал замене в течение двух часов, поэтому, как только мой коллега связался с поставщиком, тот сразу прислал к нам специалистов. Сервер имел три отсека для жестких дисков и BIOS с поддержкой RAID. Когда прибыли специалисты, мы узнали, что человек, который собирал сервер полтора года назад, почему-то решил не настраивать RAID, а вместо этого создал три отдельных тома. Операционная система находилась как раз на неисправном томе, и мой коллега потратил немало времени на восстановление работоспособности сервера. Если бы тот, кто собирал сервер полтора года назад, настроил встроенный аппаратный массив RAID 5, то восстановить сервер было бы проще, и он заработал бы гораздо раньше.

## Занятие 1. Подготовка данных

Данные бесполезны, если они недоступны. От тома, недоступного из-за неисправности оборудования, прока столько же, сколько от диска, упакованного в коробку от мороженого и спрятанного в холодильнике. На этом занятии подробно рассказывается о том, как обеспечить доступность данных, от основ создания резервных хранилищ на важных серверах организации до более сложных схем с использованием репликации данных и автономного доступа. Также вы узнаете, как индексировать данные и повышать эффективность поиска документов. Наконец, мы обсудим использование SharePoint Foundation 2010 для расширения возможностей совместного использования файлов и управления документами.

---

### Изучив материал этого занятия, вы сможете:

- ✓ Планировать доступ к данным.
- ✓ Настраивать DFS.
- ✓ Настраивать индексирование.
- ✓ Предоставлять автономный доступ к данным.
- ✓ Настраивать совместный доступ.

**Продолжительность занятия — примерно 60 мин.**

---

## Планирование доступности данных

Доступность данных имеет ключевое значение для работы организации и обеспечивается на нескольких уровнях. Данные должны быть доступны не только на уровне сервера, но и на уровне организации. Этого можно достичь тремя основными способами:

- **Аппаратная избыточность.** Доступ к данным в случае отказа аппаратного компонента обеспечивается за счет избыточности оборудования. Это может означать установку нескольких блоков питания, но чаще всего подразумевается настройка дисков в избыточных массивах. Подробнее об избыточных массивах см. ниже.

- **Избыточность серверов.** В случае неисправности сервера можно обеспечить доступ к данным путем добавления дополнительных серверов. Для этого может хватить настройки внутрисайтовой репликации с помощью DFS. Можно также использовать отказоустойчивые кластеры. Подробнее о хранилищах, используемых кластерами, см. на занятии 2. Подробнее о кластеризации рассказывается в гл. 11.
- **Избыточность сайтов.** Отказоустойчивые кластеры помогают в случае выхода из строя отдельного сервера, однако не обеспечивают доступность данных из других сайтов в случае неисправности каналов WAN-связи. Глобальная стратегия должна гарантировать доступность данных даже в том случае, если один из сайтов недоступен для других.

## Аппаратная избыточность

Чем большее значение для организации имеет сервер, тем больше внимания следует уделить обеспечению его доступности. Если бухгалтеры будут против того, чтобы потратить лишнюю пару тысяч долларов на приобретение дополнительного серверного оборудования, попросите их посчитать, во что обойдется вынужденное бездействие сотрудников организации, пока будут ремонтировать вышедший из строя сервер. Подробнее об избыточности дисков рассказывается далее; сейчас приведем лишь несколько общих правил подготовки серверной аппаратуры для обеспечения доступности.

- **Разработайте план действий на случай выхода оборудования из строя.** По возможности имейте на местах запасные компоненты, чтобы в случае неисправности быстро произвести замену и спокойно ждать, пока поставщик заменит неисправное оборудование.
- **Установите на сервер несколько блоков питания.** Поскольку источники питания и жесткие диски имеют подвижные части, именно эти компоненты чаще всего выходят из строя. Дополнительный блок питания обеспечит нормальную работу сервера в случае неисправности.
- **Подключайте блоки питания к разным источникам бесперебойного питания.** Худший момент, чтобы обнаружить, что ИБП не работает — сразу после отключения электричества. Но именно так часто и бывает.
- **Установите на сервер несколько сетевых карт.** Если сервер не имеет сетевых карт с возможностью замены во время работы, неисправность сетевой карты гарантированно приведет к отключению сервера от сети, как и перегоревшая материнская плата.
- **Установите дополнительные коммутаторы.** Резервные сетевые карты — это замечательно, однако нельзя допустить, чтобы все серверы центра данных стали недоступными из-за неисправности одного коммутатора.
- **Постарайтесь найти единые точки отказа и поработать с ними.** Чаще всего системный администратор должен быть пессимистом. Подумайте, отказ какой аппаратуры доставит наибольшие неудобства, а затем разработайте план по решению подобных проблем.

## Избыточный массив недорогих дисков

Избыточный массив недорогих дисков (RAID) позволяет использовать несколько дисков для обеспечения избыточности. Windows Server 2008 и 2008 R2 поддерживают несколько вариантов программных массивов RAID, в том числе зеркалирование дисков и чередование дисков с контролем четности. Хотя операционные системы поддерживают программные RAID, на практике чаще используются аппаратные RAID, а не программные. Аппаратный RAID реализуется через BIOS или посредством специальных контроллеров. Наиболее распространены следующие массивы RAID:

- **RAID 0 — чередование дисков.** Улучшает производительность, но в случае неисправности диска в массиве RAID 0 происходит потеря всех данных, находящихся на этом томе. Такой массив можно настроить средствами Windows Server 2008 R2. Требуется минимум два диска.
- **RAID 1 — зеркальное отражение дисков.** Один диск является полной копией другого. Преимущества в производительности по сравнению с обычным томом отсутствуют, однако, если диск выйдет из строя, его работу возьмет на себя зеркало. В Windows Server 2008 R2 такой массив можно настроить программно, однако при выходе из строя одного диска потребуются перезагрузка. Требуется не менее двух дисков.
- **RAID 5 — чередование дисков с контролем четности.** Повышает эффективность чередования дисков за счет вычислений для контроля четности, благодаря которому содержимое диска можно восстанавливать в случае неисправности одного из дисков в наборе. Требуется не менее трех дисков, при этом объем, эквивалентный одному диску занят данными для контроля четности. В Windows Server 2008 R2 такой массив можно создать программно.
- **RAID 1+0 — чередование зеркал.** Иногда называется «RAID 10». Например, создается три зеркальных набора, а затем чередуются данные в них. При использовании Windows Server 2008 R2 такой массив можно реализовать только на аппаратном уровне.
- **RAID 0+1 — зеркалирование чередующихся дисков.** На нескольких дисках создается массив с чередованием, а затем с помощью такого же числа дисков создается зеркальное отражение этого массива. При использовании Windows Server 2008 R2 такой массив можно реализовать только на аппаратном уровне.

Для создания тома RAID 5 программными средствами Windows Server 2008 R2 требуется не менее трех дисков и выполнение следующих действий:

1. Откройте диспетчер серверов и раскройте узел **Хранилище | Управление дисками** (Storage | Disk Management).
2. Убедитесь, что диски, которые вы хотите добавить в том RAID 5, исправны и инициализированы.
3. Щелкните правой кнопкой мыши один из дисков и выберите команду **Создать том RAID 5** (New RAID 5 Volume). Запустится мастер создания томов RAID 5.
4. Добавьте диски в том RAID (рис. 10-1) и щелкните **Далее**.

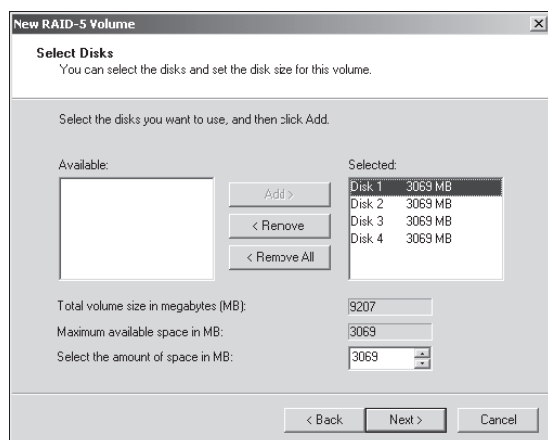


Рис. 10-1. Создание тома RAID

5. Назначьте тому букву диска или точку подсоединения и щелкните **Далее**.  
Отформатируйте диск и выберите метку тома, после чего щелкните **Готово**.

## Распределенная файловая система (DFS)

DFS предоставляет способ упрощения структуры общих папок организации и обеспечения избыточности данных путем репликации. DFS позволяет собирать общие папки, расположенные на разных серверах, в одно или несколько логически структурированных пространств имен. Вместо того чтобы запоминать, на каком сервере находится та или иная общая папка, можно обращаться к пространству имен DFS и находить там все общие папки.

Пространство имен и папки DFS можно реплицировать внутри узла и по каналам связи WAN. Пользователь, подключающийся к файлам в структурах общих папок в пространстве имен DFS, будет автоматически подключаться к общим папкам в своем узле AD DS (если таковые имеются), а не через WAN-связь. Можно создать несколько серверов DFS в одном сайте или распределить их по нескольким сайтам, чтобы в случае выхода из строя одного сервера пользователь все равно имел доступ к файлам в структуре общих папок. Архитектура DFS гарантирует, что изменение файла в общей папке DFS будет быстро и эффективно реплицировано во все остальные реплики этой общей папки DFS.

### Создание пространства имен DFS

Пространство имен можно создать в процессе установки службы роли **Управление DFS (DFS Management)** (рис. 10-2) или позже. Можно добавлять дополнительные пространства имен, щелкнув правой кнопкой узел **Пространства имен (DFS Namespaces)** в консоли **Управление DFS** и выбрав команду **Создать пространство имен (New Namespace)**. Пространства имен можно создавать на рядовом сервере или на контроллере домена под управлением Windows Server 2008. Однако нельзя создать больше одного пространства имен на сервере под управлением Windows Server 2008 Standard Edition. На серверах под управлением Windows Server 2008 Enterprise и Datacenter можно создать несколько пространств имен.



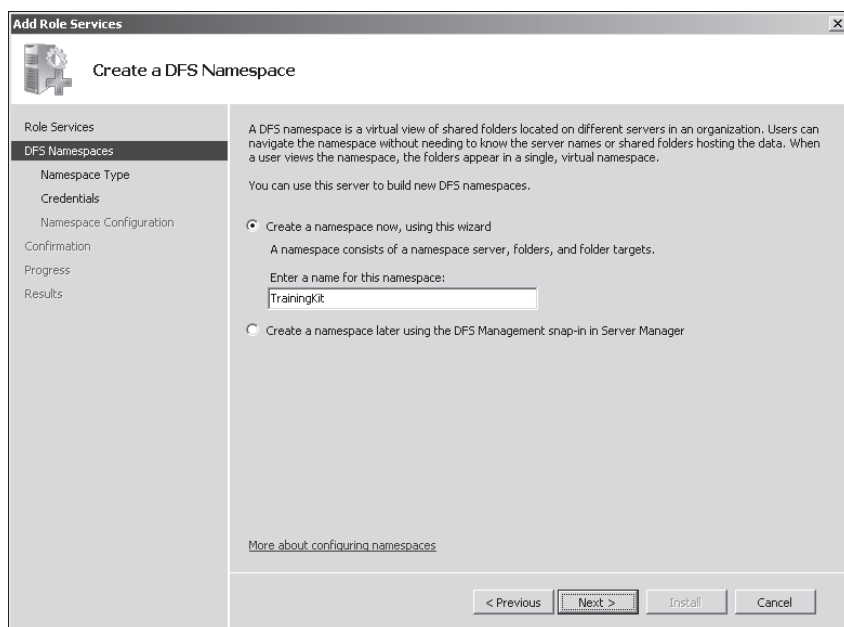


Рис. 10-2. Создание пространства имен во время установки службы роли Управление DFS

Пространство имен — это виртуальное представление общих папок в сети, путь к которому указывается в формате, аналогичном пути UNC к общей папке. Можно создавать пространства имен двух типов:

- Доменное пространство имен. В качестве корневого пространства имен используется домен, например, `\\adatum.com\MyNameSpace`. Для повышения доступности доменное пространство имен можно разместить на нескольких серверах пространств имен, а его метаданные хранить в AD DS. Можно создавать доменные пространства имен на одном или нескольких рядовых серверах или контроллерах домена в одном домене, а метаданные для пространства имен хранить в AD DS. Каждый сервер должен иметь том NTFS для хранения пространства имен. Наличие нескольких серверов пространств имен повышает доступность пространства имен. Доменное пространство имен не может быть кластерным ресурсом в отказоустойчивом кластере. Тем не менее, можно разместить пространство имен на сервере, который является также узлом в отказоустойчивом кластере, при условии, что это пространство имен будет использовать только локальные ресурсы на данном сервере.
- Изолированное пространство имен. В качестве корневого пространства имен используется сервер пространства имен, например, `\\ServerA\MyNameSpace`. Изолированное пространство имен хранится только на одном сервере. Такое пространство имен следует использовать, если организация не использует AD DS, если требуется создать одно пространство имен с более чем 5000 папками DFS, но сеть не поддерживает режим Windows Server 2008, или если требуется создать отказоустойчивый кластер для повышения надежности.

## Режим пространства имен Windows Server 2008

При выборе доменного пространства имен можно использовать режим Windows 2000 Server или Windows Server 2008. Последний поддерживает перечисление на основе доступа и обладает повышенной расширяемостью (более 5000 папок DFS). Microsoft рекомендует выбирать режим Windows Server 2008, когда это возможно. Для использования этого режима домен должен иметь функциональный уровень Windows Server 2008 или выше, а все серверы пространств имен должны работать под управлением Windows Server 2008 или более поздней версии. На рис. 10-3 показано создание доменного пространства имен в режиме Windows Server 2008.

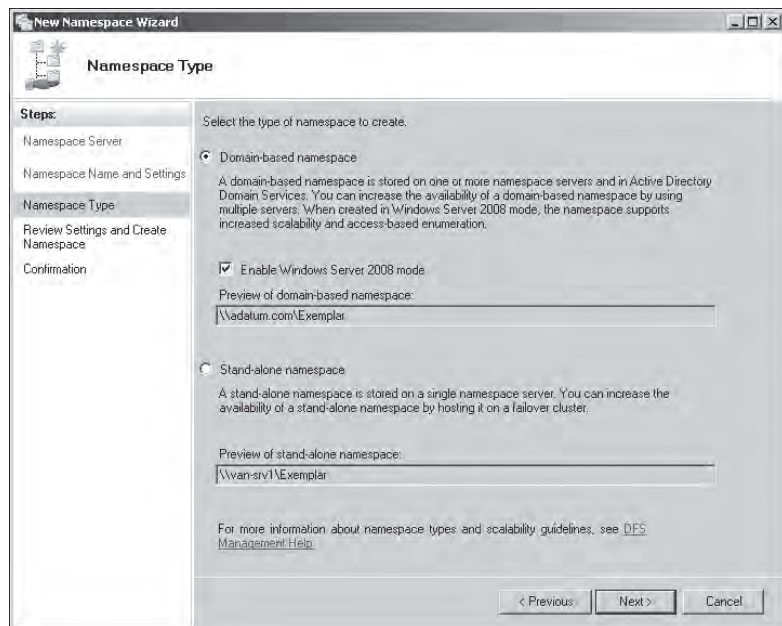


Рис. 10-3. Выбор режима пространства имен

---

### Дополнительная информация    Выбор пространства имен DFS

Подробнее о выборе пространства имен DFS см. по адресу [http://technet.microsoft.com/ru-ru/library/cc770287\(WS.10\).aspx](http://technet.microsoft.com/ru-ru/library/cc770287(WS.10).aspx).

---

## Настройка приоритета конечного объекта для переопределения сортировки ссылок

Ссылка — это упорядоченный перечень конечных объектов, которые клиент получает от контроллера домена или сервера пространств имен, когда пользователь переходит к корневому пространству имен или к папке, содержащей конечные объекты папки в пространстве имен. Все конечные объекты папки в ссылке сортируются в порядке, выбранном для корневого пространства имен или папки, например, в случайном порядке или по убыванию цены. Можно изменить порядок конечных объектов, установив приоритет для отдельных конечных объектов. Например, можно указать, что конечный объект будет рас-

полагаться первым (последним) в списке конечных объектов или первым (последним) в списке всех конечных объектов равной цены.

Чтобы задать приоритет корневому конечному объекту в доменном пространстве имен, раскройте узел пространства имен в консоли **Управление DFS**, выберите соответствующую папку, щелкните правой кнопкой мыши конечный объект папки и выберите команду **Свойства** (Properties). На вкладке **Дополнительно** (Advanced) (рис. 10-4) установите флажок **Переопределить сортировку ссылок** (Override Referral Ordering) и выберите один из следующих вариантов:

- **Первый из всех конечных объектов** (First Among All Targets) — пользователи всегда направляются к этому конечному объекту, если он доступен;
- **Последний из всех конечных объектов** (Last Among All Targets) — пользователи направляются к этому конечному объекту, только если недоступны все остальные;
- **Первый из конечных объектов равной цены** (First Among Targets Of Equal Cost) — пользователи направляются к этому конечному объекту раньше, чем к другим конечным объектам равной цены (обычно в том же сайте);
- **Последний из конечных объектов равной цены** (Last Among Targets Of Equal Cost) — пользователи никогда не направляются к этому конечному объекту, если доступны другие конечные объекты равной стоимости (обычно в том же сайте).

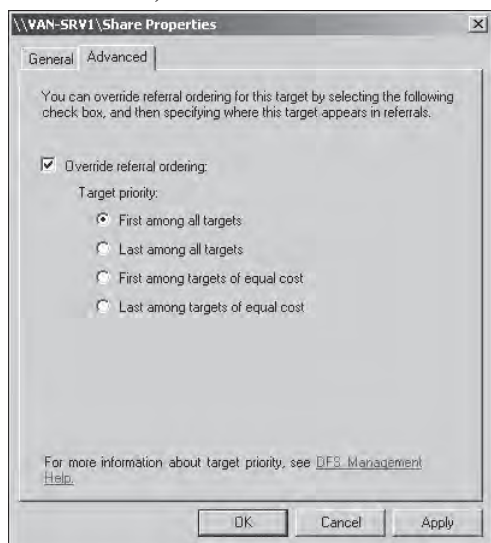


Рис. 10-4. Переопределение сортировки ссылок

## Перечисление на основе доступа

С помощью перечисления на основе доступа пользователи могут видеть только те файлы и папки на файловом сервере, к которым им разрешен доступ. Перечисление на основе доступа поддерживается в пространстве имен DFS, только если пространство имен является изолированным и находится на компьютере под управлением Windows Server 2008 или доменным пространством имен в режиме Windows Server 2008. Чтобы включить перечисление на основе доступа

в пространстве имен, измените свойства пространства имен, как показано на рис. 10-5.

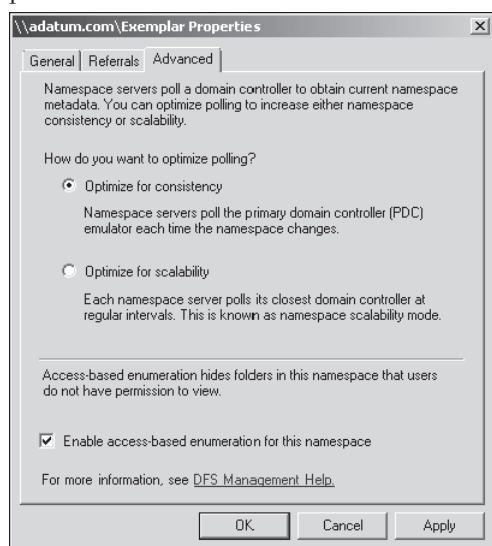


Рис. 10-5. Включение перечисления на основе доступа

## Настройка репликации

Репликация DFS (DFSR) обеспечивает репликацию изменений файлов в одной общей папке в другие реплики в сети. Можно создать новую группу репликации, используя мастер создания групп репликации, доступный в консоли **Управление DFS**, и добавить новые члены репликации с помощью мастера создания нового члена репликации. Мастер создания новых реплицированных папок, доступный в этой же консоли, добавляет копию папки в группу репликации. Обратите внимание на то, что добавленная копия папки реплицируется не сразу. Сначала на все контроллеры домена должны быть реплицированы параметры DFSR, а каждый член группы репликации должен опросить ближайший контроллер домена, чтобы получить новые параметры. Затраченное на это время зависит от задержки репликации AD DS и длительности интервала опроса (обычно 60 минут) у каждого участника репликации.

В процессе настройки групп репликации необходимо выбрать один из двух типов групп:

- **Универсальная группа репликации** (Multipurpose Replication Group) — самый распространенный тип групп репликации. Позволяет настраивать репликацию между двумя и более серверами.
- **Группа репликации для сбора данных** (Replication Group For Data Collection) — используется для передачи данных с узлового сайта в сайт филиала.

Чтобы создать группу репликации, выполните следующие действия:

1. Убедитесь, что компонент DFSR установлен на всех серверах, которые требуется добавить в группу репликации.

2. Откройте консоль **Управление DFS** и выберите узел **Репликация** (Replication). Щелкните **Новая группа репликации** (New Replication Group) на панели **Действия** (Actions). Запустится мастер создания новой группы репликации.
3. На странице **Тип репликации** (Replication Type) установите переключатель **Универсальная группа репликации** (Multipurpose Replication Group).
4. На странице **Имя и домен** (Name And Domain) введите имя для группы репликации, а затем укажите домен, с которым будет связана эта группа.
5. На странице **Члены группы репликации** (Replication Group Members) щелкните **Добавить** (Add) и добавьте компьютеры, которые будут входить в группу репликации. На этих компьютерах должен быть установлен компонент DFSR. Щелкните **Далее**.
6. На странице **Выбор топологии** (Topology Selection) выберите **Полная сетка** (Full Mesh). Подробнее о топологиях будет рассказано далее в данном уроке.
7. На странице **Расписание и пропускная способность группы репликации** (Replication Group Schedule And Bandwidth) выберите **Реплицировать постоянно с использованием следующей пропускной способности** (Replicate Continuously Using The Specified Bandwidth), убедитесь, что выбран параметр **Полная** (Full), и щелкните **Далее**.
8. На странице **Основной член репликации** (Primary Member) выберите сервер с исходным содержимым, которое требуется реплицировать на другие серверы, и щелкните **Далее**.
9. На странице **Папки для репликации** (Folders To Replicate) щелкните **Добавить**. В диалоговом окне **Добавить папку для репликации** (Add Folder To Replicate) (рис. 10-6) введите локальный путь к исходному серверу, где размещается содержимое, которое требуется реплицировать, щелкните **ОК**, а затем щелкните **Далее**.



Рис. 10-6. Выбор папки для репликации

10. На странице **Локальный путь <имя папки> на другие члены репликации** (Local Path Of <имя папки> On Other Members) измените свойства других членов группы репликации, чтобы указать локальный путь, по которому будет реплицирована папка. Щелкните **Далее**, а затем щелкните **Создать** (Create), чтобы создать группу репликации.

## Управление DFS

Можно настроить фильтры репликации, чтобы исключить из репликации определенные типы файлов. Для этого выполните следующее:

1. Выберите в консоли **Управление DFS** группу репликации, содержащую реплицированную папку, для которой требуется настроить фильтр.
2. На вкладке **Реплицированные папки** (Replicated Folders) панели сведений выберите папку, которую требуется изменить, а затем щелкните **Свойства** на панели **Действия** (Actions).
3. Измените параметры фильтров на вкладке **Общие** (General), как показано на рис. 10-7.

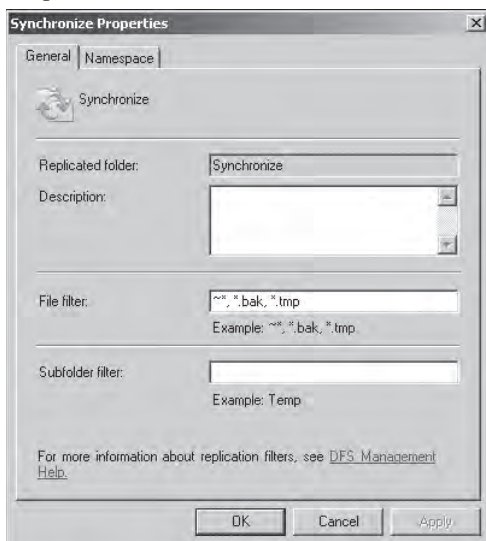


Рис. 10-7. Фильтр репликации

Когда участник репликации обнаруживает новый или измененный фильтр, он сканирует его базу данных и удаляет записи файлов, которые соответствуют параметрам фильтра. Поскольку файлы больше не включены в базу данных, дальнейшие изменения файлов игнорируются. Когда участник репликации обнаруживает, что фильтр удален, он сканирует файловую систему, добавляет записи для всех файлов, которые соответствуют параметрам удаленного фильтра, и реплицирует файлы.

Можно включить общий доступ к файлам в реплицированной папке и указать, следует ли добавить (опубликовать) папку в пространство имен DFS. Для этого выполните следующее:

1. В консоли **Управление DFS** щелкните группу репликации, содержащую реплицированную папку, к которой требуется открыть общий доступ.

2. На вкладке **Реплицированные папки** (Replicated Folders) панели сведений щелкните правой кнопкой мыши реплицированную папку, к которой требуется открыть общий доступ, и выберите команду **Доступ и публикация в пространстве имен** (Share And Publish In Namespace).
3. В мастере предоставления общего доступа и публикации реплицированной папки щелкните **Открыть общий доступ к реплицированной папке** (Share The Replicated Folder) и следуйте дальнейшим инструкциям мастера, указав, следует ли опубликовать папку, когда получите соответствующий запрос. Если нет существующего пространства имен, можно создать его на странице мастера **Путь к пространству имен** (Namespace Path). Для этого щелкните **Обзор** (Browse), а затем щелкните **Новое пространство имен** (New Namespace).

### Определение топологии репликации

Топология репликации определяет логические подключения, используемые DFS для репликации файлов между серверами. Выбирая или изменяя топологию, помните, что между выбранными членами репликации создаются два одно-сторонних подключения, позволяющих перемещать данные в обоих направлениях. Чтобы создать или изменить топологию репликации, в консоли **Управление DFS** щелкните правой кнопкой группу репликации, для которой требуется определить новую топологию, и выберите команду **Новая топология** (New Topology). Запустится мастер создания топологии, позволяющий выбрать один из следующих параметров:

- **Звезда** (Hub and spoke). Требуется три или более участников репликации. Для каждого лучевого члена нужно выбрать обязательный центральный член и дополнительный центральный член. Дополнительный член нужен для репликации лучевого члена в случае неисправности одного из центральных членов. Если указать больше одного центрального члена, то между центральными членами будет топология «полная сетка».
- **Полная сетка** (Full mesh). В этой топологии каждый член выполняет репликацию со всеми остальными членами группы репликации. Эта топология эффективна, когда в группе репликации имеется 10 или менее членов.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ DFS в Windows Server 2008 R2

Подробнее о DFS в Windows Server 2008 R2 см. по адресу [http://technet.microsoft.com/ru-ru/library/ee307957\(Ws.10\).aspx](http://technet.microsoft.com/ru-ru/library/ee307957(Ws.10).aspx).

---

#### Проверьте себя

- Что необходимо установить на серверы перед добавлением их в группу репликации?

#### Ответ

- Службу роли **Репликация DFS**.



## Настройка автономного доступа к данным

Автономные файлы позволяют получать доступ к файлам, находящимся в общих папках, когда они не подключены к сети. Чтобы файл можно было использовать в автономном режиме, в локальном зашифрованном кэше создается его копия, которая синхронизируется с общей папкой, когда восстанавливается подключение к сети. В редких случаях, когда файл изменяется и в общей папке, и на клиенте в автономном режиме, пользователь получает уведомление и запрос на разрешение ситуации путем создания копии, отмены изменений или замены измененного файла, хранящегося на файловом сервере. Для настройки параметров автономных файлов можно использовать консоль **Управление общими ресурсами и хранилищами** (Share and Storage Management). Настроить доступ пользователей к автономным файлам можно с помощью групповой политики.

В консоли **Управление общими ресурсами и хранилищами** выберите общую папку на вкладке **Общие ресурсы** (Shares) и щелкните **Свойства** (Properties). Затем щелкните **Дополнительно** (Advanced) на вкладке **Общий доступ** (Shares) в диалоговом окне свойств общей папки. После этого вы получите доступ к параметрам на вкладке **Кэширование** (Caching) диалогового окна **Дополнительно** (Advanced) (рис. 10-8).

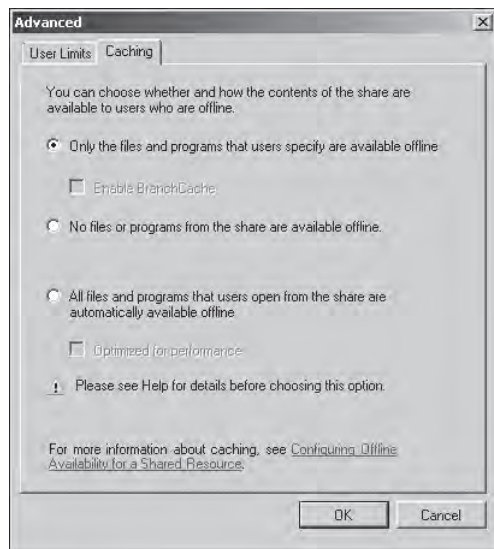


Рис. 10-8. Параметры автономных файлов

Для каждого общего ресурса можно выбрать параметры доступа в автономном режиме. При желании это можно сделать для всех общих ресурсов на сервере. Доступны следующие параметры:

- **Вне сети доступны только указанные пользователем файлы и программы** (Only The Files And Programs That Users Specify Are Available Offline). Это параметр по умолчанию. Никакие файлы и программы не доступны в автономном режиме без разрешения пользователя. Пользователь выбирает файлы, которые будут синхронизированы и доступны в автономном режиме.

Этот параметр следует использовать, если пользователи достаточно опытны и могут самостоятельно выбирать файлы, с которыми хотят работать. Если на сервере установлен компонент BranchCache, его можно использовать совместно с этим параметром.

- **Все открываемые пользователем файлы и программы доступны в автономном режиме** (All Files And Programs That Users Open From The Share Are Automatically Available Offline). Каждый раз, когда пользователь получает доступ к общей папке или тому и открывает файл, этот файл автоматически становится доступным для пользователя в автономном режиме. Преимущество такого подхода в том, что пользователям не нужно выбирать файлы для синхронизации.
- **Все файлы или программы с общего ресурса недоступны в автономном режиме** (No Files Or Programs From The Share Are Available Offline). Этот параметр не позволяет клиентскому компоненту для работы с автономными файлами делать копии файлов и программ из общего ресурса. Обычно этот параметр выбирается, когда требуется запретить хранение защищенных общих ресурсов в автономном режиме на незащищенных компьютерах.

---

#### **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Автономные файлы**

Подробнее о настройке функций автономных файлов см. по адресу <http://technet.microsoft.com/ru-ru/library/cc732663.aspx>.

---

## **Настройка индексирования в службе поиска Windows**

Служба поиска Windows предоставляет решение для индексирования — создает индекс наиболее распространенных файловых и нефайловых типов данных на сервере. Индексирование файлов и типов данных дает возможность выполнять быстрый поиск файлов на сервере с клиентов под управлением Windows 7, Vista, Windows XP или Windows Server 2003 с установленной панелью поиска Windows.

Вместо этой службы можно установить старую службу индексирования, которая использовалась в предыдущих версиях Windows, как часть службы роли Windows Server 2003. Однако это требуется только в том случае, если на сервере установлены нестандартные приложения, требующие запуска этой службы. Службу поиска Windows и службу индексирования нельзя установить на один компьютер, поэтому Microsoft рекомендует обновлять все приложения, которым требуется служба индексирования, чтобы они могли использовать службу поиска Windows, предоставляющую ряд улучшений, особенно в области расширяемости, производительности и удобства использования.

### **Выбор томов и папок для индексирования**

При добавлении службы поиска Windows предоставляется возможность выбрать тома для индексации. Всегда следует индексировать только общие ресурсы. Служба поиска Windows позволяет искать файлы на сервере с клиента, так что нет особого смысла индексировать папки, к которым нельзя получить доступ из сети.

Microsoft рекомендует выбрать том, который будет использоваться исключительно для размещения общих папок. При установке службы роли не обязательно указывать том, и добавлять общие папки можно после установки службы. После установки службы поиска Windows будут выбраны пути индексирования по умолчанию, даже если том для индексирования не указан. Расположения по умолчанию можно просмотреть, открыв апплет Панели управления **Параметры индексирования** (Indexing Options).

После добавления нового расположения начнется индексирование. Если требуется прервать индексирование, чтобы сделать что-то еще, щелкните **Пауза** (Pause). Как обычно, сначала требуется утвердительно ответить в диалоговом окне УАС. Можно также щелкнуть **Дополнительно** (Advanced) в диалоговом окне **Параметры индексирования** (Indexing Options), чтобы настроить дополнительные параметры индексирования.

На вкладке **Параметры индексирования** (Index Settings) этого диалогового окна (рис. 10-9) можно включить индексирование зашифрованных файлов и различение похожих слов с диакритическими знаками. Диакритические знаки — это отметки над, поперек или под буквами (например, штрихи). Можно также перестроить индекс или изменить путь к нему. Если изменить путь к индексу, потребуется остановить и перезапустить службу.

На вкладке **Типы файлов** (File Types) того же окна можно добавлять или удалять типы файлов, которые требуется индексировать, и определять, как следует индексировать файлы: только по свойствам или по свойствам и по содержанию. Можно также указать и добавить расширение, отсутствующее в списке.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Служба поиска Windows

Подробнее о службе поиска Windows см. по адресу [http://technet.microsoft.com/en-us/library/dd364879\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd364879(WS.10).aspx) (на английском языке).

---

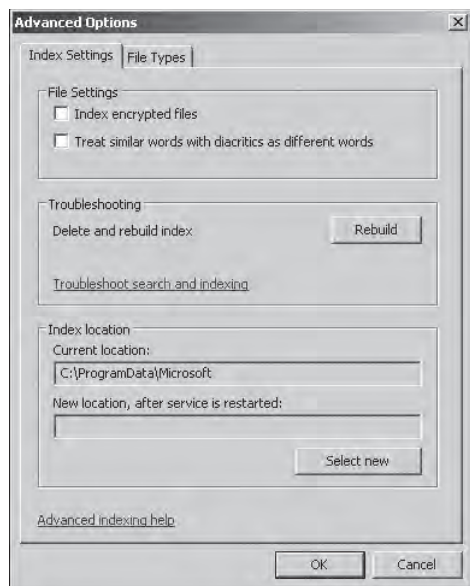


Рис. 10-9. Дополнительные параметры индексирования

## SharePoint Foundation 2010

SharePoint Foundation 2010 — наследник служб Windows SharePoint, предоставляющий более широкие возможности по совместной работе над файлами, чем DFS и стандартные общие папки. SharePoint Foundation 2010 обладает многими функциями более функционального продукта SharePoint Server 2010, но, в отличие от него, является бесплатным для пользователей, имеющих лицензию на Windows Server 2008 или 2008 R2. SharePoint Foundation 2010 поддерживает службы доступа, службы Business Connectivity Services, централизованное администрирование, мониторинг работоспособности, изолированные решения и PowerShell, однако не имеет расширенных функций, таких как управление цифровыми активами, система Enterprise Search, службы Excel, управляемые метаданные, службы PerformancePoint Services, управление записями, социальные вычисления и службы Visio Services.

SharePoint Foundation 2010 позволяет организациям применять функции рабочего процесса и совместной работы для подготовки данных. Это означает, что можно разрешать пользователям создавать собственные библиотеки документов и определять, кто может открывать и изменять файлы. Кроме того, SharePoint Foundation 2010 позволяет создавать разные версии файлов, благодаря чему изменения, сделанные в одном документе, могут быть легко отменены другим автором. При использовании DFS или стандартных общих папок это затруднительно, поскольку инфраструктура стандартных общих папок не предназначена для отслеживания версий документов, а только для хранения последней копии обновленного документа.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ SharePoint Foundation

SharePoint Foundation — крупный продукт, который вполне заслуживает отдельного экзамена. Главное, что вы должны помнить — SharePoint следует развертывать, если требуется предоставить пользователям инфраструктуру для совместной работы и создания версий файлов.

---

SharePoint Foundation 2010 работает, используя веб-приложения, узлы, семейства узлов и библиотеки документов. Веб-приложение представляет собой набор параметров и функций, связанных с URL. После установки SharePoint Foundation 2010 на сервере доступно веб-приложение по умолчанию, связанное с URL-адресом по умолчанию. Важно отметить, что приложения Microsoft Office могут подключаться к SharePoint, как к обычной общей папке. Это означает, что вместо подключения к веб-сайту, загрузки документа и последующего редактирования этого документа весь процесс может выполняться прозрачно, как будто пользователь работает с документом из общей папки DFS.

Чтобы создать новый сайт в веб-приложении SharePoint Foundation 2010, выполните следующее:

1. Откройте центр администрирования SharePoint. На странице узла центра администрирования (рис. 10-10) щелкните **Управление веб-приложениями** (Manage Web Applications).

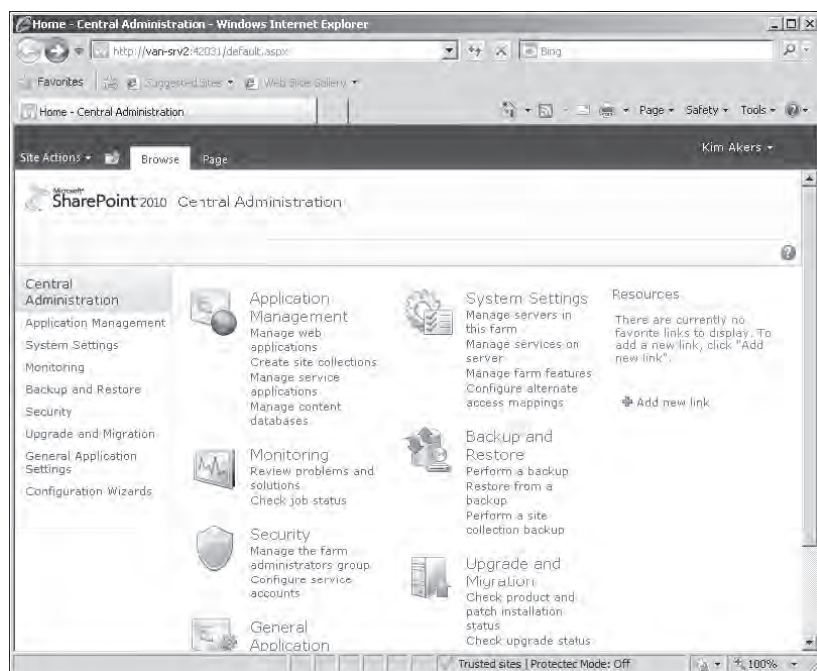


Рис. 10-10. Центр администрирования SharePoint Foundation

- Щелкните **Создать** (New) на панели инструментов, чтобы создать новое веб-приложение.
- Просмотрите параметры на странице **Создать новое веб-приложение** (Create New Web Application), в частности, общедоступный URL сайта, номер порта и учетную запись безопасности, используемые веб-приложением, и щелкните **ОК**.

Библиотеки SharePoint — это наборы документов. При использовании SharePoint для хранения документов общие документы хранятся в библиотеках SharePoint. Для управления общими документами внутри библиотеки веб-приложения SharePoint Foundation подключитесь к приложению с помощью Internet Explorer и выполните следующее:

- Откройте Internet Explorer и перейдите к веб-приложению SharePoint. На странице приветствия щелкните **Общие документы** (Shared Documents).
- В разделе **Инструменты библиотек** (Library Tools) щелкните **Документы** (Documents), чтобы перейти в меню **Документы**.
- Щелкните **Новая папка** (New Folder), чтобы создать папку с документами. Введите имя папки в диалоговом окне (рис.10-11) и щелкните **Сохранить**.
- На сервере щелкните **Пуск | Все программы | Стандартные** и откройте WordPad.
- Создайте документ с именем **Example** и сохраните его в формате Office Open XML на рабочем столе.
- Введите имя папки **Example** в Internet Explorer и щелкните **Отправить документ** (Upload Document) на ленте.

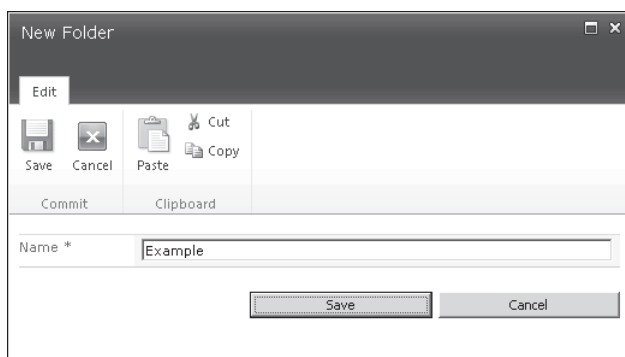


Рис. 10-11. Новая папка SharePoint

7. Перейдите к документу **Example** на рабочем столе и щелкните **ОК**.
8. Наведите курсор мыши на документ, чтобы появилось меню, изображенное на рис. 10-12, а затем щелкните **Извлечь** (Check Out). После успешного извлечения документа щелкните **Просмотр свойств** (View Properties).

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ SharePoint Foundation 2010

Подробнее о SharePoint Foundation 2010 см. по адресу <http://technet.microsoft.com/ru-ru/library/cc288070.aspx>.

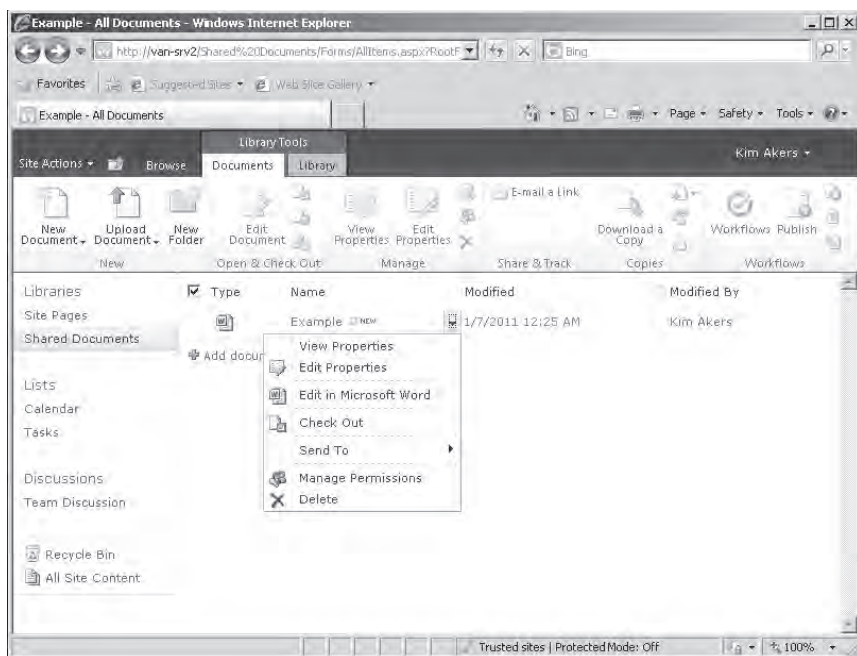


Рис. 10-12. Извлечение документа

## Резюме

- Windows Server 2008 и 2008 R2 поддерживают программные массивы RAID 0 (чередование), RAID 1 (зеркальное отражение) и RAID 5 (чередование с контролем четности).
- Инструмент **Пространства имен DFS** в оснастке **Управление DFS** позволяет объединять общие папки из разных расположений в логически структурированные пространства имен. Пользователи видят каждое пространство имен как одну общую папку с набором подпапок. Эта структура обеспечивает отказоустойчивость и возможность автоматического подключения пользователей к локальным общим папкам, если те доступны.
- Инструмент **Репликация DFS** в оснастке **Управление DFS** позволяет управлять репликацией DFS, которая предоставляет механизм репликации с несколькими хозяевами, с помощью которого можно синхронизировать папки на серверах в локальных или глобальных сетях. При этом обновляются только те файлы, которые были изменены с момента последней репликации. DFSR можно использовать совместно с пространствами имен DFS или самостоятельно.
- С помощью консоли **Управление общими ресурсами и хранилищами** можно настраивать автономный доступ к файлам и программам в общей папке или томе на сервере под управлением Windows Server 2008.
- Служба поиска Windows индексирует файлы, папки и тома, позволяя выполнять быстрый поиск файлов на сервере с клиента. Параметры индексирования можно настроить с помощью апплета Панели управления **Параметры индексирования**.

## Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных на занятии 1. Эти вопросы предоставлены также в электронном виде на прилагаемом к книге компакт-диске.

---

### ПРИМЕЧАНИЕ Ответы

Ответы на вопросы и пояснения к их вариантам размещены в разделе «Ответы» в конце книги.

---

1. Том какого типа следует создать в Windows Server 2008 R2, если имеется два диска, а отказоустойчивость важнее производительности?
  - a. RAID 0.
  - b. RAID 1.
  - c. RAID 5.
  - d. RAID 1+0.
2. Вы планируете развертывание доменного пространства имен DFS в домене wingtiptoy.com. Пространство имен получит имя Accounting, сервер пространства имен, на котором будет располагаться это пространство имен — имя Actuary-Alpha. Какое имя будет использоваться для доступа к папкам из этого пространства имен?



- a. \\Accounting\Wingtiptoys.com.
  - b. \\wingtiptoys.com\Accounting.
  - c. \\Accounting\Actuary-Alpha.
  - d. \\Actuary-Alpha\Accounting.
3. Вы хотите предоставить группе пользователей из исследовательского отдела вашей организации возможность совместной работы и поддержки версий. Какая технология позволит сделать это с минимумом административных усилий?
- a. Диспетчер ресурсов файлового сервера.
  - b. Изолированная DFS.
  - c. Доменная DFS.
  - d. SharePoint Foundation 2010.
4. Вы хотите, чтобы пользователи могли видеть файлы и папки только в пространстве имен DFS, к которому у них есть доступ. Какой из следующих компонентов позволит сделать это?
- a. Переопределение сортировки ссылок.
  - b. Автономные файлы.
  - c. BranchCache.
  - d. Перечисление на основе доступа.
5. Вы настраиваете автономный доступ на файловом сервере под управлением Windows Server 2008 R2. Пользователи в домене вашей организации используют клиенты под управлением Windows 7 Enterprise, настроенные с помощью групповой политики для использования автономных файлов. Вы хотите, чтобы исполняемые файлы, которые клиент запускает из общего ресурса, автоматически кэшировались на этом клиенте, и в следующий раз, когда клиенту потребуется запустить один из этих исполняемых файлов, он получал доступ к своему локальному кэшу, а не к общему ресурсу на сервере. В оснастке **Управление общими ресурсами и хранилищами** (Share and Storage Management) вы открыли вкладку **Автономный режим** (Offline) диалогового окна дополнительных свойств общей папки, где хранятся файлы, которые требуется синхронизировать и использовать в автономном режиме. Какие параметры следует настроить? (Каждый ответ является частью решения. Выберите два.)
- a. Установить переключатель **Вне сети доступны только указанные пользователем файлы и программы** (Only The Files And Programs That Users Specify Are Available Offline).
  - b. Установить переключатель **Все файлы или программы с общего ресурса недоступны в автономном режиме** (No Files Or Programs From The Share Are Available Offline).
  - c. Установить переключатель **Все открываемые пользователем файлы и программы доступны в автономном режиме** (All Files And Programs That Users Open From The Share Are Automatically Available Offline).
  - d. Установить флажок **Оптимизировать производительность** (Optimize For Performance).

## Занятие 2. Планирование хранилища Windows Server 2008 R2

На этом занятии рассказывается о LUN, SAN, iSCSI, многопутевом вводе-выводе (MPIO), службе виртуальных дисков (VDS) и Fibre Channel. Хотя эти сокращения могут показаться устрашающими, к концу занятия вы поймете, как работают обозначаемые ими технологии, и сможете планировать развертывание SAN в среде Windows Server 2008.

---

### Изучив материал этого занятия, вы сможете:

- ✓ Планировать назначение LUN.
- ✓ Планировать развертывание SAN iSCSI.
- ✓ Планировать развертывание SAN Fibre Channel.
- ✓ Планировать MPIO.
- ✓ Планировать развертывание VDS.

**Продолжительность занятия — примерно 60 мин.**

---

### Логические номера устройств

Логический номер устройства (LUN) — это логическая ссылка на часть подсистемы хранилища данных. LUN может представлять диск, раздел диска, целый массив дисков или раздел массива дисков в подсистеме хранилища. Концептуально есть сходства с понятием тома, которое тоже может обозначать часть диска, целый диск или несколько дисков. При назначении LUN серверу этот номер действует как физический диск, с которым сервер может выполнять операции чтения и записи. LUN используются для упрощения управления ресурсами хранилища в SAN.

Можно использовать любой тип LUN, который поддерживается развертываемой подсистемой хранилища данных. Существуют следующие типы LUN:

- **простой** — использует весь физический диск или его часть. Выход из строя диска в простом LUN приводит к потере всех данных, хранящихся в этом LUN;
- **составной** — простой LUN, который охватывает несколько физических дисков. Выход из строя любого из дисков составного LUN приводит к потере всех данных, хранящихся на LUN;
- **чередующийся** — данные записываются на несколько физических дисков. Этот тип LUN, называемый также RAID 0, обладает улучшенной производительностью ввода-вывода, благодаря возможности чтения и записи данных одновременно на несколько дисков. Как и в случае с составным LUN, выход из строя одного диска приводит к потере всех данных;
- **отраженный** — отказоустойчивый LUN, называемый также RAID 1. На двух физических дисках создаются идентичные копии LUN. Все операции чтения и записи производятся одновременно на двух дисках. Если один диск выйдет из строя, LUN продолжает работу на неповрежденном диске;

- **чередующийся с контролем четности** — этот тип LUN, называемый также RAID 5, обладает отказоустойчивостью и улучшенной производительностью при чтении, но производительность записи ограничена из-за вычисления четности. Этот тип LUN требует наличия минимум трех дисков, при этом сегмент хранилища, эквивалентный объему одного диска, резервируется для данных проверки четности. Этот тип LUN сохраняет данные, если один диск выйдет из строя, но если одновременно выйдут из строя два диска, все данные будут потеряны. Если диск выйдет из строя, его следует заменить как можно быстрее.

Мастер подготовки хранилища, который можно запустить из диспетчера хранилища для сетей SAN (Storage Manager For SANs), позволяет создавать LUN для подсистемы хранилища диска Fibre Channel или iSCSI. Прежде чем создать LUN, убедитесь, что выполняются следующие требования:

- подсистема хранилища данных поддерживает VDS;
- установлен поставщик аппаратуры VDS для подсистемы хранилища данных;
- в подсистеме хранилища имеется свободное место;
- если LUN назначается серверу, должны быть настроены подключения сервера. Подробнее о настройке подключений сервера к сетям SAN iSCSI и Fibre Channel рассказывается далее на этом занятии.

После назначения LUN серверу или кластеру можно создать том на диске. Производительность и степень надежности диска зависят от типа LUN.

## Управление LUN

Можно расширить LUN, если имеется свободное место в подсистеме, в которой этот LUN создан. Расширение LUN не приведет к расширению его раздела в файловой системе. Расширение разделов выполняется при помощи оснастки **Управление дисками** (Disk Management) или аналогичного инструмента на сервере, имеющем доступ к LUN, после расширения LUN с помощью диспетчера хранилищ для сетей SAN.

Удаление LUN ведет к удалению всех данных со всех томов в этом LUN. Эта операция необратима. Удалить LUN можно, только когда отключены все приложения, имеющие доступ к LUN. Альтернативой удалению LUN является отмена его назначения. Когда отменяется назначение LUN, он становится невидимым для сервера или кластера, однако хранящиеся в нем данные сохраняются. Позже можно вновь назначить LUN. Номера LUN удаляются с помощью диспетчера хранилищ для сетей SAN. Выберите LUN конечного объекта под узлом **Управление LUN** (LUN Management) и щелкните **Удалить LUN** (Delete LUN) на панели **Действия**. Для отмены назначения LUN выполните те же действия, но щелкните **Отменить назначение LUN** (Unassign LUN) вместо **Удалить LUN**.

## Служба виртуальных дисков (VDS)

VDS предоставляет стандартный набор интерфейсов API, составляющих единый интерфейс для управления дисками. VDS предлагает готовое решение для управления аппаратурой хранилища и дисками и дает возможность создавать тома на этих дисках. Это означает, что можно использовать единый инструмент

для управления устройствами в смешанной среде хранилища вместо инструментов, предлагаемых различными поставщиками аппаратуры. Чтобы иметь возможность управлять LUN с помощью диспетчера хранилищ для сетей SAN, необходимо установить соответствующий аппаратный поставщик VDS. Обычно он предоставляется производителем аппаратуры. Прежде чем приобретать запоминающее устройство для использования в сетях SAN организации, следует убедиться, что существует совместимый аппаратный поставщик VDS.

VDS определяет программный и аппаратный интерфейсы поставщика. Каждый из этих поставщиков реализует различные части API VDS. Программный поставщик — это программа, которая работает на хосте и поддерживается драйвером режима ядра. Такие поставщики работают с томами, дисками и сегментами. Аппаратный поставщик управляет самой подсистемой хранилища. Обычно аппаратные поставщики — это платы адаптеров или массивов дисков, которые позволяют создавать логические диски для каждого типа LUN. Тип LUN, который можно настроить, зависит от параметров, допускаемых поставщиком аппаратуры VDS. Например, некоторые поставщики аппаратуры VDS допускают создание чередующихся LUN с контролем четности, другие — только зеркальные или составные LUN.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Установка поставщиков VDS

Подробнее об установке поставщиков VDS см. по адресу [http://technet.microsoft.com/en-us/library/gg232643\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/gg232643(Ws.10).aspx) (на английском языке).

---

#### Проверьте себя

1. Ваша подсистема хранилища данных состоит из пяти дисков объемом 1 ТБ. Какой тип LUN позволит создать том объемом примерно 5 ТБ?
2. Вы только что расширили LUN с помощью диспетчера хранилищ для сетей SAN. Какой инструмент следует использовать, чтобы расширить раздел файловой системы на этом LUN?

#### Ответы

1. Составной LUN.
2. Оснастку управления дисками или аналогичный инструмент. С помощью диспетчера хранилищ для сетей SAN можно увеличить только объем LUN, но не размер раздела файловой системы.

## Диспетчер хранилища для сетей SAN

С помощью диспетчера хранилища для сетей SAN можно создавать LUN в массивах хранилищ Fibre Channel и iSCSI. В Windows Server 2008 и 2008 R2 диспетчер хранилищ для сетей SAN устанавливается как компонент. Чтобы можно было управлять LUN с помощью этого диспетчера, необходимо выполнение следующих условий:

- подсистемы хранилища данных должны поддерживать VDS;
- на компьютер под управлением Windows Server 2008 должен быть установлен поставщик аппаратуры VDS для каждой подсистемы.

Диспетчер хранилища для сетей SAN, который можно запустить из меню **Администрирование**, имеет три основных узла:

- **Управление LUN (LUN Management)** — содержит список всех LUN, созданных с помощью диспетчера хранилищ для сетей SAN. В этом узле можно создавать новые LUN, увеличивать размеры существующих LUN, назначать и отменять назначения или удалять LUN. Этот узел можно использовать также для настройки подключений к Fibre Channel и iSCSI, используемых серверами для доступа к LUN.
- **Подсистемы (Subsystems)** — содержит список всех подсистем хранилища данных, обнаруженных на текущий момент в окружении SAN, и позволяет переименовывать подсистемы.
- **Диски (Drives)** — содержит список всех дисков в подсистемах хранения данных, обнаруженных в SAN. Позволяет проводить визуальную идентификацию дисков, включая мигание подсветки диска.

## Управление LUN в среде Fibre Channel

В среде Fibre Channel номера LUN, созданные для подсистемы хранилища Fibre Channel, назначаются непосредственно серверу или кластеру. Серверы получают доступ к LUN посредством одного или нескольких портов адаптеров шины (HBA) Fibre Channel. С помощью диспетчера хранилищ для сетей SAN можно идентифицировать сервер, который получит доступ к LUN, а затем определить, какие порты HBA будут использоваться для передачи данных LUN. Можно добавлять порты вручную, указав их имена WWN (World Wide Name). Можно также просматривать подробную информацию о HBA Fibre Channel для серверов в сети SAN с помощью проводника хранилищ (Storage Explorer). Подробнее о проводнике хранилищ см. далее.

## Управление LUN в подсистемах iSCSI

iSCSI — протокол SAN, использующий традиционные сетевые технологии, а не специальные кабельные подключения, которые использует Fibre Channel, для отправки команд SCSI из установленных на серверах инициаторов для запоминающих устройств на основе SCSI, расположенных в сети. В отличие от Fibre Channel, номера LUN iSCSI назначаются не напрямую серверу или кластеру, а логическим элементам, которые называются целевыми объектами. Эти целевые объекты управляют подключениями между аппаратурой iSCSI и серверами, имеющими к ней доступ. Целевой объект содержит портал (IP-адрес) устройства iSCSI и параметры безопасности этого устройства. Последние, как правило, являются учетными данными, которые должен предоставить сервер для проверки подлинности этим устройством. Учетные данные различаются в зависимости от поставщика.

Для подключения к целевому объекту сервер использует инициатор iSCSI. Инициатор iSCSI — логический элемент, обеспечивающий связь с конечным объектом на сервере. В Windows Server 2008 R2 инициатор iSCSI расположен в панели управления. Инициатор iSCSI выполняет вход в конечный объект и, получив доступ, позволяет серверу выполнять чтение и запись на всех LUN, назначенных этому конечному объекту. Каждый инициатор iSCSI может осу-

ществлять связь через один или несколько сетевых адаптеров. На рис. 10-13 показан инициатор iSCSI Windows Server 2008 R2.

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Инициатор iSCSI

Подробнее об инициаторе iSCSI см. по адресу [http://technet.microsoft.com/ru-ru/library/ee338477\(WS.10\).aspx](http://technet.microsoft.com/ru-ru/library/ee338477(WS.10).aspx).

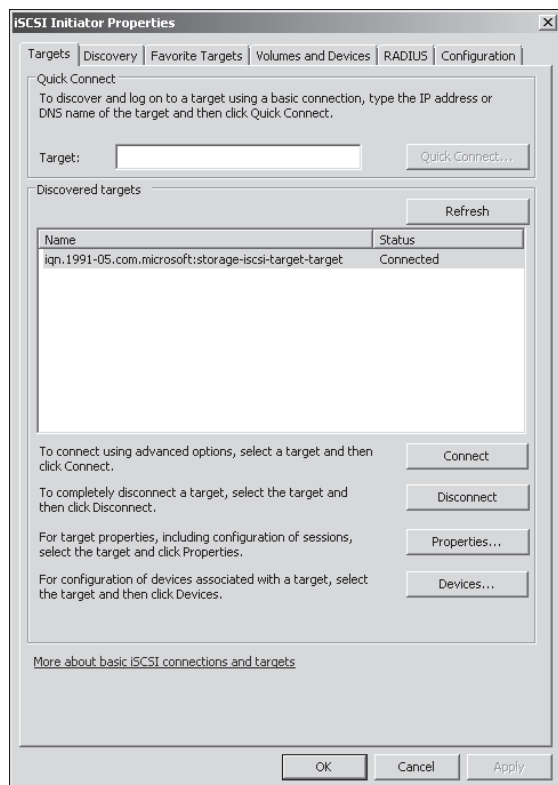


Рис. 10-13. Инициатор iSCSI Windows Server 2008 R2

## Многопутевой ввод-вывод

МPIO — функция Windows Server 2008, позволяющая серверу использовать несколько путей данных к запоминающему устройству. За счет этого повышается надежность ресурсов хранилища, поскольку в случае неисправности пути предоставляются дополнительные пути от сервера или кластера к подсистеме хранилища данных. МPIO использует резервные компоненты физического пути (в частности, адаптеры, переключатели и кабели) для создания отдельных путей между сервером или кластером и запоминающим устройством. Если выйдет из строя одно из устройств в этих отдельных путях, то будет задействован дополнительный путь к устройству в сети SAN, обеспечивающий доступ сервера к важным данным. Сроки переходов на другой ресурс настраиваются с помощью драйвера Microsoft iSCSI Software Initiator или путем изменения значений параметров драйвера Fibre Channel HBA, в зависимости от технологии SAN, развернутой в вашей среде.

Если сервер будет иметь доступ к LUN через несколько портов Fibre Channel или несколько адаптеров инициатора iSCSI, необходимо установить MPIO на серверы. Прежде чем включать несколько адаптеров инициатора iSCSI или несколько портов Fibre Channel для доступа к LUN, убедитесь, что сервер поддерживает MPIO. Если этого не сделать, может произойти потеря данных. Если вы не уверены, поддерживает ли сервер MPIO, включите только один адаптер инициатора iSCSI или порт Fibre Channel на сервере.

В Windows Server 2008 R2 MPIO поддерживает подключения iSCSI, Fibre Channel и интерфейса SAS к сетям SAN путем установки нескольких подключений или сеансов для запоминающего устройства. Реализация MPIO в Windows Server 2008 R2 включает модуль специфического устройства (DSM), который работает с запоминающими устройствами, поддерживающими модель контроллера асимметричного доступа к логическому элементу (ALUA), и с устройствами хранилищ, использующими модель контроллера Active/Active. MPIO поддерживает следующие политики балансировки нагрузки:

- **Отказоустойчивость (Failover).** Если применена эта политика, балансировка нагрузки не выполняется. Приложение указывает основной путь и группу резервных путей. Основной путь используется для всех запросов устройств. Резервные пути используются только в случае неисправности основного пути. Резервные пути отображаются в порядке убывания приоритета.
- **Восстановление размещения (Failback).** Если эта политика настроена, ввод-вывод ограничен предпочтительным путем, когда тот исправен. В случае неисправности предпочтительного пути ввод-вывод направляется на дополнительный путь. После полного восстановления предпочтительного пути ввод-вывод автоматически переключается обратно на него.
- **Циклический перебор (Round-robin).** Все доступные пути используются для ввода-вывода в равной мере. Если один путь выйдет из строя, ввод-вывод будет перераспределен между оставшимися.
- **Циклический перебор с подмножеством путей (Round-robin with a subset of paths).** Когда настроена эта политика, указывается набор предпочтительных путей для ввода-вывода и набор резервных путей для отказоустойчивости. Набор предпочтительных путей будет использоваться, пока все пути не выйдут из строя, после чего будут использоваться резервные пути. Предпочтительные пути используются методом циклического перебора.
- **Динамическая наименьшая глубина очереди (Dynamic Least Queue Depth).** Ввод-вывод направляется по пути с наименьшим количеством ожидающих запросов.
- **Взвешенный путь (Weighted path).** Каждому пути присваивается вес. Для ввода-вывода выбирается путь с наименьшим весом.

Политики балансировки нагрузки зависят от модели контроллера (ALUA или Active/Active) массива хранилища данных, подключенного к компьютеру под управлением Windows Server 2008. MPIO добавляется на компьютер под управлением Windows Server 2008 R2 с помощью элемента **Добавить компоненты (Add Features)** в разделе **Компоненты (Features)** диспетчера сервера.



---

**ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Многопутевой ввод-вывод**

Подробнее о многопутевом вводе-выводе см. по адресу [http://technet.microsoft.com/en-us/library/ee619734\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/ee619734(Ws.10).aspx) (на английском языке).

---

## Проводник хранилищ

Оснастка **Проводник хранилищ** (Storage Explorer) (рис. 10-14), доступная в меню **Администрирование**, используется для управления структурами Fabric Fibre Channel и iSCSI в сетях SAN. Структура Fabric (коммутирующая матрица) — это сетевая топология, в которой запоминающие устройства связаны между собой посредством одного или нескольких путей данных. В структуре Fabric Fibre Channel сеть содержит несколько коммутаторов Fibre Channel, которые используются для подключения серверов и запоминающих устройств друг к другу посредством виртуальных соединений типа точка-точка. В структурах Fabric iSCSI сети содержат несколько серверов службы имен хранилищ Интернета (iSNS), позволяющих обнаруживать и разделять ресурсы.

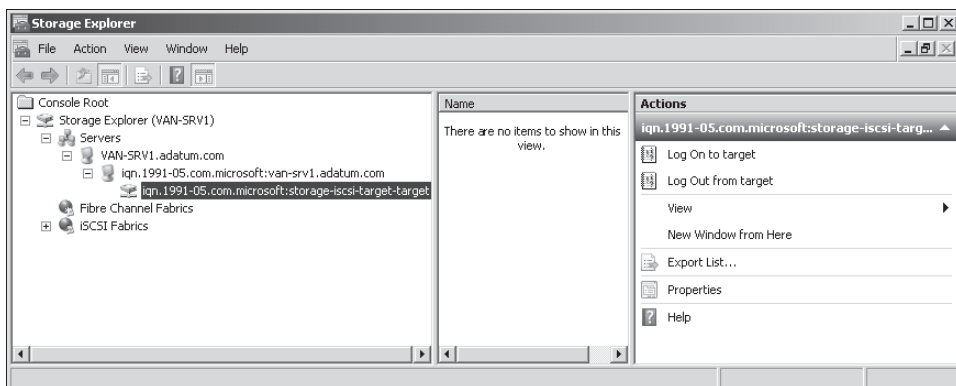


**Рис. 10-14.** Проводник хранилищ

Проводник хранилищ может отображать подробную информацию о серверах, подключенных к SAN, а также данные о компонентах структуры Fabric, таких как адаптеры шин, коммутаторы Fibre Channel, инициаторы iSCSI и целевые объекты iSCSI. Проводник хранилищ позволяет настраивать безопасность iSCSI, настраивать целевые порталы iSCSI, добавлять серверы iSNS, управлять доменами обнаружения и наборами доменов обнаружения. Для просмотра и управления структурой Fabric iSCSI необходимо включить исключение WMI в брандмауэре Windows на каждом сервере под управлением Windows Server 2008, который является частью структуры Fabric. Многие задачи по управлению iSCSI, выполняемые с помощью проводника хранилищ, можно также выполнять с помощью инициатора iSCSI (находится в Панели управления) или с сервера Microsoft iSNS.

---

**ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Проводник хранилищ**

Подробнее о проводнике хранилищ см. по адресу <http://technet.microsoft.com/ru-ru/library/cc731884.aspx>.

---

## Резюме

- LUN — логическая ссылка на раздел подсистемы хранилища данных. LUN может представлять диск, раздел диска, целый массив дисков или раздел массива диска в подсистеме хранилища.
- Многопутевой ввод-вывод (MPIO) поддерживает несколько путей данных к запоминающим устройствам. MPIO требуется установить на сервере, если доступ к LUN будет осуществляться через несколько портов Fibre Channel HBA или несколько инициаторов iSCSI.
- Серверы и кластеры подключаются к массивам Fibre Channel с помощью портов HBA. Серверы и кластеры используют инициаторы iSCSI для подключения к целевым объектам iSCSI, которые управляют массивами iSCSI.
- Диспетчер хранилища для сетей SAN позволяет создавать и управлять номерами LUN на устройствах iSCSI и Fibre Channel. Проводник хранилищ используется для управления структурами Fabric iSCSI и Fibre Channel.

## Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных на занятии 2. Эти вопросы предоставлены также в электронном виде на прилагаемом к книге компакт-диске.

---

### ПРИМЕЧАНИЕ Ответы

Ответы на вопросы и пояснения к их вариантам размещены в разделе «Ответы» в конце книги.

---

1. Какой компонент Windows Server 2008 R2 следует установить перед активацией доступа к LUN через несколько портов Fibre Channel?
  - a. Удаленное разностное сжатие.
  - b. Универсальное обнаружение, описание и интеграция (UDDI).
  - c. Многопутевой ввод-вывод (MPIO).
  - d. RPC через прокси HTTP.
2. Если запоминающее устройство iSCSI поддерживает все типы LUN, какой тип LUN вы выберете для максимального увеличения производительности ввода-вывода, сохранив при этом отказоустойчивость?
  - a. Составной.
  - b. Чередующийся.
  - c. Простой.
  - d. Чередующийся с контролем четности.
3. Какую политику MPIO следует выбрать, чтобы сервер, на котором настроено четыре пути между сервером и массивом SAN, направлял трафик равномерно по всем путям в обычном режиме работы?
  - a. Восстановление размещения.
  - b. Циклический перебор.
  - c. Взвешенный путь.
  - d. Динамическая наименьшая глубина очереди.

4. Какой инструмент Windows Server 2008 R2 используется для создания LUN в массиве хранилища данных Fibre Channel?
  - a. Диспетчер хранилищ для сетей SAN.
  - b. Проводник хранилищ.
  - c. Диспетчер устройств.
  - d. Управление дисками.

## Практикум. Установка и настройка DFS

На этом практикуме вы установите и настроите DFS, после чего настроите автономный доступ к общим папкам DFS.

### Упражнение 1. Установка DFS

В этом упражнении вы установите роль DFS на серверы VAN-SRV1 и VAN-SRV2.

1. Включите компьютер VAN-DC1. Когда загрузка полностью завершится, включите серверы VAN-SRV1 и VAN-SRV2.
2. Зайдите на сервер VAN-SRV1 под учетной записью пользователя Kim\_Akers. Откройте административную командную строку Windows PowerShell и введите следующие команды:

```
Import-Module ServerManager
Add-WindowsFeature FS-DFS
```

3. Зайдите на сервер VAN-SRV2 под учетной записью пользователя Kim\_Akers. Откройте административную командную строку Windows PowerShell и введите следующие команды:

```
Import-Module ServerManager
Add-WindowsFeature FS-DFS
```

### Упражнение 2. Настройка пространства имен DFS и добавление сервера пространств имен

В этом упражнении вы используете консоль **Управление DFS** для создания пространства имен DFS. Затем вы обеспечите высокую доступность этого пространства имен, добавив второй сервер пространства имен.

1. Зайдите на сервер VAN-SRV1 под учетной записью Kim\_Akers, откройте консоль **Управление DFS** (DFS Management) из меню **Администрирование**.
2. Выберите узел **Пространства имен** (Namespaces). Щелкните **Новое пространство имен** (New Namespace) на панели **Действия** (Actions). Откроется мастер создания нового пространства имен.
3. На странице **Сервер пространств имен** (Namespace Server) введите имя **VAN-SRV1** и щелкните **Далее**.
4. На странице **Имя и параметры пространства имен** (Namespace Name and Settings) введите имя **TrainingKit** и щелкните **Далее**.

5. Убедитесь, что на странице **Тип пространства имен** (Namespace Type) установлен переключатель **Доменное пространство имен** (Domain-Based Namespace) и флажок **Включить режим Windows Server 2008** (Enable Windows Server 2008 Mode), после чего щелкните **Далее**. Щелкните **Создать** (Create), а затем **Заккрыть** (Close).
6. Щелкните узел \\adatum.com\TrainingKit под узлом **Пространства имен**. Щелкните **Добавить сервер пространства имен** (Add Namespace Server) на панели **Действия**.
7. В диалоговом окне **Добавить сервер пространства имен** (Add Namespace Server) Введите VAN-SRV2 (рис. 10-15) и щелкните **ОК**.

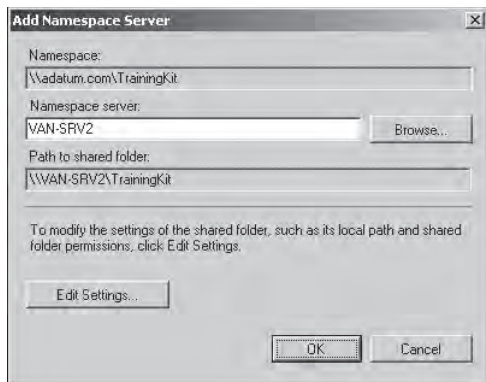


Рис. 10-15. Добавление сервера пространства имен

### Упражнение 3. Создание новой папки DFS и группы репликации

В этом упражнении вы создадите новую общую папку, которая будет использовать DFS для выполнения репликации между VAN-SRV1 и VAN-SRV2.

1. Щелкните узел \\adatum.com\TrainingKit под узлом **Пространства имен** (Namespaces). Щелкните **Создать папку** (New Folder) на панели **Действия** (Actions).
2. Введите имя **Synchronize** в диалоговом окне **Новая папка** (New Folder), а затем щелкните **Добавить** (Add). В диалоговом окне **Добавление конечного объекта папки** (Add Folder Target) щелкните **Обзор** (Browse).
3. В диалоговом окне **Обзор общих папок** (Browse For Shared Folders) щелкните **Новая общая папка** (New Shared Folder). В диалоговом окне **Создание общего ресурса** (Create Share) введите имя **Synchronize**. Щелкните **Обзор** рядом с полем **Локальный путь общей папки** (Local Path Of Shared Folder). В диалоговом окне **Обзор папок** (Browse For Folder) выберите **c\$** и щелкните **Создать папку** (Make New Folder). Введите имя **Synchronize** и **ОК**. Проверьте, совпадает ли диалоговое окно **Создание общего ресурса** (Create Share) с рис. 10-16, и трижды щелкните **ОК**, чтобы вернуться в диалоговое окно **Новая папка**.

4. Еще раз щелкните **Добавить**. На окне **Добавление конечного объекта папки** (Add Folder Target) щелкните **Обзор**. Снова щелкните **Обзор** и выберите VAN-SRV2. Щелкните **Создать папку**. В диалоговом окне **Создание общего ресурса** введите имя **Synchronize**. Щелкните **Обзор** рядом с полем **Локальный путь общей папки**. В диалоговом окне **Обзор папок** щелкните **c\$**, а затем щелкните **Создать папку**. Введите имя **Synchronize**, а затем четырежды щелкните **ОК**, пока не отобразится диалоговое окно **Репликация** (Replication).
5. В диалоговом окне **Репликация** щелкните **Да**. Запустится мастер папок репликации. Убедитесь, что на странице **Группа репликации и имя реплицированной папки** (Replication Group And Replicated Folder Name) указано имя **adatum.com\trainingkit\synchronize**, а параметр **Имя реплицированной папки** (Replicated Folder Name) имеет значение **Synchronize**, и щелкните **Далее**.
6. На странице **Приемлемость репликации** (Replication Eligibility) щелкните **Далее**.
7. С помощью раскрывающегося меню на странице **Основной член репликации** (Primary Member) выберите **VAN-SRV1** и щелкните **Далее**.

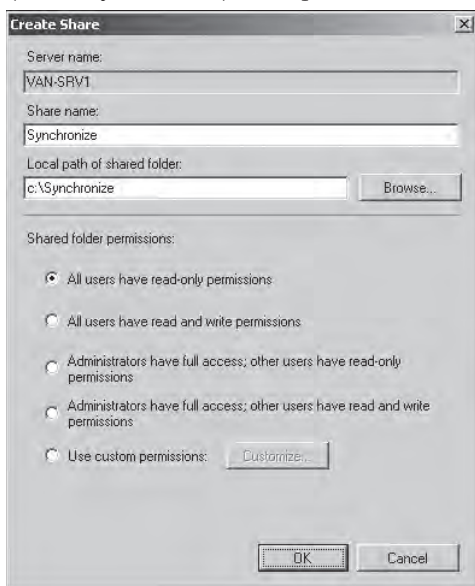


Рис. 10-16. Создание общей папки DFS

8. На странице **Выбор топологии** (Topology Selection) выберите **Полная сетка** (Full Mesh) и щелкните **Далее**.
9. Убедитесь, что на странице **Расписание и пропускная способность группы репликации** (Replication Group Schedule And Bandwidth) выбран параметр **Реплицировать постоянно с использованием следующей пропускной способности** (Replicate continuously using the specified bandwidth), а параметр **Пропускная способность** (Bandwidth) имеет значение **Полная** (Full). Щелкните **Далее**. Щелкните **Создать**, а затем **Заккрыть**. Щелкните **ОК**, чтобы закрыть диалоговое окно.

## Упражнение 4. Настройка параметров автономных файлов для общих папок

В этом упражнении вы настроите параметры автономных файлов для общей папки Synchronize и включите перечисление на основе доступа для общей папки, а не для всего пространства имен DFS.

1. Зайдите на VAN-SRV1 под учетной записью Kim\_Akers.
2. Откройте оснастку **Управление общими ресурсами и хранилищами** (Share And Storage Management) из меню **Администрирование**.
3. На панели сведений оснастки **Управление общими ресурсами и хранилищами** выберите папку **Synchronize**. На панели **Действия** щелкните **Свойства** (Properties).
4. На вкладке **Доступ** (Sharing) диалогового окна свойств папки **Synchronize** щелкните кнопку **Дополнительно** (Advanced). Установите флажок **Включить перечисление на основе доступа** (Enable Access-Based Enumeration).
5. На вкладке **Кэширование** (Caching) установите переключатель **Все открываемые пользователем файлы и программы доступны режиме работы вне сети** (All Files And Programs That Users Open From The Share Are Automatically Available Offline), а затем установите флажок **Оптимизация производительности** (Optimized For Performance). Щелкните **ОК** два раза.

## Закрепление материала главы

Чтобы попрактиковаться и закрепить знания, полученные при изучении этой главы, выполните следующее:

- прочитайте резюме главы;
- просмотрите список основных терминов, представленных в этой главе;
- выполните задания лабораторной работы, моделирующей реальные ситуации, требующие применения полученных знаний;
- выполните рекомендуемые упражнения;
- пройдите пробный тест.

## Резюме главы

- Избыточность хранилищ в Windows Server 2008 и 2008 R2 можно обеспечить с помощью программных массивов RAID 1 и RAID 5, если имеется достаточное количество дисков.
- DFS позволяет передавать данные в сайты организации посредством репликации.
- SharePoint Foundation 2010 позволяет создать в организации инфраструктуру для совместной работы над файлами и поддержки версий, имеющую более широкие возможности, чем службы общего доступа к файлам и DFS.
- LUN — логическая ссылка на часть подсистемы хранилища данных, которой может быть раздел на диске или целый массив хранилищ.

- Многопутевой ввод-вывод позволяет создавать отказоустойчивые пути от серверов к массивам SAN.

## Основные термины

Проверьте, знаете ли вы, что означают перечисленные ниже термины из этой главы:

- DFS;
- LUN;
- поддержка версий.

## Лабораторная работа

Для выполнения заданий лабораторной работы используйте знания о планировании установки и обновления сервера, полученные из этой главы. Ответы можно найти в разделе «Ответы» в конце книги.

### Задание 1. DFS в Wingtip Toys

Компания Wingtip Toys имеет несколько офисов в разных городах Австралии. Вам требуется организовать репликацию важных документов во все сайты, поэтому вы планируете установить DFS. Все сайты связаны друг с другом посредством VPN, и в каждом из офисов есть компьютер под управлением Windows Server 2008 R2, предназначенный для хранения локальных реплик каждой общей папки DFS. Вы хотите, чтобы пространство имен оставалось доступным в случае отключения Интернета в офисе на несколько часов. Учитывая это, ответьте на следующие вопросы:

- Какую службу следует добавить на компьютер под управлением Windows Server 2008 R2 в каждом офисе, прежде чем настроить его как реплику?
- Как обеспечить доступность пространства имен в случае отсутствия подключений VPN?
- Как сделать так, чтобы любая реплика могла обновлять любую другую реплику?

### Задание 2. Подготовка данных в Contoso

Вы разрабатываете стратегию подготовки данных для компании Contoso. Вы хотите, чтобы пользователи из группы **Бухгалтерия** могли отслеживать, кто делал изменения в файлах, а пользователи из группы **Менеджеры** имели доступ к файлам, хранящимся в общих папках, даже в командировках. Кроме того, вы хотите, чтобы файловые серверы с документами группы **Менеджеры** могли работать в случае выхода из строя жесткого диска. Учитывая это, ответьте на следующие вопросы:

1. Какую технологию следует использовать, чтобы удовлетворить требования группы **Бухгалтерия**?
2. Какой компонент следует включить, чтобы пользователи из группы **Менеджеры** имели доступ к общим файлам, когда берут домой портативные компьютеры?



3. Какой программный массив RAID следует установить на серверы, где размещены общие файлы для группы **Менеджеры**, чтобы выполнить предъявляемые требования?

## Рекомендуемые упражнения

Чтобы успешно справиться с экзаменационными заданиями по темам этой главы, выполните следующие упражнения.

### Подготовка данных

Выполните все упражнения, если имеете доступ к соответствующей аппаратуре.

- Создайте дополнительное пространство имен DFS и наполните его реплицированными папками.
- Загрузите и установите SharePoint Foundation 2010. Создайте, внесите и извлеките документы.

### Настройка хранилища

Выполните все упражнения, если имеете доступ к соответствующей аппаратуре SAN.

- Настройте инициатор iSCSI для подключения к целевому объекту iSCSI.
- Настройте LUN типа RAID 5 для SAN.
- Назначьте LUN компьютеру под управлением Windows Server 2008 R2.

## Пробный экзамен

Тренировочные тесты на прилагаемом к книге компакт-диске позволяют проверить знания только по одной или сразу по всем темам сертификационного экзамена 70-646. Тестирование можно организовать так, чтобы оно проводилось как настоящий экзамен, а можно проходить в режиме обучения, просматривая правильные ответы и объяснения после каждого ответа.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Пробный экзамен

Подробнее о пробном экзамене рассказано во Введении.

---

## Кластеризация и высокая доступность

**Занятие 1. Циклическое обслуживание DNS и балансировка сетевой нагрузки 490**

**Занятие 2. Средства кластеризации Windows Server 2008 R2 500**

Высокая доступность подразумевает обеспечение доступности важных служб и приложений для клиентов в сети в случае аварийного сбоя сервера. Существует несколько подходов к обеспечению высокой доступности. Выбор зависит от имеющихся в наличии ресурсов. Самый дешевый способ — использование циклического обслуживания DNS. Преимущество циклического обслуживания DNS состоит в том, что оно является межплатформенным решением. Недостаток — в отсутствии механизма оповещения о выходе из строя одного из целевых серверов. Балансировка сетевой нагрузки (NLB) позволяет равномерно распределять трафик между несколькими серверами и имеет механизм оповещений о сбоях, однако недостаточно эффективно работает непосредственно с серверными приложениями, например, с файловыми серверами. Отказоустойчивая кластеризация обеспечивает доступ к сетевой службе или приложению в случае аварийного сбоя сервера, но требует доступа к сети хранения данных (SAN). В этой главе вы узнаете о каждом из этих решений для обеспечения высокой доступности и научитесь определять, какое из них подходит для развертывания в различных условиях.

### Темы экзамена

- Планирование высокой доступности.

### Прежде всего

Для выполнения упражнений этой главы потребуется:

- выполнить задания по установке, приведенные в упражнениях 1-4 Приложения.

Дополнительной настройки не требуется.

**Реальный мир***Орин Томас*

Существенный недостаток отказоустойчивой кластеризации не только в том, что приходится изрядно потрудиться, чтобы заставить хранилище в сети SAN исправно работать, но и в том, что необходимо выделить дорогостоящий сервер, который будет бездействовать, пока не произойдет сбой другого сервера, который в это время работает. Именно поэтому высокая надежность многих приложений все чаще обеспечивается непрерывной репликацией, а не традиционным подходом «один узел активен, а другой ничего не делает», который используется в стандартных отказоустойчивых кластерах. Отличный пример этого нового подхода — группы обеспечения доступности баз данных в Microsoft Exchange Server 2010. Такие группы предоставляют основные функции отказоустойчивого кластера без создания сети SAN. Если выйдет из строя один сервер почтовых ящиков Exchange Server 2010, то автоматически заработает другой, на котором расположена пассивная копия баз данных почтовых ящиков первого сервера. Поэтому, несмотря на то, что в Windows Server 2008 и 2008 R2 Microsoft значительно упростила настройку отказоустойчивых кластеров, появление таких технологий, как группы обеспечения доступности баз данных, означает, что в будущем, вероятно, уже не придется настраивать отказоустойчивые кластеры.

## Занятие 1. Циклическое обслуживание DNS и балансировка сетевой нагрузки

Это занятие посвящено двум технологиям обеспечения высокой доступности — циклическому обслуживанию DNS и NLB. Циклическое обслуживание DNS и NLB поддерживаются всеми версиями Windows Server 2008 и 2008 R2.

---

**Изучив материал этого занятия, вы сможете:**

- ✓ Планировать и разворачивать циклическое обслуживание DNS для обеспечения доступности.
- ✓ Планировать и разворачивать NLB для обеспечения доступности.

**Продолжительность занятия — примерно 60 мин.**

---

## Простые стратегии обеспечения доступности

Циклическое обслуживание DNS и NLB — две относительно простые технологии, с помощью которых можно обеспечивать доступность приложений. Эти технологии позволяют наращивать ресурсы перегруженной службы за счет добавления дополнительных серверов. Например, если веб-сайт, поддерживаемый с помощью одной из этих технологий, не справляется с нагрузкой, можно добавить дополнительные веб-серверы. Циклическое обслуживание DNS или NLB позволит распределить трафик между серверами, снизив нагрузку и увеличив производительность.

Для применения этих технологий необходимо, чтобы каждый узел имел одинаковое содержимое. Например, если используется удаленный рабочий стол, то на каждом сервере удаленных рабочих столов должны быть установлены одни и те же приложения; если используются веб-сайты, каждый из них должен подключаться к одной и той же внутренней базе данных SQL Server. Циклическое обслуживание DNS или NLB невозможно использовать для поддержки общих папок и аналогичных служб, поскольку содержимое общей папки должно находиться в одном месте, а не распределяться по нескольким серверам.

## Циклическое обслуживание DNS

Циклическое обслуживание DNS (DNS Round Robin) действует путем предоставления DNS-сервером разных IP-адресов в ответ на запросы для одного имени узла хоста. Например, с помощью циклического обслуживания DNS можно связать DNS-запись для полного доменного имени (FQDN) *www.contoso.internal* с двумя IP-адресами: 10.10.111.111 и 10.10.222.222. Когда один клиент запрашивает у DNS-сервера адрес узла *www.contoso.internal*, DNS-сервер отправляет в ответ адрес 10.10.111.111. Следующий клиент, запрашивающий адрес того же DNS-сервера, получит адрес 10.10.222.222.

Если с одним именем узла связано более двух IP-адресов, DNS-сервер предоставляет клиентам каждый адрес по очереди. Это обеспечивает некоторую агрегацию трафика. Несмотря на отсутствие жестких ограничений на число IP-адресов, связанных с конкретным именем узла, возможности DNS-сервера, где располагается зона, функционально ограничивают число записей, которые могут существовать в DNS-зоне. С помощью циклического обслуживания DNS можно связать 200 или 2000 разных IP-адресов с одним именем узла. Отвечая на запросы имени узла, DNS-сервер предоставит каждый IP-адрес из списка, прежде чем вернуться к первому адресу и начать сначала.

## Расстановка по адресу

Расстановка по адресу — расширение технологии циклического обслуживания DNS, позволяющее DNS-серверу учитывать IP-адрес запрашивающего клиента во время предоставления ответа. Если включена расстановка по адресу, DNS-сервер попытается вернуть IP-адрес узла, расположенного в той же подсети, что и запрашивающий клиент. Например, если связать с именем узла *www.contoso.internal* IP-адреса 10.10.111.111 и 10.10.222.222 и включить расстановку по адресу, то клиент с IP-адресом 10.10.222.100, запросивший у DNS-сервера это имя узла, всегда будет получать в ответ IP-адрес 10.10.222.222. При включении расстановки по адресу сервер пытается предоставить клиенту адрес узла из подсети клиента. Если для подсети запрашивающего клиента нет ни одной записи DNS, циклическое обслуживание работает как обычно.

При установке роли DNS в Windows Server 2008 и 2008 R2 циклическое обслуживание DNS и расстановка по адресу включаются по умолчанию. Для проверки состояния циклического обслуживания DNS и расстановки по адресу выполните на DNS-сервере следующее:

1. Откройте консоль диспетчера DNS из меню **Администрирование** (Administrative Tools).

- Откройте вкладку **Дополнительно** (Advanced) диалогового окна свойств DNS-сервера.
- Убедитесь, что установлены флажки **Включить циклическое обслуживание** (Enable Round Robin) и **Включить расстановку по адресу** (Enable Netmask Ordering) (рис. 11-1).

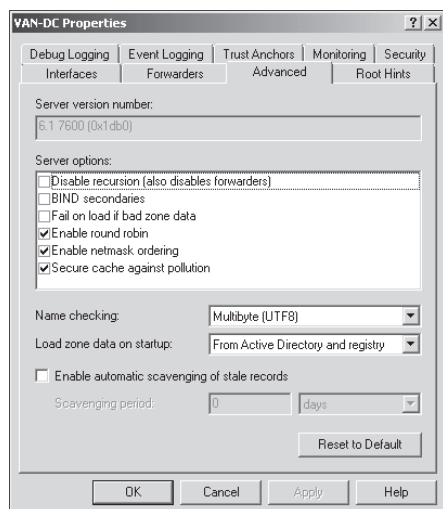


Рис. 11-1. Состояние циклического обслуживания DNS и расстановки по адресу

## Создание записей циклического обслуживания DNS

DNS-серверы под управлением Windows Server 2008 и 2008 R2 по умолчанию поддерживают циклическое обслуживание DNS, поэтому для его использования требуется только создать несколько записей A или AAAA, связанных с одним именем узла. Например, чтобы добавить несколько записей для имени узла *www.contoso.internal* на DNS-сервере, содержащем основную зону Contoso.internal, используйте команду `dnscmd` следующим образом:

```
Dnscmd /recordadd Contoso.internal www A 10.10.111.111
Dnscmd /recordadd Contoso.internal www A 10.10.111.222
Dnscmd /recordadd Contoso.internal www A 10.10.222.222
Dnscmd /recordadd Contoso.internal www A 10.10.222.111
```

На рис.11-2 показан результат добавления этих записей в зону Contoso.internal.

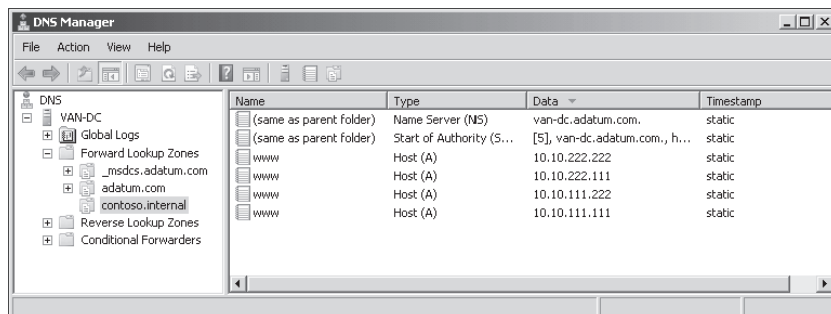


Рис. 11-2. Записи циклического обслуживания DNS

Чтобы удалить запись циклического обслуживания DNS, просто удалите ее из зоны, где она находится.

Помните, что DNS-сервер не знает, существует ли узел, к которому он направляет клиента, и доступен ли он. При создании записи DNS проверка доступности указанного узла не выполняется. В случае сбоя узла DNS-сервер продолжит направлять на него клиенты, пока не будет удалена соответствующая запись DNS.

### Проверьте себя

- Какую функцию следует включить, чтобы при использовании циклического обслуживания DNS клиенты получали IP-адрес из той же подсети?

### Ответ

- Расстановка по адресу.

## Балансировка сетевой нагрузки

Если создать кластер NLB, он создаст виртуальный сетевой адрес и адаптер, а трафик к этому адресу будет распределяться между несколькими узлами. Виртуальный сетевой адаптер имеет IP-адрес и MAC-адрес.

В Windows Server 2008 R2 кластер NLB поддерживает до 32 узлов, хотя тестирование Microsoft показало, что использование более 8 узлов в одном кластере снижает эффективность кластера. Если требуется более 8 кластеров, Microsoft рекомендует создавать несколько кластеров, каждый из которых содержит не более 8 узлов, и распределять трафик между этими кластерами с помощью циклического обслуживания DNS.

Значительное преимущество NLB над циклическим обслуживанием DNS заключается в том, что NLB автоматически перенастраивает конфигурацию, когда узлы присоединяются к кластеру или выходят из него. Добавлять и удалять узлы можно с помощью интерфейса диспетчера NLB или командной строки. Например, когда требуется применить обновление операционной системы, требующее перезагрузки сервера, можно обновлять узлы кластера по очереди: блокировать новые входящие подключения к одному узлу, устанавливать обновление, пока этот узел не обслуживает активных клиентов, перезагружать узел и возвращать в кластер. Эту процедуру можно выполнить для каждого узла кластера, обеспечив при этом непрерывность обслуживания узлов, имеющих доступ к кластеру через сеть.

Обычно все члены кластера NLB должны работать под управлением одной операционной системы, но можно запускать кластер NLB в смешанном режиме, включая в него узлы, работающие под управлением Windows Server 2003, 2008 и 2008 R2. Если разные узлы кластера работают под управлением разных версий Windows Server, следует обновить узлы со старыми операционными системами, чтобы они работали под управлением самой новой из ОС, присутствующих в кластере. На практике этой главы вы создадите кластер NLB.

---

**ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ    Руководство по развертыванию NLB**

Подробнее о развертывании NLB см. по адресу [http://technet.microsoft.com/en-us/library/cc754833\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc754833(WS.10).aspx) (на английском языке).

---

**Такт и схождение**

Серверы с кластерами NLB постоянно взаимодействуют друг с другом, проверяя, какие узлы доступны, используя процедуру под названием «такт и схождение». Такт — сообщение, ежесекундно отправляемое каждым узлом NLB-кластера другим узлам. Если узлу кластера не удастся передать пять тактов подряд, начинается схождение, и кластер перенастраивается. Схождение может быть вызвано неожиданной потерей узла, возобновлением функционирования узла, добавлением или удалением узлов из кластера администратором. Схождение происходит также при изменении правил портов.

**Режим работы кластера**

При создании нового кластера NLB необходимо выбрать режим его работы. Режим в первую очередь зависит от числа сетевых адаптеров, установленных на каждом узле кластера. NLB имеет два режима работы: одноадресный и многоадресный. Все серверы в кластере должны работать в одном режиме. Нельзя смешивать два режима работы.

**Одноадресный режим NLB**

MAC-адрес, созданный для виртуального сетевого адаптера, совместно используется участниками кластера. Если узлы кластера имеют только одну сетевую карту, виртуальный MAC-адрес кластера логически заменяет физический MAC-адрес этой сетевой карты, и сервер отвечает на сетевой трафик, направляемый по виртуальному MAC-адресу. Хотя сервер сохраняет свой исходный IP-адрес, этот IP-адрес будет разрешаться в виртуальный MAC-адрес, а не в физический.

При использовании одноадресного режима NLB на серверах, имеющих единственный сетевой адаптер, только компьютеры из той же подсети, что и сервер, могут взаимодействовать с этим сервером, используя его исходный IP-адрес. Таким образом, для выполнения административных задач на этом сервере необходимо подключиться к нему из той же подсети, где находится NLB-кластер. К примеру, один из серверов NLB-кластера с одноадресным режимом имеет исходный IP-адрес 192.168.15.10. IP-адрес кластера — 192.168.15.100. Веб-сервер поддерживается с помощью NLB, а для порта 80 установлено правило портов. Если потребуется подключиться к этому серверу с помощью удаленного рабочего стола, к IP-адресу 192.168.15.10 можно подключиться только с узла из той же подсети. Выполнить подключение удаленного рабочего стола к IP-адресу 192.168.15.10 из удаленной подсети не удастся, поскольку одноадресная настройка заменяет физический MAC-адрес виртуальным MAC-адресом кластера.

Одноадресный режим NLB подходит лучше всего, когда на узле установлены две сетевые карты, одна из которых участвует в кластере, а другая используется для управления и взаимодействия между серверами. Если сервер, имеющий две сетевые карты, настроен как член NLB-кластера с одноадресным режимом, к нему можно подключаться из удаленных подсетей.



## Многоадресный режим NLB

Многоадресный режим NLB лучше подходит для компьютеров с одним сетевым адаптером, чем одноадресный, так как сервер сохраняет исходные MAC- и IP-адреса и получает возможность использовать виртуальные адреса, созданные для кластера. Это означает, что можно выполнять удаленное администрирование из разных подсетей, как в описанном выше сценарии, несмотря на то, что у сервера имеется только одна сетевая карта. Единственный недостаток многоадресного режима в том, что сетевые устройства, такие как сетевые коммутаторы и маршрутизаторы, должны поддерживать многоадресную MAC-адресацию. Впрочем, сегодня это уже не такая серьезная проблема, как раньше.

## Многоадресный режим IGMP

Многоадресный режим IGMP — специальная версия многоадресного режима NLB, увеличивающая производительность сети за счет ограничения переполнения коммутатора. В этом режиме многоадресный трафик проходит только через те порты коммутатора, которые обслуживают NLB-кластер, а не через все, как в стандартном многоадресном режиме NLB. Использование многоадресного режима IGMP возможно, только если аппаратура коммутатора поддерживает эту технологию.

## ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Режим работы кластера

Подробнее о режимах работы кластеров NLB см. по адресу [http://technet.microsoft.com/ru-ru/library/cc731616\(WS.10\).aspx](http://technet.microsoft.com/ru-ru/library/cc731616(WS.10).aspx).

## Управление NLB-кластерами

Для управления NLB-кластерами используется оснастка диспетчера балансировки сетевой нагрузки (рис. 11-3), доступная в меню **Администрирование**. С помощью этой оснастки можно изменять правила и параметры портов, через которые работает кластер. Для управления NLB-кластерами учетная запись должна входить в локальную группу администраторов на каждом узле кластера.

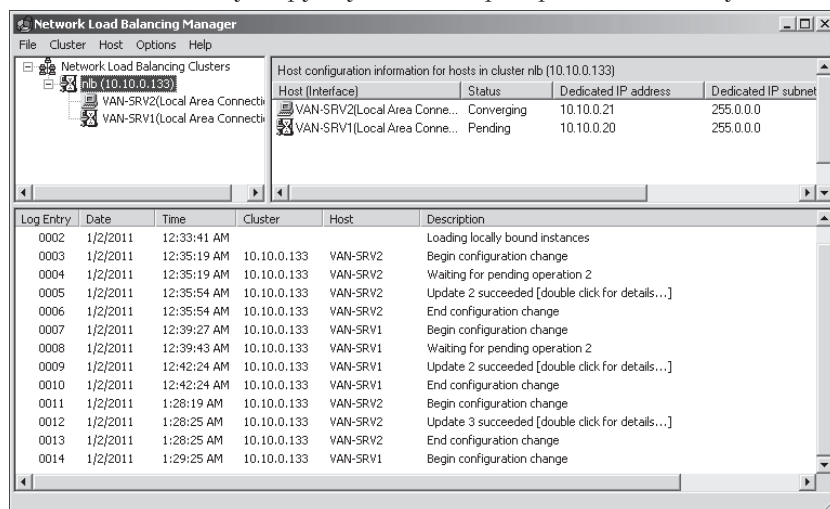


Рис. 11-3. Диспетчер балансировки сетевой нагрузки

Чтобы удалить узел из NLB-кластера, в диспетчере балансировки сетевой нагрузки щелкните правой кнопкой узел, который хотите удалить, и выберите команду **Удалить узел** (Delete Host). Можно удалить весь кластер, выбрав в контекстном меню команду **Удалить кластер** (Delete Cluster).

Если требуется выполнить техническое обслуживание узла кластера, можно блокировать новые входящие подключения, и дожидаться, когда завершатся существующие подключения, после чего приступить к обслуживанию. Для управления узлами NLB-кластера используются следующие команды:

- **Запустить** (Start) — запускает кластер, который был остановлен;
- **Остановить** (Stop) — останавливает кластер, прерывая все активные подключения;
- **Остановить сток** (Drainstop) — прекращает прием новых подключений узлом кластера, но не прерывает существующие подключения; используется для безопасного отключения узла кластера;
- **Приостановить** (Suspend) — приостанавливает узел кластера до выполнения команды **Возобновить**; отличие от команды **Остановить** в том, что та отключает службу кластера на целевом узле;
- **Возобновить** (Resume) — возобновляет работу узла кластера после его приостановки.

---

#### **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ**    **Остановка и запуск обработки трафика на NLB-узле**

Подробнее об остановке стока, запуске и остановке на NLB-узлах обработки трафика см. по адресу [http://technet.microsoft.com/ru-ru/library/cc770345\(WS.10\).aspx](http://technet.microsoft.com/ru-ru/library/cc770345(WS.10).aspx).

---

## **Правила для портов NLB**

Правила для портов NLB позволяют управлять действиями NLB-кластеров по отношению к трафику для конкретного порта, например, порта 80 для веб-трафика. Правила для портов устанавливаются на вкладке **Правила для портов** (Port Rules) диалогового окна свойств кластера (рис. 11-4). Правила для портов должны быть одинаковыми у каждого узла NLB-кластера. Если правила для портов настраиваются на уровне кластера, они автоматически настраиваются на всех узлах кластера. Узел не сможет присоединиться к кластеру, если имеет отличающийся набор правил для портов. По умолчанию NLB-кластер имеет правило для портов, равномерно распределяющее трафик по всем узлам кластера. Если требуется создать отдельные правила, то правило по умолчанию нужно удалить.

При создании правила для портов NLB-кластера выбирается режим фильтрации. Режимы фильтрации позволяют определять, сколько узлов будет отвечать на запросы с одного клиента во время сеанса: один, несколько или все узлы. Это важно для некоторых приложений, в частности, веб-сайтов электронной коммерции, требующих, чтобы весь трафик сеанса перемещался только между одним узлом и клиентом. Используется три режима фильтрации:

- **Один узел.** Отдельный узел обрабатывает весь отправляемый кластеру трафик, соответствующий правилу для портов. Например, весь трафик к IP-адресу через порт 25 идет к серверу ALPHA.

- **Отключить диапазон портов.** Используется, когда кластер не должен отвечать на трафик, проходящий через определенные порты. NLB отклоняет трафик, отправляемый по IP-адресу кластера через эти порты.
- **Фильтрация нескольких узлов.** Этот режим позволяет направлять трафик ко всем узлам кластера. Если настраиваются параметры нескольких узлов, требуется также настроить параметр соответствия. Доступны следующие параметры соответствия:
  - **Отсутствует (None)** — все запросы распределяются равномерно по кластеру, даже если клиент имеет установленный сеанс;
  - **Сеть (Network)** — аналогичен расстановке по адресу. Направляет клиенты к ближайшему узлу на основе подсети;
  - **Один (Single)** — после того как клиент установит сеанс, все последующие запросы в сеансе направляются к одному и тому же узлу кластера. Это позволяет завершать сеансы, требующие отслеживания состояния данных, например, транзакции электронной коммерции. Правила для портов по умолчанию используют этот режим.

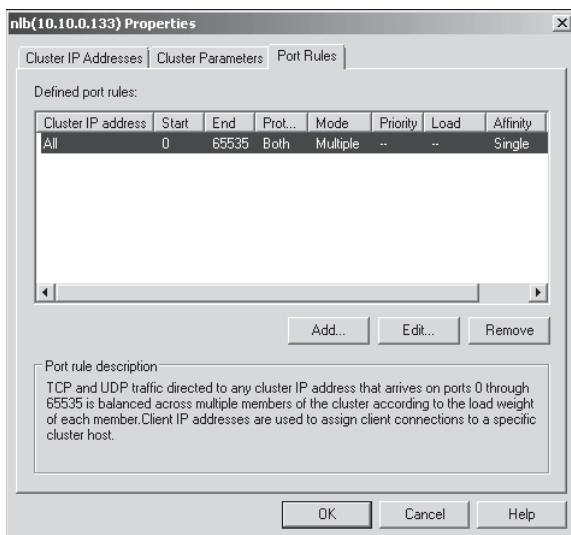


Рис. 11-4. Установка правил для портов кластера

Чтобы создать правило для портов NLB-кластера, выполните следующее:

1. Откройте консоль NLB из меню **Администрирование**.
2. Щелкните кластер правой кнопкой и выберите команду **Свойства кластера**.
3. В диалоговом окне свойств на вкладке **Правила для портов (Port Rules)** щелкните **Добавить (Add)**.
4. В диалоговом окне **Добавление или изменение правила для портов (Add/Edit Port Rule)** укажите диапазон портов, к которым применяется правило, протоколы, к которым применяется правило, и режим фильтрации (рис. 11-5).

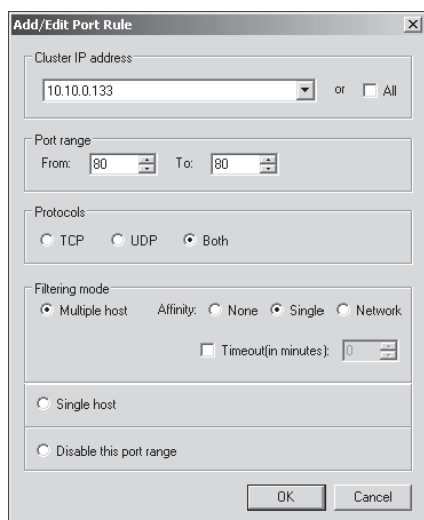


Рис. 11-5. Установка нового правила для портов NLB

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Настройка параметров NLB

Подробнее о настройке параметров NLB см. по адресу <http://technet.microsoft.com/ru-ru/library/cc754230.aspx>.

## Сравнение циклического обслуживания DNS с балансировкой сетевой нагрузки

Как уже говорилось, циклическое обслуживание DNS может работать совместно с NLB. Можно создать несколько NLB-кластеров, а затем использовать циклическое обслуживание DNS для распределения трафика по этим кластерам. Одно из преимуществ циклического обслуживания DNS в том, что оно не привязано к конкретной операционной системе, и можно настраивать его для пересылки клиентских запросов не только веб-серверам под управлением Windows, но и веб-серверам под управлением других ОС.

Циклическое обслуживание DNS имеет следующие недостатки по сравнению с NLB:

- **DNS не управляет распределением нагрузки.** Циклическое обслуживание DNS не позволяет балансировать нагрузку между узлами. Это может привести к неравномерному распределению нагрузки, когда большая часть клиентов использует один сервер, а меньшая часть — другой.
- **Циклическое обслуживание DNS не является отказоустойчивым.** Нет возможности компенсировать потерю узла. DNS-сервер будет по-прежнему направлять клиентов к неисправному узлу, пока администратор вручную не обновит зону DNS. Следует также соблюдать осторожность при настройке короткого срока жизни (TTL) для записей узла DNS, чтобы записи, относящиеся к неисправным узлам, не сохранялись в кэше клиентов DNS после удаления их из зоны DNS. Если DNS-сервер выйдет из строя, то циклическое обслуживание DNS перестанет работать.

- **Циклическое обслуживание DNS не поддерживает сеансы.** Если настроить слишком короткое время TTL для DNS, оно может истечь, когда клиент активно использует приложение. В этом случае клиент запросит адрес сервера. Циклическое обслуживание DNS не позволяет определять, какой адрес получит клиент, следовательно, следующий запрос клиента может быть отправлен к другому серверу, у которого нет информации о сеансе для данного клиента.

## Резюме

- Циклическое обслуживание DNS предоставляет клиентам DNS разные IP-адреса для одного имени узла.
- Можно настроить циклическое обслуживание DNS для использования расстановки по адресу. Если включена расстановка по адресу, DNS-сервер пытается предоставить клиенту адрес узла из той же подсети.
- При установке роли DNS-сервера на компьютеры под управлением Windows Server 2008 или 2008 R2 циклическое обслуживание DNS и расстановка по адресу включаются по умолчанию.
- NLB — компонент, который можно устанавливать на компьютеры под управлением любой из версий Windows Server 2008 и 2008 R2.
- Одноадресный режим NLB рекомендуется для компьютеров с двумя и более сетевыми картами. Этот режим можно использовать и на серверах с одной сетевой картой, однако управлять таким сервером можно только из его локальной подсети.
- Многоадресный режим NLB использует адреса многоадресной рассылки для передачи трафика кластера. Многоадресный режим IGMP использует специальные функции сетевых коммутаторов для уменьшения воздействия многоадресного режима на сетевые устройства.
- Правила для портов NLB позволяют определять способ управления трафиком кластерами NLB. Параметры соответствия определяют, будет ли трафик отправляться к одному конкретному узлу или к любому из имеющихся узлов. Параметры соответствия можно настроить так, чтобы отключаемые сеансы всегда повторно подключались к тому же узлу.
- Команда **Остановить сток** позволяет блокировать новые сеансы на определенном узле, не прерывая существующие подключения к нему.

## Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных на занятии 1. Эти вопросы предоставлены также в электронном виде на прилагаемом к книге компакт-диске.

---

### ПРИМЕЧАНИЕ Ответы

Ответы на вопросы и пояснения к их вариантам размещены в разделе «Ответы» в конце книги.

---

1. Вы настроили циклическое обслуживание DNS для имени узла www.contoso.com. Вы хотите, чтобы DNS-сервер возвращал IP-адрес сервера из той же подсети, где расположен запрашивающий клиент, если возникнет такая необходимость. Как это сделать?
  - a. Включить расстановку по адресу.
  - b. Настроить дополнительную зону DNS.
  - c. Настроить зону-заглушку DNS.
  - d. Настроить параметры сходства.
2. Вам требуется поместить SMTP-сервер в один узел NLB-кластера, включающего четыре узла. Какое из следующих правил для портов следует настроить для этого?
  - a. Один узел.
  - b. Отключить диапазон портов.
  - c. Фильтрация нескольких узлов, одно сходство.
  - d. Фильтрация нескольких узлов, без сходства.
3. Вы настраиваете правила для портов NLB-кластера в вашей организации. Вы хотите, чтобы клиенты перенаправлялись к узлу NLB из своей подсети. Какой из перечисленных режимов следует использовать при создании правила для портов?
  - a. Один узел, без сходства.
  - b. Фильтрация нескольких узлов, без сходства.
  - c. Фильтрация нескольких узлов, сетевое сходство.
  - d. Фильтрация нескольких узлов, одно сходство.
4. Вы готовитесь выполнить обновление операционной системы, которое потребует перезагрузки в четырех узлах NLB-кластера вашей организации. Вы хотите запретить создание новых сеансов в каждом узле, который будете обслуживать, не прерывая существующих сеансов. Какую из следующих команд следует использовать для этого?
  - a. Остановить.
  - b. Запустить.
  - c. Остановить сток.
  - d. Приостановить.

## Занятие 2. Средства кластеризации Windows Server 2008 R2

Отказоустойчивая кластеризация в Windows Server 2008 и 2008 R2 предоставляет решение для обеспечения доступности сетевых служб, использующих один источник данных, который может располагаться одновременно только в одном месте (пример — виртуальная машина Hyper-V). Управление отказоустойчивыми кластерами в Windows Server 2008 и 2008 R2 выполняется с помощью оснастки **Диспетчер отказоустойчивости кластеров**. Отказоустойчивая кластеризация доступна только для компьютеров под управлением Windows Server 2008 и 2008 R2 Enterprise и Datacenter.

---

**Изучив материал этого занятия, вы сможете:**

- ✓ Понимать принципы работы отказоустойчивой кластеризации.
- ✓ Настраивать отказоустойчивые кластеры.
- ✓ Выполнять перенос кластеров.

---

**Продолжительность занятия — примерно 60 мин.**

---

Отказоустойчивые кластеры поддерживают два типа приложений: с единственным экземпляром и с несколькими экземплярами. Различие между такими приложениями заключается в следующем:

- **Приложение с одним экземпляром** может работать только на одном сервере одновременно. Пример — сервер проверки подлинности. Если служба сервера проверки подлинности работает одновременно на нескольких серверах, клиент может получать несколько ответов на запрос проверки подлинности, и некоторые из этих ответов могут конфликтовать, когда один сервер сообщает об успешном прохождении проверки, а другой — о неудачном. При объединении в кластер приложения с одним экземпляром должны работать на одном узле, пока другие узлы находятся в режиме ожидания.
- **Приложения с несколькими экземплярами** могут совместно использовать данные или разделять их так, что один узел кластера будет предоставлять ответы для определенной части этих данных. В такой манере могут работать некоторые почтовые серверы и СУБД. Приложения с несколькими экземплярами менее распространены, чем приложения с одним экземпляром.

Для работы в кластере приложение должно соответствовать следующим критериям:

- приложение кластера должно использовать протокол на основе IP;
- приложения, требующие доступа к локальным базам данных, должны позволять настраивать место хранения данных, например, размещать виртуальную машину в общем хранилище, а не на локальном жестком диске;
- если приложению требуется доступ к данным, не зависящий от узла кластера, в котором оно работает, данные должны храниться в общем ресурсе, отказоустойчивость которого будет обеспечиваться группой **Службы и приложения** (Services And Applications). Этот общий ресурс может работать на устройствах iSCSI, SCSI последовательным подключением или Fibre Channel;
- если приложение может работать и хранить данные только в локальной системе или на загрузочном диске, следует выбрать модель кворума «Большинство узлов» (Node Majority) или «Большинство узлов и общих ресурсов» (Node and File Share Majority). Также потребуется механизм репликации отдельных файлов для этих приложения. Подробнее о моделях кворумов рассказывается далее;
- если приложение столкнется со сбоем сети или аварийно перейдет к дополнительному узлу кластера, сеансы клиента должны иметь возможность восстановить подключение. В процессе переключения клиентские подключения будут отсутствовать, пока приложение не вернется в сеть. Если после раз-



рыва связи с сетью клиентская программа не пытается повторно подключиться, а переходит в режим ожидания, это приложение не подходит для отказоустойчивых кластеров (или кластеров NLB).

---

## **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Требования к отказоустойчивым кластерам Windows Server 2008 R2**

Подробнее о требованиях к отказоустойчивым кластерам Windows Server 2008 R2 см. по адресу [http://technet.microsoft.com/ru-ru/library/ff182359\(WS.10\).aspx](http://technet.microsoft.com/ru-ru/library/ff182359(WS.10).aspx).

---

## **Принципы работы кластеров**

Для создания кластера в Windows Server 2008 и 2008 R2 необходимо выполнение ряда требований. Как и Windows Server 2003, Windows Server 2008 требует одинаковой архитектуры процессора, 32- или 64-разрядной, и смешивать архитектуры процессоров в кластере нельзя. В отличие от Windows Server 2003, кластеризация в Windows Server 2008 и 2008 R2 больше не поддерживает прямые подключения SCSI к общему хранилищу. Для общего сетевого хранилища можно использовать Fibre Channel, SCSI с последовательным подключением (SAS) и iSCSI. Все серверы в кластере должны входить в один домен AD DS и работать под управлением одинаковых ОС.

## **Модели кворума кластера**

Кластеры прекращают работу после определенного числа сбоев, чтобы защитить целостность данных и предотвратить проблемы, которые могут возникнуть из-за нарушения связи между узлами. Кворум определяет число сбоев, которые выдерживает кластер перед прекращением работы. Кворум существует как база данных в реестре и поддерживается на диске-свидетеле или общем ресурсе-свидетеле. Диск-свидетель или общий ресурс-свидетель хранит копию данных конфигурации, чтобы серверы могли в любое время присоединиться к кластеру, получив копию этих данных, чтобы стать частью кластера. Данными ресурса кворума управляет один сервер, однако у всех серверов-участников также имеется копия. Windows Server 2008 и 2008 R2 используют четыре модели кворума:

- **Большинство узлов.** Эта модель кворума подходит для развертывания отказоустойчивых кластеров, содержащих нечетное число узлов кластера. Кластер модели «Большинство узлов» сохраняет кворум, если число доступных узлов превышает число вышедших из строя узлов. Например, чтобы кластер из семи узлов продолжал работать, должны быть доступны четыре узла. Если в таком кластере выйдут из строя четыре узла, то весь кластер отключится. Кластеры модели «Большинство узлов» следует использовать для объединения в кластер узлов, распределенных географически или по сети. Для успешной работы этой модели требуется очень надежная сеть, высококачественное оборудование и сторонний механизм репликации данных.
- **Большинство узлов и дисков.** Эта модель кворума подходит для кластеров, содержащих четное число узлов. Пока доступен диск-свидетель, кластер модели «Большинство узлов и дисков» продолжает работать, если доступна половина или более узлов. Например, кластер из шести узлов сохранит кворум, если доступно три или более узлов и диск-свидетель. В этой модели

кворум кластера хранится на диске кластера, который располагается на общем запоминающем устройстве и доступен всем узлам кластера посредством подключений SCSI с последовательным подключением (SAS), Fibre Channel или iSCSI. Эту модель следует использовать в отказоустойчивых кластерах с общим хранилищем, подключенных к одной сети и имеющих четное число узлов. В случае сбоя диска-свидетеля должно работать большинство узлов. Например, кластер из шести узлов будет работать, если доступны три узла и диск-свидетель. Если диск-свидетель недоступен, такой кластер должен иметь четыре доступных узла.

- **Большинство узлов и общих ресурсов.** Эта модель аналогична модели «Большинство узлов и дисков», но квorum хранится в сетевом общем ресурсе, а не на диске-свидетеле. Развертывание кластера модели «Большинство узлов и общих ресурсов» аналогично развертыванию кластера модели «Большинство узлов».
- **Без большинства: только диск.** Эту модель можно использовать для кластеров, имеющих нечетное число узлов, однако Microsoft не рекомендует использовать ее в производственной среде, поскольку квorum является единственной точкой отказа. Кластеры модели «Без большинства: только диск» лучше всего подходят для тестирования развертывания встроенных или пользовательских служб и приложений в отказоустойчивом кластере Windows Server 2008 R2. В этой модели кластер может поддерживать отказоустойчивость всех узлов, кроме одного, если доступен диск, содержащий квorum. В случае отказа диска, содержащего квorum, происходит отказ кластера, даже если доступны остальные узлы.

---

### СОВЕТ Подготовка к экзамену

Несмотря на то, что во время создания кластера модель кворума кластера выбирается автоматически, вы должны знать требования для каждой модели, включая необходимое число доступных узлов.

---

Перед развертыванием отказоустойчивого кластера решите, следует ли использовать общее хранилище. Если будете использовать общее хранилище, убедитесь, что каждый узел может взаимодействовать с каждым номером логического устройства (LUN), который представляет запоминающее устройство. Доступность общего хранилища для каждого узла с помощью мастера проверки конфигурации (рис. 11-6).

Когда вы настроите кластер, мастер создания кластера предложит для него наиболее подходящую модель кворума. Например, если создается кластер с одним узлом, мастер предложит модель кворума «Большинство узлов». Если вас не устроит предложенная модель, можно изменить ее при помощи диспетчера отказоустойчивости кластеров. Если выбранная модель использует общее хранилище и диск-свидетель, для этого диска будет выбран наименьший из имеющихся номеров LUN. При необходимости можно изменить его после создания кластера.

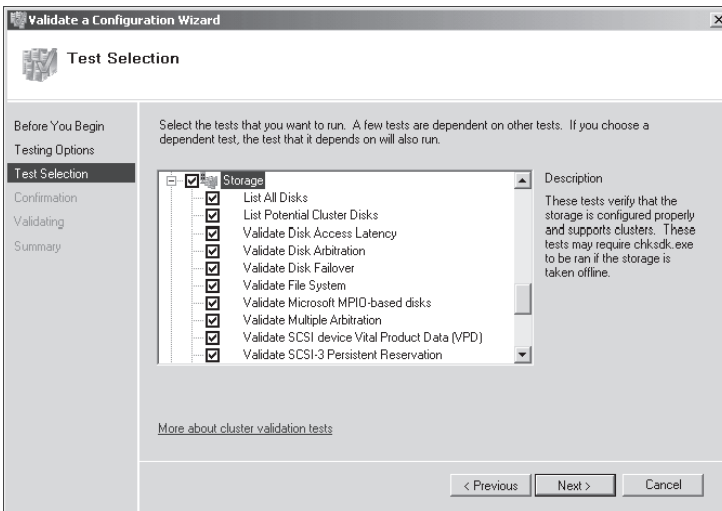


Рис. 11-6. Проверка общего хранилища кластера

Для просмотра используемой в текущий момент модели кворума кластера выполните следующее:

1. Откройте **Диспетчер отказоустойчивости кластеров** (Failover Cluster Manager). На панели **Действия** (Actions) щелкните **Дополнительные действия** (More Actions), а затем щелкните **Настроить параметры кворума кластера** (Configure Cluster Quorum Settings). Откроется мастер настройки кворума кластера.
2. На странице **Выбрать конфигурацию кворума** (Select Quorum Configuration) выберите модель кворума. На этой странице будет выбрана рекомендуемая модель кворума (рис. 11-7).

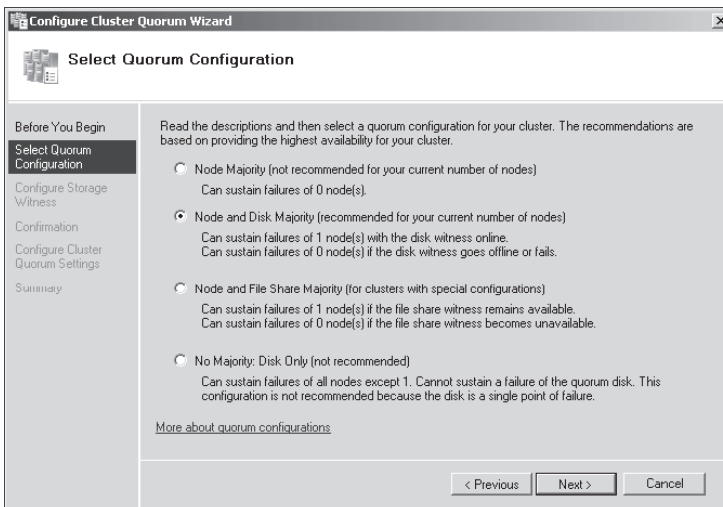


Рис. 11-7. Настройка кворума

## Установка средства отказоустойчивости кластеров

В Windows Server 2008 и Windows Server 2008 R2 компонент **Средство отказоустойчивости кластеров** (Failover Clustering) можно установить с помощью диспетчера серверов. Если в Windows Server 2008 R2 установлен модуль PowerShell диспетчера сервера, можно также использовать следующую команду Windows PowerShell:

```
Add-WindowsFeature Failover-Clustering
```

Отказоустойчивая кластеризация поддерживается только в версиях Enterprise и Datacenter Windows Server 2008 и 2008 R2.

## Проверка конфигурации отказоустойчивости кластера

Перед созданием кластера следует проверить конфигурацию компьютеров, которые будут узлами этого кластера. В Windows Server 2008 и 2008 R2 есть несколько тестов для проверки кластеров. Проверка конфигурации хранилища, сети и самого сервера выполняется с помощью мастера проверки конфигурации. Проверка серверов, которые станут частью кластера, позволяет убедиться в совместимости и функциональности предложенной конфигурации кластера.

В кластер рекомендуется добавлять аналогичные компоненты, включая соответствующие компьютеры. Кроме того, при создании отказоустойчивых кластеров учитывайте следующее:

- Устраняйте отдельные точки отказа, например, узлы с одним или несколькими сетевыми подключениями, выполняющимися к одному коммутатору. Если не сделать этого, при проверке может появиться предупреждение, хотя тесты успешно завершатся.
- Параллельные устройства SCSI нельзя использовать в качестве хранилищ, а для разделов кластера рекомендуется NTFS. Для диска-свидетеля также требуется NTFS.
- Все хранилища, использующие многопутевой ввод-вывод, должны быть проверены поставщиком, чтобы убедиться, что они подходят для отказоустойчивых кластеров Windows Server 2008 и 2008 R2.

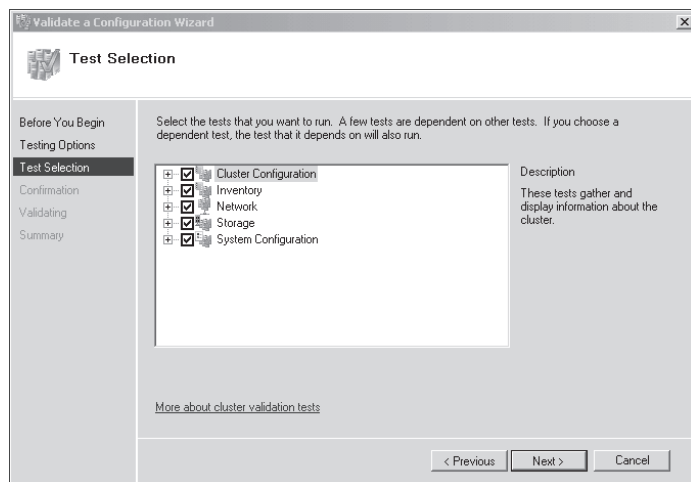


Рис. 11-8. Проверки кластера

Мастер проверки конфигурации содержит 5 категорий проверок (рис. 11-8):

- **проверки конфигурации кластера** — проверяют совместимость компонентов с предлагаемой конфигурацией на уровне кластера.
- **проверки учета** — обеспечивают учет компонентов и параметров в узле;
- **проверки сети** — проверяют, подходят ли параметры сети для кластеризации;
- **проверки хранилища** — проверяют возможность кластеризации хранилища;
- **проверки конфигурации системы** — проверяют параметры системы на серверах.

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Проверки кластера

Подробнее о проверках кластеров см. по адресу <http://technet.microsoft.com/ru-ru/library/cc726064.aspx>.

## Создание отказоустойчивого кластера

Перед созданием отказоустойчивого кластера убедитесь, что на всех потенциальных узлах кластера установлен компонент **Средство отказоустойчивости кластеров** (Failover Cluster). Для создания отказоустойчивого кластера выполните следующее:

1. На одном из узлов, который хотите сделать членом отказоустойчивого кластера, откройте Оснастку **Диспетчер отказоустойчивости кластеров** (Failover Cluster Manager) из меню **Администрирование** (Administrative Tools).
2. На панели **Действия** (Actions) щелкните **Создать кластер** (Create A Cluster). Запустится мастер создания кластеров. Щелкните **Далее**.
3. На странице выбора серверов введите имена всех серверов, которые будут действовать как узлы кластера, и щелкните **Добавить** (Add). Щелкните **Далее**.

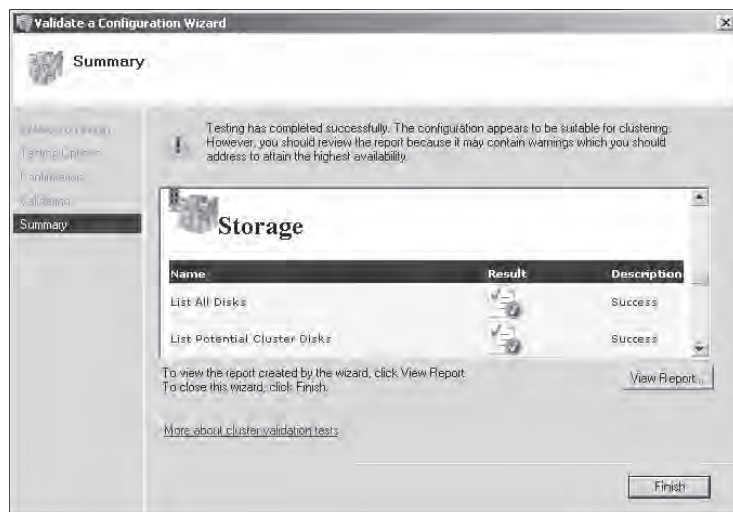


Рис. 11-9. Конфигурация, подходящая для кластеризации

4. На странице **Предупреждение проверки** (Validation Warning) укажите, нужно ли выполнять проверки, и щелкните **Далее**. Если выбрано выполнение проверок, запустится мастер проверки конфигурации. Выберите проверки, которые требуется выполнить, и начните их выполнение. Этот процесс займет несколько минут, после чего мастер сообщит, подходит ли конфигурация для кластеризации (рис. 11-9). Щелкните **Готово**, чтобы закрыть мастер.
5. В диалоговом окне **Точка доступа для администрирования кластера** (Access Point For Administering The Cluster) введите имя и IP-адрес кластера и щелкните **Далее**. На странице подтверждения щелкните **Далее**. После этого будет создан кластер. Щелкните **Готово**, чтобы закрыть мастер.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Создание кластеров

Подробнее о создании отказоустойчивых кластеров и добавлении узлов к существующим отказоустойчивым кластерам см. по адресу <http://technet.microsoft.com/ru-ru/library/cc730647.aspx>.

---

## Настройка служб для обеспечения высокой доступности

Для использования в отказоустойчивом кластере можно настроить несколько служб и приложений. Для настройки этих служб и приложений используется мастер высокой надежности. Некоторые приложения и службы имеют специфические параметры и доступны в мастере высокой надежности. Службы и приложения, отсутствующие в мастере, должны использовать параметр **Универсальная служба** (Generic Service), **Универсальное приложение** (Generic Application) или **Универсальный сценарий** (Generic Script). В мастер включены следующие службы и приложения:

- **Сервер пространств имен DFS** — предоставляет виртуальное представление общих папок организации;
- **Сервер DHCP** — предоставляет клиентам IP-адреса;
- **Координатор распределенных транзакций (DTC)** — обеспечивает поддержку распределенных приложений, используемых для выполнения транзакций. Транзакция — набор задач, которые должны одновременно выполняться успешно или не выполняться совсем;
- **Файловый сервер** — предоставляет возможность хранения файлов в сети;
- **Служба имен хранилищ Интернета (iSNS)** — предоставляет каталог конечных объектов iSCSI;
- **Очередь сообщений** — используется распределенными приложениями для связи;
- **Другой сервер** — предоставляет клиентскую точку доступа и хранилище для приложения, которое настраивается после создания кластера;
- **Сервер печати** — управляет очередью печати для общего принтера;
- **Посредник подключений к удаленному рабочему столу** — позволяет балансировать нагрузку сеансов в ферме удаленных рабочих столов;
- **Виртуальная машина** — обеспечивает высокую надежность виртуальной машины в кластере Hyper-V;

■ **Сервер WINS** — обеспечивает доступность сервера WINS.

Чтобы настроить службу для обеспечения высокой надежности, выполните следующее:

1. Откройте диспетчер отказоустойчивости кластеров. Щелкните **Настроить службу или приложение** (Configure A Service Or Application) на панели **Действия**. Запустится мастер высокой надежности. Щелкните **Далее**.
2. На странице выбора службы или приложения (рис. 11-10) выберите службу, для которой хотите настроить высокую надежность, и щелкните **Далее**. Эта служба уже должна быть установлена на узлах кластера.

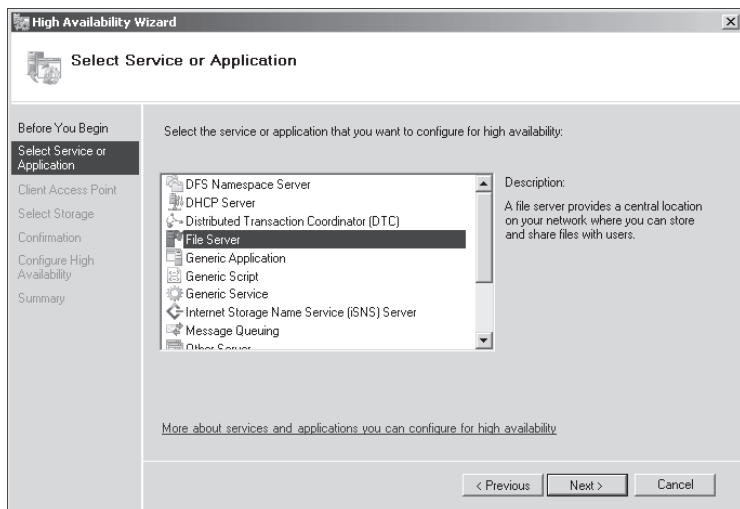


Рис. 11-10. Добавление службы в кластер

3. На странице **Точка доступа клиента** (Client Access Point) укажите адрес, который клиент будет использовать для доступа к службе с высокой надежностью, и щелкните **Далее**.
4. На странице **Выбор хранилища** (Select Storage) выберите тома хранилища, которые хотите назначить приложению с высокой надежностью, и щелкните **Далее**. На странице подтверждения щелкните **Далее**. Приложение станет высоконадежным. Щелкните **Готово**, чтобы закрыть мастер.

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Настройка приложения или службы с высокой надежностью

Подробнее о настройке службы или приложения с высокой надежностью см. по адресу <http://technet.microsoft.com/ru-ru/library/cc731960.aspx>.

## Управление отказоустойчивым кластером

Управление кластером выполняется при помощи диспетчера отказоустойчивости кластеров. Раскройте кластер в дереве консоли, чтобы просмотреть его параметры, включая узлы, сети, события кластера и хранилище (рис. 11-11).

Чтобы приостановить работу узла, выберите его и щелкните **Приостановить** (Pause) на панели **Действия**. Для возобновления работы узла щелкните **Воз-**



**обновить.** Для приостановки и возобновления работы узлов можно использовать также утилиту командной строки Cluster.exe. Чтобы приостановить работу узла VAN-SRV1 из кластера DEMO-CLUSTER, откройте командную строку, щелкнув **Пуск | Командная строка**, и введите следующую команду:

```
cluster DEMO-CLUSTER node VAN-SRV1 /pause
```

Для возобновления работы узла введите следующую команду:

```
cluster DEMO-CLUSTER node VAN-SRV1 /resume
```

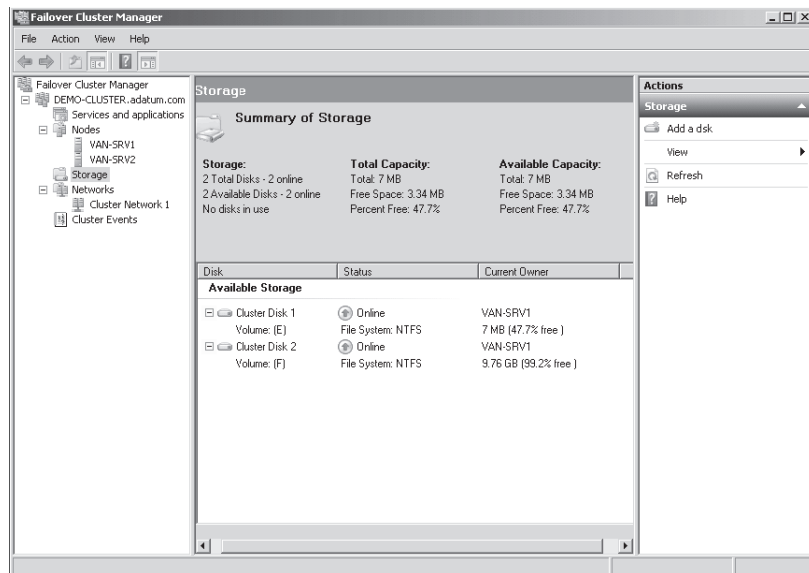


Рис. 11-11. Диспетчер отказоустойчивости кластеров

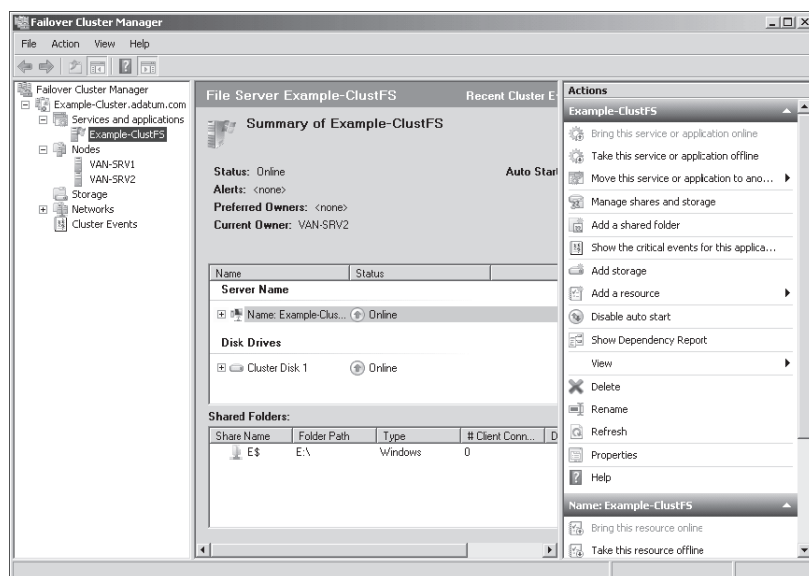


Рис. 11-12. Управление приложениями кластера

Обслуживание служб и приложений кластера выполняется из узла **Службы и приложения** (Services And Applications) диспетчера отказоустойчивости кластеров (рис. 11-12). Доступны три основные управляющие команды:

- **Перевести службу или приложение в автономный режим.** Если требуется выполнить обслуживание приложения, это можно сделать в автономном режиме. Все активные подключения к приложению будут отключены.
- **Перевести службу или приложение в оперативный режим.** После выполнения задач в автономном режиме переведите службу или приложение обратно в оперативный режим.
- **Переместить службу или приложение на другой узел кластера.** Это чаще всего выполняется для выполнения обслуживания узла, а не приложения. Сначала выполните обслуживание пассивного узла, после чего переместите в него приложение и выполните обслуживание узла, который изначально был активным.

## Резюме

- Отказоустойчивая кластеризация используется для взаимодействующих с сеансами приложений, которые нуждаются в общем хранилище данных и способны его использовать.
- В Windows Server 2008 используется четыре модели кворума: «Большинство узлов», «Большинство узлов и дисков», «Большинство узлов и общих ресурсов» и «Без большинства: только диск».
- Для управления отказоустойчивыми кластерами используется оснастка **Диспетчер отказоустойчивости кластеров** файлов и утилиты командной строки Cluster.exe.
- Общее хранилище должно быть доступно для всех узлов кластера. Наиболее распространенные типы общего хранилища — iSCSI и Fibre Channel.
- Проверка кластеров, узлов, сети и хранилища, а также настройка кластеров выполняется с помощью мастеров.

## Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных на занятии 2. Эти вопросы предоставлены также в электронном виде на прилагаемом к книге компакт-диске.

---

### ПРИМЕЧАНИЕ Ответы

Ответы на вопросы и пояснения к их вариантам размещены в разделе «Ответы» в конце книги.

---

1. Какие модели кворума можно использовать для отказоустойчивых кластеров с нечетным числом узлов? (Каждый ответ является самостоятельным решением. Выберите два.)
  - a. Большинство узлов и общих ресурсов.
  - b. Большинство узлов.
  - c. Без большинства: только диск.

- d. Большинство узлов и дисков.
- 2. У вас есть кластер с двумя узлами, использующими общий ресурс, расположенный на другом сервере, работающий в режиме «Большинство узлов и общих ресурсов». Что произойдет с приложением и кластером после выхода из строя аппаратуры на одном из серверов?
  - a. Приложение будет продолжать работать, так как модель кворума позволяет это делать.
  - b. Произойдет сбой приложения, так как диск-свидетель будет недоступен.
  - c. Ответ зависит от того, на каком сервере на тот момент находился ресурс кластера.
  - d. Произойдет сбой приложения, так как используемая модель кворума требует прекращения обслуживания, если половина узлов станет недоступной.
- 3. Какая из перечисленных операционных систем поддерживает отказоустойчивую кластеризацию? (Каждый ответ является самостоятельным решением. Выберите два.)
  - a. Windows Server 2008 R2 Foundation.
  - b. Windows Server 2008 R2 Standard.
  - c. Windows Server 2008 R2 Enterprise.
  - d. Windows Server 2008 R2 Datacenter.
- 4. Ваш кластер использует модель кворума «Большинство узлов и дисков» и имеет восемь узлов. Учитывая, что общий диск остается в оперативном режиме, каково минимальное число серверов, у которых должен произойти сбой, прежде чем произойдет отключение кластера?
  - a. Один.
  - b. Три.
  - c. Четыре.
  - d. Пять.

## **Практикум. Установка и настройка кластера NLB в Windows Server 2008 R2**

На этом практикуме вы создадите и протестируете кластер NLB.

### **Упражнение 1. Подготовка DNS и рядовых серверов для создания кластера NLB**

В этом упражнении вы подготовите VAN-DC1, VAN-SRV1 и VAN-SVR2 для развертывания кластера NLB.

1. Выполните вход на сервер VAN-DC1 под учетной записью пользователя Kim Akers. Откройте командную строку с повышенными привилегиями и введите следующую команду:

```
Dnscmd /recordadd adatum.com nlb-cluster A 10.10.0.131
```

2. Выполните вход на сервер VAN-SRV1 под учетной записью пользователя Kim Akers и запустите сеанс PowerShell с повышенными привилегиями. Введите следующие команды:  
`Import-Module ServerManager`  
`Add-WindowsFeature NLB,Web-Server`
3. Выполните вход на сервер VAN-SRV2 под учетной записью пользователя Kim Akers и запустите сеанс PowerShell с повышенными привилегиями. Введите следующие команды:  
`Import-Module ServerManager`  
`Add-WindowsFeature NLB,Web-Server`  
`Mspaint.exe \inetpub\wwwroot\welcome.png`
4. В Paint проведите кистью по изображению Welcome.png и сохраните его. Это измененное изображение вы будете использовать, чтобы различать VAN-SRV1 и VAN-SRV2.
5. Откройте Internet Explorer на VAN-DC1 и перейдите к страницам *http://van-SRV1* и *http://van-SRV2*. Убедитесь, что страницы приветствия отличаются.

## Упражнение 2. Настройка и тестирование NLB-кластера

В этом упражнении вы настроите NLB-кластер, создадите правило для портов и проверите работу кластера.

1. Убедитесь, что вы выполнили вход на сервер VAN-SRV1 под учетной записью пользователя Kim Akers.
2. Из меню **Администрирование** откройте консоль диспетчера балансировки сетевой нагрузки. Получив запрос от службы контроля учетных записей, щелкните **Да**.
3. В меню **Кластер (Cluster)** выберите **Создать (New)**. Откроется мастер подключения к новому кластеру. В текстовом поле **Узел (Host)** введите **VAN-SRV1** и щелкните **Подключить (Connect)**. Щелкните **Далее**.
4. Убедитесь, что на странице **Создать кластер: Параметры узла (New Cluster: Host Parameters)** параметр **Приоритет (Уникальный идентификатор узла) [Priority (Unique Host Identifier)]** имеет значение **1**, и щелкните **Далее**.
5. На странице **Создать кластер: IP-адреса кластера (New Cluster: Cluster IP Addresses)** щелкните **Добавить (Add)**. В поле **Добавить IP-адрес (Add IP Address)** введите IP-адрес 10.10.0.131 и маску подсети 255.0.0.0, после чего щелкните **ОК**. На странице **Создать кластер: IP-адрес кластера (New Cluster: Cluster IP Address)** щелкните **Далее**.
6. На странице **Создать кластер: Параметры кластера (New Cluster: Cluster Parameters)** введите полное имя **nlb-cluster.adatum.com** и установите переключатель **Многоадресный (Multicast)** (рис. 11-13). Щелкните **Далее**.
7. На странице **Создать кластер: Правила для портов (New Cluster: Port Rules)** щелкните **Готово**.
8. Щелкните правой кнопкой узел **nlb-cluster.adatum.com** и выберите команду **Добавить узел к кластеру (Add Host To Cluster)**. В диалоговом окне **До-**

**бавить узел к кластеру: Подключить** (Add Host To Cluster: Connect) введите имя VAN-SRV2 и щелкните **Подключить**. Убедитесь, что в списке доступных интерфейсов появился интерфейс локального подключения к сети с IP-адресом 10.10.0.21. Дважды щелкните **Далее**, а затем щелкните **Готово**.

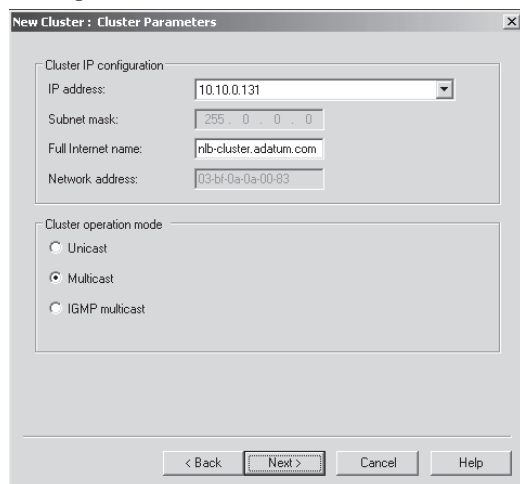


Рис. 11-13. Настройка многоадресного режима

9. Когда оба узла NLB-кластера будут отображаться в списке с состоянием **Схождение выполнено** (Converged), щелкните правой кнопкой узел nlb-cluster.adatum.com и выберите команду **Свойства кластера** (Cluster Properties). На вкладке **Правила для портов** (Port Rules) выберите существующее правило и щелкните **Удалить** (Remove).
10. Щелкните **Добавить**. В разделе **Диапазон портов** (Port Range) введите **80** в полях **От** (From) и **До** (To). Установите переключатель **Несколько узлов** (Multiple Host) в секции **Режим фильтрации** (Filtering Mode) и переключатель **Отсутствует** (None) в секции **Сходство** (Affinity), после чего щелкните **ОК**. Еще раз щелкните **ОК**, чтобы закрыть диалоговое окно свойств кластера. Дождитесь, когда оба узла отобразятся в списке с состоянием **Схождение выполнено**. Возможно, потребуется щелкнуть **Обновить** (Refresh).
11. На сервере VAN-DC1 запустите Internet Explorer и перейдите по адресу <http://nlb-cluster.adatum.com>. Закройте Internet Explorer и снова запустите, открыв ту же страницу <http://nlb-cluster.adatum.com>. Повторяйте эти действия, пока не увидите измененную и исходную страницы приветствия служб IIS 7.
12. Выключите сервер VAN-SRV2. На сервере VAN-DC1 проверьте, сохранилось ли подключение к <http://nlb-cluster.adatum.com>.

### Упражнение 3. Удаление кластера NLB и компонента NLB

В этом упражнении вы удалите кластер NLB, а затем удалите компоненты NLB и IIS с серверов VAN-SRV2 и VAN-SRV1.

1. Включите сервер VAN-SRV2 и выполните вход под учетной записью пользователя Kim Akers.

2. Откройте диспетчер балансировки сетевой нагрузки из меню **Администрирование**. Щелкните **Да**, когда получите запрос от службы контроля учетных записей. Когда получите предупреждение, щелкните **ОК**.
3. Щелкните правой кнопкой мыши узел nlb-cluster.adatum.com и выберите **Удалить кластер (Delete Cluster)**. Получив предупреждение, щелкните **Да**.
4. После удаления кластера запустите сеанс PowerShell с повышенными привилегиями и введите следующие команды:  

```
Import-Module ServerManager
Remove-WindowsFeature NLB,Web-Server -Restart
```
5. Выполните вход на сервер VAN-SRV1, запустите сеанс PowerShell с повышенными привилегиями и введите следующие команды:  

```
Import-Module ServerManager
Remove-WindowsFeature NLB,Web-Server -Restart
```
6. Для завершения упражнения выключите все серверы.

## Закрепление материала главы

Чтобы попрактиковаться и закрепить знания, полученные при изучении этой главы, выполните следующее:

- прочитайте резюме главы;
- просмотрите список основных терминов, представленных в этой главе;
- выполните задания лабораторной работы, моделирующей реальные ситуации, требующие применения полученных знаний;
- выполните рекомендуемые упражнения;
- пройдите пробный тест.

## Резюме главы

- В Windows Server 2008 и 2008 R2 используются следующие три основных способа обеспечения высокой доступности и избыточности: циклическое обслуживание DNS, NLB и отказоустойчивая кластеризация.
- Циклическое обслуживание DNS и NLB можно развертывать для приложений, которые могут использовать собственные хранилища данных, например, для веб-сайтов. Отказоустойчивую кластеризацию следует развертывать для приложений, имеющих общее хранилище данных, например, для виртуальных машин или баз данных Microsoft SQL Server.
- Если вы собираетесь использовать отказоустойчивый кластер Windows Server 2008 с общим хранилищем данных, то общий том должен быть доступен всем узлам кластера.
- NLB создает виртуальный сетевой адаптер и имеет два режима работы: одноадресный и многоадресный. Одноадресный режим подходит для узлов, имеющих два и более сетевых адаптеров. Его можно использовать и для NLB-кластеров, в которых узлы имеют один адаптер, однако это затрудняет

удаленное управление. Многоадресный режим NLB подходит для узлов, имеющих один адаптер. Многоадресный режим IGMP можно использовать для предотвращения заполнения коммутаторов многоадресным трафиком.

## Основные термины

Проверьте, знаете ли вы, что означают перечисленные ниже термины из этой главы:

- Циклическое обслуживание DNS.
- Отказоустойчивая кластеризация.
- Балансировка сетевой нагрузки (NLB).
- Модель кворума.

## Лабораторная работа

Для выполнения заданий лабораторной работы используйте знания о планировании установки и обновления серверов, полученные из этой главы. Ответы можно найти в разделе «Ответы» в конце книги.

### Задание 1. Выбор подходящей стратегии доступности

Вы администратор в компании, работающей в сети, где 98% серверов работают под управлением Windows Server 2008, а 2% — под управлением Linux. Руководство компании пришло к выводу, что наиболее важными для бизнеса являются три приложения, которые в случае отказа сервера должны оставаться доступными без потери данных. Эти приложения имеют следующие характеристики:

- Первое приложение — база данных SQL Server 2008 R2, содержащая данные о связях с клиентами. СУБД SQL Server 2008 R2 установлена на компьютере под управлением Windows Server 2008 R2.
- Второе приложение — основной веб-сайт компании, содержащий только статичные информационные страницы и работающий под управлением IIS в Windows Server 2008 R2.
- Третье приложение — внутренняя служебная программа, использующая веб-серверы под управлением Linux.

Вы имеете доступ к дополнительным компьютерам под управлением Windows Server 2008 R2. Кроме того, есть возможность использовать SAN для удовлетворения требований доступности. Учитывая эти факты, ответьте на следующие вопросы:

- Как повысить доступность приложений?
- Что следует предпринять для реализации отказоустойчивой кластеризации?
- Если вы выберете отказоустойчивую кластеризацию для любого из приложений, какую модель кворума следует использовать и почему?



## Рекомендуемые упражнения

Чтобы успешно справиться с экзаменационными заданиями по темам этой главы, выполните следующие упражнения.

### Планирование высокой доступности

1. Создайте отказоустойчивый кластер, не имеющий доступа к общему хранилищу.
2. Настройте службу DHCP как службу с высокой доступностью.
3. Добавьте два дополнительных узла в NLB-кластер, который вы создали во время выполнения упражнений практикума
4. Создайте два новых правила для портов NLB. Создайте правило для порта 25, которое будет направлять весь трафик этого порта одному узлу отказоустойчивого кластера. Второе правило настройте так, чтобы кластер отклонял весь трафик, полученный через порты 1025–2024.

## Пробный экзамен

Тренировочные тесты на прилагаемом к книге компакт-диске позволяют проверить знания только по одной или сразу по всем темам сертификационного экзамена 70-646. Тестирование можно организовать так, чтобы оно проводилось как настоящий экзамен, а можно проходить в режиме обучения, просматривая правильные ответы и объяснения после каждого ответа.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Пробный экзамен

Подробнее о пробном экзамене рассказано во Введении.

---

## Оценка и оптимизация производительности

### Занятие 1. Данные мониторинга

519

В этой главе рассказывается о планировании мониторинга ресурсов и производительности на компьютере под управлением Windows Server 2008 R2. Мы рассмотрим различные инструменты, позволяющие узнать, какие ресурсы доступны на компьютере, и сообщающие о проблемах, возникающих при использовании того или иного ресурса. Затем мы обсудим мониторинг серверов и служб для повышения производительности и оптимизации работы, формирование базовых показателей и журналов для выявления и интерпретации тенденций, а также определение возможных узких мест.

Кроме этого, мы поговорим об оценке потенциала компьютера для выполнения ресурсоемких задач, о получении локальных событий и событий с других компьютеров. Эта глава посвящена предварительному планированию, выявлению тенденций и решению проблем до того, как они станут заметны пользователю. Однако для планирования требуется точно знать, что может предложить тот или иной инструмент, поэтому мы опишем доступные средства. Иногда в работе служб, процессов и приложений возникают проблемы, и мы обсудим способы их решения.

### Темы экзамена

- Мониторинг серверов для оценки и оптимизации производительности.

### Прежде всего

Для выполнения упражнений этой главы потребуется:

- Сервер с именем VAN-DC1, работающий под управлением Windows Server 2008 R2 Enterprise, настроенный как контроллер домена adatum.com, как описано в Приложении.
- Учетная запись пользователя Kim Akers с паролем Pa\$\$w0rd в домене adatum.com, включенная в группы администраторов домена, администраторов предприятия и администраторов схемы. Процедура создания этой учетной записи описана в Приложении.

- Дополнительный сервер VAN-SRV1, работающий под управлением Windows Server 2008 R2 Enterprise, настроенный как рядовой сервер в домене Adatum.com, как описано в Приложении. Этот сервер не используется для выполнения практических упражнений этой главы, но потребуется для настройки компьютера-источника и компьютера-сборщика для подписок на события.
- Для выполнения практических упражнений рекомендуем использовать изолированную сеть, не входящую в рабочую сеть. Доступ к Интернету не требуется, как и настройка шлюза по умолчанию. Для экономии времени и затрат на настройку физических компьютеров используйте виртуальные машины, например, созданные с использованием роли сервера Hyper-V.
- Для выполнения практикума этой главы необходим доступ к дополнительному запоминающему устройству, подключенному к контроллеру домена VAN-DC1. Потребуется лишь небольшой объем для хранения данных, и если вы используете физические компьютеры, достаточно будет флэш-накопителя USB объемом 500 МБ. Однако в гл. 13 потребуется дополнительный диск объемом 40 ГБ. Этот диск может быть дополнительным виртуальным диском, если вы используете виртуальные машины. Если используются физическое оборудование, это может быть физический диск, накопитель USB 2.0 или IEEE 1394. Если вы установите такой диск для практикума этой главы, его можно будет использовать и на практикуме гл. 13.

## Реальный мир

*Йен Маклин*

В предыдущей книге я сделал довольно глупое заявление. Я сказал, что обычно проще получить деньги на обновление серверов, чем на обновление клиентов. Мои доводы были основаны на том, что серверов требуется не так много, а за счет виртуализации и того меньше. Я утверждал, что проще обосновать расходы на обновление полудюжины серверов, чем на обновление 500 рабочих станций.

Почти одновременно с выходом книги разразился мировой финансовый кризис (надеюсь, эти два события не связаны). В нынешних нелегких финансовых условиях трудно получить деньги на обновление вообще чего-либо. Кроме того, большинству руководителей серверы кажутся таинственными черными ящиками, которые делают непонятные вещи. Прежде чем руководство согласится потратить деньги на серверы, потребуется доказать их важность. Как правило, старшие менеджеры технически не очень подкованы, но отнюдь не дураки. Они знают, что серверы имеют большое значение для организации, хотя и не вполне понимают, почему. Поэтому, если администратор сети говорит, что серверы необходимо обновить, его готовы выслушать, но только если он представит убедительные доводы, подкрепленные четкой статистикой.

Таким образом, сбор статистики о производительности серверов сегодня стал важнее, чем когда-либо. Вам в любом случае придется обновлять оборудование, если не сейчас, то через год-два. Начните готовить свои аргументы. Не забудьте сформировать базовые показатели производи-

тельности. Отслеживайте незначительные, но накапливающиеся ухудшения производительности по мере старения оборудования и увеличения потребностей пользователей. Начните формировать убедительные доводы в пользу обновлений, которые потребуются в будущем. Не откладывайте это на завтра, иначе завтра кто-то может сделать вашу работу вместо вас.

## Занятие 1. Данные мониторинга

Опытные администраторы наверняка уже имели дело с большинством инструментов и утилит, рассматриваемых в этой главе. Windows Server 2008 R2 предоставляет инструменты для измерения производительности, формирования базовых показателей производительности, обнаружения узких мест, просмотра ресурсов, измерения стабильности и надежности системы, а также для выполнения других функций. Вы, вероятно, хорошо понимаете важность определения базовых показателей для оценки периодов интенсивной, малой и обычной загрузки и сравнения с ними текущих результатов мониторинга для выявления тенденций. Важно помнить, что сравнение результатов и анализ тенденций следует выполнять не в произвольном порядке, а по плану.

Порой непросто выбрать нужный инструмент для работы, и в этом случае важную роль играет планирование. Зачастую можно использовать несколько инструментов для получения одной и той же информации или выполнения одной и той же настройки, однако при этом один из них более эффективен или предоставляет больше данных, помогающих выявлять тенденции и составлять отчеты для обоснования необходимости обновлений. Сбор информации о системе с помощью одного-двух инструментов не представляет особой сложности, но интерпретация этой информации может быть более сложной задачей. На этом занятии мы попытаемся разделить инструменты по функциональным группам и составить общий план возможного сочетания инструментов в каждой из групп.

---

### Изучив материал этого занятия, вы сможете:

- ✓ Использовать инструменты измерения производительности для просмотра данных производительности в режиме реального времени.
- ✓ Собирать данные в группы сборщиков данных (DCS).
- ✓ Создавать отчеты для выявления существующих и потенциальных узких мест ресурсов.
- ✓ Изучать свои и возможные проблемы, связанные с установкой программ и другими существенными изменениями системы.
- ✓ Отслеживать работающие службы и использовать инструмент **Службы** (Services).
- ✓ Собирать подписки на события с компьютеров-источников и пересылать их конечному компьютеру.

**Продолжительность занятия — примерно 50 мин.**

---

## Мониторинг производительности и создание отчетов

Мониторинг данных производительности и их сравнение с определенными базовыми показателями крайне важны для определения работоспособности сервера. Многие события имеют информационный характер, но это не значит, что их можно игнорировать. Знания и опыт должны подсказывать администратору, на что следует обратить особое внимание, а что можно пропускать. Никогда не игнорируйте предупреждения и сообщения об ошибках, которые сообщают о проблемах, требующих срочного решения.

Вы, вероятно, имеете опыт работы с инструментами измерения производительности Windows, такими как системный монитор и средство создания отчетов. Возможно, вам не знакомы группы DCS, которые используют счетчики производительности для создания журналов производительности и могут предоставлять данные для системного монитора и средства создания отчетов. Группы DCS заменяют журналы и оповещения производительности, используемые в предыдущих серверных ОС.

Ваша цель — спланировать оптимальный способ мониторинга и повышения производительности, выявить потенциальные узкие места и обновить соответствующие ресурсы. Особенно важно выявить источники критических проблем с производительностью, способных сделать работу компьютера недопустимо медленной или полностью невозможной.

### Системный монитор

В Windows Server 2008 R2 оснастку **Системный монитор** (Performance Monitor) можно открыть из меню **Администрирование** или командой perfmon. Эта оснастка (рис. 12-1) предоставляет доступ к системному монитору, группам сборщиков данных и инструменту **Отчеты** (Reports). Чтобы перейти к системному монитору, щелкните **Системный монитор** (Performance Monitor) в дереве консоли.

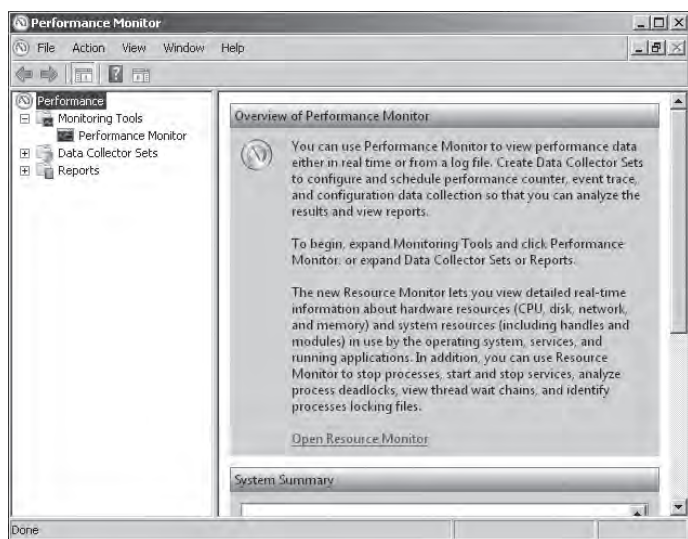


Рис. 12-1. Системный монитор

Чтобы добавить счетчики, щелкните зеленую кнопку «+» на панели инструментов системного монитора, раскройте категорию (например, **Память**), выберите счетчик и щелкните **Добавить** (Add). Можно отображать один экземпляр счетчика или сводку по всем экземплярам. Например, если сервер имеет несколько ЦП, можно выбрать счетчик, отслеживающий использование одного ЦП, или счетчик, отслеживающий использование всех ЦП. На рис. 12-2 показан системный монитор, отображающий данные в режиме реального времени.

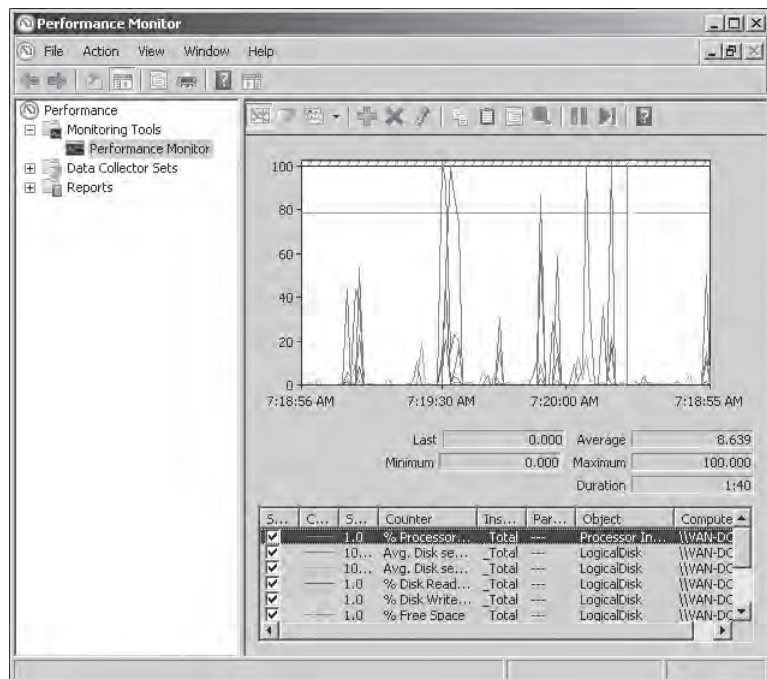


**Рис. 12-2.** Системный монитор, отображающий данные в режиме реального времени

Все линии графика имеют разный цвет. Чтобы было удобнее просматривать отдельный график, выберите его счетчик и нажмите **Ctrl+N**. Выбранный счетчик будет выделен на графике жирным черным цветом. Чтобы изменить внешний вид и частоту обновления диаграммы, щелкните правой кнопкой узел **Системный монитор** (Performance Monitor) и выберите команду **Свойства** (Properties). Пять вкладок диалогового окна свойств системного монитора предоставляют доступ к различным параметрам конфигурации:

- **Общие** (General) (рис. 12-3). В группе **Элементы диаграммы** (Graph Elements) можно ввести значение в поле **Съем показаний каждые** (Sample Every), чтобы изменить частоту изменения графика, и в поле **Длительность** (Duration), чтобы определить период сканирования. Можно указать, будет ли отображаться легенда, строка значений и панель инструментов, и какие значения будут показаны при просмотре данных в виде отчета и гистограммы: **По умолчанию** (Default), **Максимальные** (Maximum), **Минимальные** (Minimum), **Средние** (Average) или **Текущие** (Current).
- **Источник** (Source). На этой вкладке можно выбрать отображение текущей активности в режиме реального времени или файлов журнала, которые вы

сохранили с помощью групп DCS. Если в сети имеется сервер под управлением Microsoft SQL Server и используется подключение ODBC, можно указать базу данных по имени источника данных (DSN) и выбрать набор журналов.

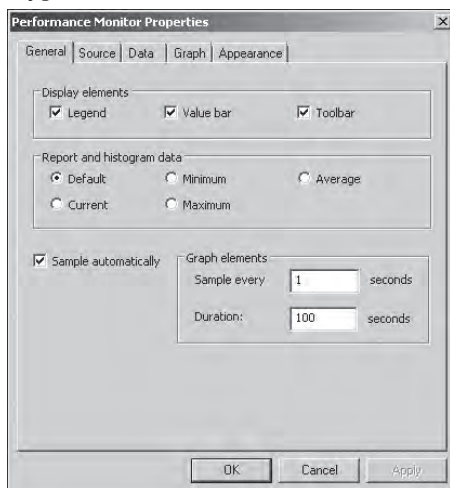


Рис. 12-3. Вкладка Общие окна свойства системного монитора

### СОВЕТ Подготовка к экзамену

На экзамене вряд ли будут подробные вопросы относительно баз данных SQL, ODBC или DSN.

- **Данные (Data).** В списке счетчиков на этой вкладке можно выбрать счетчик и настроить для него параметры **Цвет (Color)**, **Масштаб (Scale)**, **Ширина (Width)** и **Стиль (Style)**.
- **График (Graph).** По умолчанию по достижении указанной длительности системный монитор начинает переписывать графические значения счетчика в левой части графика. Если значения счетчика будут записываться в течение длительного промежутка времени, лучше изменить тип прокрутки на **Продвижение (Scroll)**. Можно также выбрать тип диаграммы, щелкнув кнопку **Изменить тип диаграммы (Change Graph Type)** на панели инструментов или нажав Ctrl+G:
  - **Строка (Line)** — этот тип выбран по умолчанию, значения отображаются в виде линий на диаграмме;
  - **Линейчатая гистограмма (Histogram Bar)** — линейчатый график текущих, максимальных, минимальных или средних значений счетчиков. Если счетчиков много, гистограмму читать проще, чем линейный график;
  - **Отчет (Report)** — отображает список текущих, максимальных, минимальных или средних значений счетчиков в текстовом отчете.
- **Оформление (Appearance).** Если одновременно открыто несколько окон системного монитора, на этой вкладке можно изменить цвет фона и других элементов.



### Проверьте себя

- На какой вкладке диалогового окна свойств системного монитора можно указать частоту обновления графиков?

### Ответ

- Для изменения частоты обновления графиков используется поле **Съем показаний каждые** (Sample Every), расположенное в группе **Элементы диаграммы** (Graph Elements) на вкладке **Общие** (General)

## Группы сборщиков данных

Группы сборщиков данных (DCS) собирают информацию о системе, в том числе параметры конфигурации и данные производительности, и хранят их в файле данных. С помощью системного монитора можно изучать файл данных и анализировать подробные данные производительности или создать отчет, объединяющий эту информацию.

Windows Server 2008 R2 содержит следующие встроенные группы DCS:

- **Производительность системы** (System Performance) — используется для решения проблем, связанных с замедлением работы системы или перебоями в производительности. Эта группа записывает данные счетчиков производительности процессора, диска, памяти и сети (IPv4 и IPv6), а также данные трассировки ядра.
- **Диагностика системы** (System Diagnostics) — используется для решения проблем, связанных с надежностью, таких как сбои оборудования, неисправности драйверов и STOP-ошибки. Эта группа записывает все те же данные, что и группа **Производительность системы**, и подробную информацию о системе. На рис. 12-4 показаны некоторые счетчики, включенные в набор данных **Диагностика системы**.

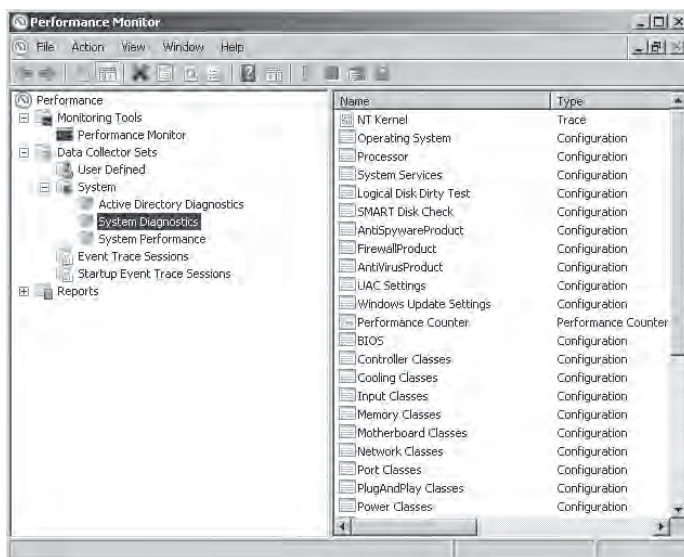


Рис. 12-4. Счетчики из набора данных Диагностика системы

- **Диагностика Active Directory** (Active Directory Diagnostics) — используется, если сервер под управлением Windows Server 2008 R2 является контроллером домена. Эта группа позволяет собирать данные производительности (например, в счетчик производительности ADDS) и создавать диагностические отчеты, помогающие анализировать проблемы производительности AD DS.

Чтобы использовать группу DCS, щелкните ее правой кнопкой и выберите команду **Пуск** (Start). Группа **Производительность системы** по умолчанию имеет общую длительность 10 минут, группа **Диагностика системы** — 1 минуту, а группа **Диагностика Active Directory** — 5 минут. Чтобы остановить группу DCS вручную, щелкните ее правой кнопкой и выберите команду **Стоп** (Stop).

После запуска группы DCS можно просматривать сводку собранных данных в узле **Отчеты** (Reports) системного монитора. Чтобы просмотреть последний отчет для группы DCS, щелкните ее правой кнопкой и выберите команду **Последний отчет** (Latest Report). После этого можно просмотреть отчет, выбрав его под узлом **Отчеты** (Reports). На рис. 12-5 показан отчет, сгенерированный запуском группы **Диагностика Active Directory** на VAN-DC1. Для доступа к подробной информации раскройте заголовки на правой панели.

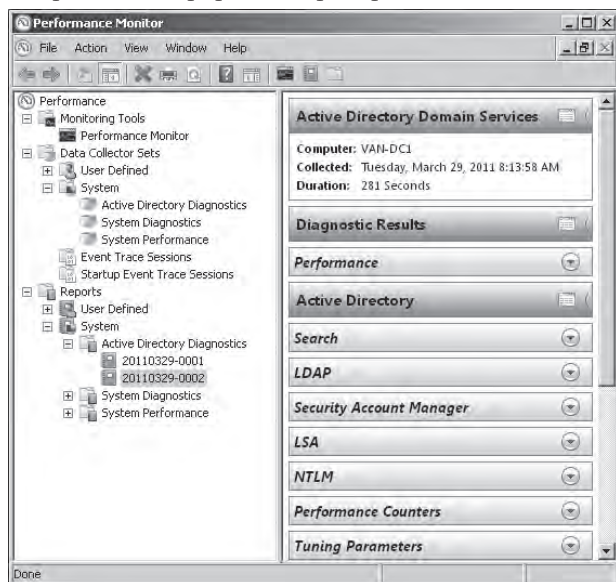


Рис. 12-5. Отчет диагностики Active Directory

В группы DCS можно добавлять оповещения счетчиков производительности. Это позволяет выполнять мониторинг счетчика и определять оповещение, которое затем можно использовать для запуска пакетного файла, отправки сообщения электронной почты или вызова на пейджер. Например, можно настроить оповещение, которое будет запускаться, когда свободного пространства на логическом томе остается меньше 30%, добавить это оповещение в группу DCS и использовать для запуска пакетного файла, архивирующего данные на этом томе.

Для ведения журнала требуется много системных ресурсов, а файлы журнала производительности могут становиться очень большими. Чтобы уменьшить падение производительности при ведении журнала, записывайте только мини-

мум необходимой информации. Например, по возможности следует использовать группу **Производительность системы** вместо **Диагностика системы**, так как она содержит меньше счетчиков.

## Создание группы сборщиков данных

Если возникает проблема с производительностью или требуется проанализировать и, если возможно, улучшить производительность сервера, можно использовать группы DCS для сбора данных производительности и сравнивать их с базовыми показателями. Настраиваемая группа DCS создается следующим образом:

1. Откройте оснастку **Системный монитор** (или утилиту **Системный монитор**), раскройте узел **Группы сборщиков данных** (Data Collector Sets), щелкните правой кнопкой **Особый** (User Defined), и выберите команду **Создать | Группа сборщиков данных** (New | Data Collector Set). Запустится мастер создания новой группы сборщиков данных.
2. На странице **Создать новую группу сборщиков данных** (Create New Data Collector Set) укажите имя группы. Убедитесь, что установлен переключатель **Создать из шаблона (рекомендуется)** [Create From A Template (Recommended)] и щелкните **Далее**.
3. На странице **Какие шаблоны следует использовать?** (Which Template Would You Like To Use?) выберите один из стандартных шаблонов: **Основной** (Basic), **Диагностика системы** (System Diagnostics) или **Производительность системы** (System Performance). На контроллере домена можно также выбрать **Диагностика Active Directory** (Active Directory Diagnostics). Щелкните **Далее**.
4. На странице **Где необходимо сохранить данные?** (Where Would You Like The Data To Be Saved?) щелкните **Далее**, чтобы принять расположение для данных по умолчанию.
5. На странице **Создать группу сборщиков данных?** (Create The Data Collector Set), оставьте параметры по умолчанию, чтобы создать и запустить группу DCS, используя учетные данные пользователя, выполнившего вход. Если требуется, щелкните **Изменить** (Change) и укажите альтернативные учетные данные администратора.
6. Установите один из трех переключателей и щелкните **Готово** (Finish):
  - **Открыть свойства группы сборщиков данных** (Open Properties For This Data Collector Set);
  - **Запустить группу сборщиков данных сейчас** (Start This Data Collector Set Now);
  - **Сохранить и закрыть** (Save And Close).

Настраиваемые группы DCS расположены под узлом **Особые** (User Defined) в группе DCS. Можно запланировать расписание запуска группы DCS и настроить условия ее остановки. Группу DCS можно запустить вручную, щелкнув ее правой кнопкой и выбрав **Пуск** (Start).

---

## ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Создание групп DCS

Подробнее о способах создания групп DCS см. по адресу <http://technet.microsoft.com/ru-ru/library/cc749337.aspx>.

---

### Настройка групп сборщиков данных

После создания группа DCS записывает только данные производительности, определенные в выбранном шаблоне. Чтобы добавить в группу DCS собственные источники данных, необходимо обновить ее после создания.

Для добавления источника данных производительности (например, счетчика производительности) в группу DCS щелкните правой кнопкой эту группу DCS и выберите команду **Создать | Сборщик данных** (New | Data Collector). Откроется мастер создания нового сборщика данных. На странице **Сборщик данных какого типа следует создать?** (What Type Of Data Collector Would You Like To Create?) укажите имя сборщика данных, выберите его тип и щелкните **Далее**. Доступны следующие типы сборщиков данных:

- **Сборщик данных счетчика производительности** (Performance Counter Data Collector) — позволяет собирать статистику производительности за длительные периоды времени для последующего анализа. Можно использовать его для установки отправных точек и анализа тенденций.
- **Сборщик данных отслеживания событий** (Event Trace Data Collector) — позволяет собирать информацию о событиях и активности системы.
- **Сборщик данных конфигурации** (Configuration Data Collector) — собирает информацию о разделах реестра, путях управления WMI и состоянии системы.
- **Оповещение счетчика производительности** (Performance Counter Alert) — позволяет настраивать оповещение, которое генерируется, когда показания определенного счетчика производительности превышают или опускаются ниже заданного значения.

В группу DCS можно добавить столько сборщиков данных, сколько требуется. Например, если на странице **Какой тип сборщика данных нужно создать?** выбрать **Сборщик данных счетчика производительности**, то на странице **Какие счетчики производительности следует записывать в журнал?** (рис. 12-6) можно щелкнуть **Добавить** и добавить счетчик производительности так же, как добавляется счетчик в монитор производительности. Затем можно снова щелкнуть **Добавить** и добавить еще один счетчик. Эту процедуру можно повторять до тех пор, пока не будут добавлены все необходимые счетчики.

Чтобы изменить сборщик данных в пользовательской группе DCS, выберите эту группу под узлом **Группы сборщиков данных | Особый** (Data Collector Sets | User Defined), в левой части окна щелкните правой кнопкой сборщик данных, который требуется отредактировать, и выберите команду **Свойства**.

---

## ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Свойства групп DCS

Подробнее о настройке свойств групп DCS см. по адресу <http://technet.microsoft.com/ru-ru/library/cc749267.aspx>.

---

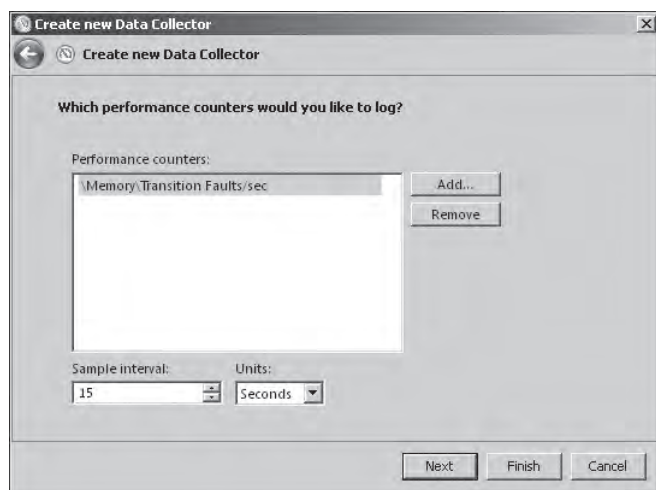


Рис. 12-6. Страница Какие счетчики производительности вы хотите записать?

Если группа DCS содержит счетчики производительности, их значения можно просматривать при помощи системного монитора. Для этого выберите отчет, созданный при запуске группы DCS, щелкните его правой кнопкой и выберите команду **Вид | Системный монитор** (View | Performance Monitor). В системном мониторе будут показаны данные, записанные группой DCS, а не полученные в режиме реального времени. При отображении в виде графика или линейчатой гистограммы данные могут выглядеть очень запутанными, поэтому лучше всего просматривать их в виде отчета.

## Создание сборщиков данных из командной строки

Сборщики данных можно создавать из командной строки с повышенными привилегиями, используя утилиту Logman. Например, можно использовать следующие команды для создания различных типов сборщиков данных, описанных в предыдущем разделе:

- `logman create counter` — создает сборщик данных **Счетчик производительности** (Performance Counter). Например, следующая команда создает счетчик с именем `my_perf_log`, который записывает значения для счетчика **% загрузки процессора** (% Processor Time) в экземпляре счетчика **Процессор(\_Total)**:

```
logman create counter my_perf_log -c «\Processor(_Total)\% Processor Time»
```

- `logman create trace` — создает сборщик данных **Трассировка событий** (Event Trace). Например, следующая команда создает сборщик данных трассировки событий с именем `my_trace_log` и выводит результаты в расположение `C:\trace_log_file`:

```
logman create trace my_trace_log -o c:\trace_log_file
```

- `logman create config` — создает сборщик данных **Конфигурация** (Configuration). Например, создать сборщик данных конфигурации с именем `my_cfg_log`, использующий раздел реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\\`, можно с помощью следующей команды:

```
logman create cfg my_cfg_log -reg
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\\
```

- **logman create alert** — создает сборщик данных **Оповещение (Alert)**. Например, для создания оповещения с именем `my_alert`, которое запускается, когда значение счетчика производительности **% загрузки процессора** в экземпляре счетчика **Общая загрузка процессора** превышает 90, используется следующая команда:

```
logman create alert my_alert -th «\Processor(_Total)\% Processor Time>90»
```

Утилиту Logman можно использовать также для запроса выходных данных сборщика данных. Например, следующая команда отображает список сборщиков данных, содержащихся в группе DCS `my_perf_log`:

```
logman query «my_perf_log»
```

На рис. 12-7 показаны выходные данные этой команды.

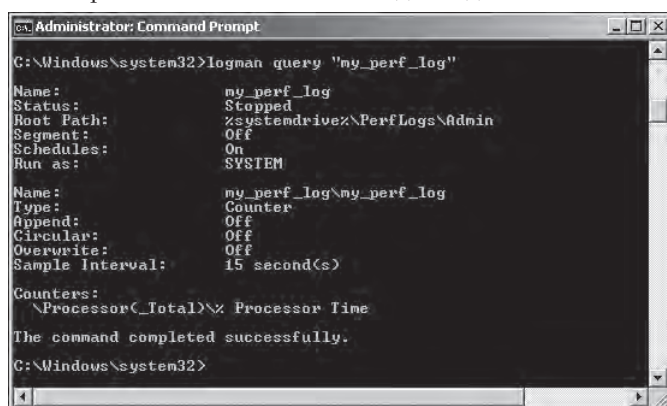


Рис. 12-7. Список сборщиков данных из группы DCS `my_perf_log`

С помощью команд `logman start` и `logman stop` можно запускать и останавливать группы DCS, например, `logman start my_perf_log` и `logman stop my_perf_log`. Для удаления группы DCS используется команда `logman delete`, например, `logman delete my_perf_log`. Для обновления счетчика производительности, счетчика трассировки, оповещения или конфигурации используется команда `logman update`. С помощью утилиты Logman можно экспортировать информацию из групп DCS в XML-файл и импортировать информацию из XML-файла.

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Logman

Подробнее об утилите Logman см. по адресу [http://technet.microsoft.com/en-us/library/cc753820\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc753820(WS.10).aspx) (на английском языке).

### Составление отчета диагностики системы

В процессе создания и использования группы DCS генерируется отчет, который размещается в разделе **Особый (User Defined)** под узлом **Отчеты (Reports)** оснастки **Системный монитор**. Под узлом **Отчеты** может также отображаться отчет диагностики системы, иногда называемый проверкой работоспособности компьютера.



Отчет диагностики системы содержит сведения о состоянии аппаратных ресурсов, времени ответов системы и процессах на локальном компьютере, а также информацию о системе и конфигурации. Для максимального увеличения производительности и оптимизации работы системы следует создать отчет диагностики системы. Создавать такие отчеты могут члены локальной группы администраторов или другой группы с аналогичными правами.

Если для просмотра отчета диагностики системы используется системный монитор, будет показана последняя копия этого отчета (если отчет никогда не создавался, он не будет показан). Чтобы создать и просмотреть самый свежий отчет диагностики системы, используйте команду `perfmon /report`.

Если предпочитаете, можете ввести `perfmon.exe /report` в командной строке с повышенными привилегиями. В обоих случаях созданный отчет диагностики (обычно его создание занимает 60 секунд) автоматически откроется в окне **Монитор ресурсов и производительности** (Resource And Performance Monitor) (рис. 12-8). Отчет можно прокручивать и разворачивать любые его разделы.

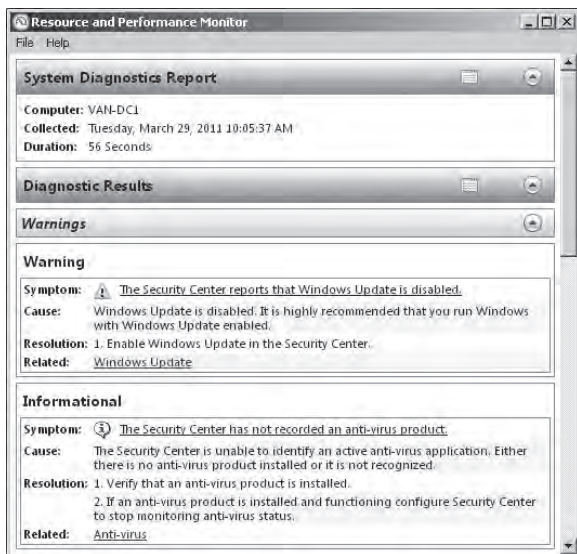


Рис. 12-8. Отчет диагностики системы в мониторе ресурсов и производительности

Например, на рис. 12-9 показан раздел отчета с предупреждением о проблеме с антивирусной защитой на VAN-DC1. Поскольку VAN-DC1 располагается в изолированной тестовой сети, не подключенной к Интернету, на нем не установлено антивирусное ПО.

Отчет содержит информацию о производительности, конфигурации программного и аппаратного обеспечения, процессоре, сети, дисках и памяти, а также отчет о статистике. В разделе **Отчет о статистике** (Report Statistics) содержится информация о компьютере, файлах и обработанных событиях (рис. 12-10).





Рис. 12-9. Сведения о базовых системных проверках

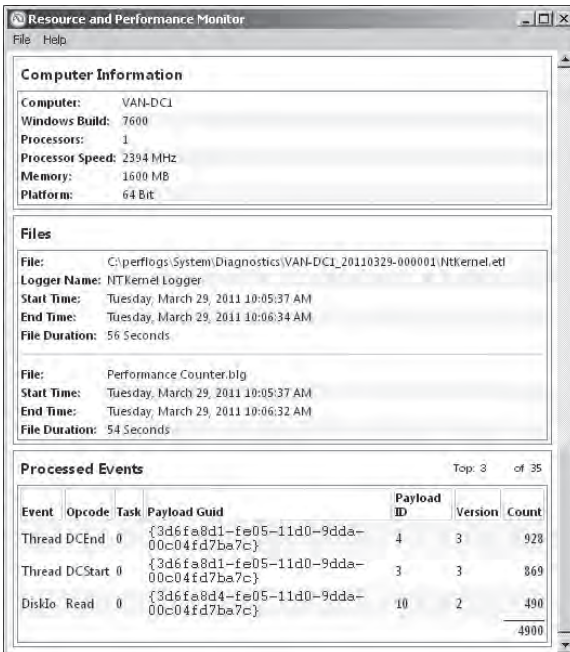


Рис. 12-10. Отчет о статистике в мониторе ресурсов и производительности

## Слежение за надежностью, стабильностью и общей производительностью системы

Windows Server 2008 R2 предоставляет инструменты для оценки надежности и стабильности системы. Монитор стабильности системы (Reliability Monitor) за-

писывает изменения и обновления ПО и позволяет проводить связь между изменениями системы и сбоями. Монитор стабильности создает индекс стабильности, измеряющий надежность и стабильность компьютера в течение 28 дней. Центр поддержки (Action Center) выполняет мониторинг компьютера и сообщает о проблемах с безопасностью, обслуживанием и соответствующими службами.

## Монитор стабильности системы

Монитор стабильности системы следит за стабильностью компьютера. Компьютеры, не имеющие перезагрузок и сбоев, считаются стабильными и могут в конечном итоге получить максимальный индекс стабильности системы, равный 10. Чем больше перезагрузок и сбоев, тем ниже стабильность системы. Минимальное значение индекса равно нулю. Индекс стабильности системы не является точным показателем стабильности, так как установка нового пакета обновлений требует перезагрузки, что поначалу снижает значение индекса, но в итоге делает систему более надежной, чем раньше. Тем не менее, монитор стабильности предоставляет ценную информацию о том, какие изменения системы были сделаны, прежде чем возникла проблема.

Монитор стабильности использует данные, предоставляемые назначенным заданием RACTask. В Windows Server 2008 R2 это задание включается при первом запуске монитора стабильности. Если сбор данных отключен, необходимо включить RACTask вручную из оснастки планировщика заданий. Для этого учетная запись должна входить в локальную группу администраторов или иметь аналогичные права. Чтобы включить назначенное задание RACTask, выполните следующее:

1. Щелкните кнопку **Пуск**, введите **taskschd.msc** в поле **Поиск** и нажмите Enter.
2. В дереве консоли разверните узлы **Библиотека планировщика заданий** (Task Scheduler Library), **Microsoft** и **Windows**. и щелкните узел **RAC**.
3. На панели **Действия** (Actions) щелкните **Вид** (View), а затем щелкните **Отобразить скрытые задачи** (Show Hidden Tasks).
4. В области результатов щелкните **RACTask**.
5. В меню **Действие** (Action) щелкните **Включить** (Enable). На рис. 12-11 показано включенное задание RACTask.

Самый простой способ открыть монитор стабильности — выполнить команду `perfmon /rel`. Монитор стабильности будет отображать индекс стабильности и информацию об определенных событиях 24 часа после запуска.

С помощью монитора стабильности можно диагностировать непостоянные проблемы. Например, если установлено приложение, из-за которого иногда происходят сбои в операционной системе, трудно связать эти сбои с установкой приложения. На рис. 12-12 показано, как с помощью монитора стабильности связать аппаратную ошибку видео и сбои ОС и приложений, произошедшие 22 июня на VAN-DC1, с обновлением драйвера видео 21 июня. Если это произошло в тестовой сети, можно попробовать получить дополнительную информацию, прежде чем обновлять драйверы в производственной сети.

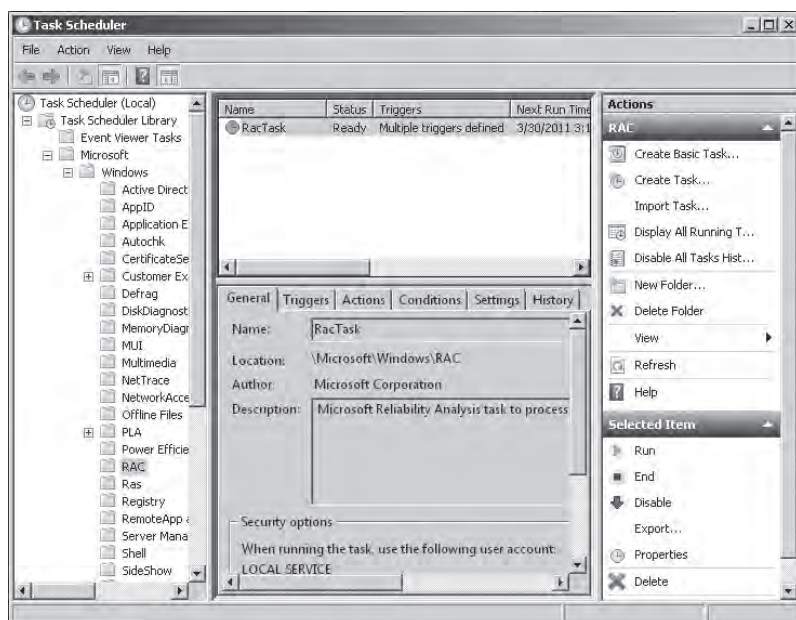


Рис. 12-11. Включенное задание RACTask

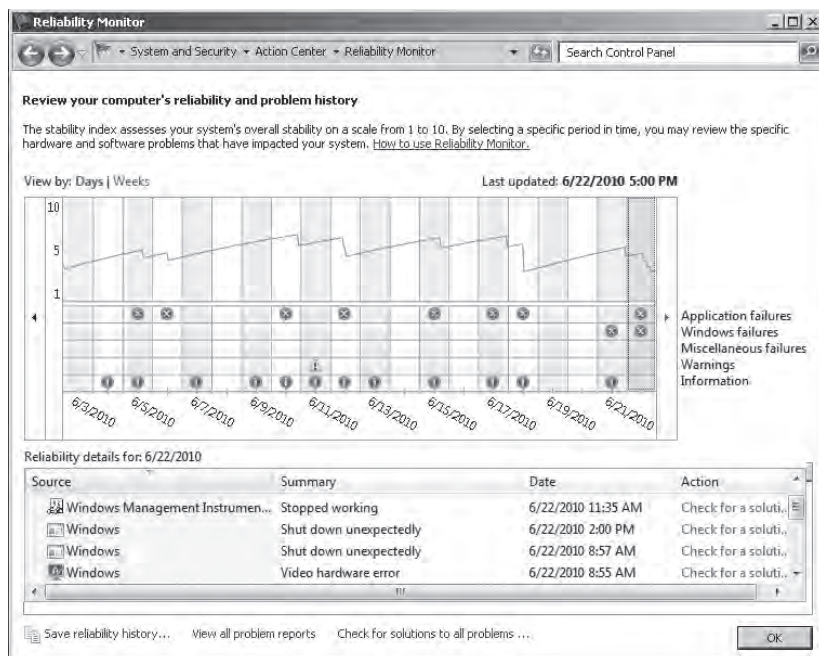


Рис. 12-12. Монитор стабильности системы

## Индекс стабильности

Индекс стабильности основан на данных, собранных в течение жизненного цикла системы. Каждому дню в диаграмме стабильности соответствует опреде-

ленная точка, обозначающая значение индекса стабильности. Индекс стабильности — взвешенная величина, вычисляемая по числу сбоев, наблюдавшихся за просматриваемый период времени. Значение индекса рассчитывается за предыдущие 28 дней, хотя результаты могут отображаться за гораздо более длительный период.

Последние сбои имеют больший вес, чем давние, поэтому после решения проблемы индекс стабильности растет. Дни, когда компьютер был выключен, при вычислении индекса стабильности не учитываются. Когда изучаете индекс стабильности на клиенте, а не на сервере, учитывайте, что время нахождения компьютера в спящем режиме тоже не учитывается.

Если данных для вычисления устойчивого индекса стабильности недостаточно, линия в графике отображается пунктиром. Например, пока у монитора стабильности нет данных за 28 дней, индекс стабильности изображается в виде пунктирной линии, показывая, что надежные базовые показатели еще не определены. Когда данных записано достаточно для генерации устойчивого индекса стабильности, линия становится сплошной. Если происходили существенные изменения в системном времени, то для каждого дня, когда системное время изменялось, на графике отображается информационный значок.

Монитор стабильности системы сохраняет историю событий сроком до года. Диаграмма стабильности отображается в виде графика с прокруткой, упорядоченного по дате.

### Проверьте себя

- Что означает индекс стабильности 10?

### Ответ

- 10 — Максимальное значение индекса стабильности. Оно означает, что компьютер работал стабильно в течение предыдущих 28 дней без сбоев и перезагрузок. Также оно показывает, что за этот период не устанавливались исправления и пакеты обновлений, требующие перезагрузки.

## Диаграмма стабильности

Диаграмма стабильности в мониторе стабильности системы показывает график индекса стабильности по дням. Строки в нижней части диаграммы отслеживают события стабильности, которые связаны с измерением стабильности для системы или предоставляют соответствующую информацию об установке и удалении программ. При обнаружении одного или нескольких событий стабильности любого типа в столбце для соответствующей даты появляется значок.

Для установок и удалений программ информационный значок обозначает успешное событие, а значок предупреждения обозначает сбой. Для всех остальных типов событий надежности сбой обозначается значком ошибки. Если имеются данные более чем за 30 дней, можно использовать клавиши со стрелками влево и вправо для поиска дат вне видимого диапазона.

## Использование центра поддержки

Центр поддержки (рис. 12-13), доступный в разделе **Система и безопасность** (System and Security) в Панели управления, осуществляет мониторинг компьютера и сообщает о проблемах с безопасностью и обслуживанием, а также о соответствующих параметрах, помогающих оценить производительность компьютера в целом. Он уведомляет пользователей в случае возникновения на сервере под управлением Windows Server 2008 R2 проблем с брандмауэром, антивирусным и антишпионским ПО или центром обновлений Windows. Когда изменяется состояние наблюдаемого элемента (например, устаревает антивирус), центр поддержки показывает сообщение в области уведомлений на панели задач. Значок в области уведомлений меняет цвет, обозначая серьезность сообщения, а центр поддержки рекомендует то или иное действие.

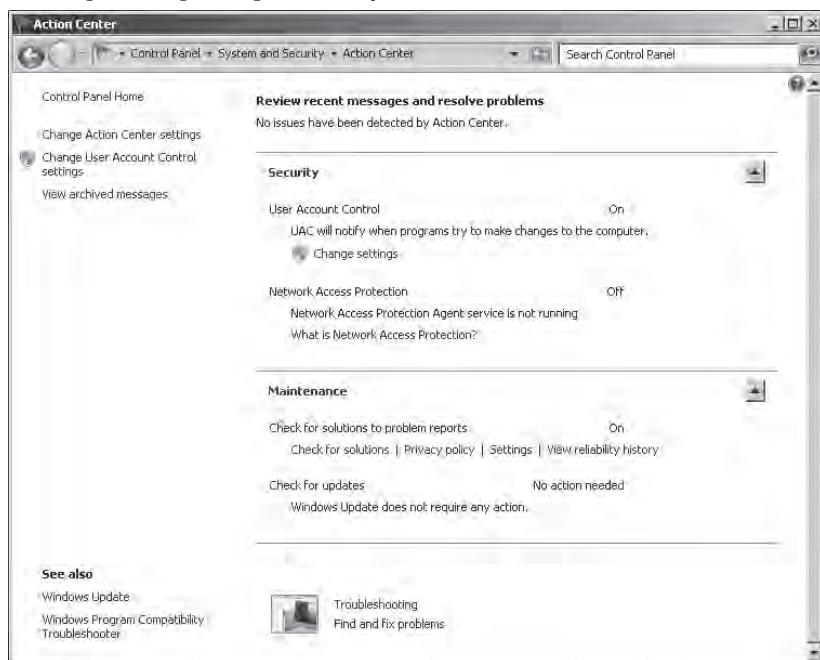


Рис. 12-13. Центр поддержки

## Изменение параметров центра поддержки

Если вы предпочитаете самостоятельно наблюдать за элементом и не хотите видеть уведомления о его состоянии, можно отключить уведомления для этого элемента в диалоговом окне **Настройка центра поддержки** (Change Action Center Settings) (рис. 12-14).

Если в этом диалоговом окне снять флажок для элемента, центр поддержки не будет отображать его состояние и сообщать о нем пользователю. Microsoft рекомендует проверять состояние всех элементов списка во избежание проблем с безопасностью.

В центре поддержки можно архивировать сообщения и просматривать их в архиве. Можно также отключить сообщения контроля учетных записей пользователей (UAC).

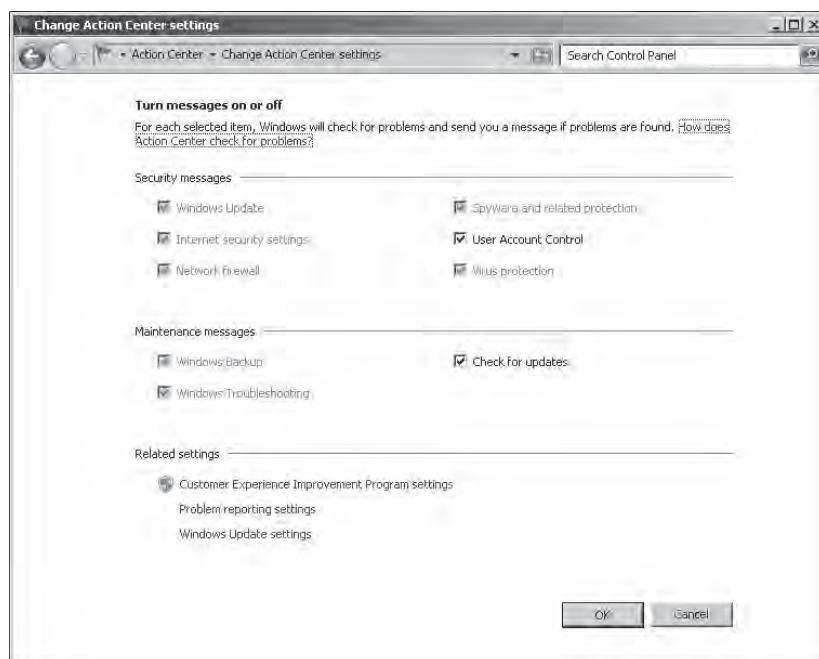


Рис. 12-14. Настройка центра поддержки

## Использование системных инструментов для изучения процессов и служб

Вы наверняка пользовались диспетчером задач и обращались из него к диспетчеру ресурсов, но можете не знать о расширенных возможностях диспетчера ресурсов в Windows Server 2008 R2. Process Explorer — доступный для скачивания системный инструмент с широкими возможностями, позволяющий выполнять многие из функций диспетчера задач и диспетчера ресурсов. Его можно использовать для наблюдения за использованием ресурсов, дескрипторов и файлов библиотек DLL.

В процессе планирования требуется решить, какие системные инструменты следует использовать для регулярных проверок или при обнаружении проблем, и как часто следует выполнять регулярные проверки системы. Некоторые задачи можно выполнять с помощью нескольких инструментов. Например, многое из того, что можно сделать с помощью диспетчера задач и диспетчера ресурсов, можно выполнить с помощью Process Explorer. Чтобы запланировать проверки системы и выбрать наилучший инструмент для работы, необходимо знать, как работает каждый инструмент и какими функциями обладает.

### Диспетчер задач

Если приложение перестает отвечать, Windows Server 2008 R2 автоматически пытается найти проблему и устранить ее. Если приложение полностью вышло из строя, и операционной системе не удалось решить проблему, можно завершить работу этого приложения, используя вкладку **Приложения** (Applications) диспетчера задач.



На вкладке **Быстродействие** (Performance) диспетчера задач показаны сведения об использовании компьютером ресурсов системы, таких как оперативная память и ЦП. Эта вкладка имеет четыре диаграммы (рис. 12-15). Первые две показывают объем используемых ресурсов ЦП в процентах, в настоящий момент и за несколько прошедших минут. Высокий процент в течение долгого периода говорит о том, что программы или процессы требуют много ресурсов ЦП. Это может повлиять на быстродействие компьютера. Если цифра в процентах не меняется или доходит до 100, то программа, вероятно, не отвечает.

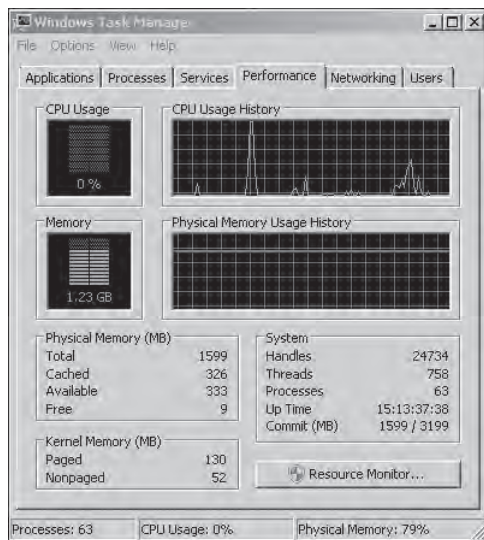


Рис. 12-15. Диспетчер задач, вкладка Быстродействие

#### ПРИМЕЧАНИЕ Разделенный график хронологии загрузки ЦП

Если график хронологии загрузки ЦП разделен, то у компьютера имеется несколько ЦП, или один двухъядерный ЦП, или несколько двухъядерных ЦП.

Если загрузка процессора в течение долгого времени остается интенсивной, например, 80% или выше, то желательно установить второй процессор или заменить действующий. Однако перед этим стоит проверить данные загрузки процессора с помощью системного монитора, а не полагаться на данные диспетчера задач.

Следующие две диаграммы показывают, сколько оперативной памяти используется в текущий момент и за последние несколько минут. В нижней части окна диспетчера задач показан объем используемой памяти в процентах. Если объем используемой памяти высок, или скорость работы компьютера значительно упала, попробуйте уменьшить число программ, работающих одновременно. Если проблема остается, установите дополнительную оперативную память.

Три таблицы под диаграммами содержат сведения об использовании памяти и ресурсов. В таблице **Физическая память** (Physical Memory) строка **Всего** (Total) показывает объем оперативной памяти, установленной на компьютере; строка **Кэшировано** (Cached) — объем физической памяти, используемый в данный момент системными ресурсами; строка **Доступно** (Available) — объем



памяти, доступной в данный момент; строка **Свободно** (Free) — объем неиспользуемой памяти.

Таблица **Память ядра** (Kernel Memory) показывает, сколько памяти используется основной частью Windows, которая называется ядром. Строка **Выгружаемая** (Paged) показывает объем виртуальной памяти, которую использует ядро, а строка **Невыгружаемая** (Nonpaged) — объем оперативной памяти, используемой ядром.

Таблица **Система** (System) содержит пять строк: **Дескрипторов** (Handles), **Потоков** (Threads), **Процессов** (Processes), **Время работы** (Up Time) и **Выделено (МБ)** [Commit (MB)]. Дескрипторы — уникальные идентификаторы объектов или указатели, используемые процессами, которые ссылаются на элементы системы. Они включают файлы, разделы реестра, события, каталоги и другие элементы.

Потоки — объекты или процессы, работающие внутри более крупных процессов или программ. Процессы ссылаются на несколько отдельных процессов, работающих на компьютере (более подробную информацию о процессах можно увидеть на вкладке **Процессы**). **Время работы** показывает, сколько времени прошло с момента последней перезагрузки компьютера. Значение **Выделено (МБ)** показывает использование виртуальной памяти (использование файла подкачки). Файл подкачки — пространство на жестком диске, которое Windows использует в дополнение к оперативной памяти. Первое число — объем оперативной и виртуальной памяти, которая используется в данный момент, второе — доступный объем оперативной и виртуальной памяти на компьютере.

Если требуется дополнительная информация об использовании памяти и ресурсов ЦП, щелкните кнопку **Монитор ресурсов** (Resource Monitor). Откроется монитор ресурсов, о котором будет рассказано далее, в разделе «Монитор ресурсов». Для использования монитора ресурсов необходимы повышенные привилегии.

Можно определить, сколько памяти использует отдельный процесс. Для этого перейдите на вкладку **Процессы** (Processes) (рис. 12-16). Значения в отображаемом по умолчанию столбце **Память (Частный рабочий набор)** [Memory (Private Working Set)] показывают используемый одним процессом объем памяти, который другие процессы не могут использовать совместно. Эта информация может пригодиться для выявления приложения с «утечкой», т.е. приложения, которое потребляет все больше и больше памяти, не освобождая неиспользуемые ресурсы.

На вкладке **Процессы** можно выполнить команду меню **Вид | Выбрать столбцы** (View | Select Columns) и выбрать для просмотра другие значения потребления памяти, например, **Память — выгружаемый пул** (Memory — Paged Pool) или **Память — выделенная памяти** (Memory — Commit Size). На вкладке **Процессы** можно завершать процесс, завершать дерево процессов (завершается процесс и все процессы, от которых он зависит) и устанавливать приоритет процессов. Чтобы изменить приоритет процесса, щелкните процесс правой кнопкой и выберите в подменю **Приоритет** (Set Priority) один из вариантов: **Реального времени** (Realtime), **Высокий** (High), **Выше среднего** (Above Normal), **Средний** (Normal), **Ниже среднего** (Below Normal) или **Низкий** (Low).

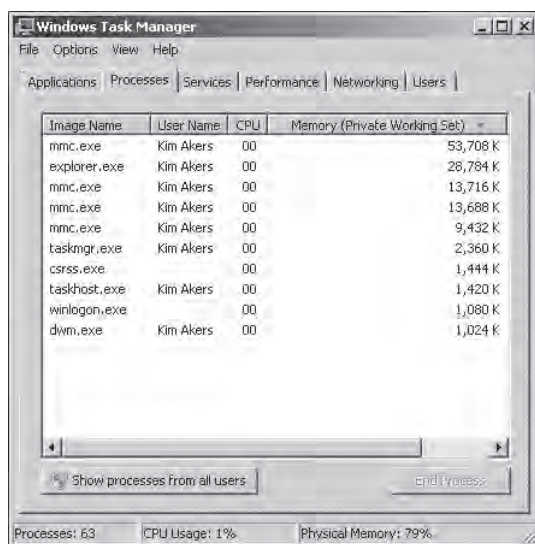


Рис. 12-16. Диспетчер задач, вкладка Процессы

На вкладке **Службы (Services)** показано, какие службы работают, а какие остановлены. Можно остановить или запустить службу или перейти к процессу, который зависит от этой службы. Если требуется больше сведений об имеющихся службах или дополнительные возможности управления, щелкните кнопку **Службы**, чтобы открыть оснастку **Службы**. Для использования оснастки **Службы** необходимы повышенные привилегии. Подробнее об этой оснастке будет рассказано далее, в посвященном ей разделе.

Вкладка **Сеть (Networking)** позволяет следить за использованием сети. Вкладка **Пользователи (Users)** содержит информацию о подключенных к компьютеру пользователях и дает возможность отключать их. Вкладка **Приложения (Applications)** содержит список работающих приложений и, как уже говорилось, позволяет закрывать зависшие приложения.

### Проверьте себя

- Вы хотите изменить приоритет процесса на компьютере. Как это сделать?

### Ответ

- Откройте диспетчер задач. На вкладке **Процессы** щелкните правой кнопкой мыши нужный процесс и в подменю **Приоритет** выберите один из вариантов: **Реального времени**, **Высокий**, **Выше среднего**, **Средний**, **Ниже среднего** или **Низкий**.

## Монитор ресурсов

Windows Server 2008 R2 предлагает улучшенную версию монитора ресурсов. Этот инструмент позволяет просматривать информацию об использовании аппаратных и программных ресурсов в режиме реального времени. Можно

фильтровать результаты по процессам или службам, за которыми требуется наблюдать. С помощью монитора ресурсов можно запускать, останавливать, приостанавливать и повторно запускать процессы и службы и решать проблемы с не отвечающими приложениями. Монитор ресурсов можно запустить с вкладки **Быстродействие** диспетчера задач или командной `resmon`.

Монитор ресурсов всегда запускается в том же расположении и с теми же параметрами отображения, что и в предыдущем сеансе. Можно в любое время сохранить состояние отображения, а затем открыть файл конфигурации для использования сохраненных параметров. С параметрами конфигурации не сохраняются параметры фильтрации.

Окно монитора ресурсов имеет пять вкладок: **Обзор** (Overview), **ЦП** (CPU), **Память** (Memory), **Диск** (Disk) и **Сеть** (Network). Вкладка **Обзор** (рис. 12-17) содержит основную информацию о потреблении ресурсов системы. На других вкладках отображается информация об отдельных ресурсах. Если отфильтровать результаты, выбрав один или несколько процессов или служб, то эти процессы или службы будут выбраны и на других вкладках, на которых отображаются.

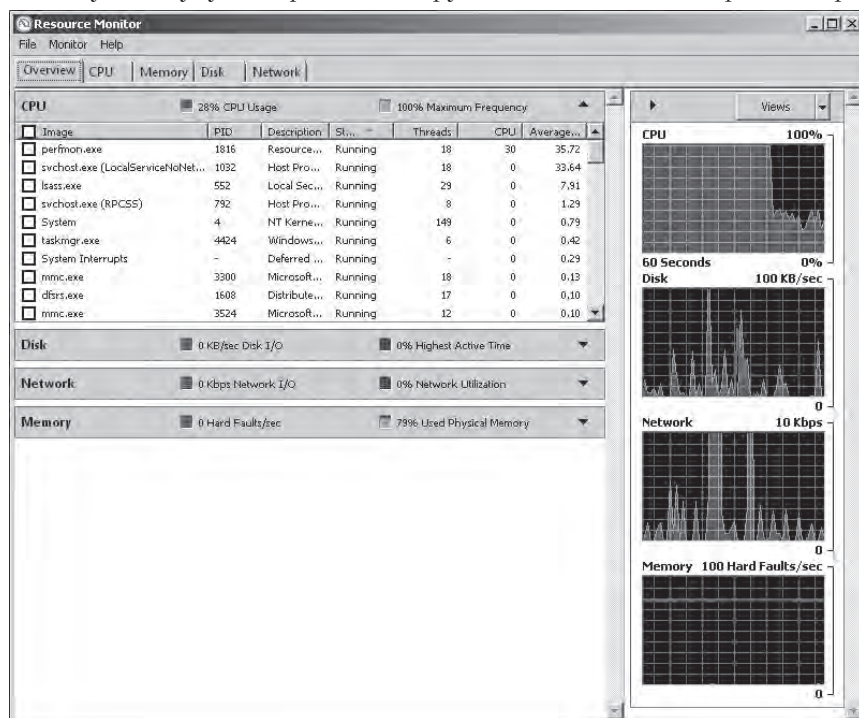


Рис. 12-17. Монитор ресурсов, вкладка Обзор

Каждая вкладка окна монитора ресурсов содержит несколько таблиц с подробной информацией о ресурсе, которому соответствует эта вкладка. Первая таблица всегда ключевая и всегда содержит полный список процессов, использующих ресурс, которому соответствует вкладка. Например, ключевая таблица на вкладке **Обзор** содержит полный список процессов, работающих в системе.

Остальные таблицы можно фильтровать по одному или нескольким процессам или службам. Для этого установите флажок в ключевой таблице рядом

с теми процессами или службами, которые хотите выделить. Для прекращения фильтрации по процессу или службе снимите соответствующий флажок. Чтобы полностью прекратить фильтрацию, снимите флажок на панели заголовков в столбце **Образ** (Image). Если результаты фильтруются, то ресурсы, потребляемые выбранными процессами или службами, отображаются на диаграмме оранжевой линией.

Размер графиков можно изменять при помощи кнопки **Вид** (Views). Панель диаграмм можно скрыть, щелкнув стрелку в верхней части панели. Для просмотра определений данных, отображаемых в таблицах, наведите курсор мыши на заголовок столбца, о котором требуется дополнительная информация.

Например, для идентификации сетевого адреса, к которому подключен процесс, перейдите на вкладку **Сеть** и щелкните заголовок **TCP-подключения** (TCP Connections), чтобы раскрыть таблицу. Найдите процесс, подключение которого хотите идентифицировать. В столбцах **Удаленный адрес** (Remote Address) и **Удаленный порт** (Remote Port) показано, к какому сетевому адресу и порту подключен процесс. На рис. 12-18 показан процесс System, подключенный к адресу IPv6 fe80::ada5:5657:9e68:c03b через локальный порт 445 и удаленный порт 58946.

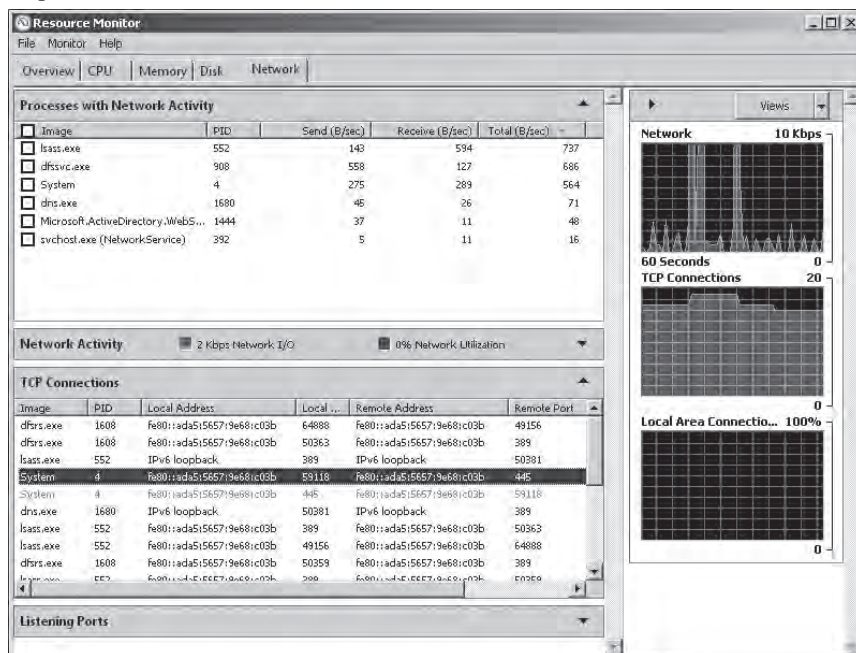


Рис. 12-18. Идентификация сетевых адресов, к которым подключен процесс

На вкладке **Память** (рис. 12-19) показаны сведения о памяти, доступной программам. Доступная память состоит из свободной и ожидающей памяти. Свободная память включает нулевую страницу памяти.

Монитор ресурсов отображает в реальном времени информацию обо всех процессах, работающих в системе. Можно просматривать только данные, относящиеся к выбранным процессам, отфильтровав результаты. Для этого установите на любой из вкладок флажки рядом с именами процессов, за которыми

требуется наблюдать. Выбранные процессы перемещаются в верхнюю часть столбца **Образ** (Image). Если выбрать хотя бы один процесс, в таблицах **Связанные дескрипторы** (Associated Handles) и **Связанные модули** (Associated Modules) на вкладке **ЦП** будут отображаться данные, относящиеся к этому выбору. Таблицы, содержащие только отфильтрованные результаты, имеют оранжевую панель информации под панелью заголовка.

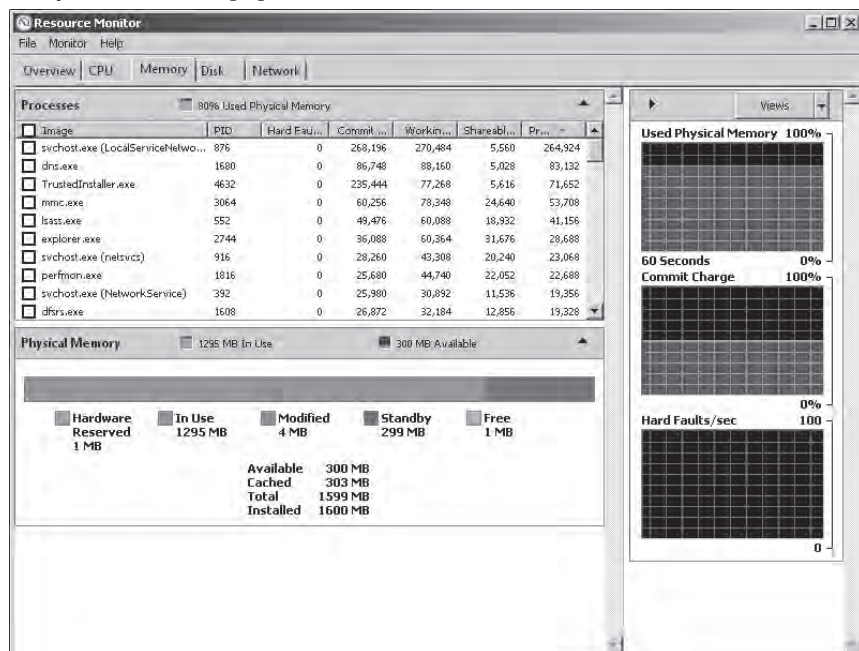


Рис. 12-19. Монитор ресурсов, вкладка Память

Монитор ресурсов позволяет завершать или приостанавливать процессы и запускать, останавливать или перезапускать службы. Монитор ресурсов следует использовать для завершения процесса только в том случае, если его невозможно завершить обычными средствами. Если с процессом связана работающая программа, она сразу закрывается, и все несохраненные данные теряются. Завершение системного процесса может привести к нестабильности системы и потере данных.

Чтобы завершить процесс, щелкните правой кнопкой его имя в столбце **Образ** ключевой таблицы на любой из вкладок монитора ресурсов и выберите команду **Завершить процесс** (End Process). Для завершения всех процессов, зависящих от выбранного процесса, выберите команду **Завершить дерево процессов** (End Process Tree). Для возобновления процесса щелкните правой кнопкой имя программы, работу которой хотите возобновить, и выберите команду **Возобновить процесс** (Resume Process).

Чтобы остановить, запустить или перезапустить службу с помощью монитора ресурсов, перейдите на вкладку **ЦП** и щелкните панель заголовков **Службы** (Services), чтобы развернуть таблицу. Щелкните правой кнопкой имя службы в столбце **Имя** (Name) и выберите команду **Остановить службу** (Stop Service), **Запустить службу** (Start Service) или **Перезапустить службу** (Restart Service).



Не отвечающие приложения могут ждать завершения других процессов или появления доступных ресурсов системы. Монитор ресурсов позволяет просматривать цепочку ожидания процесса и завершать процессы, мешающие нормальной работе программы. Не отвечающий процесс выделяется красным в таблице **ЦП** на вкладке **Обзор**. Чтобы просмотреть цепочку ожидания процесса, щелкните правой кнопкой имя этого процесса в столбце **Образ** ключевой таблицы на любой из вкладок и выберите команду **Анализ цепочки ожидания** (Analyze Wait Chain).

Если процесс работает нормально и не ожидает других процессов, цепочка ожидания не отображается. Если процесс ожидает другой процесс, то отображается дерево, упорядоченное по зависимости от других процессов. В этом случае можно завершить один или несколько процессов в дереве, установив флажки рядом с их именами и щелкнув **Завершить процесс** (End Process).

Как уже говорилось, дескрипторы являются указателями, которые ссылаются на элементы системы, включая файлы, разделы реестра, события и каталоги. Модули — вспомогательные файлы или программы. К ним относятся DLL-файлы.

Чтобы просмотреть в мониторе ресурсов все дескрипторы и модули, связанные с процессом, установите флажок рядом с именем этого процесса в столбце **Образ** на вкладке **ЦП**. Выбранные процессы переместятся в верхнюю часть столбца. Щелкните панели заголовков таблиц **Связанные дескрипторы** (Associated Handles) и **Связанные модули** (Associated Modules), чтобы развернуть их. Имя выбранного процесса показано в оранжевой панели под панелью заголовков. Результаты отображаются в таблицах.

Если требуется идентифицировать процессы, использующие дескриптор, щелкните в поле **Поиск дескрипторов** (Search Handles) на панели заголовков таблицы **Связанные дескрипторы**, введите имя дескриптора, который хотите найти, и щелкните **Поиск**. Например, если ввести **c:\windows**, будут показаны все дескрипторы, имеющие в имени путь **c:\windows**. Строка поиска нечувствительна к регистру и не поддерживает маски.

### Process Explorer

Утилита Process Explorer не является частью Windows Server 2008 R2, однако можно скачать ее последнюю версию с сайта <http://technet.microsoft.com/ru-ru/sysinternals/bb896653.aspx>, распаковать архив в папку (например, C:\ProcessExplorer) и запустить, введя в поле **Поиск** меню **Пуск** команду **c:\processexplorer\prosexpr.exe**. Заметьте, что скачать Process Explorer из изолированной тестовой сети не удастся, для этого потребуется компьютер с выходом в Интернет. Установочные файлы можно сохранить на внешний жесткий диск, который затем подключить к VAN-DC1, но если вы скачали эту утилиту на компьютер под управлением Windows Server 2008 R2, то проще установить и просмотреть ее там. Изучение Process Explorer входит в число рекомендуемых упражнений в конце данной главы.

Process Explorer сообщает, какая программа открыла файл или каталог, и отображает информацию о дескрипторах и DLL, открытых или загруженных

процессами. С помощью Process Explorer или монитора ресурсов можно определять, какие приложения отвечают за активность на жестком диске, в том числе, какие файлы и папки используются.

После запуска Process Explorer показывает список активных в текущий момент процессов (рис. 12-20). Нижнюю панель можно включать и отключать и переходить в режим просмотра дескрипторов или DLL. В режиме просмотра дескрипторов отображаются дескрипторы, открытые выбранным в верхнем окне процессом. Функция поиска позволяет найти процессы, которые открыли те или иные дескрипторы или загрузили DLL.

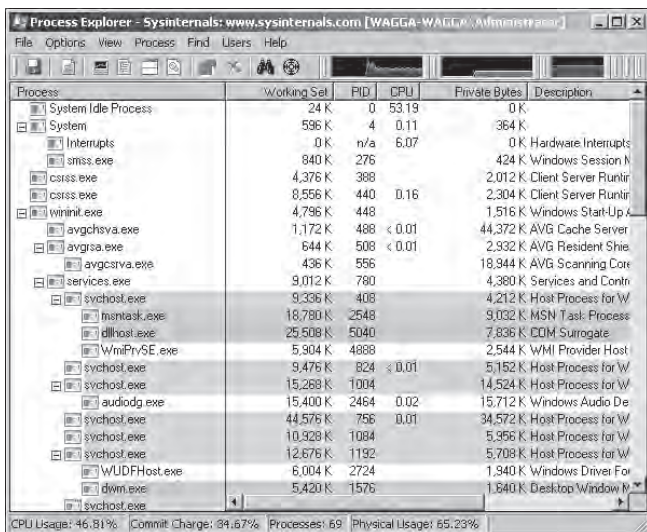


Рис. 12-20. Process Explorer

## ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Дополнительные системные инструменты и утилиты командной строки

Подробнее о дополнительных системных инструментах для Windows и утилитах командной строки см. по адресу <http://technet.microsoft.com/ru-ru/sysinternals/default.aspx>. Там же можно оценить их работу, не загружая и не устанавливая на свой компьютер.

Кнопка **System Information** (Информация о системе) открывает диалоговое окно **System Information**, содержащее вкладку **Summary** (Сводка) и вкладки с мини-графиками использования ЦП, памяти и ввода-вывода. Эти мини-графики показывают историю активности системы, а если навести указатель мыши на точку графика, то во всплывающей подсказке появится соответствующая информация о времени и процессе. Например, всплывающая подсказка для мини-графика ЦП отображает процесс, потреблявший наибольший объем ресурсов ЦП. Выделение помогает увидеть, какие элементы изменились за время между обновлениями. Элементы, которые были закрыты или завершили работу (в том числе процессы, библиотеки DLL и дескрипторы) отображаются красным цветом, а новые элементы — зеленым. На рис. 12-21 показана вкладка **Summary** диалогового окна **System Information**.



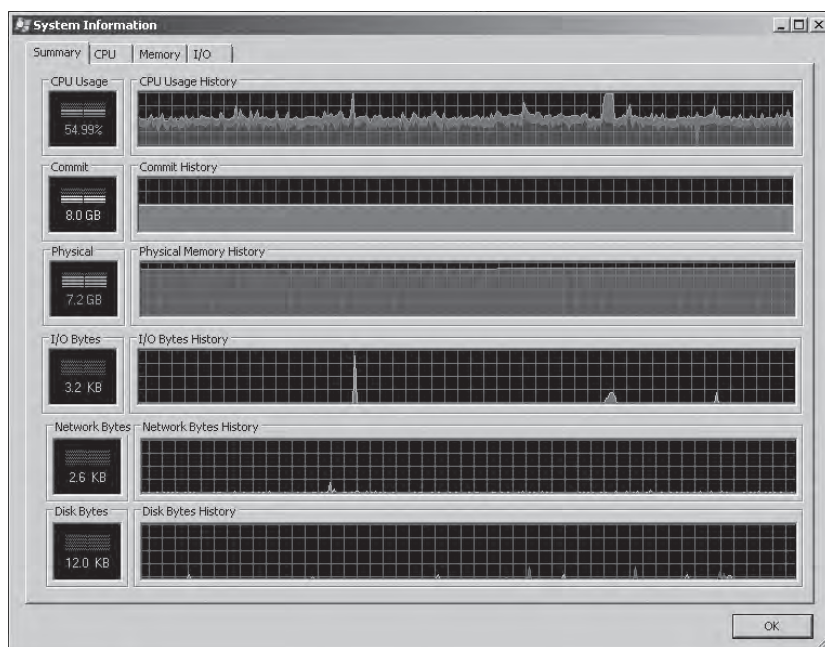


Рис. 12-21. Process Explorer, сводная информация о системе

Графики на соответствующих вкладках диалогового окна **System Information** показывают историю загрузки ЦП, выделенную виртуальную память и историю пропускной способности ввода-вывода. Красным цветом на графике загрузки ЦП обозначены ресурсы ЦП, используемые в режиме ядра, зеленым — совокупные ресурсы, используемые в пользовательском режиме и режиме ядра. Когда объем выделенной виртуальной памяти (Committed Virtual Memory) достигает предела выделения (Commit Limit), приложения и система становятся нестабильными. Предел выделения — совокупный объем доступной физической памяти и файлов подкачки. На вкладке **Memory** (Память) отображается история выделения памяти и история физической памяти.

На вкладке **I/O** (Ввод-вывод) показана побайтовая история ввода-вывода, историю использования сети и дисков. Синяя линия на каждом из графиков обозначает весь трафик, розовая — трафик записи.

Порядок столбцов на главном экране Process Explorer можно изменять, перетаскивая их на новые места. Чтобы выбрать столбцы данных, которые будут видимыми на каждой из вкладок и в строке состояния, в меню **View** (Вид) выберите команду **Select Columns** (Выбрать столбцы) или щелкните правой кнопкой заголовок столбца и выберите команду **Select Columns** (Выбрать столбцы). Конфигурацию столбцов и связанных с параметров можно сохранить, выбрав команду **Save Column Set** (Сохранить параметры столбцов) в меню **View** (Вид).

В меню **Options** (Параметры) можно настроить запуск Process Explorer вместо диспетчера задач, включить отображение Process Explorer поверх всех окон или разрешить запуск только одного экземпляра Process Explorer одновременно.

## Оснастка Службы

Список всех служб, имеющихся на компьютере под управлением Windows Server 2008 R2, можно просмотреть на вкладке **Службы** (Services) консоли **Конфигурация системы** (System Configuration), доступной в меню **Администрирование**. Здесь показано, какие службы работают, а какие остановлены. Однако для мониторинга и управления службами следует использовать оснастку **Службы** (Services), также доступную в меню **Администрирование**. Эта оснастка отображает тот же список служб, что и вкладка **Службы** инструмента **Конфигурация системы**, но предоставляет больше информации о службах и больше параметров для управления ими. Например, оснастка **Службы** показывает тип запуска службы (а не только работает она или нет) и сведения о входе в систему. Оснастку **Службы** можно запустить также командой services.msc.

Если щелкнуть правой кнопкой службу в оснастке **Службы**, ее можно запустить, остановить, перезапустить, приостановить и возобновить. Можно перейти в диалоговое окно свойств службы, имеющее вкладки **Общие** (General), **Вход в систему** (Log On), **Восстановление** (Recovery) и **Зависимости** (Dependencies).

На вкладке **Общие** можно выбрать тип запуска: **Автоматически** (Automatic), **Автоматически (Отложенный запуск)** [Automatic (Delayed Start)], **Вручную** (Manual) или **Отключена** (Disabled). При выборе типа запуска учитывайте следующее:

- Если выбрать автоматический запуск, служба будет запускаться при загрузке системы. Некоторые службы автоматически останавливаются, когда не используются. Тем не менее, если служба вам больше не нужна, выберите тип запуска **Вручную** или **Отключена**.
- Если для службы выбран тип запуска **Автоматически (отложенный запуск)**, она будет запускаться сразу после загрузки системы. При этом система может загружаться быстрее, но если служба должна запускаться во время загрузки, выберите тип **Автоматически**. Если служба не нужна, выберите тип запуска **Вручную** или **Отключена**.
- Запуск вручную позволяет операционной системе запускать службу при необходимости. На практике некоторые службы в ручном режиме не запускаются, когда требуется. Если какая-то служба должна работать, лучше выберите тип запуска **Автоматически**.
- Если выбрать тип запуска **Отключена**, служба не будет запускаться даже в случае необходимости. Если нет веских причин для отключения службы, установите режим запуска **Ручной**.

На вкладке **Общие** указано, запущена ли в данный момент служба, предоставляется возможность запустить или остановить службу и указать параметры запуска.

На вкладке **Вход в систему** обычно указано, что служба выполняет вход под учетной записью локальной системы. При необходимости можно указать другую учетную запись, например, локальную учетную запись администратора.

На вкладке **Восстановление** указаны действия, которые будут предприниматься при сбоях службы. Можно указать действия для первого, второго и

последующих сбоев. В зависимости от указанных действий доступны следующие параметры:

- Если выбрать действие **Запуск программы** (Run A Program), необходимо ввести полный путь к программе, которую требуется запускать. Указанные программы или сценарии не должны требовать пользовательского ввода.
- Если выбрать действие **Перезагрузка компьютера** (Restart The Computer), необходимо указать, сколько времени компьютер будет ждать перед перезагрузкой. Можно также указать, когда будет выполнен сброс счетчика сбоев.
- Если установить флажок **Включить действия для остановок с ошибками** (Enable Actions For Stops With Errors), можно запускать действия по восстановлению, когда служба завершит работу с ошибкой.

На вкладке **Зависимости** показаны службы, системные драйверы и списки загрузки групп, от которых зависит служба. Если служба работает не так, как ожидается, возможно, отключена другая служба, от которой имеется зависимость.

Чтобы получать уведомления о сбоях служб, можно создать программу, вызывающую механизм оповещения. Можно также создавать программы, составляющие отчеты о работе служб, за которыми требуется наблюдать. Однако многие службы не отслеживаются автоматически, поэтому рекомендуем регулярно запускать оснастку **Службы** и проверять, как работают службы.

## Запись и пересылка событий и подписки на события

Вы наверняка пользовались средством **Просмотр событий** (Event Viewer), поэтому мы рассмотрим этот инструмент лишь вкратце, а затем поговорим о пересылке событий и подписках на события, о которых вам, вероятно, известно меньше.

Планируя стратегию мониторинга для производственной сети, имеющей несколько серверов, следует рассмотреть возможность сбора журналов событий со всех компьютеров, за которыми требуется наблюдать, на одном компьютере-сборщике (который обычно является административной рабочей станцией, хотя это не обязательно). Необходимо решить, какие события будут отслеживаться, и какие действия следует предпринимать в случае обнаружении критических событий, ошибок и предупреждений. Если требуется немедленное уведомление об определенных событиях или вы хотите, чтобы событие автоматически вызвало действие, следует прикрепить к событиям задания. Перспективное планирование стратегии мониторинга событий требует времени и размышлений, однако в итоге может избавить от лишней работы и проблем.

Сведения о подписках на события можно найти на вкладке **Подписки** (Subscriptions) диалогового окна свойств журнала событий. На вкладке **Общие** этого диалогового окна указан текущий размер журнала, максимальный размер журнала, действие, которое будет выполнено при достижении максимального размера журнала, и другие сведения. Проще всего запустить средство **Просмотр событий** (Even Viewer) командой eventvwr.

В средстве просмотра событий отображаются журналы событий, представляющие собой файлы, в которые записываются значимые события, такие как

вход пользователя в систему или ошибка в программе. Данные из журналов событий очень полезны при устранении проблем. Записываемые события делятся на следующие категории:

- критические события;
- ошибки;
- предупреждения
- сведения.

Журнал безопасности содержит также две категории событий аудита: аудит успеха и аудит отказа. Подробную информацию о событии можно просмотреть на вкладке **Подробности** (Verbose).

Средство просмотра событий записывает информацию в несколько журналов:

- **Приложение** (Application) — содержит события приложений. События классифицируются, в зависимости от серьезности: ошибка, предупреждение или сведения. Классификация «критическая ошибка» в журнале **Приложение** отсутствует.
- **Безопасность** (Security) — содержит события аудита успеха или отказа, имеющие отношение к безопасности. Например, если пользователь выполнит успешный вход в систему, в этот журнал будет записано событие аудита успеха.
- **Установка** (Setup) — содержит события, связанные с установкой приложения, например, сведения о том потребовалась ли при установке перезагрузка компьютера.
- **Система** (System) — содержит системные события, записанные Windows Server 2008 R2 и системными службами. Системные события классифицируются как критические, ошибки, предупреждения и сведения.
- **Перенаправленные события** (Forwarded Events) — содержит события, пересылаемые другими компьютерами.

## Настраиваемые представления

В средстве просмотра событий можно создавать настраиваемые представления. Для этого щелкните **Настраиваемые представления** (Custom Views) на левой панели средства просмотра событий, а затем щелкните **Создать настраиваемое представление** (Create Custom View) в меню **Действие** (Action). Можно также щелкнуть правой кнопкой мыши узел **Настраиваемые представления** (Custom Views) и выбрать команду **Создать настраиваемое представление** (Create Custom View). После этого создайте фильтр, выбрав журналы событий или источники событий и фильтрацию по уровню, времени записи, коду события, категории задания, ключевым словам, пользователю или компьютерам. Вряд ли потребуется выбирать все эти критерии, однако они позволяют сузить поле поиска проблемы, избавляя от необходимости просматривать огромное количество событий. На рис. 12-22 показана настройка фильтра.

Следующий этап — сохранение выбранного фильтра в виде настраиваемого представления. Фильтры непостоянны. Если настроить фильтр для просмотра определенной информации в журнале событий, то в следующий раз, когда по-

требуется та же информация, придется настроить этот фильтр заново. Настраиваемые представления постоянны, т. е. к ним можно переходить в любое время, открыв средство просмотра событий. Фильтр можно сохранить как настраиваемое представление, чтобы он стал постоянным, и его не приходилось настраивать для каждого использования. Меню **Действие** позволяет импортировать настраиваемые представления из другого источника и подключаться к другому компьютеру. На этом компьютере требуется административная учетная запись.

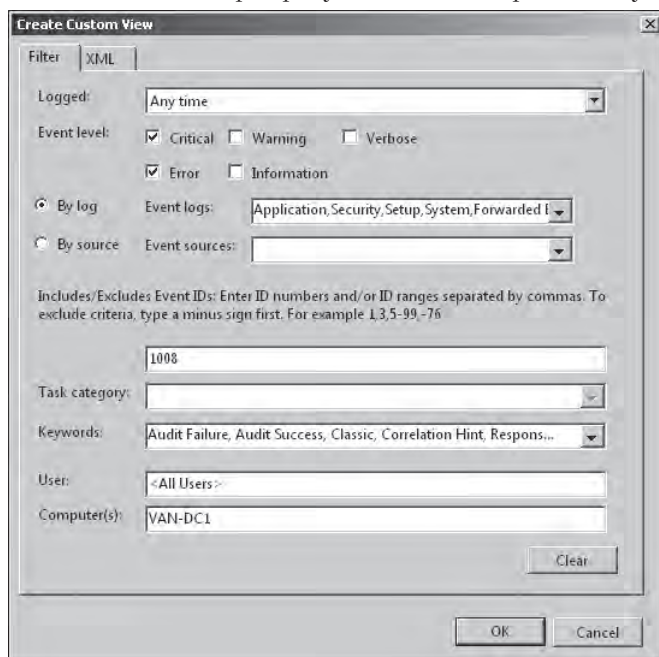


Рис. 12-22. Настройка фильтра для создания настраиваемого представления

## Журналы приложений и служб

Средство просмотра событий предоставляет несколько журналов приложений и служб. Сюда входят журналы программ, установленных на компьютере, и подробные журналы с информацией об отдельных службах Windows. Например, могут быть доступны следующие журналы:

- события оборудования;
- Internet Explorer;
- служба управления ключами;
- Media Center;
- диагностика Microsoft Office;
- сеансы Microsoft Office;
- Windows PowerShell.

Дополнительные журналы можно найти под узлом **Журналы приложений и служб | Microsoft | Windows**.

## Привязка задач к событиям

Иногда требуется получать по электронной почте уведомления об определенном событии или запускать при возникновении события указанную программу, например, активирующую пейджер. Как правило, такие действия требуются для событий из журнала безопасности, например, для неудачного входа в систему (код события 4625) или успешного входа пользователя, который не должен выполнять вход на определенный компьютер. Чтобы получить такую возможность, следует привязать задачу к событию.

Для этого откройте средство просмотра событий и перейдите к журналу, содержащему событие, о котором требуется получить уведомление. Обычно это журнал **Безопасность (Security)** из узла **Журналы Windows (Windows Logs)**, но можно выбрать любой другой журнал Windows или журнал приложений и служб. Выберите событие, перейдите и в меню **Действие** щелкните **Привязать задачу к событию (Attach Task To This Event)**.

Откроется мастер создания простой задачи. Введите имя и (если требуется) описание задачи и щелкните **Далее**. На следующей странице приводится описание события, по которому можно проверить, правильное ли событие выбрано, прежде чем щелкнуть **Далее**. На следующей странице выберите действие для задачи: запустить программу, отправить электронное письмо или отобразить сообщение. Щелкните **Далее** и настройте выбранную задачу. Например, если требуется отправлять сообщения электронной почты, укажите адрес отправителя и получателя, тему, текст, вложение (если требуется) и сервер SMTP (рис. 12-23). Щелкните **Далее**, а затем **Готово**.

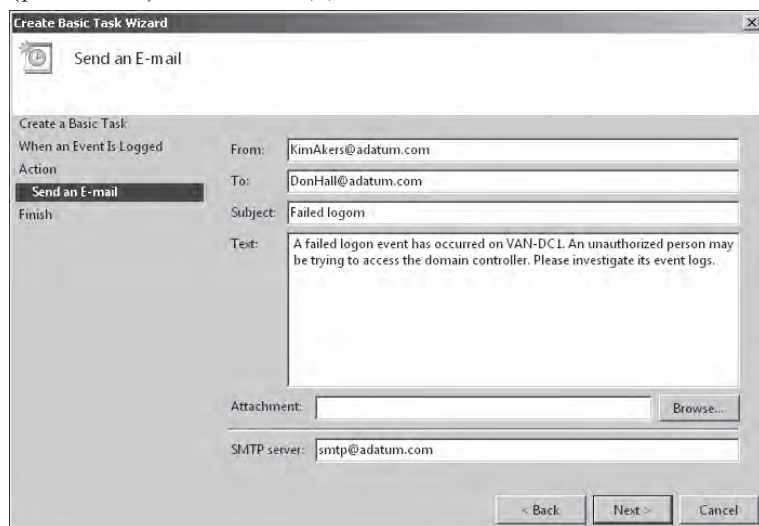


Рис. 12-23. Выбор действия, выполняемого при возникновении события

## Диагностика сети при помощи журналов событий

Когда запускается диагностика сети Windows (например, из окна браузера, когда прерывается сетевое подключение), все обнаруженные проблемы и способы их решения отображаются в диалоговом окне **Диагностика сети (Network Diagnostics)**. Однако если имеется более подробная информация, Windows



Server 2008 R2 сохраняет ее в одном или нескольких журналах событий. Эту информацию можно использовать для анализа проблем подключения и интерпретации выводов. Можно также фильтровать события диагностики сети и протоколов TCP/IP, выбрав, например, источники событий Tcprp и Tcprv6 и просматривая события из этих источников в настраиваемом представлении.

Если при диагностике сети обнаружена проблема с беспроводной сетью, данные сохраняются в журналы событий как вспомогательные или информационные события. Вспомогательные события предоставляют сводку результатов диагностики и повторяют информацию из диалогового окна **Диагностика сети** (Network Diagnostics). Они могут предоставлять дополнительную информацию для устранения неполадок, например, сведения о диагностируемом подключении, результаты диагностики и описание возможностей диагностируемой беспроводной сети и адаптера.

Информационные события могут содержать сведения о диагностируемом подключении, параметрах беспроводной сети на компьютере и в сети, сетях, маршрутизаторах и точках доступа, доступных во время диагностики, предпочтительных беспроводных сетях, истории и статистики подключений, например, пакетной статистике и истории роуминга. Также в них приводятся сведения о попытках подключения, отображается список их состояний и сообщается, какие фазы подключения были неудачными или не начались.

## Пересылка событий и подписки на события

Пересылка событий позволяет отправлять на компьютер-сборщик события, соответствующие определенным критериям, для централизованного управления событиями. Один журнал событий на компьютере-сборщике содержит важные события со всех компьютеров организации, избавляя от необходимости подключаться к локальным журналам событий на отдельных компьютерах.

Пересылка событий с компьютера-источника на компьютер-сборщик выполняется по протоколу HTTP, а если требуется обеспечить дополнительный уровень шифрования и аутентификации для повышения безопасности — по протоколу HTTPS. Так как для пересылки используются те же протоколы, что и для просмотра веб-сайтов, ее можно выполнять через большинство брандмауэров и прокси-серверов. Трафик пересылки событий шифруется при использовании обоих протоколов — HTTP и HTTPS.

Для пересылки сообщений необходимо настроить компьютер-источник и компьютер-сборщик. Запустите на обоих компьютерах службу удаленного управления Windows (Windows Remote Management, WinRM) и сборщик событий Windows (Windows Event Collector). Настройте на компьютере-источнике исключение брандмауэра Windows для протокола HTTP. В зависимости от выбранной технологии оптимизации доставки, может потребоваться также создание исключения брандмауэра Windows на компьютере-сборщике.

Подписки могут инициироваться сборщиком или источником. В подписках, инициированных сборщиком, компьютер-сборщик запрашивает события у компьютера, сгенерировавшего их. Такие подписки следует использовать при наличии ограниченного количества компьютеров-источников, которые уже идентифицированы (например, для сбора событий с серверов). В этом типе подписки каждый компьютер настраивается вручную.



В подписке, инициированной источником, компьютер, на котором сгенерировано событие (компьютер-источник), отправляет событие компьютеру-сборщику. Такие подписки следует использовать при наличии большого числа компьютеров-источников (например, клиентов), которые настраиваются с помощью групповой политики.

В инициированную источником подписку можно добавлять дополнительные компьютеры-источники, после того как подписка создана, так что необязательно сразу определять, какие компьютеры в сети должны быть источниками. В подписках, инициированных сборщиками, компьютер-сборщик получает события от одного или нескольких компьютеров-источников. Подписки, инициированные сборщиком, обычно используются в небольших сетях или в сетях, где события собираются с ограниченного числа серверов. В подписках, инициированных источником, компьютеры-источники пересылают события компьютеру-сборщику. В корпоративных сетях используются подписки, инициированные источником.

Компьютер-сборщик должен работать под управлением Windows Server 2008 или 2008 R2, Windows 7, Windows Vista или Windows Server 2003 R2. Компьютер-источник должен работать под управлением Windows XP с пакетом обновлений 2, Windows Server 2003 с пакетом обновлений 1 или 2, Windows Server 2003 R2, Windows Vista, Windows 7, Windows Server 2008 или 2008 R2.

---

#### **ПРИМЕЧАНИЕ Пересылающие компьютеры**

В специализированной литературе компьютеры-источники часто неточно называются пересылающими компьютерами. В подписках, инициированных сборщиком, компьютер-сборщик получает события от компьютера-источника, а не пересылает события. Только в подписках, инициированных источником, компьютер-источник пересылает события, и только в этом случае его правильно будет называть пересылающим компьютером. Во избежание путаницы вместо термина «пересылающий компьютер» в этой главе используется термин «компьютер-источник».

---

В подписке, инициированной сборщиком, в первую очередь вручную настраивается один или несколько компьютеров-источников и компьютер-сборщик. После настройки компьютеров-источников и компьютера-сборщика можно создать подписку событий, чтобы определить, какие события следует пересылать.

#### **Настройка подписки, инициированной сборщиком**

Чтобы настроить компьютер под управлением Windows Server 2008 R2 для получения от него событий компьютером-сборщиком, откройте командную строку с повышенными привилегиями и настройте службу удаленного управления Windows с помощью утилиты командной строки Winrm, входящей в состав службы WinRM. Введите следующую команду:

```
winrm quickconfig
```

Эту команду можно сократить до `winrm qc`. Появится сообщение, аналогичное показанному на рис. 12-24 (этот снимок экрана сделан на контроллере домена VAN-DC1). Необходимые изменения зависят от настройки операционной системы. Чтобы внести эти изменения, введите **Y**. Обратите внимание: если для

любого из сетевых разъемов выбран тип *общий* (*public*), для использования этой команды необходимо выбрать для него тип *частный* (*private*).

Затем добавьте учетную запись компьютера-сборщика в локальную группу **Читатели журнала событий** (Event Log Readers) или в локальную группу администраторов на компьютере-источнике. Это можно сделать с помощью оснастки **Локальные пользователи и группы** (Local Users And Groups) или командой Net.exe.

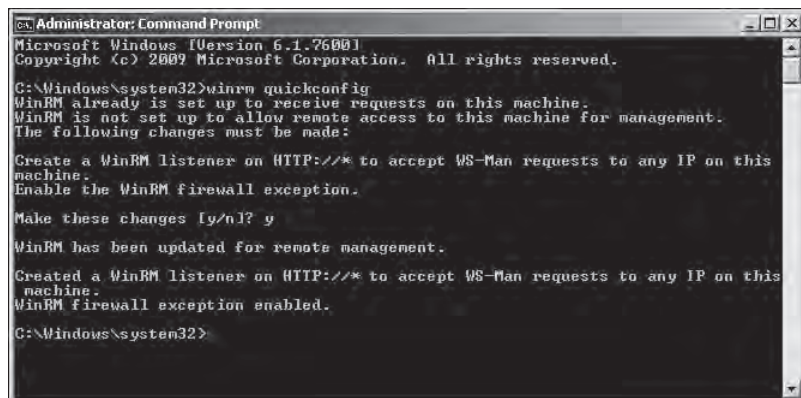


Рис. 12-24. Настройка службы удаленного управления Windows

Можно добавить учетную запись компьютера-сборщика в локальную группу **Администраторы** или группу **Читатели журнала событий** на компьютере-источнике. Если не требуется, чтобы компьютер-сборщик получал события в журнал безопасности, лучше использовать группу **Читатели журнала событий**. Однако если требуется передавать информацию из журналов безопасности, необходимо использовать локальную группу администраторов.

По умолчанию оснастка **Локальные пользователи и группы** не разрешает добавлять учетные записи компьютеров. Чтобы иметь такую возможность, в диалоговом окне выбора пользователей, компьютеров или групп щелкните кнопку **Типы объектов** (Object Types) и установите флажок **Компьютеры** (Computers).

## Настройка компьютера для хранения подписок, инициализированных сборщиком

Нельзя настроить компьютер одновременно в качестве компьютера-источника и компьютера-сборщика. Если вы настроили контроллер домена VAN-DC1 как компьютер-источник, то в качестве компьютера-сборщика используйте сервер VAN-SRV1. В производственной сети компьютер-сборщик обычно является административной рабочей станцией под управлением Windows 7.

Чтобы настроить компьютер под управлением Windows Server 2008 R2 для сбора событий, откройте командную строку с повышенными привилегиями и введите следующую команду для настройки службы сборщика событий Windows:

```
wecutil qc
```

После ввода этой команды появится сообщение о том, что режим запуска службы будет изменен на запуск с задержкой. Для продолжения введите **Y**.

После настройки компьютера-источника и компьютера-сборщика настройте подписку на события, указав, какие события и от каких источников должен получать компьютер-сборщик.

---

**СОВЕТ Подготовка к экзамену**

Не путайте команды Winrm и Wecutil. Winrm используется для настройки службы удаленного управления Windows и обычно устанавливается на компьютере-источнике. Wecutil используется для настройки сборщика событий Windows и обычно устанавливается на компьютере-сборщике.

---

---

**ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Создание подписки, инициированной сборщиком**

Подробнее о создании подписки, инициированной сборщиком, см. по адресу [http://msdn.microsoft.com/en-us/library/bb513652\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/bb513652(VS.85).aspx) (на английском языке).

---

**Настройка подписки, инициированной источником**

Подписки, инициированные сборщиком, обычно используются в корпоративных сетях, где компьютеры-источники можно настраивать с помощью групповой политики. Для настройки подписки, инициированной источником, следует вручную настроить компьютер-сборщик, а затем с помощью групповой политики настроить компьютеры-источники. После настройки компьютера-сборщика и компьютеров-источников можно создать подписку на события, чтобы определить, какие события нужно пересылать.

Подписки, инициированные источником, позволяют настроить подписку на компьютере-сборщике, не определяя компьютеры-источники. После этого с помощью групповой политики можно настроить несколько удаленных компьютеров-источников для пересылки событий компьютеру-сборщику. В отличие от этого, при использовании подписки, инициированной сборщиком, необходимо определить все источники в подписке.

Настройка компьютера-сборщика в подписке, инициированной источником, выполняется с помощью командной строки с повышенными привилегиями. Если компьютер-сборщик и компьютер-источник находятся в одном домене, необходимо создать на компьютере-источнике XML-файл подписки (например, Subscription.xml), открыть на этом компьютере командную строку с повышенными привилегиями и настроить WinRM, выполнив следующую команду:

```
winrm qc -q
```

Затем настройте сборщик событий на том же компьютере, введя следующую команду:

```
wecutil qc -q
```

Настройте подписку, инициированную сборщиком, на компьютере-сборщике, введя следующую команду:

```
wecutil cs subscription.xml
```

Нельзя настроить компьютер-источник для использования подписки, инициированной источником, если этот компьютер уже настроен для использования подписки, инициированной сборщиком. Поэтому необходимо заранее

спланировать, какой тип подписки будет использоваться в сети. Чтобы настроить компьютер-источник для использования подписки, инициированной источником, сначала настройте на этом компьютере службу WinRM, введя следующую команду:

```
winrm qc -q
```

После этого с помощью групповой политики добавьте адрес компьютера-сборщика в параметр SubscriptionManager. Запустите групповую политику из командной строки с повышенными привилегиями, введя следующую команду:

```
%SYSTEMROOT%\System32\gpedit.msc
```

Откроется редактор локальной групповой политики. Раскройте узлы **Конфигурация компьютера | Административные шаблоны | Компоненты Windows** (Computer Configuration | Administrative Templates | Windows Components) и выберите узел **Пересылка событий** (Event Forwarding).

Правой кнопкой щелкните параметр **SubscriptionManager** и выберите команду **Свойства** (Properties). Включите параметр **SubscriptionManager** и щелкните **Показать** (Show). Добавьте как минимум один параметр, указывающий компьютер-сборщик. Диалоговое окно свойств параметра SubscriptionManager имеет вкладку **Объяснение** (Explain), на которой описан синтаксис этого параметра.

Добавив параметр SubscriptionManager, введите следующую команду, чтобы обеспечить применение политики:

```
gpupdate /force
```

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ    Настройка и создание подписки, инициированной источником

Подробнее о настройке подписки, инициированной источником, см. по адресу [http://msdn.microsoft.com/en-us/library/bb870973\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/bb870973(VS.85).aspx) (на английском языке). О создании такой подписки программным способом см. по адресу [http://msdn.microsoft.com/en-us/library/bb870971\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/bb870971(VS.85).aspx) (на английском языке). Однако учитывайте, что на экзамене не потребуется писать программы на C++.

---

### Создание подписки на события

Для получения событий, пересылаемых с компьютера-источника на компьютер-сборщик, необходимо создать одну или несколько подписок на события. Прежде чем настраивать подписку, настройте компьютер-сборщик и компьютер-источник, как описано выше. Чтобы создать подписку на компьютере-сборщике, выполните следующее:

1. Откройте средство просмотра событий (Event Viewer), правой кнопкой щелкните узел **Подписки** (Subscriptions) и выберите команду **Создать подписку** (Create Subscription).
2. Если будет предложено, щелкните **Да**, чтобы настроить автоматический запуск службы сборщика событий Windows.
3. В диалоговом окне **Свойства подписки** (Subscription Properties) введите имя и, если требуется, описание подписки (рис. 12-25).

4. Выберите тип создаваемой подписки: **Инициировано сборщиком** (Collector Initiated) или **Инициировано компьютером-источником** (Source Computer Initiated). Выберите компьютеры или группы компьютеров.
5. Щелкните кнопку **Выбрать события** (Select Events), чтобы открыть диалоговое окно **Фильтр запросов** (Query Filter). В этом диалоговом окне определите критерии, которым должны соответствовать пересылаемые сообщения, и щелкните **ОК**.
6. Если хотите, в диалоговом окне свойств подписки щелкните кнопку **Дополнительно** (Advanced), чтобы открыть диалоговое окно **Дополнительные параметры подписки** (Advanced Subscription Settings), где можно выбрать один из трех способов оптимизации доставки подписок: **Обычная** (Normal), **Уменьшенная пропускная способность** (Minimize Bandwidth) и **Уменьшенная задержка** (Minimize Latency).

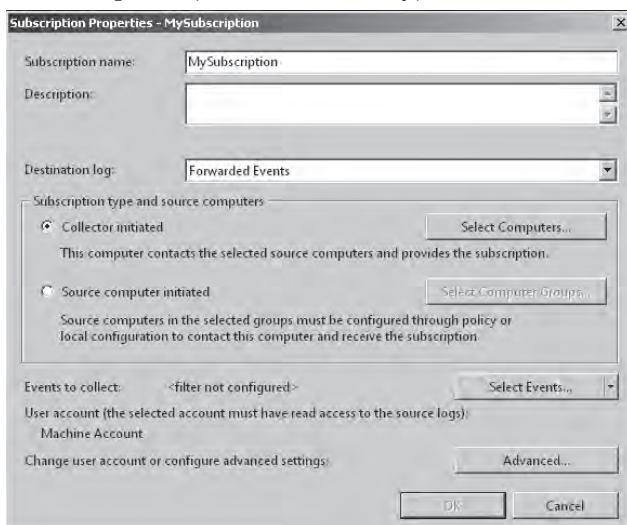


Рис. 12-25. Свойства подписки

---

**ПРИМЕЧАНИЕ** Выбор учетной записи, которую будет использовать подписка

В диалоговом окне **Дополнительные параметры подписки** можно настроить учетную запись, которую будет использовать подписка. Независимо от того, используется ли учетная запись компьютера (по умолчанию) или выбран пользователь, убедитесь, что эта учетная запись входит в группу **Читатели журнала событий** на компьютере-источнике (или в локальную группу администраторов, если собирается информация из журнала безопасности).

- 
7. Щелкните **ОК** в диалоговом окне свойств подписки, чтобы создать подписку.

---

**ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ** Использование SDK сборщика событий Windows

Если вас интересует программное использование сборщика событий, зайдите на страницу [http://msdn.microsoft.com/en-us/library/bb513659\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/bb513659(VS.85).aspx) (на английском языке). Однако программирование не входит в темы экзамена, и на экзамене вам не придется писать программы на C++.

---

## Практикум. Оценка производительности диска

На этом практикуме вы соберете данные о производительности контроллера домена VAN-DC1. Вы просмотрите эти данные в виде графика, гистограммы и отчета. В своей тестовой сети вы можете получить данные, отличающиеся от показанных на рисунках. Перед выполнением упражнений практикума подключите к компьютеру второе запоминающее устройство, например, жесткий диск или флэш-накопитель USB. Если используете виртуальные машины, можете добавить виртуальный жесткий диск.

### Упражнение 1. Добавление и мониторинг счетчиков диска

В этом упражнении вы добавите счетчики для наблюдения за производительностью жесткого диска C: вашего компьютера. Если у вас есть дополнительные тома на жестком диске или дополнительные жесткие диски, можете выполнить также и их мониторинг. Заметьте, что после выполнения упражнения 1 следует сразу начать упражнение 2, поэтому распределите время так, чтобы выполнить оба упражнения сразу.

---

#### ПРИМЕЧАНИЕ DISKPERF

По умолчанию в Windows Server 2008 R2 счетчики производительности логического и физического дисков включаются по требованию. Существует, однако, команда Diskperf, с помощью которой можно принудительно включать и отключать счетчики диска в старых приложениях, использующих интерфейс Ioctl\_disk\_performance.

---

---

#### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ IOCTL\_DISK\_PERFORMANCE

Подробнее об интерфейсе Ioctl\_disk\_performance см. по адресу [http://msdn.microsoft.com/en-us/library/ff560388\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ff560388(VS.85).aspx) (на английском языке). Однако учтите, что это старый интерфейс, который вряд ли встретится на экзамене.

---

Узкое место, влияющее на использование и скорость диска, значительно влияет на производительность компьютера в целом. Чтобы добавить счетчики для мониторинга производительности диска, выполните следующее:

1. Зайдите на VAN-DC1 под учетной записью Kim Akers.
2. Откройте консоль **Системный монитор** (Performance Monitor) и щелкните узел **Системный монитор** (Performance Monitor).
3. В системном мониторе щелкните кнопку **Добавить** (зеленый знак «+»).
4. В диалоговом окне **Добавить счетчики** (Add Counters) убедитесь, что в раскрываемом меню **Выбрать счетчики с компьютера** (Select Counters From Computer) выбран локальный компьютер.
5. Установите флажок **Отображать описание** (Show Description).
6. Выделите все счетчики, имеющиеся в панели **Добавленные счетчики** (Added Counters) и щелкните **Удалить** (Remove).
7. На панели **Имеющиеся счетчики** (Available Counters) разверните раздел **Логический диск** (LogicalDisk) и выберите счетчик **% свободного места** (% Free Space). В списке **Экземпляры выбранного объекта** (Instances Of Selected Object) выберите **C:** (рис. 12-26). Этот счетчик измеряет процент



свободного места на выбранном логическом диске. Если значение падает ниже 15%, вы рискуете лишиться свободного пространства для хранения важных системных файлов.

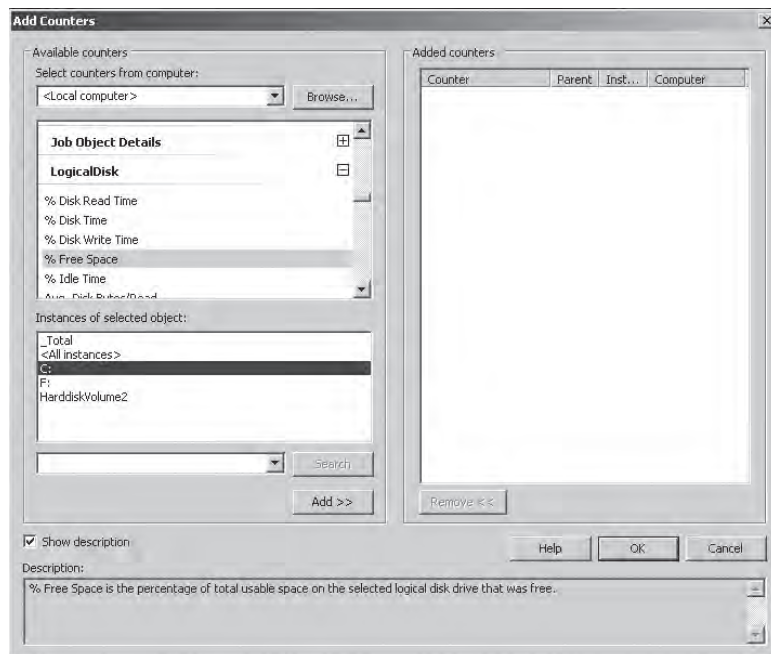


Рис. 12-26. Выбор счетчика % свободного места для диска C:

8. Щелкните **Добавить** (Add), чтобы добавить этот счетчик.
9. В секции **Имеющиеся счетчики** раскройте раздел **Физический диск** (PhysicalDisk) и выберите **Процент времени бездействия** (% Idle Time). В списке экземпляров выбранного объекта выберите **C:** (рис. 12-27). Этот счетчик измеряет процент времени бездействия диска в заданный промежуток времени. Если эта величина падает ниже 20%, ресурсы дисковой системы считаются исчерпанными и следует установить более быструю дисковую систему.
10. Щелкните **Добавить**, чтобы добавить этот счетчик.
11. Таким же образом добавьте экземпляр **C:** счетчика **Физический диск | Среднее время чтения с диска (с)** [PhysicalDisk | Avg. Disk Sec/Read]. Этот счетчик измеряет среднее время чтения данных с диска в секундах. Если эта величина превышает 25 миллисекунд (мс), дисковая система испытывает задержку при чтении с диска. В этом случае желательно установить более быструю дисковую систему.
12. Таким же образом добавьте экземпляр **C:** счетчика **Физический диск | Среднее время записи на диск (с)** [PhysicalDisk | Avg. Disk Sec/Write]. Этот счетчик измеряет среднее время записи данных на диск в секундах. Если данная величина превышает 25 миллисекунд (мс), дисковая система испытывает задержку при записи на диск, и желательно установить более быструю дисковую систему.



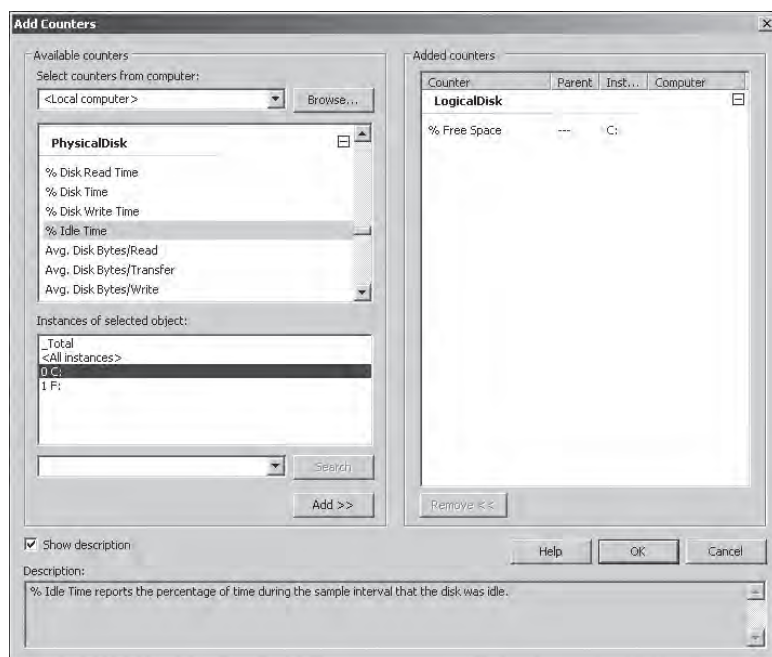


Рис. 12-27. Выбор счетчика %времени бездействия для диска C:

#### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Счетчик Физический диск | % активности диска

Поскольку значение счетчика **%активности диска** может превышать 100%, многие администраторы предпочитают использовать счетчики **Процент времени бездействия**, **Среднее время чтения (с)** и **Среднее время записи (с)** из раздела **Физический диск** для получения более точных данных об использовании жесткого диска. Подробнее о счетчике **% активности диска** см. по адресу <http://support.microsoft.com/kb/310067> (на английском языке). Эта статья не относится конкретно к Windows Server 2008 R2, но в ней можно найти необходимую базовую информацию.

13. Таким же образом добавьте экземпляр **C:** счетчика **Физический диск | Средняя длина очереди диска** (PhysicalDisk | Avg. Disk Queue Length). Этот счетчик показывает число операций ввода-вывода, ожидающих, когда жесткий диск станет доступным. Если значение этого счетчика превышает двукратное число шпинделей в массиве дисков, то, возможно, физический диск сам по себе является узким местом.
14. Таким же образом добавьте счетчик **Память | Байт кэш-памяти** (Memory | Cache Bytes). Этот счетчик показывает объем памяти, используемой для кэша файловой системы. Он может быть узким местом диска, если его значение превышает 300 МБ.
15. Убедитесь, что диалоговое окно **Добавить счетчики** (Add Counters) содержит все счетчики и экземпляры, показанные на рис. 12-28. Щелкните **ОК**.
16. Не закрывайте системный монитор. Переходите к упражнению 2.

**ПРИМЕЧАНИЕ Счетчик, включенный по умолчанию**

Счетчик **Процессор | % загруженности процессора** (Processor | % Processor Time) включен по умолчанию, и его не нужно добавлять. Он не отображается в списке на рис. 12-28, однако его можно увидеть в режимах просмотра «Строка», «Линейчатая гистограмма» и «Отчет» (см. упражнение 2).

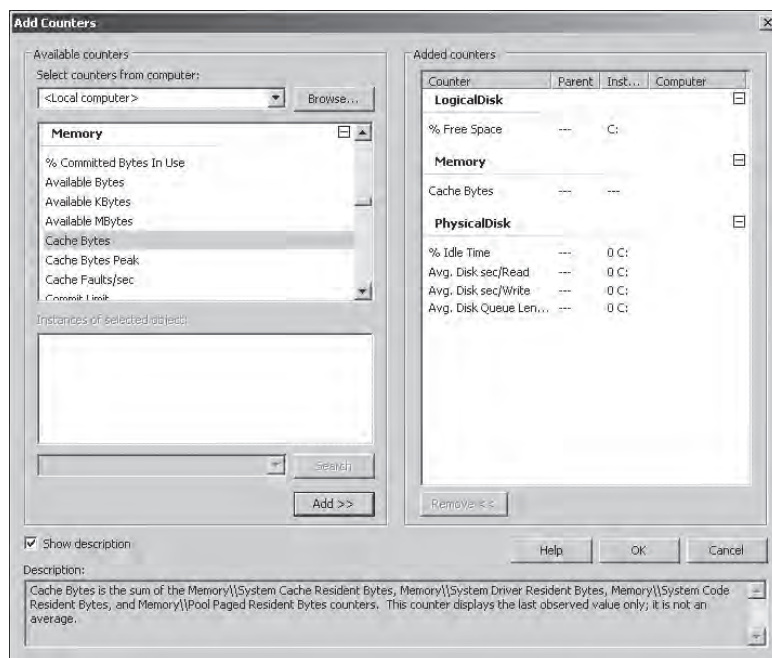


Рис. 12-28. Добавленные счетчики и экземпляры

## Упражнение 2. Настройка свойств системного монитора и мониторинг производительности диска

В этом упражнении вы зададите интервал и длительность измерения, выполните чтение и запись данных на том диске, мониторинг которого выполняете, после чего просмотрите результаты в виде строки, гистограммы и отчета.

1. В меню **Действие** (Action) системного монитора выберите команду **Свойства** (Properties).
2. В открывшемся диалоговом окне на вкладке **Общие** (General) введите в поле **Съем показаний каждые** (Sample Every) значение **5**, а в поле **Длительность** (Duration) значение **300**. Щелкните **ОК**.
3. Скопируйте файл или папку размером около 100 МБ с диска C: на подключенное запоминающее устройство. Если потребуется административное разрешение, щелкните **Продолжить** (Continue).
4. Скопируйте файл или папку размером около 100 МБ с подключенного запоминающего устройства на диск C:. Если потребуется административное разрешение, щелкните **Продолжить** (Continue).

- Просмотрите линейный график (рис. 12-29). Такой тип графика может быть не самым лучшим вариантом для просмотра нужной информации.

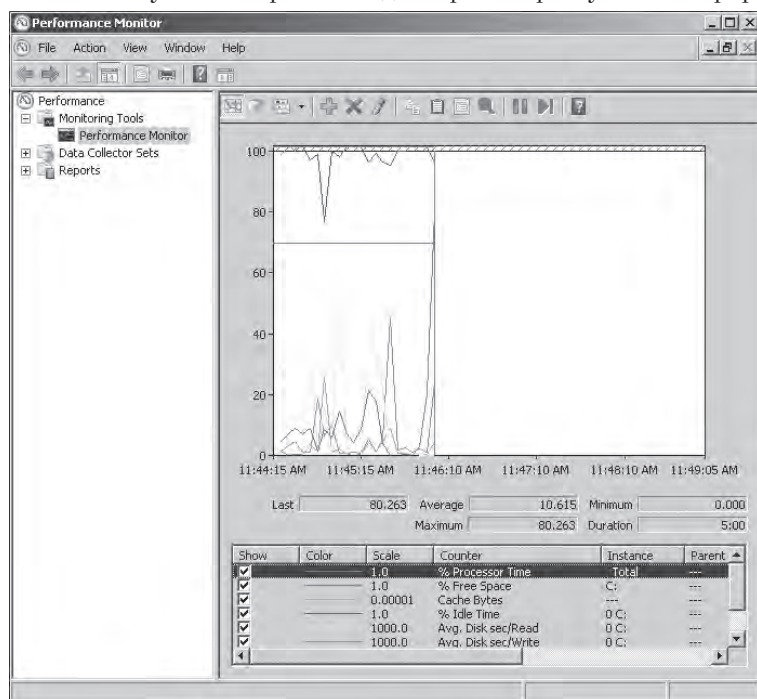


Рис. 12-29. Линейный график в системном мониторе

- В раскрывающемся меню **Изменить тип диаграммы** (Change Graph) выберите **Линейчатая гистограмма** (Histogram Bar). Просмотрите гистограмму в системном мониторе (рис. 12-30).
- Измените тип диаграммы на **Отчет** (Report). Просмотрите отчет в системном мониторе (рис. 12-31).
- Проанализируйте показания счетчика с учетом информации, полученной о каждом счетчике в упражнении 1. Результаты, показанные на снимках экрана, свидетельствуют о том, что на том C: осталось достаточно свободного пространства, поэтому не возникло проблем с копированием довольно большого файла или папки. Использование кэша памяти было значительным, но в пределах нормы и приемлемым для данной операции (Вы можете получить другие результаты.)

#### ПРИМЕЧАНИЕ Кэширование файлов

Чтобы получить в упражнении 2 имеющие значение результаты, мы предложили просмотреть в виде линейного графика, гистограммы и отчета данные для одной и той же операции копирования. Если повторять операции копирования для каждого типа графика, результаты будут другими. Причина в том, что Windows Server 2008 R2 выполняет кэширование файла или папки после первого копирования, и последующие результаты отражают только запись файла на диск и получение его из оперативной памяти. Использовать эти инструменты относительно просто, чего нельзя сказать об интерпретации результатов.

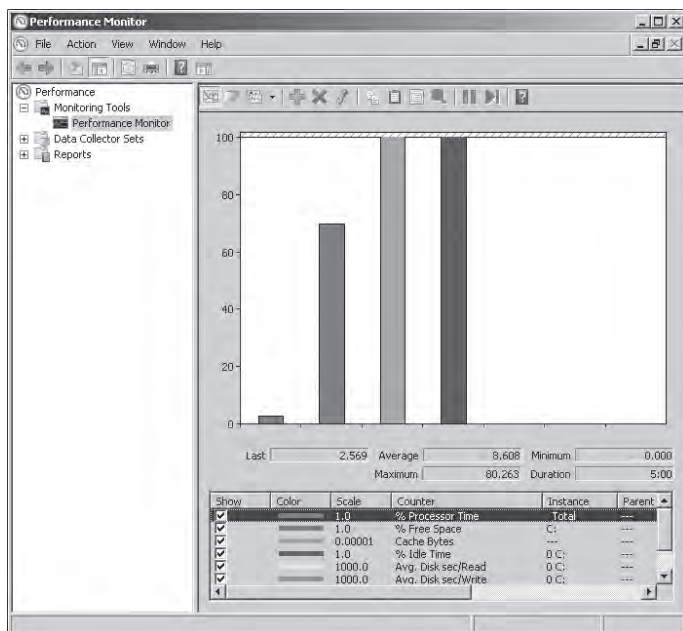


Рис. 12-30. Системный монитор, просмотр данных в виде гистограммы

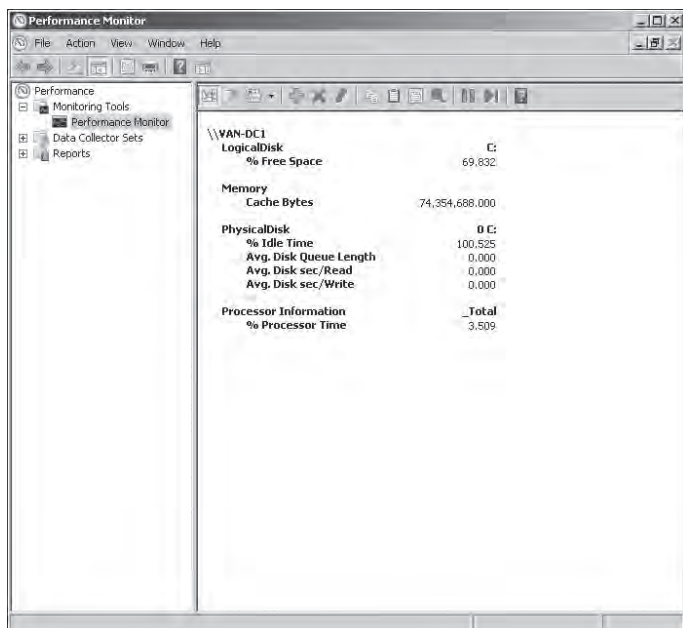


Рис. 12-31. Системный монитор, просмотр данных в виде отчета

## Резюме

- Системный монитор позволяет просматривать данные производительности в режиме реального времени или показания счетчиков производительности,

полученные группами DCS. Отчет диагностики системы содержит данные о состоянии аппаратных ресурсов, времени ответов системы и процессах на локальном компьютере, а также сведения о системе и данные конфигурации.

- **Монитор стабильности системы** позволяет наблюдать за стабильностью компьютера и сообщает, происходили ли события, способные повлиять на стабильность (такие как установка приложения), и требовалась ли после них перезагрузка. Центр поддержки следит за состоянием компьютера и сообщает о проблемах с безопасностью, обслуживанием и соответствующими параметрами. Оснастка **Службы** позволяет проверять, работает ли та или иная служба, настраивать тип ее запуска и указывать действия, которые требуется выполнить в случае сбоя службы или ее завершения с ошибками.
- **Диспетчер задач** показывает информацию об использовании ресурсов и позволяет управлять приложениями, службами и протоколами. Монитор ресурсов позволяет просматривать информацию об использовании аппаратных и программных ресурсов в реальном времени. Утилита Process Explorer выполняет те же функции, что и диспетчер задач, но предоставляет дополнительные возможности по управлению и более подробную информацию о системе.
- **Средство просмотра событий** предоставляет доступ к журналам событий и позволяет фильтровать их, а также создавать настраиваемые представления. Можно привязывать задания к событиям, настраивать пересылку событий и подписки, чтобы компьютер-сборщик мог хранить события, сгенерированные на одном или нескольких компьютерах-источниках.

## Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных на занятии 1. Эти вопросы предоставлены также в электронном виде на прилагаемом к книге компакт-диске.

1. Сервер под управлением Windows Server 2008 R2 загружается недопустимо долго. Вы выявили службу, которая долго загружается, и считаете, что она замедляет загрузку. Вам не требуется, чтобы эта служба запускалась сразу после загрузки компьютера, однако вы хотите, чтобы она запускалась автоматически вскоре после этого. Как следует настроить запуск этой службы?
  - a. Автоматически.
  - b. Вручную.
  - c. Автоматически (Отложенный запуск).
  - d. Отключена.
2. Сервер под управлением Windows Server 2008 R2 испытывает перебои в производительности. Вы подозреваете, что эти проблемы вызваны недавно установленным приложением, но не помните, когда именно установили его. Какой инструмент следует использовать, чтобы определить, когда было установлено приложение?
  - a. Монитор стабильности.
  - b. Центр поддержки.
  - c. Группы DCS.

- d. Системный монитор.
3. Данные какого типа сохраняются в мониторе стабильности? (Каждый правильный ответ является частью решения. Выберите все подходящие.)
- a. Сбой приложения, требующий его перезапуска.
  - b. Ошибка в Windows, вызвавшая перезагрузку системы.
  - c. Удаление приложения.
  - d. Завершение работы службы.
  - e. Сбой драйвера устройства.
4. Вы настраиваете сервер под управлением Windows Server 2008 R2 с именем VAN-SRV1 для получения событий с контроллера домена под управлением Windows Server 2008 R2 с именем VAN-DC1. Оба компьютера находятся в одном домене. Какую из следующих команд нужно ввести на компьютересборщике, чтобы настроить службу сборщика событий?
- a. `wecutil qc.`
  - b. `winrm qc.`
  - c. `winrm qc -q.`
  - d. `%SYSTEMROOT%\System32\gpedit.msc.`
5. Вы хотите использовать системный монитор для просмотра данных производительности, полученных группой DCS. Вы открыли диалоговое окно свойств системного монитора. На какой вкладке можно настроить отображение текущей активности в реальном времени или данных из файлов журнала, сохраненных с помощью группы DCS?
- a. Общие.
  - b. Источник.
  - c. Данные.
  - d. График.
  - e. Оформление.

## Закрепление материала главы

Чтобы попрактиковаться и закрепить знания, полученные при изучении этой главы, выполните следующее:

- прочитайте резюме главы;
- просмотрите список основных терминов, представленных в этой главе;
- выполните задания лабораторной работы, моделирующей реальные ситуации, требующие применения полученных знаний;
- выполните рекомендуемые упражнения;
- пройдите пробный тест.

## Резюме главы

- Инструменты Windows Server 2008 R2, такие как монитор производительности, монитор стабильности и центр поддержки, позволяют оценить, ис-

правно ли работает компьютер, требуются ли ему дополнительные ресурсы, и где находятся узкие места производительности.

- Такие инструменты как диспетчер задач, диспетчер ресурсов и Process Explorer показывают данные о текущей производительности компьютера, тогда как журналы событий могут хранить события истории и предупреждать о возникновении проблем. Группы DCS могут хранить как текущие, так и прошлые показания счетчиков, позволяя сравнивать производительность компьютера в настоящий момент и в определенное время в прошлом.
- Администратор должен спланировать, что, когда и с помощью каких инструментов наблюдать. Следует сформировать базовые показатели производительности, отслеживать тенденции и генерировать отчеты, показывающие любые нарушения производительности, прежде чем это станет проблемой для пользователей.

## Основные термины

Проверьте, знаете ли вы, что означают перечисленные ниже термины из этой главы:

- Группа сборщиков данных (DCS).
- Пересылка событий.
- Журнал событий.
- Подписка на события.
- Счетчик производительности.

## Лабораторная работа

Для выполнения заданий лабораторной работы используйте знания о настройке сети, полученные из этой главы. Ответы можно найти в разделе «Ответы» в конце книги.

### Задание 1. Использование групп сборщиков данных и пересылка событий

Джеймс Сеймур — администратор серверов производственной сети в компании Tailspin Toys. В последнее время пользователи периодически сталкиваются с проблемами производительности, когда обращаются к файловому серверу DEN-FS1, работающему под управлением Windows Server 2008 R2. Джеймс проверяет использование ресурсов с помощью диспетчера задач, но не видит никаких данных о потреблении ресурсов дополнительного процессора, памяти, диска и сети. Ему требуется выполнять мониторинг этих ресурсов в течение длительного периода времени, а не в реальном времени. Кроме того, ему необходимо наблюдать за ресурсами независимо от того, возникают проблемы с быстродействием или нет.

Джеймс использует сервер с именем DEN-SPARE под управлением Windows Server 2008 R2 в качестве сборщика событий, поскольку этот компьютер не слишком загружен, а административная рабочая станция под управлением



Windows 7 активно используется для других целей. Джеймс открывает монитор производительности на DEN-SPARE и подключается к файловому серверу DEN-FS1. Учитывая это, ответьте на следующие вопросы:

1. Что следует сделать Джеймсу, чтобы получать журналы с данными о производительности, которые помогут ему в анализе использования ресурсов диска, сети, процессора и памяти на сервере при возникновении проблем и при нормальном функционировании?
2. Джеймс знает, когда примерно стали происходить проблемы. Как он может проверить, какие приложения были установлены в то время?
3. В последнее время некоторые пользователи сталкиваются с проблемами во время загрузки файлов и сообщений электронной почты из-за того, что свободное место на их локальных дисках заканчивается и подходит к критическому пределу. Джеймсу необходим активный способ выявления проблем с недостаточным пространством на диске на клиентах под управлением Windows 7, чтобы он мог просить специалистов службы поддержки освобождать место на дисках клиентов, прежде чем будет достигнут критический предел. Как использовать сервер DEN-SPARE для мониторинга клиентов на предмет нехватки места на диске?

## **Задание 2. Планирование мониторинга на серверах**

Джеймс планирует стратегию мониторинга фермы серверов компании Tailspin Toys. Ему требуется выбрать наиболее подходящие инструменты для выполнения некоторых задач. Ответьте на следующие вопросы.

1. На каждом из серверов Джеймс хочет получать информацию, которая поможет максимально увеличить производительность и наладить работу системы. Джеймсу нужны данные о состоянии аппаратных ресурсов, времени ответов системы и процессах на каждом компьютере. Какой инструмент следует использовать для этого?
2. Джеймсу требуется просматривать информацию о потреблении аппаратных и программных ресурсов в режиме реального времени. Он хочет фильтровать результаты по процессам и службам, за которыми ведется наблюдение. Также он хочет использовать тот же инструмент для запуска, остановки, приостановки и возобновления процессов и служб и для решения проблем с зависшими приложениями. Какой инструмент ему следует использовать?
3. Джеймс скопировал Process Explorer на все свои серверы и предпочитает использовать его вместо диспетчера задач, чтобы использовать дополнительную функциональность. Он хочет убедиться, что его коллеги тоже используют Process Explorer вместо диспетчера задач. Как это сделать?

## **Рекомендуемые упражнения**

Чтобы успешно справиться с экзаменационными заданиями по темам этой главы, выполните следующие упражнения.

## Использование инструментов мониторинга производительности

- **Поэкспериментируйте с группами DCS.** Изучите стандартные группы DCS и поэкспериментируйте с созданием своих групп. Группы DCS предоставляют широкие возможности по управлению данными о текущей и прошлой производительности компьютера, и единственный способ научиться работать с ними — практика.
- **Тщательно изучите инструмент Отчеты.** Администратор должен не только обеспечивать нормальную работу оборудования компьютеров и сети, но и создавать отчеты о выполнении этих задач для коллег и руководства. О вашей работе будут судить по четкости и актуальности отчетов, которые, к тому же, могут повлиять на распределение бюджета. Учитесь составлять хорошие отчеты.

## Управление ведением журналов событий

- **Изучите пересылку событий и подписки.** Поначалу эта тема кажется сложной, однако после некоторой тренировки в настройке подписок и пересылке события, она становится понятнее. Если вы еще не сделали этого в процессе изучения главы, настройте VAN-DC1 как компьютер-источник, а VAN-SRV1 как компьютер-сборщик в тестовой сети. Настройте тип подписки (скорее всего, лучше использовать иницируемую сборщиком подписку), создайте подписки на события и собирайте на сервере VAN-SRV1 события, происходящие на VAN-DC1. Освойте пересылку сообщений, прежде чем делать это в производственной сети.

## Изучение Process Explorer

- **Скачайте и установите Process Explorer и изучите его возможности.** Process Explorer — сложная многофункциональная программа, предоставляющая широкие возможности. С ними можно ознакомиться только на практике. Загрузите установочный файл на компьютер с доступом к Интернету. Если этот компьютер работает под управлением Windows Server 2008 R2, можно использовать Process Explorer на нем. В противном случае, сохраните установочный файл на съемный носитель и установите на VAN-DC1 или VAN-SRV1.

## Пробный экзамен

Тренировочные тесты на прилагаемом к книге компакт-диске позволяют проверить знания только по одной или сразу по всем темам сертификационного экзамена 70-646. Тестирование можно организовать так, чтобы оно проводилось как настоящий экзамен, а можно проходить в режиме обучения, просматривая правильные ответы и объяснения после каждого ответа.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Пробный экзамен

Подробнее о пробном экзамене рассказано во Введении.

---

## Архивация и восстановление

### **Занятие 1. Архивация данных**

**568**

### **Занятие 2. Аварийное восстановление**

**587**

Архивация (резервное копирование) и восстановление всегда были одними из основных задач системного администратора. С повышением надежности оборудования у администраторов уменьшилось забот, но изменились и ожидания руководства относительно надежности серверов. В конце 90-х пользователи спокойно относились к тому, что файловый сервер может быть недоступен 24 часа. Теперь они не желают мириться с простоями в несколько часов. В этой главе вы узнаете, что нового Windows Server 2008 R2 предлагает для архивации данных и служб. Мы обсудим планирование и реализацию аварийного восстановления в среде Windows Server 2008 R2. Вы узнаете, как восстанавливать одиночные объекты Active Directory, файлы, папки, роли, тома и даже целые серверы.

### **Темы экзамена**

- Планирование резервного копирования и восстановления.

### **Прежде всего**

Для выполнения упражнений этой главы потребуется:

- Сервер с именем VAN-DC1, работающий под управлением Windows Server 2008 R2 Enterprise, настроенный как контроллер домена adatum.com, как описано в Приложении.
- Учетная запись пользователя Kim Akers с паролем Pa\$\$w0rd в домене adatum.com, включенная в группы администраторов домена, администраторов предприятия и администраторов схемы. Процедура создания этой учетной записи описана в Приложении.
- Дополнительный сервер VAN-SRV1, работающий под управлением Windows Server 2008 R2 Enterprise, настроенный как рядовой сервер в домене Adatum.com, как описано в Приложении. Этот сервер не используется на практикуме этой главы, но потребуется для выполнения рекомендуемых упражнений.

- Для выполнения практических упражнений рекомендуем использовать изолированную сеть, не входящую в рабочую сеть. Доступ к Интернету не требуется, как и настройка шлюза по умолчанию. Для экономии времени и затрат на настройку физических компьютеров используйте виртуальные машины, например, созданные с использованием роли сервера Nureg-V.
- Для выполнения практикума этой главы необходим доступ к дополнительному запоминающему устройству, подключенному к контроллеру домена VAN-DC1, объемом минимум 40 ГБ. Этот диск может быть дополнительным виртуальным диском, если вы используете виртуальные машины. Если используется физическое оборудование, это может быть физический внутренний диск, накопитель USB 2.0 или IEEE 1394. Этот диск будет использоваться для хранения данных резервного копирования. В инструкциях практикума это диск F:. Если вы назначите другую букву, учитывайте это при выполнении упражнений.

### Реальный мир

*Йен Маклин*

Мой опыт показывает, что самое важное при восстановлении после аварии — сохранять хладнокровие. Если вы спокойны и методично следуете плану, все пройдет хорошо, и вы вернете систему в то состояние, в каком она была до аварии. Если вы паникуете, вы создадите себе проблемы. При стрессе люди совершают ошибки, и операции восстановления могут пройти неправильно, если выполнять их в спешке.

Чтобы сохранять спокойствие, необходимо спланировать действия по аварийному восстановлению. Не ждите, пока произойдет авария, чтобы составить такой план. Документируйте свой план, чтобы точно знать, что следует делать в любой предсказуемой ситуации (или, как минимум, в наиболее вероятных ситуациях). Проверьте созданный план, насколько это возможно, например, попробуйте восстановить данные.

Не торопитесь и пару раз глубоко вдохните, чтобы в голове была ясность. Держите документацию с планом под рукой (иметь только одну копию на жестком диске — плохая идея). Гораздо эффективнее начинать медленно и постепенно готовиться, чем паниковать, ошибаться и начинать все сначала.

## Занятие 1. Архивация данных

Инструменты архивации, представленные в Windows Server 2008 и улучшенные в Windows Server 2008 R2, значительно отличаются от инструментов, доступных в Windows Server 2003. Способы архивации, с которыми вы могли быть знакомы по прошлому опыту, изменились. Например, при архивации по расписанию больше не используются ленточные накопители. На этом занятии вы узнаете, как использовать программу резервного копирования, появившуюся в Windows Server 2008, для резервного копирования серверов и как использовать дополнительные параметры Windows Server 2008 R2 для исключения типов файлов

и путей из архивов. Вы узнаете, как использовать утилиту командной строки Wbadmin.exe и как настраивать теневые копии общих папок — технологию, позволяющую передать задачу восстановления удаленных или поврежденных файлов из общих ресурсов обычному пользователю, а не специалистам службы поддержки.

---

**Изучив материал этого занятия, вы сможете:**

- ✓ Понимать, как использовать утилиту Wbadmin.exe для архивации серверов.
- ✓ Выполнять полную архивацию сервера.
- ✓ Выполнять архивацию данных ролей сервера и Active Directory.
- ✓ Удаленно выполнять архивацию.

**Продолжительность занятия — примерно 45 мин.**

---

## Использование теневых копий общих папок

Использование теневых копий общих папок может значительно снизить работу по восстановлению данных, поскольку почти полностью избавляет от необходимости административного участия в восстановлении удаленных, измененных или поврежденных файлов пользователей. Эта технология создает мгновенные снимки файлов, хранящихся в общих папках в определенные моменты времени по расписанию. По умолчанию теневые копии создаются в 7:00 и 12:00 каждый будний день. Для тома можно настроить несколько расписаний, и расписание, применяемое по умолчанию, состоит из двух расписаний, примененных одновременно.

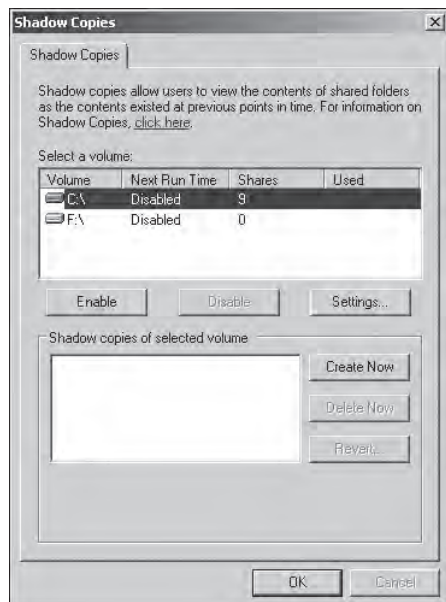


**Рис. 13-1.** Включение теневых копий общих папок

Чтобы включить теньевые копии общих папок, откройте оснастку **Управление компьютером** (Computer Management) из меню **Администрирование** (Administrative Tools), правой кнопкой щелкните узел **Общие папки** (Shared Folders) и выберите в подменю **Все задачи** (All Tasks) команду **Настроить теньевые копии** (Configure Shadow Copies). Откроется диалоговое окно **Теньевые копии** (Shadow Copies), позволяющее включать и отключать теньевые копии для отдельных томов (рис. 13-1). Здесь можно изменить параметры теньевых копий и вручную создать теньевую копию определенного тома.

При включении теньевых копий для тома автоматически будет создана первоначальная теньевая копия для этого тома. Кнопка **Параметры** (Settings) открывает диалоговое окно, в котором можно настроить место хранения, максимальный размер хранилища копий и расписание, по которому создаются копии (рис. 13-2). Чтобы определить, как часто должны создаваться теньевые копии, нажмите кнопку **Расписание** (Schedule). Для томов, хранящих общие папки с часто изменяющимися файлами, следует настроить частое создание теньевых копий. Если файлы изменяются редко, не стоит настраивать частое создание копий.

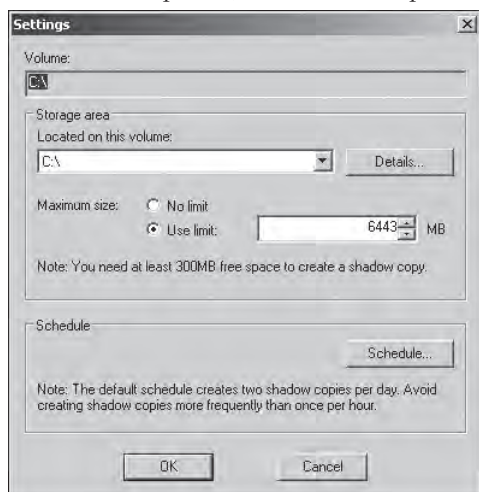


Рис. 13-2. Параметры создания теньевых копий

Если на томе регулярно выполняются интенсивные операции чтения и записи, можно уменьшить влияние операций создания теньевых копий на производительность, разместив копии на отдельном томе. Если максимальный размер хранилища теньевых копий превышает свободное место на томе, для освобождения места будут удаляться самые старые теньевые копии.

Наконец, независимо от свободного места, на одном томе можно хранить максимум 64 теньевых копии. Это непосредственно влияет на длительность хранения теньевых копий. Например, расписание, по которому копии создаются раз в день каждый понедельник, среду и пятницу, позволяет хранить копии за 21 последнюю неделю. Расписание по умолчанию позволяет хранить теньевые копии за 6 последних недель.

Планируя развертывание теньевых копий общих папок, помните, что параметры настраиваются для каждого тома в отдельности. Это значит, что место хранения, максимальный размер и расписания могут полностью различаться

для разных томов. Если общие папки спланированы таким образом, что каждая папка находится на отдельном томе, можно оптимизировать параметры создания теневых копий для каждого общего ресурса, исходя из того, как используются данные, а не искать компромисс, подстраивая расписание под совершенно разные шаблоны использования.

**Проверьте себя**

1. На какой основе настраиваются теневые копии общих папок (для каждого сервера, тома, общей папки, диска или папки)?
2. Что происходит с данными теневых копий, когда на томе, где они хранятся, заканчивается место?

**Ответ**

1. Теневые копии общих папок настраиваются в отдельности для каждого тома.
2. Когда заканчивается свободное место на томе, самые старые теневые копии автоматически удаляются.

## Система архивации данных Windows Server

Система архивации данных Windows Server включает оснастку MMC, утилиту командной строки Wbadmin и командлеты Windows PowerShell. Система архивации данных полностью удовлетворяет потребности в резервном копировании и восстановлении. Она позволяет архивировать сервер целиком (все тома), выбранные тома, данные состояния системы или отдельные файлы и папки. Можно создать архив для аварийного восстановления на новом оборудовании, например, после выхода из строя жесткого диска. Можно восстанавливать тома, папки, файлы, отдельные приложения и данные состояния системы. Система архивации данных Windows Server позволяет создавать и управлять архивами данных локального или удаленного компьютера и настраивать расписание для автоматического выполнения архивации.

**СОВЕТ Подготовка к экзамену**

Система архивации данных Windows Server в Windows Server 2008 и 2008 R2 значительно отличается от утилиты NTbackup.exe, используемой в Windows Server 2000 и 2003. Рекомендуем изучить возможности и ограничения системы архивации, представленной в Windows Server 2008, и улучшения, появившиеся в Windows Server 2008 R2, поскольку многие аспекты функциональности отличаются.

Перечислим основные характеристики системы архивации в Windows Server 2008:

- система архивации данных Windows Server не использует ленточные носители;
- нельзя выполнять запись в сетевые папки или на оптические диски во время запланированной архивации;



- наименьший объект, архивацию которого можно выполнять при помощи системы архивации данных Windows Server — том;
- архивировать можно только тома NTFS;
- файлы системы архивации имеют формат виртуального жесткого диска (VHD). Файлы VHD можно монтировать при помощи соответствующих программ и считывать напрямую или посредством виртуальных машин, таких как Hyper-V.

Перечислим основные характеристики системы архивации в Windows Server 2008 R2:

- **Возможность архивации или исключения отдельных файлов и включения или исключения из тома типов файлов и путей.** Система архивации данных Windows Server позволяет архивировать выбранные файлы. Новые возможности мастера расписания архивации и мастера однократной архивации позволяют выбирать файлы и папки (а не только целые тома) для создания в резервной копии. Можно также исключать из архивации файлы по типу или пути. Такую же возможность предоставляют обновленные команды `wbadmin enable backup` и `wbadmin start backup`.
- **Повышенная производительность и использование добавочной архивации.** По умолчанию система архивации данных Windows Server создает добавочные архивы, позволяющие восстанавливать любой элемент из одного архива, но занимающие гораздо меньше места. Все архивы файлов и папок (за исключением первого) являются добавочными, содержащими только те файлы, которые изменены с момента создания предыдущего архива. Кроме того, система архивации не требует периодического удаления старых архивов для освобождения места. Старые архивы удаляются автоматически. Для выполнения добавочной архивации участие пользователя не требуется. Однако если выполняется архивация томов целиком, можно настроить параметры производительности, используя диалоговое окно **Оптимизация производительности архивации** (Optimize Backup Performance) (рис. 13-3).

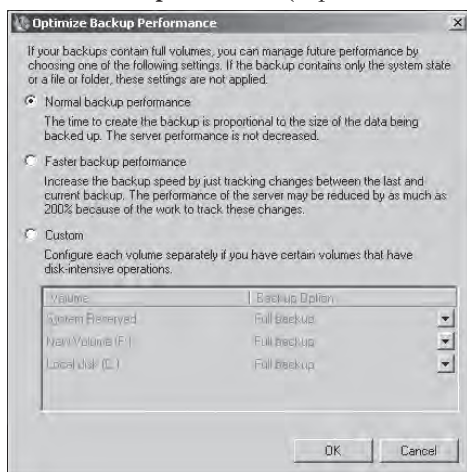


Рис. 13-3. Диалоговое окно Оптимизация производительности архивации

- **Расширенные параметры хранилища архивов.** Windows Server 2008 R2 позволяет хранить архивы, созданные при запланированной архивации, в удаленной общей папке или томе. Однако если архивы хранятся в удаленной общей папке, будет поддерживаться только одна их копия. Архивы можно хранить на виртуальных дисках (VHD). Мастер расписания архивации позволяет выбрать удаленную общую папку или том в качестве хранилища архивов. Такую возможность предоставляет и обновленная команда `wbadmin enable backup`.
- **Параметры и улучшенная производительность архивации данных состояния системы.** Система архивации данных Windows Server позволяет создавать резервные копии данных состояния системы. Один архив может включать данные состояния системы и другие данные с сервера. В Windows Server 2008 R2 для создания нескольких версий архивов данных состояния системы требуется меньше места, так как для этого используются теневые копии, а не создаются отдельные папки для каждой версии. Кроме того, команды `wbadmin enable backup` и `wbadmin start backup` теперь имеют параметр `-SystemState`, позволяющий включать данные состояния системы в запланированную или однократную архивацию.
- **Расширенная поддержка командной строки.** Улучшенные команды `wbadmin enable backup` и `wbadmin start backup` обеспечивают поддержку использования новых возможностей системы архивации из командной строки. Сюда входит возможность архивации файлов, а не только целых томов, возможность исключения типов файлов и путей и возможность сохранять архивы, полученные при запланированной архивации, в удаленных общих папках и томах.

---

**ПРИМЕЧАНИЕ WBADMIN START SYSRECOVERY**

Новые возможности команды `wbadmin start sysrecovery`, появившиеся в Windows Server 2008 R2, обсуждаются на занятии 2.

- 
- **Расширенная поддержка Windows PowerShell.** В Windows Server 2008 R2 командлеты Windows PowerShell позволяют автоматизировать рутинные задачи и повышают эффективность управления сценариями архивации. Новый модуль Active Directory для Windows PowerShell (см. занятие 2) и улучшенные командлеты PowerShell отражают изменения в системе архивации данных Windows Server, позволяя архивировать отдельные файлы, исключать типы файлов и пути и сохранять архивы, полученные при запланированной архивации, в удаленных общих папках и томах.

---

**ПРИМЕЧАНИЕ Восстановление архивов, полученных при помощи NTbackup**

Архивы, полученные при помощи `NTbackup.exe`, восстанавливать нельзя. Специальную версию `NTbackup.exe`, предоставляющую только возможность чтения, совместимую с Windows Server 2008, можно скачать по адресу <http://www.microsoft.com/downloads/en/details.aspx?FamilyID=7da725e2-8b69-4c65-afa3-2a53107d54a7&DisplayLang=en>. Такую же версию для Windows Server 2008 R2 можно найти по адресу <http://www.microsoft.com/downloads/details.aspx?FamilyID=60480F87-39DF-410A-92E1-F2CBC8442FDC&amp;displaylang=zh-tw&displaylang=en>.

---

## ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Новые возможности в Windows Server 2008 R2

Подробнее о новых возможностях и улучшениях системы архивации данных Windows Server, появившихся в Windows Server 2008 R2, см. по адресу [http://technet.microsoft.com/ru-ru/library/ee344835\(Ws.10\).aspx](http://technet.microsoft.com/ru-ru/library/ee344835(Ws.10).aspx).

В Windows Server 2008 и 2008 R2 система архивации данных по умолчанию не устанавливается. На практикуме этой главы вы установите ее, щелкнув **Добавить компоненты** (Add Features) под узлом **Компоненты** (Features) в диспетчере сервера. После установки можно открыть оснастку **Система архивации данных Windows Server** (Windows Server Backup) из меню **Администрирование** (Administrative Tools). Устанавливается также утилита командной строки Wbadmin.exe, о которой рассказывается в соответствующем разделе ниже.

Для выполнения архивации по расписанию с помощью системы архивации или команды Wbadmin обычно требуется дополнительный внутренний или внешний жесткий диск. Внешний диск должен быть совместим с USB 2.0 или IEEE 1394. Планируя развертывание дисков для размещения архивов, созданных по расписанию, проведите тестирование, чтобы выяснить, какой объем дискового пространства необходим, и как долго такой объем позволит хранить архивы, прежде чем развертывать диски в производственной сети.

При настройке первой запланированной архивации диск, на котором будут размещены архивы, будет скрыт из Проводника Windows. Если этот диск содержит тома и данные, они будут удалены. Заметьте, что это относится только к запланированной архивации, но не к архивации, выполняемой вручную. При создании архивов вручную можно выбирать внешний диск или расположение в сети, не беспокоясь о том, что имеющиеся там данные будут потеряны. Форматирование и изменение разделов выполняется только при первом использовании устройства для размещения данных запланированной архивации. При последующем сохранении архивов этого не происходит.

Если для хранения данных запланированной архивации выбрать расположение в сети, там будет сохраняться только последний архив, а предыдущий архив будет переписан. Если для хранения данных запланированной архивации выбран том, а не целый жесткий диск, Microsoft рекомендует не хранить там другие данные, поскольку производительность тома может значительно падать во время архивации.

Важно также помнить, что на томе может храниться максимум 512 архивов. Если требуется хранить больше архивов, их придется записывать на другой том. На практике, учитывая объем данных на большинстве серверов, вряд ли найдется диск, на который поместится столько архивов. Если место на диске заканчивается, система архивации автоматически удалит самые старые данные, чтобы выполнить запланированную архивацию. Вручную очищать диск и удалять старые архивы не требуется.

## Выполнение запланированной архивации

Запланированная архивация позволяет автоматизировать процесс резервного копирования. После настройки расписания система архивации данных Windows Server выполняет все остальное. По умолчанию запланированная архивация выполняется в 21:00. Если в вашей организации в это время еще идет работа, ука-

жете другое время. Планируя расписание архивации, убедитесь, что в архивы попадут все изменения, внесенные за день. Настраивать запланированную архивацию и управлять ей могут только члены локальной группы администраторов.

Чтобы настроить запланированную архивацию, выполните следующее:

1. Откройте оснастку **Система архивации данных Windows Server** (Windows Server Backup) и щелкните **Расписание архивации** (Backup Schedule) на панели **Действия** (Actions). Откроется мастер расписания архивации. Щелкните **Далее**.
2. На странице **Выбрать конфигурацию архива** (Select Backup Configuration) выберите тип архивации: **Весь сервер (рекомендуется)** [Full Server (Recommended)] или **Настраиваемый** (Custom). Если вы выбрали настраиваемый тип, щелкните **Далее**, щелкните **Добавление элементов** (Add Items) и выберите **Восстановление исходного состояния системы** (Bare Metal Recovery), **Состояние системы** (System State), один или несколько томов, или одну или несколько папок на томе. На странице выбора элементов можно щелкнуть кнопку **Дополнительные параметры** (Advanced Settings) и указать файлы и папки, которые требуется исключить. На вкладке **Параметры VSS** (VSS Settings) окна дополнительных параметров можно выбрать полную архивацию VSS или копирование архива VSS. Щелкните **Далее**, чтобы перейти к странице **Указать время архивации** (Specify Backup Time).
3. Если на странице **Выбрать конфигурацию архива** выбрать **Весь сервер (рекомендуется)** и щелкнуть **Далее**, откроется сразу страница **Указать время архивации**.

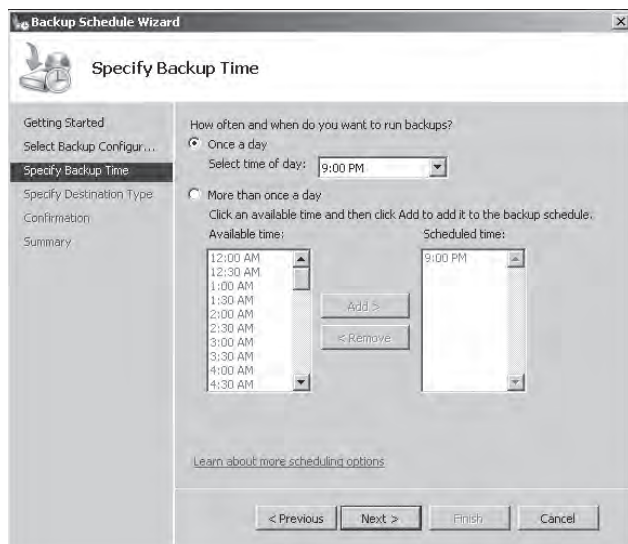


Рис. 13-4. Страница Указать время архивации

4. На странице **Указать время архивации** (рис. 13-4) укажите, сколько раз в день будет выполняться архивация. По умолчанию архивация выполняется один раз в день в 21:00. Если данные на сервере изменяются часто, лучше выполнять архивацию несколько раз в день. Если данные изменяются не

часто, например, как на веб-серверах, следует выполнять архивацию один раз в день. В любом случае архивацию следует выполнять в периоды относительно низкой активности сервера. Настроив время архивации, щелкните **Далее**, чтобы перейти к странице **Указать тип места назначения** (Specify Destination Type).

5. На странице **Указать тип места назначения** (рис. 13-5) можно выбрать выделенный жесткий диск, том или общую папку. Заметьте, что при выполнении незапланированной однократной архивации нельзя выбрать архивацию на том. Архивацию такого типа вы выполните на практикуме этой главы.

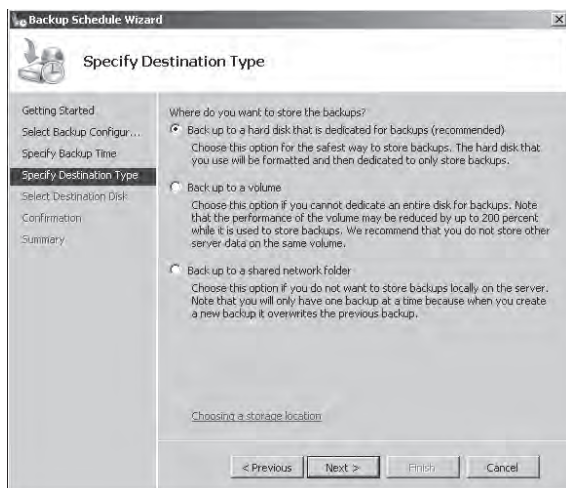


Рис. 13-5. Страница Указать тип места назначения

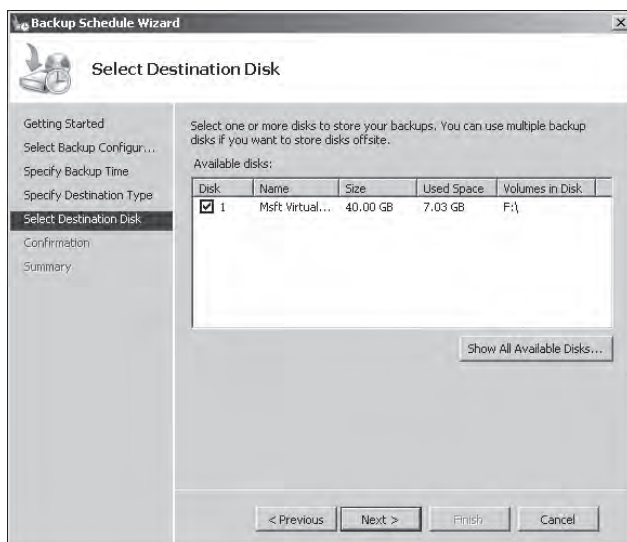


Рис. 13-6. Страница Выбрать диск назначения

6. На странице **Выбрать диск назначения** (Select Destination Disk) (рис. 13-6) выберите диск, на который будут записываться архивы. Если выбрать не-

сколько дисков, будет записываться несколько копий архива. Обратите внимание: использоваться будет диск целиком. Все существующие тома и данные будут удалены, и программа архивации отформатирует и скроет диск или диски, прежде чем выполнить первую архивацию.

7. Щелкните **Далее**. Если диск назначения указан как один из архивируемых дисков (обычно это происходит при выборе полной архивации сервера), появится сообщение об этом и будет предоставлена возможность удалить этот диск из списка. Также будет показано предупреждение о том, что диск назначения будет скрыт и отформатирован. Примите предупреждение, чтобы перейти на страницу подтверждения. Щелкните **Готово**, чтобы закрыть мастер. Архивация будет выполняться по расписанию.
8. После завершения работы мастера диск назначения будет отформатирован. Первая архивация будет выполнена в назначенное время.

Важное ограничение системы архивации данных Windows Server состоит в том, что можно запланировать только одно задание архивации. Это значит, что нельзя запланировать разные задания, как это делалось в предыдущих версиях Windows (до Windows Server 2008), например, полная архивация в понедельник ночью и добавочная архивация в остальные дни недели. В Windows Server 2008 R2 система архивации автоматически выполняет добавочную архивацию после первой полной архивации.

## Выполнение незапланированной однократной архивации

Незапланированная однократная архивация, называемая также ручной архивацией, позволяет записывать архивы в общие сетевые папки, на локальные и внешние жесткие диски и на локальные носители DVD. Если для архивации требуется больше места, чем доступно на одном DVD, можно разделить архив на несколько DVD. Если подсчитанный размер архива превышает свободное место в другом месте назначения, архивация не будет выполнена. На практике этой главы вы выполните архивацию вручную.

Если при выполнении архивации вручную или по расписанию выбрать настраиваемую архивацию, а не архивацию всего сервера, можно выбрать один из двух типов архивации службы теневого копирования тома (VSS), щелкнув кнопку **Дополнительные параметры** (Advanced Settings) на странице выбора элементов в соответствующем мастере. Доступны следующие варианты:

- **Полная архивация VSS** (VSS Full Backup). Выбирайте этот вариант, если для создания архивов приложений не используются другие программы архивации. При этом обновляется атрибут архивации каждого файла и очищаются файлы журнала приложения.
- **Копировать архив VSS** (VSS Copy Backup). Выбирайте этот вариант, если для архивации приложения на томах, включенных в архив, используется другая программа. При этом сохраняются файлы журнала приложения.

## Оптимизация производительности архивации

Используя систему архивации данных Windows Server для создания задания архивации на компьютере под управлением Windows Server 2008 или 2008 R2, нельзя выбрать тип архивации (полная, разностная или добавочная), как в



предыдущих версиях Windows Server. При первой архивации создается полный архив, а затем выполняется добавочная архивация. Выбрать разностную архивацию нельзя, а восстановление можно выполнить при помощи одного добавочного архива. Настраивая производительность архивации, можно установить переключатель **Выборочная** (Custom) и выбрать полную или добавочную архивацию для каждого тома. Первая архивация, выполняемая по расписанию, эквивалентна полной архивации.

Если в архивацию включены тома целиком, можно настроить производительность архивации, щелкнув **Настройка параметров производительности** (Configure Performance) на панели **Действия**. Откроется диалоговое окно, позволяющее выбрать один из трех параметров (рис. 13-7). Вариант **Выборочная** (Custom) позволяет выбрать полную или добавочную архивацию для каждого тома. Последняя позволяет хранить на носителе больше архивов, и обычно следует использовать ее, так как она дает больший диапазон, из которого можно восстанавливать данные. Если выбрать обычную или повышенную производительность архивации, настраивать параметры для отдельных томов нельзя.

Преимущество системы архивации данных Windows Server состоит в том, что администратору не приходится искать нужные наборы добавочных архивов для восстановления. Когда выполняется восстановление, используются архивы, соответствующие выбору параметров восстановления. О восстановлении рассказывается на занятии 2.



Рис. 13-7. Настройка производительности архивации

## Утилита командной строки Wbadmin

Утилита Wbadmin доступна в режиме Server Core и в обычных установках Windows Server 2008 и 2008 R2. Заметьте, что на компьютерах, работающих в режиме Server Core, оснастка системы архивации недоступна, хотя можно использовать ее, если подключиться к такому компьютеру удаленно. Утилита Wbadmin позволяет делать все то же, что и оснастка системы архивации, и даже больше. В обычной установке Windows Server 2008 и 2008 R2 эта утилита уста-



навливается вместе с компонентом **Возможности системы архивации данных Windows Server**, если выбрать **Программы командной строки** (Command-Line Tools) (см. практикум этой главы). В режиме Server Core утилиту Wbadmin можно установить следующей командой:

```
Ocsetup WindowsServerBackup
```

Для резервного копирования файлов Windows Server 2008 и 2008 R2 можно использовать следующие команды утилиты Wbadmin.exe:

- **wbadmin enable backup** — позволяет создавать и изменять расписание архивации. В Windows Server 2008 R2 доступны дополнительные параметры:
  - **include** — этот параметр поддерживается и в Windows Server 2008, однако в Windows Server 2008 R2 он позволяет указывать отдельные файлы, папки и тома;
  - **nonRecureInclude** — указывает нерекурсивный разделенный запятыми список элементов для включения в архив;
  - **exclude** — указывает разделенный запятыми список элементов для исключения из архива;
  - **nonRecurseExclude** — указывает нерекурсивный разделенный запятыми список элементов, которые необходимо исключить из архива;
  - **systemState** — создает архив, включающий данные состояния системы в дополнение ко всем элементам, которые указаны с помощью параметра **-include**;
  - **vssFull** и **vssCopy** — указывают тип архивации VSS: полную и копирующую, соответственно;
  - **user** — указывает имя пользователя с разрешением на запись в место хранения архивов (если это удаленная общая папка);
  - **password** — указывает пароль пользователя, указанного с помощью параметра **-user**.

---

#### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ **WBADMIN ENABLE BACKUP**

Подробнее о команде **wbadmin enable backup** см. по адресу [http://technet.microsoft.com/en-us/library/cc742130\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc742130(WS.10).aspx) (на английском языке).

- **wbadmin start systemstatebackup** — позволяет вручную выполнить архивацию данных состояния системы. В архив будут включены только данные состояния системы, и в него нельзя включить другие файлы, папки или тома. Эта команда работает только в Windows Server 2008 и 2008 R2 и имеет одинаковый синтаксис в обеих ОС.

---

#### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ **WBADMIN START SYSTEMSTATEBACKUP**

Подробнее о команде **wbadmin start systemstatebackup** см. по адресу [http://technet.microsoft.com/en-us/library/cc742124\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc742124(WS.10).aspx) (на английском языке).

- **wbadmin start backup** — позволяет вручную выполнить однократную архивацию. Если не указаны параметры архивации, используются параметры архивации по расписанию. В Windows Server 2008 R2 доступны следующие дополнительные параметры:

- include, exclude, nonRecurseInclude, nonRecurseExclude, systemState и vssCopy. Эти параметры аналогичны параметрам команды wadmin enable backup. Параметры -name, -password и -vssFull доступны также в Windows Server 2008.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ WBADMIN START BACKUP

Подробнее о команде wadmin start systemstatebackup см. по адресу [http://technet.microsoft.com/en-us/library/cc742083\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc742083(WS.10).aspx) (на английском языке).

- wadmin get versions — позволяет просматривать сведения о созданных архивах. Синтаксис одинаков в Windows Server 2008 и 2008 R2.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ WBADMIN GET VERSIONS

Подробнее о команде wadmin get versions см. по адресу [http://technet.microsoft.com/en-us/library/cc742116\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc742116(WS.10).aspx) (на английском языке).

- wadmin get items — позволяет определять, какие элементы содержатся в указанном архиве. Синтаксис одинаков в Windows Server 2008 и 2008 R2.

---

### Дополнительная информация WBADMIN GET ITEMS

Подробнее о команде wadmin get items см. по адресу [http://technet.microsoft.com/en-us/library/cc742041\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc742041(WS.10).aspx) (на английском языке).

Администраторы Windows Server 2008 могут выполнять архивацию вручную при помощи команды wadmin start backup, используя параметр -backuptarget: \\Share\Folder, где расположение общей папки указывается в виде пути UNC. (Это ограничение не действует в Windows Server 2008 R2, хотя команда работает точно так же.) Если для записи в общую папку требуется предоставить учетные данные, можно использовать параметры -user и -password. Например, чтобы выполнить архивацию томов E, F и G в общую папку Store на контроллере домена VAN-DC1, используя учетные данные пользователя Kim Akers, выполните следующую команду:

```
Wbadmin start backup -backuptarget:\\VA-DC1\Store -include:E:,F:,G:
-user:KimAkers@adatum.com -password:Pa$$w0rd
```

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Дополнительные команды WBADMIN

Мы описали наиболее часто используемые команды, но есть и другие. Подробнее о командах Wbadmin см. по адресу [http://technet.microsoft.com/en-us/library/cc754015\(WS.10\).aspx?ppud=4](http://technet.microsoft.com/en-us/library/cc754015(WS.10).aspx?ppud=4) (на английском языке).

Команды утилиты Wbadmin.exe можно вызывать из пакетного файла, а пакетные файлы можно запускать из планировщика задач, что позволяет настраивать архивацию подробнее, чем это возможно при помощи архивации по расписанию системы архивации данных Windows Server. Windows Server 2008, в отличие от Windows Server 2008 R2, не позволяет записывать данные, полученные при обычной запланированной архивации, в сетевые папки, но такой способ позволяет обойти это ограничение. Например, следующая команда создает в папке C:\Scripts пакетный файл Ssbackup.bat, выполняющий архивацию данных состояния системы в сетевую папку \\Server\Share, используя учетные данные пользователя RemoteUser:

```
Echo wadmin start systemstatebackup -backupTarget:\\Server\Share
-user:RemoteUser -password:RemotePassword -quiet >> c:\scripts\ssbackup.bat
```

С помощью планировщика заданий можно настроить запуск этого пакетного файла по расписанию, имитирующему расписание системы архивации данных Windows Server. Планируя использование этого метода, учитывайте следующее:

- в команде `wadmin` необходим параметр `-quiet`, так как назначенное задание не должно останавливаться, ожидая ввода данных пользователем;
- назначенное задание должно выполняться с учетными данными локального администратора, поскольку `Wbadmin.exe` необходимо запускать с повышенными привилегиями;
- если назначенное задание записывает данные в сетевую папку, необходимо включить в сценарий, вызываемый этим заданием, учетные данные пользователя. Для защиты этих учетных данных можно использовать шифрованную файловую систему. Файл будет зашифрован, и его содержимое сможет просмотреть только локальный администратор.

## Архивация ролей серверов и приложений

В целом, архивация определенной роли сервера, например, роли DNS или DHCP, и всех связанных с ней данных заключается в архивации данных состояния системы. Архивацию данных состояния системы вы выполните на практике этой главы. В Windows Server 2008 единственный способ архивации данных состояния системы — использовать `Wbadmin.exe` с параметром `start systemstatebackup`. В Windows Server 2008 R2 это можно сделать при помощи оснастки системы архивации данных и команды `wadmin start backup -systemState`. О восстановлении данных состояния системы рассказывается на занятии 2.

## Архивация приложений

Система архивации данных Windows Server уделяет особое внимание приложениям, поддерживающим VSS и систему архивации данных, позволяя отдельно восстанавливать такие приложения, вместе со всеми связанными данными, из полного архива сервера или тома. Чтобы можно было использовать эту функциональность, приложение должно быть зарегистрировано в системе архивации данных Windows Server, что выполняется автоматически во время установки приложения. Таким образом, эта функциональность доступна только приложениям, разработанным специально для Windows Server 2008 и 2008 R2.

Архивировать и восстанавливать данные, имеющие отношение к приложению, можно даже в том случае, если само это приложение не зарегистрировано в системе архивации данных Windows Server. Преимущество этой функции в том, что она упрощает процесс восстановления приложения, обеспечивая архивацию всех данных приложения, от исполняемых файлов до параметров реестра, и позволяя восстановить только это приложение со всеми его зависимостями и данными.

## Архивация Active Directory

Active Directory архивируется автоматически при архивации на контроллере домена томов, содержащих системные файлы. Архивировать Active Directory

можно, выполнив архивацию состояния системы. Копии базы данных доменных служб Active Directory (AD DS) хранятся на всех контроллерах домена, поэтому если контроллер домена выйдет из строя, а у вас не будет его резервной копии, восстановление можно выполнить переустановкой контроллера домена и репликацией базы данных с других контроллеров домена.

Хотя при архивации данных состояния системы архивируются все объекты Active Directory, природа репликации Active Directory делает восстановление некоторых объектов более сложным. Процедура выполнения принудительного восстановления подробно описана на занятии 2. Однако действия по восстановлению удаленных объектов значительно отличаются от восстановления учетных записей или дерева подразделений. Объекты GPO архивируются при помощи консоли управления групповой политикой (GPMC), и для восстановления удаленных GPO следует использовать эту консоль, а не режим восстановления служб каталогов (DRSM). Подробнее об архивации и восстановлении GPO рассказывается в гл. 4.

### Проверьте себя

1. Какая команда используется для установки Wbadmin.exe на компьютере под управлением Windows Server 2008 R2, работающем в режиме Server Core.
2. Что произойдет с томами и данными, хранящимися на диске, выбранном для хранения архивов, созданных при запланированной архивации, настроенной в системе архивации данных Windows Server?

### Ответ

1. Ocsetup WindowsServerBackup.
2. Все тома и данные на целевом диске будут удалены, прежде чем система архивации данных Windows Server запишет первый набор архивов. Кроме того, этот диск не будет виден в Проводнике Windows.

## Удаленная архивация компьютеров

При помощи системы архивации данных Windows Server можно подключаться к удаленному компьютеру, работающему под управлением Windows Server 2008 или Windows Server 2008 R2, и выполнять архивацию так же, как на локальном компьютере. Это позволяет использовать рабочие станции под управлением Windows Vista и Windows 7 с установленными средствами удаленного администрирования серверов (RSAT) для подключения к серверам под управлением Windows Server 2008 или Windows Server 2008 R2 для выполнения задач архивации. При этом пользователь, устанавливающий подключение, должен входить в группу операторов архива или локальных администраторов на сервере, к которому подключается.

Для удаленных подключений при помощи консоли системы архивации действуют те же ограничения, что и при локальном запуске. Пользователи, входящие только в группу операторов архива, не могут выполнять запланированную репликацию. Пользователи, входящие в локальную группу администраторов на

целевом сервере, могут выполнять через удаленное подключение все обычные задачи архивации.

Система архивации Windows Server не позволяет записывать на локальный источник данные, полученные при выполнении запланированной архивации на удаленном компьютере. Записывать данные на локальный источник можно только при выполнении однократной архивации, если компьютер, на который выполняется запись, имеет общую папку. Нельзя использовать утилиту Wbadmin.exe для управления архивами на удаленных компьютерах.

## Дальнейшие соображения по планированию архивации

В Windows Server 2008 наименьшим блоком архивации является том, тогда как в Windows Server 2003 можно было архивировать отдельные файлы и папки. Это значительно влияет на настройку серверов перед развертыванием. Однако Windows Server 2008 R2 предоставляет больше гибкости, позволяя указывать папки и отдельные файлы. Можно также исключать из архивации папки и типы файлов.

Еще один аспект, который следует учитывать при планировании архивации — частота архивации определенных элементов. Получить представление о том, как часто изменяются файлы на определенном томе, можно при помощи отчетов хранилища. Папку с редко изменяющимися документами не требуется архивировать каждый день. Эту папку можно исключить из обычной запланированной архивации и настроить для нее менее частую архивацию при помощи пакетного файла и планировщика задач, как описано выше. В Windows Server 2008 такую папку пришлось бы помещать в отдельный раздел, чтобы настроить отдельное расписание архивации. С повышением гибкости системы архивации в Windows Server 2008 R2 это больше не требуется.

С другой стороны, какая-то папка может содержать важные данные, которые обновляются столь часто, что их требуется архивировать каждые несколько часов. Гибкая система архивации Windows Server 2008 R2 позволяет настроить более частую архивацию этой папки. Администратор может разработать собственную стратегию архивации, подходящую для конкретной ситуации, а не мириться с ограничениями доступных инструментов.

Последнее соображение — разработка стратегии хранения без привязки к месту. Если архивы хранятся в другом месте, их можно будет использовать для восстановления, если здание с серверами будет уничтожено наводнением, пожаром или землетрясением. Планируя такую стратегию, учитывайте следующее:

- резервные копии должны храниться в безопасном месте. Не позволяйте сотрудникам уносить архивные данные домой, так как это небезопасно;
- если данные шифруются, ключи восстановления должны храниться вместе с архивами в удаленном расположении;
- убедитесь, что в резервном расположении достаточно оборудования для восстановления серверов.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Резервное копирование данных в Windows Server 2008 R2

Подробнее о резервном копировании данных в Windows Server 2008 R2, включая пошаговое руководство, см. по адресу [http://technet.microsoft.com/ru-ru/library/ee849849\(WS.10\).aspx](http://technet.microsoft.com/ru-ru/library/ee849849(WS.10).aspx).

---

## System Center Data Protection Manager

System Center Data Protection Manager (DPM) 2010 обеспечивает защиту данных серверов Windows, включая SQL Server, Exchange Server, SharePoint, Hyper-V и файловые серверы. Его можно использовать также для защиты клиентов Windows. DPM — решение для резервного копирования и восстановления данных в среде Windows. Оно поддерживает Windows Server 2008 и 2008 R2 и предоставляет следующие преимущества:

- **Защита клиентов Windows, подключенных к сети и работающих в автономном режиме.** Один сервер DPM может обеспечивать защиту более тысячи клиентов Windows и позволять восстанавливать данные при помощи Проводника Windows или Microsoft Office.
- **Защита платформ виртуализации.** Например, DPM 2010 может защищать виртуальные машины, созданные при помощи роли сервера Hyper-V. Можно также восстанавливать отдельные файлы из резервных копий хоста виртуальной машины.
- **Улучшенная защита SQL Server и Exchange Server.** DPM 2010 поддерживает более 2000 баз данных на одном сервере и автоматически обеспечивает защиту новых баз данных. Администраторы баз данных теперь могут восстанавливать собственные базы данных при помощи самообслуживаемой утилиты восстановления для SQL Server. Кроме того, DPM 2010 поддерживает более 40 ТБ электронных писем, а также группы доступности баз данных Exchange 2010.
- **Резервные копии на уровне байтов.** В добавочной архивации в архив записываются только те файлы, которые были изменены с момента выполнения предыдущей архивации. В архивации на уровне байтов в архив записываются только изменившиеся байты файлов, что значительно уменьшает объем записываемых данных.
- **Нулевые потери при восстановлении данных Exchange, SQL Server и SharePoint.** Интеграция архивов баз данных, полученных в определенные моменты времени, с журналами приложений позволяет восстанавливать данные до состояния на тот момент времени, когда произошел сбой, а не только до момента, когда была создана последняя резервная копия.
- **Программы-агенты устанавливаются на серверах в офисах филиалов.** Это позволяет пересылать данные архивов по каналам WAN. Программы-агенты могут использоваться также для пересылки данных по локальным сетям, что позволяет записывать удаленные архивы на локальные носители.
- **Поддержка записи архивов в хранилища с прямым подключением.** Архивы можно записывать на устройства SAN Fibre Channel и iSCSI. Заметьте, что устройства USB и IEEE 1394 не поддерживаются.
- **Подробные отчеты,** включающие данные об успешной и неудачной защите и об использовании носителей, на которые ведется запись.
- **Пакет управления для System Center Operations Manager 2010.** Этот пакет позволяет централизованно управлять защитой и восстановлением данных на нескольких серверах DPM 2010 и серверах с установленными программа-

ми-агентами DPM 2010. Этот компонент лучше всего подходит для окружений с большим числом серверов и клиентов DPM 2010.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ DPM 2010

Подробное описание и пробную версию DPM 2010 можно найти по адресу <http://www.microsoft.com/ru-ru/download/details.aspx?id=22615>.

---

## Резюме

- Система архивации данных Windows Server позволяет выполнять архивацию данных на серверах Windows Server 2008 и 2008 R2 по расписанию и вручную.
- Только члены локальной группы администраторов могут выполнять запланированную архивацию в Windows Server 2008 и 2008 R2, хотя члены группы операторов архива могут выполнять архивацию вручную.
- Windows Server 2008 R2 позволяет указывать файлы и папки, которые будут включены в архив или исключены из него. В Windows Server 2008 минимальный блок для архивации — том.
- Утилита командной строки Wbadmin.exe предоставляет больше функциональности, чем система архивации данных Windows Server, но ее можно использовать только из командной строки с повышенными привилегиями. Все новые возможности системы архивации, появившиеся в Windows Server 2008 R2, доступны и в утилите командной строки.
- В Windows Server 2008 данные, полученные при архивации по расписанию, можно записывать только на локальные диски или внешние диски USB 2.0 и IEEE 1394, хотя при использовании файла сценария и планировщика заданий данные можно записывать на внутренние или внешние жесткие диски, тома на таких дисках или в сетевые папки. В обеих операционных системах данные архивации, выполняемой вручную, можно записывать на локальные жесткие диски, в сетевые папки и на DVD помощи локальных записывающих устройств.
- Система архивации данных Windows Server позволяет создать только одно расписание архивации. Однако можно создать дополнительные расписания, создав сценарий с использованием команды Wbadmin.exe и настроив его выполнение при помощи планировщика заданий.
- Архивация данных состояния системы позволяет архивировать Active Directory. Обычно для архивации ролей и служб ролей Windows Server 2008 достаточно выполнить архивацию данных состояния системы.

## Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных на занятии 1. Эти вопросы предоставлены также в электронном виде на прилагаемом к книге компакт-диске.

---

### ПРИМЕЧАНИЕ Ответы

Ответы на вопросы и пояснения к их вариантам размещены в разделе «Ответы» в конце книги.

---



1. Вы хотите предоставить пользователю в удаленном расположении возможность выполнять раз в неделю ручную архивацию файлового сервера, записывая данные на съемное устройство USB 2.0, которое затем будет передаваться курьером в главный офис организации. В какую группу на файловом сервере следует добавить этого пользователя, чтобы он мог выполнять описанную задачу, но не имел лишних административных привилегий?
  - a. Опытные пользователи.
  - b. Операторы архива.
  - c. Администраторы.
  - d. Пользователи удаленного рабочего стола.
2. Вы хотите выполнять архивацию папки, содержащей важные часто обновляемые файлы, в сетевую папку каждые три часа. Вы уже создали расписание архивации, по которому каждые 24 часа выполняется архивация всего сервера, работающего под управлением Windows Server 2008 R2. Какие действия следует выполнить, чтобы создать расписание для более частой архивации? (Каждый ответ составляет часть решения; выберите два.)
  - a. Создать пакетный файл, содержащий команду `wbadmin start backup`, обращающийся по пути UNC сетевой папки, используя учетные данные с соответствующим доступом. Использовать параметр `-include`, чтобы указать папку для архивации.
  - b. Создать пакетный файл, содержащий команду `wbadmin start backup`, обращающийся к локальному тому, используя учетные данные локального администратора.
  - c. С помощью планировщика заданий настроить задание, запускающее пакетный файл каждые три часа, используя учетные данные локального администратора.
  - d. С помощью планировщика заданий настроить задание, запускающее пакетный файл каждые три часа, используя учетные данные с соответствующим доступом к сетевой папке.
  - e. С помощью планировщика заданий настроить задание, запускающее пакетный файл раз в день, используя учетные данные локального администратора.
3. В какие из следующих расположений можно записывать данные, созданные системой архивации данных Windows Server при архивации по расписанию на компьютере под управлением Windows Server 2008 R2? (Каждый ответ является самостоятельным решением. Выберите четыре.)
  - a. Внешний диск USB 2.0.
  - b. Внешний диск IEEE 1394.
  - c. Внутренний диск IDE.
  - d. Устройство SAN iSCSI.
  - e. Том на внешнем жестком диске.
  - f. Привод DVD.

4. Вы оптимизируете производительность резервного копирования на компьютере под управлением Windows Server 2008 R2. Операции, интенсивно использующие диск, выполняются на томе H: этого компьютера, и вы хотите настроить архивацию отдельно для каждого тома. Какой параметр оптимизации производительности следует выбрать?
  - a. Обычная производительность архивации.
  - b. Повышенная производительность архивации.
  - c. Выборочная.
  - d. Полная архивация VSS.
  - e. Копировать архив VSS.
5. Вы разрабатываете политику организации, относящуюся к изменениям в AD DS. Вы хотите, чтобы перед любыми изменениями в AD DS выполнялась архивация состояния системы. Вы хотите архивировать только данные состояния системы на контроллере домена, работающем под управлением Windows Server 2008 R2, и собираетесь использовать мастер однократной архивации из оснастки системы архивации данных Windows Server. Какие расположения для записи данных можно выбирать? (Каждый ответ является самостоятельным решением. Выберите три.)
  - a. Сетевая папка.
  - b. Привод DVD.
  - c. Внешний жесткий диск USB 2.0.
  - d. Устройство SAN iSCSI.

## Занятие 2. Аварийное восстановление

Часть процесса аварийного восстановления — определение первоначальной причины сбоя. Если ее не устранить, сбой может произойти снова. Например, если диск выходит из строя из-за проблемы с материнской платой, а вы не можете диагностировать причину, с новым диском, взятым на замену, произойдет то же самое. На этом занятии вы научитесь выполнять аварийное восстановление, используя существующие архивы. Вы узнаете, как восстанавливать сервер целиком на новом оборудовании, как восстанавливать данные состояния системы и как выполнять принудительное восстановление удаленных из Active Directory элементов.

---

### Изучив материал этого занятия, вы сможете:

- ✓ Восстанавливать серверы.
- ✓ Восстанавливать роли и службы ролей.
- ✓ Восстанавливать данные.
- ✓ Восстанавливать Active Directory.

**Продолжительность занятия — примерно 40 мин.**

---

## Режимы восстановления системы архивации данных Windows Server

Чтобы иметь возможность выполнять операции восстановления при помощи системы архивации Windows Server, учетная запись пользователя должна входить в группу операторов архива или администраторов, или иметь соответствующие делегированные полномочия. Как говорилось в начале главы, архивы, полученные при помощи NTbackup.exe, нельзя восстановить при помощи системы архивации данных Windows Server или Wbadmin.exe. Существует версия NTbackup.exe, совместимая с Windows Server 2008 R2, и еще одна версия, совместимая с Windows Server 2008. Эти утилиты можно найти на сайте Microsoft, и ссылки на них приводились на занятии 1.

### Восстановление файлов и папок

Даже если архив получен для тома целиком, из него можно восстанавливать отдельные файлы и папки. На рис. 13-8 показано, как восстановить набор файлов и папок или даже отдельный файл.

При планировании восстановления файла или папки необходимо знать следующее:

- дату архивации файла или папки;
- расположение файла или папки;
- требуется ли восстановить параметры безопасности файла или папки;
- расположение, в которое требуется восстановить файл или папку;
- что делать, если в выбранном расположении находится дубликат.

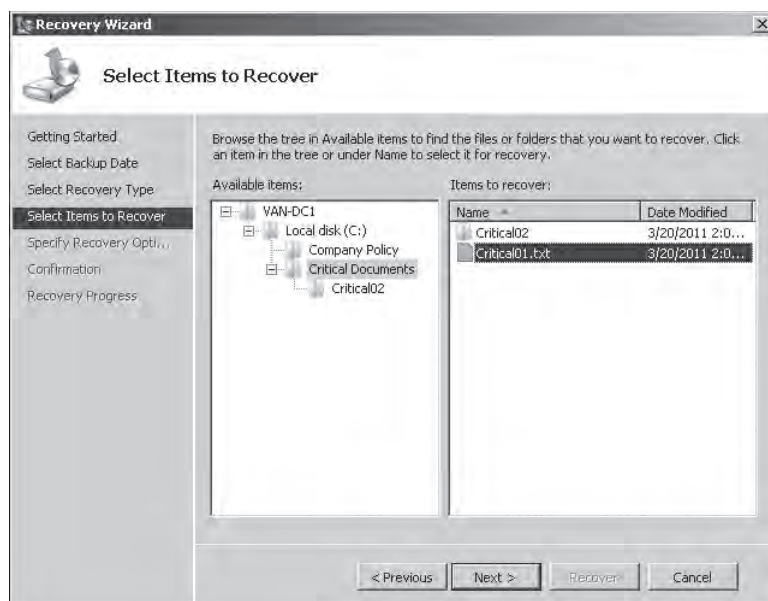


Рис. 13-8. Выбор элементов для восстановления

Если в выбранном для восстановления расположении находится дубликат, можно автоматически создать копию, переписать существующие файлы вос-

становленными или не восстанавливать файлы, для которых существуют дубликаты.

Система архивации данных Windows Server отвечает за управление существующими файлами архивов, так что если архивные данные требуется считать из нескольких разных файлов архивов (например, когда требуется восстановить несколько папок на томе, для которого выполнялась добавочная архивация), этот происходит автоматически. Раньше самым большим недостатком восстановления из добавочных архивов была необходимость определять, какие архивы требуются. На практикуме этой главы вы выполните восстановление файла и папки.

## Восстановление приложений и данных приложений

Система архивации данных Windows Server в Windows Server 2008 R2 позволяет восстанавливать отдельные приложения. При этом восстанавливается приложение, его параметры и связанные с ним данные. Это возможно, если приложение зарегистрировано в системе архивации данных Windows Server. Регистрация выполняется во время установки приложения.

Когда выполняется восстановление приложения, предоставляется список приложений, зарегистрированных в системе архивации, которые можно восстановить до состояния в момент создания архива. Если по данным, хранящимся в каталоге архивации, архив, из которого выполняется восстановление, является наиболее свежим архивом этого приложения, предоставляется возможность выполнить для базы данных приложения восстановление с повтором. По умолчанию восстановление с повтором разрешено. Устанавливать флажок **Не выполнять восстановление баз данных приложений с повтором всех завершенных транзакций** (Do Not Perform A Roll-Forward Recovery Of The Application Database) следует только в том случае, если требуется запретить восстановление с повтором. Этот параметр можно использовать, если после получения архива внесено изменение (например, удалена важная таблица из базы данных SQL Server), которое требуется отменить.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Восстановление приложений и связанных с ними данных

Подробнее о восстановлении приложений, поддерживающих систему архивации данных Windows Server, и связанных с ними данных см. по адресу <http://technet.microsoft.com/ru-ru/library/cc725726.aspx>.

---

## Восстановление томов

Восстановление томов — это восстановление всего содержимого томов. Его можно выполнять, когда том потерян из-за сбоя диска, но выполнять полное восстановление операционной системы или сервера не требуется. Важно помнить, что при восстановлении томов все существующие данные в конечном расположении будут потеряны. Восстанавливать можно один или несколько томов.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Восстановление томов при помощи Wbadmin

Подробнее о восстановлении томов при помощи утилиты командной строки Wbadmin см. по адресу [http://technet.microsoft.com/en-us/library/dd364720\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/dd364720(Ws.10).aspx) (на английском языке).

---

## Полное восстановление сервера и операционной системы

Полное восстановление сервера позволяет восстановить сервер, загрузившись при помощи установочного носителя Windows Server 2008 R2 или среды восстановления Windows. Функция полного восстановления сервера расширяет функцию автоматического восстановления системы (ASR), используемую в предыдущих версиях Windows, поскольку восстанавливает все данные операционной системы, приложений и другие данные на сервере. ASR не обеспечивает настолько полное восстановление, и после завершения восстановления ASR приходится восстанавливать данные из других архивов.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Полное восстановление сервера и операционной системы

Подробнее о полном восстановлении сервера и операционной системы см. по адресу <http://technet.microsoft.com/ru-ru/library/cc755163.aspx>.

---

Восстановление операционной системы аналогично полному восстановлению сервера за тем исключением, что восстанавливаются только тома с критически важными данными. Например, если на файловом сервере данные операционной системы и пользовательские данные хранятся на разных томах, и из строя выходят диски с данными операционной системы, следует восстанавливать только операционную систему.

Выполняя полное восстановление сервера или восстановление операционной системы, убедитесь, что конечный диск имеет как минимум такой же объем, что и диск, содержащий восстанавливаемые тома, независимо от размера томов на этом диске. Например, если выполнить полную архивацию сервера, использующего один раздел объемом 30 ГБ на диске с общим объемом 100 ГБ, то для восстановления потребуется диск объемом минимум 100 ГБ.

Для восстановления операционной системы и полного восстановления сервера требуется загрузка с установочного носителя Windows Server 2008 R2 или загрузка в среду восстановления и использование параметров восстановления компьютера. Чтобы выполнить восстановление операционной системы или полное восстановление сервера, выполните следующее:

1. Выполните загрузку с установочного носителя Windows Server 2008 R2.
2. Выберите языковые параметры и щелкните **Далее**.
3. На странице **Установка Windows** (Install Windows) щелкните **Восстановить компьютер** (Repair Your Computer).
4. Если восстановление выполняется на новом оборудовании, список **Параметры восстановления системы** (System Recovery Options) будет пустым. В противном случае он будет содержать все обнаруженные на компьютере операционные системы, включая поврежденные. В любом случае, щелкните **Далее**.
5. В диалоговом окне **Параметры восстановления системы** (System Recovery Options) щелкните **Восстановление образа системы** (Windows Complete PC Restore) (рис. 13-9).
6. Если выбрать восстановление образа системы, будет выполнен поиск наиболее актуального архива на всех локальных и подключенных запоминающих устройствах. Можно выполнить восстановление из обнаруженного ар-

хива или указать другой архив, щелкнув **Восстановить другой архив** (Restore a Different Backup). На рис. 13-10 показано несколько доступных архивов, которые можно восстановить с одного внешнего устройства USB 2.0. Щелкнув на кнопке **Дополнительно** (Advanced), можно выполнить поиск архивов в сети или установить драйвер для локально подключенного диска (например, SCSI), который система не видит из-за того, что не загружено соответствующее ПО.

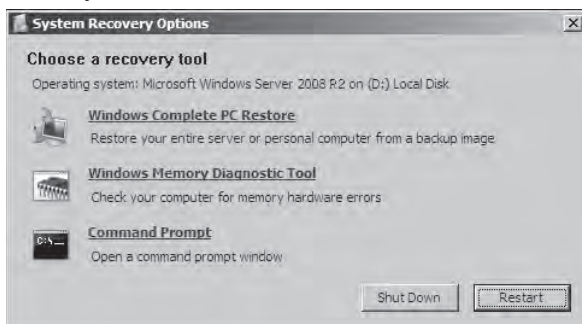


Рис. 13-9. Выбор способа восстановления

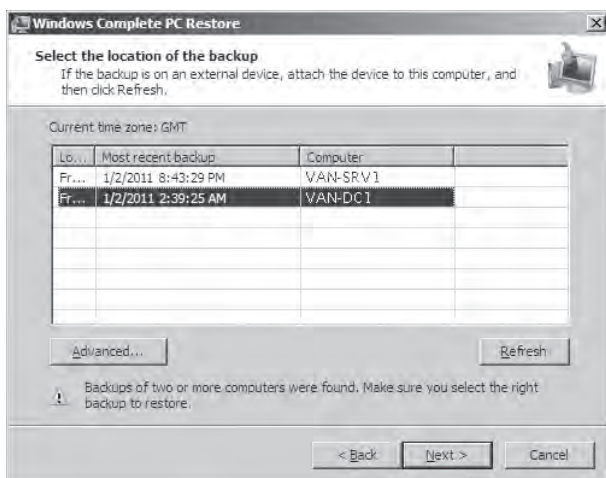


Рис. 13-10. Выбор архива для восстановления

- На странице **Выберите дополнительные параметры восстановления** (Choose How to Restore The Backup) установите флажок **Форматировать и перераспределить разделы диска** (Format and Repartition Disks), если еще не подготовили диски для восстановления. Это сделает доступной кнопку **Исключить диски** (Exclude Disks). Нажмите эту кнопку, если есть диски, которые не требуется форматировать и перераспределять. Диск, на котором размещены архивные данные, исключается автоматически. Если есть диски, не содержащие критически важные данные, можете установить флажок **Восстанавливать только системные диски** (Only restore System Disks), чтобы восстановить только операционную систему. Сейчас можно установить дополнительные драйверы, если таковые требуются для работы дисков, на

которые выполняется восстановление. Нажмите кнопку **Дополнительно** (Advanced), если требуется проверить диски на наличие ошибок сразу после завершения восстановления.

## Восстановление состояния системы

Восстановление состояния системы — наиболее распространенный способ восстановления Active Directory или поврежденных данных роли сервера. Восстановление состояния системы невозможно выполнить частично; оно всегда выполняется полностью. Такое восстановление вы выполните на практикуме этой главы. Высокоуровневая процедура восстановления состояния системы при помощи утилиты Wbadmin выполняется следующим образом:

1. Откройте административную командную строку и выполните команду `wbadmin get versions`, возвращающую список архивов. Наиболее свежий архив показан первым.
2. Запишите идентификатор версии архива, который будет иметь формат ММ/ДД/ГГГГ-ЧЧ:ММ. Его необходимо указать при выполнении восстановления.
3. Выполните команду `wbadmin Start SystemStateRecovery -version:ММ/ДД/ГГГГ-ЧЧ:ММ`. Введите **Y**, чтобы подтвердить восстановление состояния системы, и нажмите Enter, чтобы начать процесс восстановления. Когда восстановление завершится, перезагрузите сервер.
4. Сервер может потребовать несколько перезагрузок, в зависимости от того, какие роли были установлены на момент архивации состояния системы.

### Проверьте себя

1. При каких условиях можно выполнить восстановление приложения?
2. Как обратиться к инструменту, позволяющему выполнить полное восстановление сервера на компьютере под управлением Windows Server 2008 R2?

### Ответ

1. Приложение должно быть зарегистрировано в системе архивации данных Windows Server. Зарегистрированное приложение можно восстановить без восстановления других данных, не относящихся к этому приложению.
2. Необходимо загрузиться с установочного носителя Windows Server 2008 R2 или загрузить среду восстановления Windows.

## Восстановление Active Directory и ролей сервера

Восстановление Active Directory выполняется посредством восстановления данных состояния системы контроллера домена. При восстановлении данных состояния системы восстанавливаются роли сервера (включая AD DS) и службы ролей. Восстановление данных состояния системы называется *непринудительным* восстановлением. При таком восстановлении база данных AD DS



возвращается на сервер в том состоянии, в котором была в момент создания архива.

После перезагрузки в конце процесса репликации состояния системы контроллер домена выполняет репликацию данных с других контроллеров домена, и база данных Active Directory обновляется, получая изменения, произошедшие со времени резервного копирования. Если требуется не просто восстановить контроллер домена, а восстановить определенные объекты Active Directory, удаленные из базы данных, необходимо выполнить *принудительное восстановление*.

## Принудительное восстановление

Когда выполняется непринудительное восстановление, объекты, удаленные после создания архива, снова будут удалены во время репликации восстановленного контроллера домена с другими контроллерами домена. На всех остальных контроллерах домена объект помечен как удаленный, поэтому в процессе репликации локальная копия объекта тоже будет помечена как удаленная. Если выполняется принудительное восстановление, удаленный объект помечается так, что во время репликации он восстанавливается в домене в активном состоянии. Важно помнить, что при удалении объект не убирается из Active Directory навсегда, а только получает атрибут, который помечает его как удаленный до тех пор, пока не истечет срок захоронения. Срок захоронения определяет время, в течение которого удаленный объект остается в AD DS; по умолчанию это 180 дней.

Чтобы база данных AD DS не обновлялась до выполнения принудительного восстановления, используется режим восстановления служб каталогов (DSRM). Этот режим позволяет пометить объекты как восстановленные, после чего следует перезагрузить контроллер домена для репликации изменений на другие контроллеры домена.

---

### ПРИМЕЧАНИЕ Принудительное восстановление не обязательно на единственном контроллере домена

Если в домене имеется только один контроллер домена, принудительное восстановление выполнять не требуется, так как в домене нет другой копии базы данных AD DS.

---

## Загрузка в режиме восстановления служб каталогов

Загрузить DSRM можно тремя способами. Первый — нажать F8 во время загрузки компьютера и выбрать режим восстановления службы каталогов, как показано на рис. 13-11.

Чтобы использовать этот способ, надо успеть нажать клавишу F8 в течение небольшого промежутка времени, и если нажать слишком поздно, будет выполнена обычная загрузка. Второй способ — открыть административную командную строку и выполнить следующую команду:

```
Bcdedit /set safeboot dsrepair
```

Эта команда изменяет параметры загрузки так, что Windows Server 2008 R2 автоматически загружается в режиме DSRM. Обычно эта команда используется на контроллерах домена, работающих в режиме Server Core. Чтобы удалить

этот параметр загрузки, откройте административную командную строку и выполните следующую команду:

```
Bcdedit /set safeboot
```

Третий способ — открыть консоль **Конфигурация системы** (System Configuration) из меню **Администрирование** (Administrative tools) и на вкладке **Загрузка** (Boot) установить флажок **Безопасный режим** (Safe boot) и выбрать переключатель **Восстановление Active Directory** (Active Directory Repair) (см. рис. 13-23 в разделе практикума в конце главы).

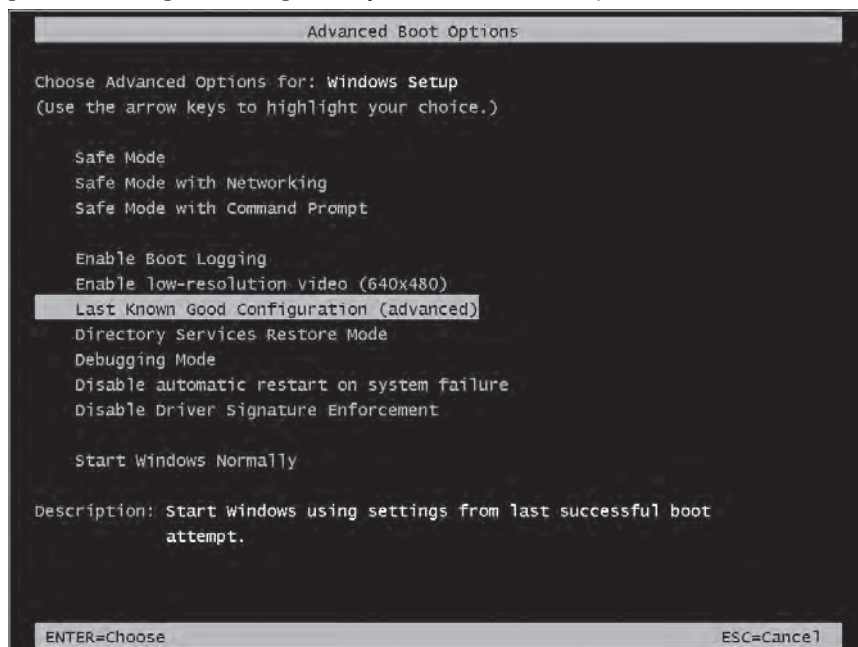


Рис. 13-11. Загрузка DSRM после нажатия F8

Для входа в режим DSRM требуется пароль DSRM. Пароль DSRM устанавливается отдельно для каждого сервера во время его повышения до контроллера домена. Пароль DSRM может потребоваться нескоро, и администраторы часто забывают его. Если вспомнить его не удастся, можно переустановить его, выполнив следующие действия (рис. 13-12):

1. Зайдите на контроллер домена под учетной записью, входящей в группу администраторов домена.
2. Откройте административную командную строку и выполните команду `ntdsutil`.
3. В приглашении `ntdsutil` введите `set dsrm password` и нажмите Enter.
4. В приглашении **Переустановите пароль администратора DSRM:** (Reset DSRM Administrator Password:) выполните одно из следующих действий:
  - Для переустановки пароля DSRM на локальном контроллере домена введите команду `reset password on server null`. Введите и подтвердите новый пароль.

- Для переустановки пароля DSRM на другом контроллере домена введите команду `reset password on server имя_сервера`, где *имя\_сервера* — полное доменное имя (FQDN) сервера, на котором требуется переустановить пароль.
5. В приглашении **Переустановите пароль администратора DSRM:** введите **q** и нажмите Enter, чтобы вернуться к приглашению `ntdsutil:`, после чего введите **q** и нажмите Enter, чтобы выйти.

Перезагрузив контроллер домена в режиме DSRM и войдя с использованием учетной записи администратора и пароля DSRM, выполните непринудительное восстановление, восстановив данные состояния системы при помощи утилиты `Wbadmin.exe`. Этот процесс описан выше в разделе «Восстановление состояния системы». Если требуется выполнить принудительное восстановление `SYSVOL`, выполните восстановление состояния системы, используя параметр `-AuthSysVol`. Этот параметр не является стандартным для процесса принудительного восстановления и его следует использовать, только когда требуется выполнить откат `SYSVOL` до предыдущей версии, отличающейся от текущей.

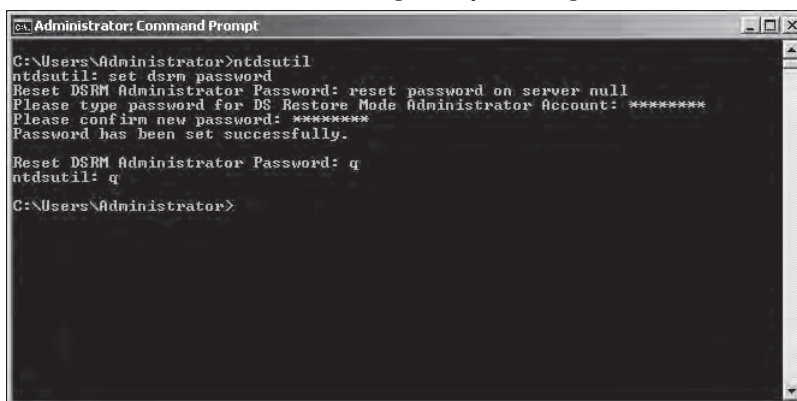


Рис. 13-12. Переустановка пароля DSRM

## Выполнение принудительного восстановления

После завершения процесса восстановления состояния системы используйте утилиту `ntdsutil` для входа в режим принудительного восстановления, в котором можно восстанавливать объекты, ссылаясь на их различающееся имя (DN).

Чтобы восстановить объект, введите `Restore Object` и DN объекта. Чтобы восстановить контейнер и все его содержимое, введите `Restore Subtree` и DN контейнера. Например, чтобы восстановить подразделение `Platapus` со всем его содержимым в домене `Tailspintoys.com`, введите следующую команду:

```
Restore Subtree «OU=Platapus,DC=Tailspintoys,DC=com»
```

Если объекты имеют обратные ссылки, в каталоге, куда выполняется принудительное восстановление, будет создан файл `LDIF`. Обратная ссылка включает информацию, которая не была автоматически включена при выполнении принудительного восстановления, например, членство в группах, имевшееся у восстановленного объекта. Файл `ldif` необходимо использовать в каждом домене, где могут иметься GPO, включенные в восстановленный объект во время

его удаления. Чтобы выполнить эту операцию, выполните на каждом контроллере домена, где это необходимо, следующую команду:

```
Ldifde -I -k ldif.filename
```

На практикуме этой главы вы выполните принудительное восстановление объектов AD DS.

## ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Восстановление AD DS

Подробнее о выполнении принудительного восстановления объектов AD DS см. по адресу [http://technet.microsoft.com/en-us/library/cc816751\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc816751(WS.10).aspx) (на английском языке).

## Восстановление удаленных GPO

Удаленные GPO нельзя восстановить при помощи принудительного восстановления и необходимо восстанавливать при помощи GPMC. Для этого откройте GPMC, щелкните правой кнопкой мыши контейнер **Объекты групповой политики** (Group Policy Objects) и выберите команду **Управление архивами** (Manage Backups). Перейдите в расположение, где хранятся архивы GPO, выберите GPO, который хотите восстановить (рис. 13-13) и нажмите кнопку **Восстановить** (Restore).

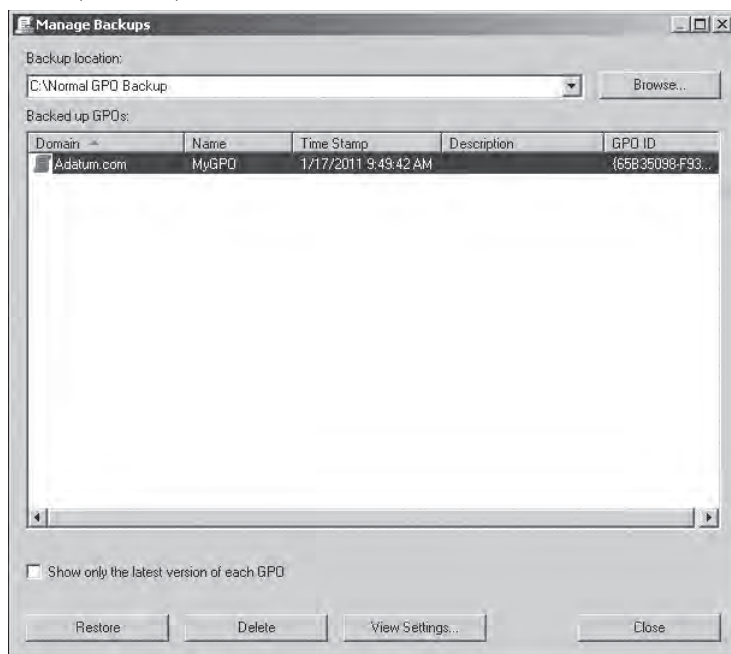


Рис. 13-13. Восстановление GPO

## Полное восстановление сервера на контроллере домена

При полном восстановлении сервера на контроллере домена автоматически выполняется непринудительное восстановление Active Directory. Природа процесса полного восстановления сервера такова, что его сложно использовать для принудительного восстановления, поскольку высока вероятность того, что сер-

вер перезагрузится и выполнит репликацию до того, как администратор сможет перевести его в режим DSRM для принудительного восстановления. Технически это возможно, если успеть нажать F8 в нужный момент, но выполнение полного восстановления сервера на контроллере домена не следует рассматривать в качестве штатного способа восстановления удаленных данных объектов Active Directory. Конечно, после выполнения полного восстановления ничто не мешает выполнить принудительное восстановление, используя описанные на этом занятии способы. Для выполнения полного восстановления сервера на контроллере домена выполняется так же, как на обычном сервере (см. выше).

## Средство подключения баз данных AD DS

Средство подключения баз данных AD DS (Dsamain.exe) позволяет создавать и просматривать данные, хранящиеся в AD DS, не перезагружая контроллер домена в режиме DSRM. Dsamain.exe можно использовать для сравнения состояния AD DS в разных моментальных снимках, не восстанавливая несколько архивов. Это очень полезно, когда требуется определить, содержит ли определенный архив AD DS нужные объекты.

Кроме того, Dsamain.exe можно использовать совместно с ntdsutil и системой архивации данных Windows Server 2008 R2. Для этого требуется подключить моментальный снимок каталога при помощи ntdsutil, после чего можно просматривать и изменять его при помощи Dsamain.exe. В целях безопасности просматривать эти моментальные снимки могут только администраторы домена и администраторы предприятия.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Восстановление объектов-захоронений

Подробнее о восстановлении удаленных из AD DS объектов см. по адресу <http://technet.microsoft.com/ru-ru/magazine/2007.09.tombstones.aspx>. Там приводится общая информация, не относящаяся конкретно к Windows Server 2008 R2.

---

Модуль Active Directory для Windows PowerShell в Windows Server 2008 R2 позволяет использовать командлеты PowerShell для управления доменами AD DS, наборами конфигурации AD LDS и экземплярами средства подключения баз данных AD DS.

## Модуль Active Directory для Windows PowerShell

Модуль Active Directory для Windows PowerShell по умолчанию устанавливается при установке Windows PowerShell и .NET Framework 3.5.1. Для корректной работы модуля необходима установка обоих этих компонентов.

Если хотите использовать этот модуль для управления доменом AD DS, экземпляром средства подключения баз данных AD DS, экземпляром или набором конфигурации AD LDS, необходимо установить веб-службы Active Directory как минимум на одном контроллере домена или сервере, на котором размещен экземпляр AD LDS.

Чтобы открыть командную строку модуля, запустите **Модуль Active Directory для Windows PowerShell** (Active Directory Module For Windows PowerShell) из меню **Администрирование** (Administrative Tools). Модуль предоставляет команды PowerShell для поиска и изменения объектов и управления следующими элементами:

- группы;
- учетные записи служб;
- подразделения;
- политики паролей;
- дополнительные компоненты (такие как Корзина);
- леса и домены;
- контроллер домена и хозяин операций.

Для примера рассмотрим возможность поиска и изменения объектов, в частности, восстановление отдельного объекта AD DS и восстановление контейнера вместе с дочерними элементами.

Для восстановления в AD DS отдельного объекта используются командлеты `Get-ADObject` и `Restore-ADObject`. В следующем примере показано, как восстановить удаленное подразделение `Sales_Department` в локальном домене:

```
Get-ADObject -ldapFilter:»(msDS-LastKnownRDN=Sales_Department)» -IncludeDeletedObjects | Restore-ADObject
```

Как показано на рис. 13-14, эта команда не выводит данные в консоль Windows PowerShell. Если удаленный объект найден, он восстанавливается. Недостаток этого метода в том, что вы не получаете предупреждения, если удаленный объект не найден.

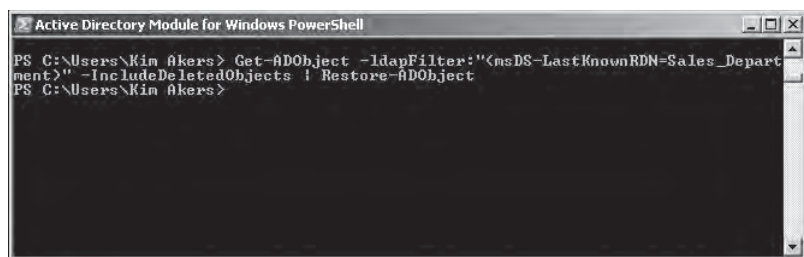


**Рис. 13-14.** Восстановление отдельного объекта AD DS

Для восстановления объекта-контейнера вместе с дочерними объектами используются те же команды Windows PowerShell, что и для восстановления отдельного объекта, но процедура выполняется в два этапа. Например, чтобы восстановить в домене `adatum.com` подразделение `HR_Department` вместе со всеми дочерними объектами, используйте следующую команду:

```
Get-ADObject -ldapFilter:»(msDS-LastKnownRDN=HR_Department)» -IncludeDeletedObjects | Restore-ADObject
```

Для восстановления удаленных дочерних объектов подразделения `HR_Department` выполните следующую команду:

```
Get-ADObject -SearchBase «CN=Deleted Objects,DC=adatum,DC=com» -Filter {lastKnownParent -eq «OU=HR_Department,DC=adatum,DC=com»} -IncludeDeletedObjects | Restore-ADObject
```

Эти команды показаны на рис. 13-15. Как и при восстановлении отдельного объекта, выходные данные не отображаются, и требуется проверять, восстановился ли объект и его дочерние объекты.

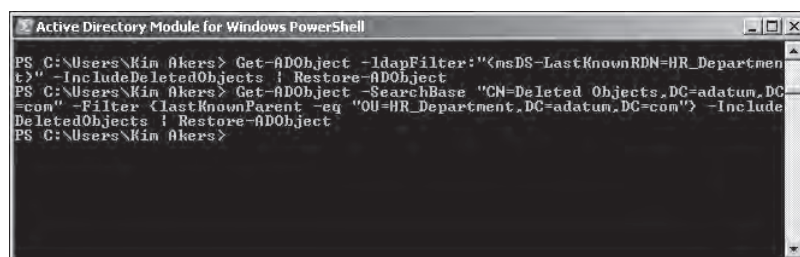


Рис. 13-15. Восстановление объекта AD DS и его дочерних объектов

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ **Get-ADObject и Restore-ADObject**

Для получения подробной информации о параметрах, которые можно передавать командам `Get-ADObject` и `Restore-ADObject`, откройте командную строку модуля Active Directory и выполните команду `Get-Help Get-ADObject -detailed` или `Get-Help Restore-ADObject -detailed`.

---

### ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ **Администрирование Active Directory при помощи PowerShell**

Подробнее об использовании Windows PowerShell для управления объектами AD DS см. по адресу [http://technet.microsoft.com/en-us/library/dd378937\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/dd378937(Ws.10).aspx) (на английском языке).

---

## Hyper-V и аварийное восстановление

Система архивации данных Windows Server записывает данные архивов как файлы образов в формате VHD. При помощи системы архивации и `Wbadmin.exe` можно выполнять восстановление операционной системы и восстанавливать тома или отдельные файлы и папки на исходный или другой сервер. Можно также восстанавливать виртуальные машины, работающие под управлением Hyper-V.

С точки зрения планирования аварийного восстановления это означает, что Windows Server 2008 R2 Datacenter Edition можно использовать в качестве платформы для восстановления, когда требуется восстановить серверы, но доступного оборудования для этого нет (например, после пожара). Выполнять восстановление на виртуальной машине можно и в том случае, если вышел из строя важный сервер, а для замены компонентов требуется какое-то время.

Можно также подключать образы архивов как тома к существующим виртуальным машинам, редактируя свойства этих машин и добавляя образ VHD как новый виртуальный диск. Обычно проще выполнять восстановление средствами системы архивации данных Windows Server, но такой способ может быть полезным для быстрого переноса разделов с физического сервера на виртуальный без копирования файлов.

## Резюме

- Восстановление может выполнять пользователь, входящий в группу операторов архива или администраторов.
- Если восстановление операционной системы или полное восстановление сервера выполняется на новый жесткий диск, необходимо убедиться, что объ-



ем нового диска не меньше объема исходного диска, содержавшего восстанавливаемые тома.

- Восстановление приложения можно выполнять только в том случае, если это приложение зарегистрировано в системе архивации данных Windows Server.
- При восстановлении данных состояния системы восстанавливается большинство ролей сервера, включая AD DS.
- Принудительное восстановление выполняется после перезагрузки контроллера домена в режиме DSRM. Принудительно восстановление AD DS используется для восстановления удаленных объектов AD DS.
- Модуль Active Directory для Windows PowerShell позволяет выполнять различные задачи восстановления, включая восстановление отдельного объекта AD DS или объекта AD DS со всеми дочерними объектами.

## Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных на занятии 2. Эти вопросы предоставлены также в электронном виде на прилагаемом к книге компакт-диске.

---

### ПРИМЕЧАНИЕ Ответы

Ответы на вопросы и пояснения к их вариантам размещены в разделе «Ответы» в конце книги.

---

1. Вы перезагрузили контроллер домена adatum.com в режиме DSRM, выполнили восстановление состояния системы и перевели утилиту ntdsutil в режим принудительного восстановления. Какую команду следует использовать для принудительного восстановления случайно удаленной учетной записи компьютера Pluto из подразделения Solar?
  - a. Restore Object “cn=Solar,OU=Pluto,dc=Adatum,dc=com”
  - b. Restore Computer “cn=Pluto,OU=Solar,dc=Adatum,dc=com”
  - c. Restore Object “cn=Pluto,OU=Solar,dc=Adatum,dc=com”
  - d. Restore Computer “cn=Solar,OU=Pluto, dc=Adatum,dc=com”
2. Ким Акерс — член локальной группы администраторов на сервере Glasgow, работающем под управлением Windows Server 2008 R2. На этом сервере находится сетевая папка, которую Сэм Аболрус, член локальной группы администраторов на компьютере Dundee, работающем под управлением Windows Server 2008 R2, использует в качестве целевого расположения, когда вручную выполняет архивацию данных на сервере Dundee. Сэм на этой неделе отсутствует, и пользователи сервера Dundee просят Кима восстановить некоторые удаленные папки, к которым не могут получить доступ через VSS. В какую группу должен входить Ким, чтобы иметь возможность восстанавливать данные на сервере Dundee с сервера Glasgow при помощи системы архивации данных Windows Server, соблюдая принцип наименьших привилегий?
  - a. Группа **Опытные пользователи** (Power Users) на сервере Glasgow.

- b. Локальная группа **Опытные пользователи** (Power Users) на сервере Dundee.
  - c. Группа **Операторы архива** (Backup Operators) на сервере Dundee.
  - d. Группа администраторов на сервере Dundee.
3. Вы используете модуль Active Directory для Windows PowerShell, чтобы восстановить в домене adatum.com случайно удаленное подразделение Australia, содержащее учетную запись компьютера Melbourne. Вы восстановили подразделение при помощи командлетов Get-ADObject и Restore-ADObject. Какую команду следует теперь использовать для восстановления учетной записи компьютера Melbourne?
- a. Никаких команд не требуется. При восстановлении подразделения автоматически восстанавливаются его дочерние объекты.
  - b. `Get-ADObject -SearchBase "CN=Deleted Objects,DC=adatum,DC=com" -Filter lastKnownParent -eq "OU=Melbourne,DC=adatum,DC=com"} | Restore-ADObject.`
  - c. `Restore-ADObject -SearchBase "CN=Deleted Objects,DC=adatum,DC=com" -Filter {lastKnownParent -eq "OU=Australia,DC=adatum,DC=com"} | Get-ADObject.`
  - d. `Get-ADObject -SearchBase "CN=Deleted Objects,DC=adatum,DC=com" -Filter {lastKnownParent -eq "OU=Australia,DC=adatum,DC=com"} | Restore-ADObject.`
4. На важном сервере в интрасети удаленного офиса вашей организации вышла из строя материнская плата. Это единственный компонент, требующий замены, но для доставки новой платы в удаленный офис потребуются несколько дней. За 12 часов до сбоя была вручную выполнена полная архивация сервера. Архив записан на съемный диск USB. В том же сайте установлена роль сервера Hyper-V и размещен виртуализованный контроллер домена. Что следует сделать, чтобы вышедший из строя сервер был доступен, пока вышедшая из строя плата не будет заменена?
- a. Выполнить автоматическое восстановление на компьютере под управлением Windows Server 2008 R2 Datacenter Edition.
  - b. На компьютере под управлением Windows Server 2008 R2 Datacenter Edition подключить архивные образы как дополнительные тома.
  - c. Выполнить полное восстановление сервера на виртуальной машине Hyper-V.
  - d. Восстановить данные состояния системы из архивных образов на компьютере под управлением Windows Server 2008 R2 Datacenter Edition.

## Практикум. Архивация Windows Server 2008 R2

На этом практикуме вы выполните три типа архивации: обычную архивацию операционной системы при помощи системы архивации данных Windows Server, архивацию тома при помощи Wbadmin.exe и архивацию состояния системы.

**ПРИМЕЧАНИЕ Дополнительный диск**

Как указано в начале главы, для выполнения заданий практикума потребуется дополнительный диск, подключенный к VAN-DC1. Это может быть виртуальный диск, если вы используете виртуальные машины. Если вы используете физическое оборудование, можете использовать внутренний диск или подключенный диск USB 2.0 или IEEE 1394. Диск должен иметь объем минимум 40 ГБ, чтобы на него вместились все архивные данные, полученные на практикуме.

**Упражнение 1. Архивация вручную при помощи системы архивации данных Windows Server**

В этом упражнении вы установите систему архивации данных Windows Server и вручную выполните архивацию сервера VAN-DC1. Сначала вы создадите набор объектов Active Directory, которые затем архивируете. Эти объекты будут удалены и восстановлены на втором практикуме этой главы.

1. Зайдите на VAN-DC1, используя учетную запись Kim Akers. Если диспетчер сервера не открылся автоматически, откройте его из меню **Администрирование**.
2. В консоли диспетчера сервера выберите узел **Компоненты (Features)** и щелкните **Добавить компоненты (Add Features)**. На странице выбора компонентов раскройте узел **Возможности системы архивации данных Windows Server (Windows Server Backup Features)** и установите флажки **Система архивации данных Windows Server (Windows Server Backup)** и **Программы командной строки (Command-line Tools)** (рис. 13-16).

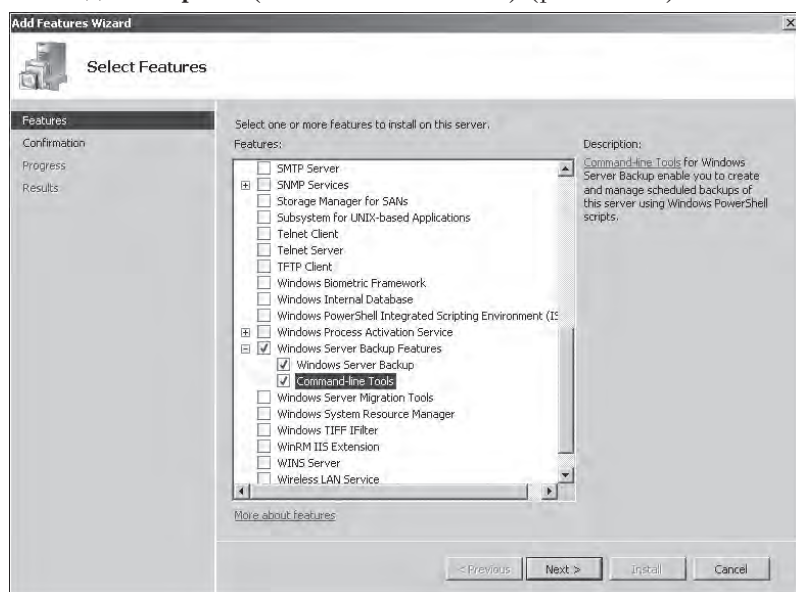


**Рис. 13-16.** Установка компонентов системы архивации данных Windows Server

3. Щелкните **Далее (Next)**, а затем **Установить (Install)**. Когда установка компонента завершится, щелкните **Заккрыть (Close)**.

**ПРИМЕЧАНИЕ Windows PowerShell и система архивации данных Windows**

В зависимости от текущей конфигурации VAN-DC1 может потребоваться подтверждение установки компонента Windows PowerShell. В Windows Server 2008 R2 система архивации данных Windows Server имеет расширенные командлеты Windows PowerShell для автоматизации стандартных задач и управления сценариями архивации (PowerShell устанавливается в Windows Server 2008 R2 по умолчанию).

4. Откройте оснастку **Active Directory — пользователи и компьютеры** из меню **Администрирование**. Создайте подразделение Planets в домене adatum.com. В этом подразделении создайте четыре учетных записи компьютеров: Saturn, Jupiter, Neptune и Uranus. Закройте оснастку **Active Directory — пользователи и компьютеры**.
5. Убедитесь, что дополнительный диск подключен к компьютеру. Если диск не отформатирован, отформатируйте его в файловой системе NTFS.

**ПРИМЕЧАНИЕ NTFS и FAT32**

Хотя при выполнении архивации вручную данные можно записывать на диски с файловой системой FAT32, NTFS предоставляет больше возможностей и обеспечивает более высокую производительность.

6. Откройте оснастку **Система архивации данных Windows Server** (Windows Server Backup) из меню **Администрирование**. На панели **Действия** (Actions) щелкните **Однократная архивация** (Backup Once), чтобы запустить мастер однократной архивации.
7. Убедитесь, что установлен переключатель **Другие параметры** (Different Options), и щелкните **Далее**.
8. На странице **Выбор конфигурации архивации** (Select Backup Configuration) установите переключатель **Настраиваемый** (Custom) и щелкните далее (рис. 13-17).

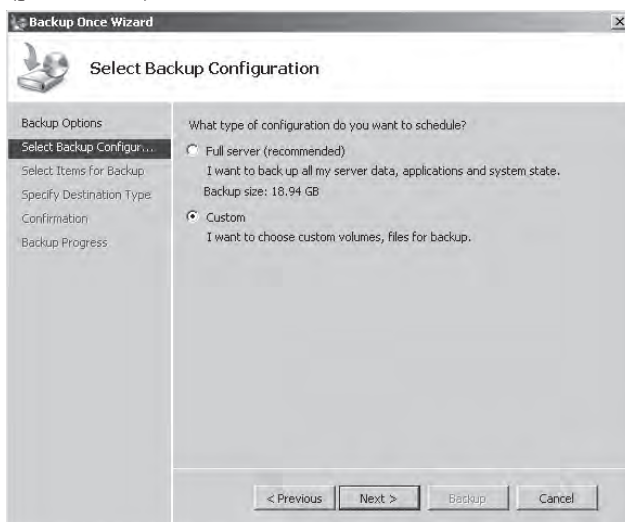


**Рис. 13-17.** Выбор конфигурации архивации

9. На странице **Выберите объекты, подлежащие архивации** (Select Items For Backup) нажмите кнопку **Добавление элементов** (Select Items). В диалоговом окне выберите локальный диск C: и щелкните **ОК** (рис. 13-18).

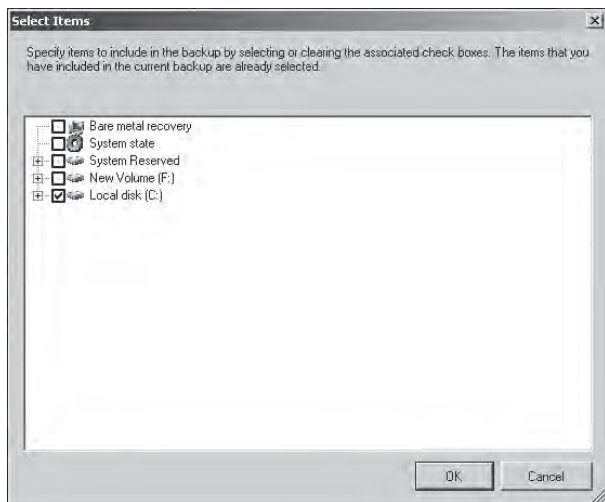


Рис. 13-18. Выбор объектов для архивации

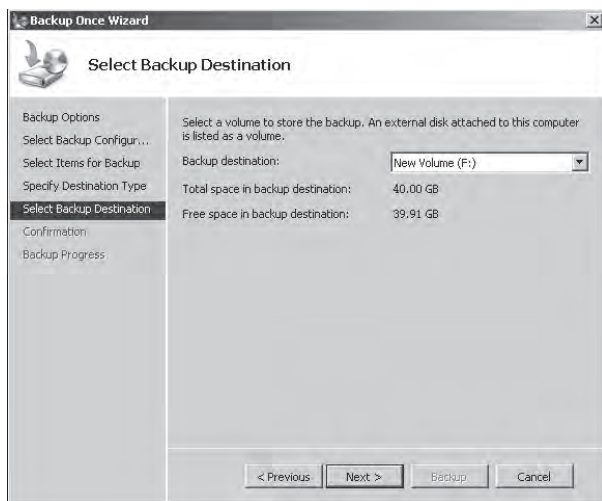


Рис. 13-19. Выбор места назначения архивации

10. На странице **Выберите объекты, подлежащие архивации** (Select Items For Backup) нажмите кнопку **Дополнительные параметры** (Advanced Settings). В открывшемся диалоговом окне на вкладке **Исключения** (Exclusions) щелкните **Добавить исключение** (Add Exclusion). Посмотрите, какие элементы можно исключать, но ничего не исключайте. Щелкните **Отмена**.
11. На вкладке **Параметры VSS** (VSS Settings) установите переключатель **Полная архивация VSS** (VSS Full Backup) и щелкните **ОК**. На странице выбора объектов для архивации щелкните **Далее**.

12. Убедитесь, что на странице **Укажите тип места назначения** (Specify Destination Type) установлен переключатель **Локальные диски** (Local Drives), и щелкните **Далее**.
13. На странице **Выбор места назначения архивации** (Select Backup Destination) выберите диск, который добавили на VAN-DC1 (рис. 13-19) и щелкните **Далее** (Next).
14. На странице подтверждения щелкните **Архивировать** (Backup). Когда архивация завершится, щелкните **Заккрыть**. Архивация может занять довольно много времени, но вы можете щелкнуть **Заккрыть** на странице **Ход архивации** (Backup Progress), чтобы архивация выполнялась в фоновом режиме.

## Упражнение 2. Архивация тома и состояния системы при помощи Wbadmin.exe

В этом упражнении вы выполните архивацию тома и архивацию состояния системы при помощи утилиты командной строки Wbadmin.exe.

1. Если требуется, зайдите на VAN-DC1 под учетной записью пользователя Kim Akers.
2. Создайте на томе C: папку Континенты. Создайте в этой папке пять текстовых файлов со следующими именами: Европа.txt, Антарктида.txt, Африка.txt, Австралия.txt и Азия.txt. Содержимое файлов должно совпадать с именами.
3. Откройте командную строку с административными привилегиями. Если требуется, щелкните **Да** в диалоговом окне службы контроля учетных записей.
4. Введите следующую команду и нажмите Enter:

```
wbadmin start backup -backuptarget:f: -include:c: -vssFull -quiet
```

---

### ПРИМЕЧАНИЕ Целевой том для архивации

Если дополнительный том на вашем компьютере имеет другую букву (не F), измените команду соответствующим образом. Например, если это том E:, следует использовать аргумент -backuptarget:e:.

5. Когда архивация завершится, запишите дату и время создания архива (это потребуется для следующего упражнения) и удалите папку C:\Континенты.
6. Введите следующую команду и нажмите Enter:  

```
wbadmin start systemstatebackup -backuptarget:f: -quiet
```
7. Когда архивация завершится, введите следующую команду и нажмите Enter:  

```
wbadmin get versions
```
8. Убедитесь, что все три задания архивации успешно выполнены.

## Практикум. Восстановление Windows Server 2008 R2

Перед выполнением заданий этого практикума требуется выполнить все упражнения предыдущего практикума. На этом практикуме вы восстановите файлы

и папки, которые архивировали, а затем удалили. Вы выполните загрузку в режиме DSRM, выполните принудительное восстановление объектов Active Directory и восстановите каталог архивации.

## Упражнение 1. Восстановление файлов и папок

В этом упражнении вы восстановите удаленную папку Континенты и все файлы, содержащиеся в ней. Также вы подготовитесь ко второму упражнению, удалив несколько объектов Active Directory.

1. Зайдите на VAN-DC1 под учетной записью Kim Akers. Убедитесь, что на томе C: нет папки Континенты.
2. Откройте оснастку **Система архивации данных Windows Server** (Windows Server Backup) из меню **Администрирование**.
3. На панели **Действия** (Actions) щелкните **Восстановление** (Recover), чтобы запустить мастер восстановления. На странице **Приступая к работе** (Getting Started) установите переключатель **Этот сервер (VAN-DC1)** [This Server (VAN-DC1)] и щелкните **Далее**.
4. На странице **Выберите дату архивации** (Select Backup Date) выберите дату и время создания архива из предыдущего практикума и щелкните **Далее**.
5. На странице **Выберите тип восстановления** (Select Recovery Type) установите переключатель **Файлы и папки** (Files and Folders) и щелкните **Далее**.
6. На странице **Выберите восстанавливаемые элементы** (Select Items To Recover) раскройте узел **VAN-DC1** на панели **Доступные элементы** (Available Items) и выберите том **Локальный диск (C:)**. В списке **Восстанавливаемые элементы** (Items to Recover) выберите папку **Континенты** и щелкните **Далее** (рис. 13-21).

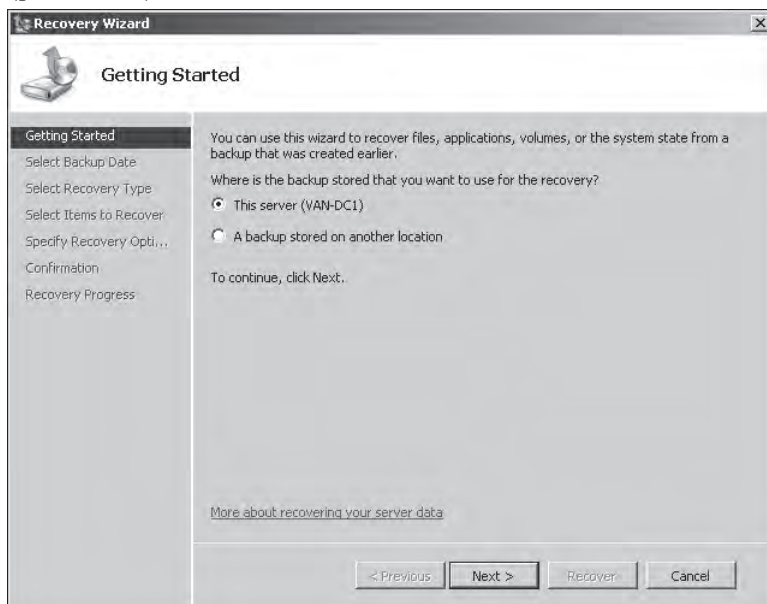


Рис. 13-20. Выбор сервера для восстановления



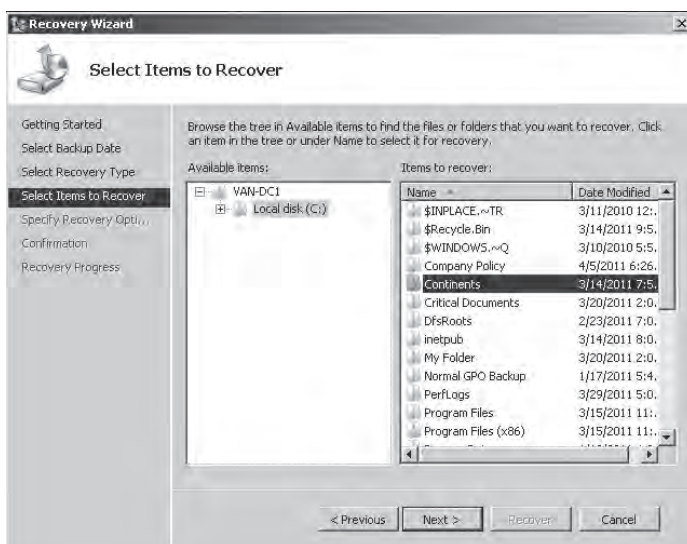


Рис. 13-21. Восстановление папки Континенты

7. На странице **Укажите параметры восстановления** (Specify Recovery Options) в разделе **Конечные объекты восстановления** (Recovery Destination) установите переключатель **Исходное расположение** (Original Location) и убедитесь, что установлен флажок в разделе **Параметры безопасности** (Security Settings) (рис. 13-22).

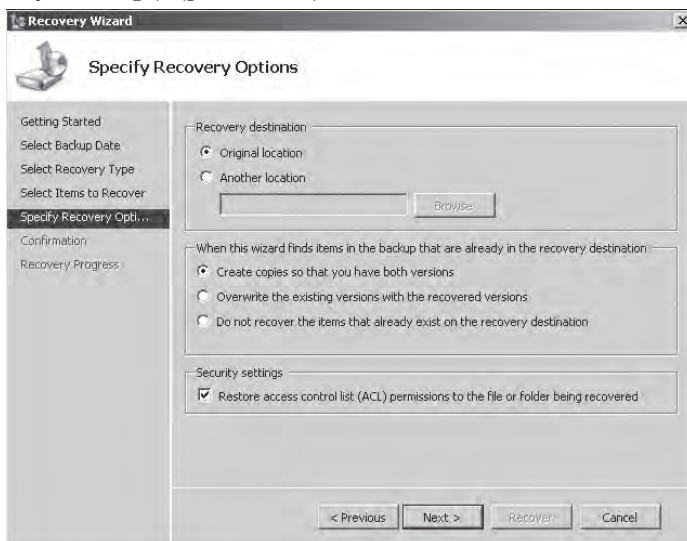


Рис. 13-22. Параметры восстановления

8. На странице подтверждения нажмите кнопку **Восстановить** (Recover). Когда восстановление завершится, щелкните **Заккрыть**.
9. Убедитесь, что папка Континенты восстановилась вместе со всем содержимым.

10. Откройте оснастку **Active Directory — пользователи и компьютеры** из меню **Администрирование**. В меню **Вид (View)** выберите команду **Дополнительные компоненты (Advanced Features)**.
11. Правой кнопкой щелкните подразделение **Planets**. На вкладке **Объект (Object)** снимите флажок **Защитить объект от случайного удаления (Protect Object From Accidental Deletion)** и щелкните **ОК**. Щелкните правой кнопкой подразделение **Planets** и выберите команду **Удалить (Delete)**. Щелкните **Да**, чтобы подтвердить удаление, а затем щелкните **Да**, чтобы подтвердить удаление всех объектов из подразделения **Planets**.
12. Закройте оснастку **Active Directory — пользователи и компьютеры**.

## Упражнение 2. Выполнение принудительного восстановления

В этом упражнении вы используете архив состояния системы контроллера домена VAN-DC1, полученный на предыдущем практикуме, для выполнения принудительного восстановления отдельных объектов в удаленном подразделении Planets. Для этого вам потребуется пароль DSRM. Если вы забыли пароль DSRM, восстановите его, как описано в разделе «Загрузка в режиме восстановления служб каталогов» этого занятия.

1. Если требуется, зайдите на VAN-DC1 под учетной записью Kim Akers. Откройте консоль **Конфигурация системы (System Configuration)** из меню **Администрирование**. Если требуется, щелкните **Да** в диалоговом окне службы контроля учетных записей.
2. На вкладке **Загрузка (Boot)** установите флажок **Безопасный режим (Safe Boot)** и переключатель **Восстановление Active Directory (Active Directory Repair)** (рис. 13-23). Щелкните **ОК**, чтобы закрыть консоль.

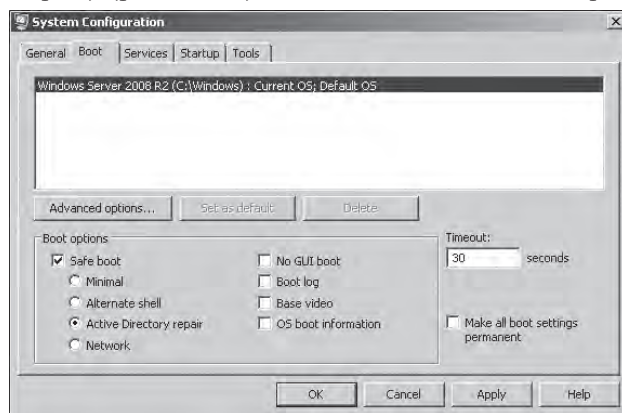


Рис. 13-23. Выбор восстановления Active Directory

3. Когда будет предложено, щелкните **Перезагрузка (Restart)**. Сервер перезагрузится.
4. После перезагрузки зайдите под учетной записью администратора, используя пароль DSRM.

5. Убедитесь, что сервер загрузился в безопасном режиме. Рабочий стол должен иметь черный фон со словами «Безопасный режим» («Safe mode») по углам. Если компьютер не перезагрузился в безопасном режиме, начните упражнение с шага 1.
6. Откройте командную строку с повышенными привилегиями и выполните команду `wbadmin get versions`.
7. Последний архив в списке должен позволять восстановить приложения и состояние системы. Обратите внимание на идентификатор версии (Version Identifier). На рис. 13-24 идентификатор версии архива состояния системы — 03/14/2011-19:57.

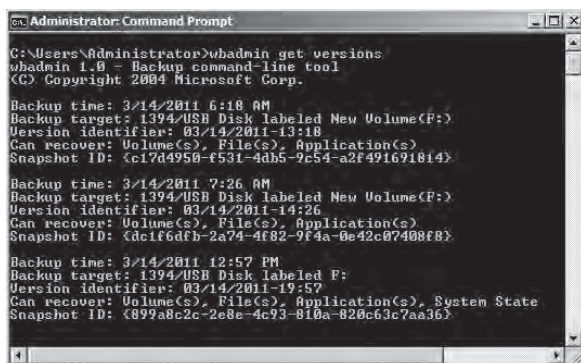


Рис. 13-24. Выяснение идентификатора версии архива

8. Выполните команду `wbadmin Start SystemStateRecovery -version:03/14/2011-19:57 -backupTarget:f:`, заменив идентификатор версии и расположение архива состояния системы своими данными. Когда будет предложено, введите **Y** и нажмите Enter, чтобы начать восстановление состояния системы. Выполните это еще раз, чтобы продолжить.
9. Когда восстановление состояния системы завершится, контроллер домена потребует перезагрузки. Введите **Yes** и нажмите Enter, чтобы перезагрузить сервер.
10. После перезагрузки зайдите с использованием учетной записи администратора и пароля DSRM.
11. Система загрузится в безопасном режиме, и откроется командная строка. Нажмите Enter, чтобы продолжить. Командная строка закроется.
12. Откройте командную строку с повышенными привилегиями. Введите `ntdsutil` и нажмите Enter.
13. Введите **Activate Instance NTDS** и нажмите Enter.
14. Введите **Authoritative Restore** и нажмите Enter.
15. Введите **Restore Object "OU=Planets,dc=adatum,dc=com"** и нажмите Enter. Щелкните **Да**, чтобы подтвердить восстановление. Убедитесь, что утилита `ntdsutil` сообщила об успешном завершении восстановления (рис. 13-25).

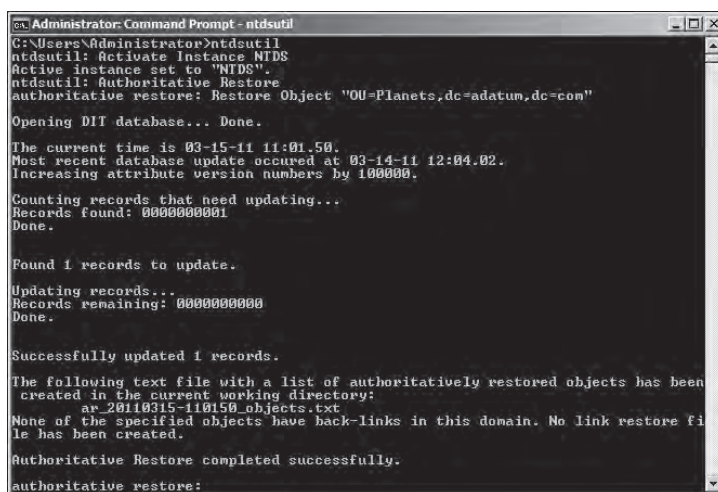


Рис. 13-25. Успешное завершение принудительного восстановления

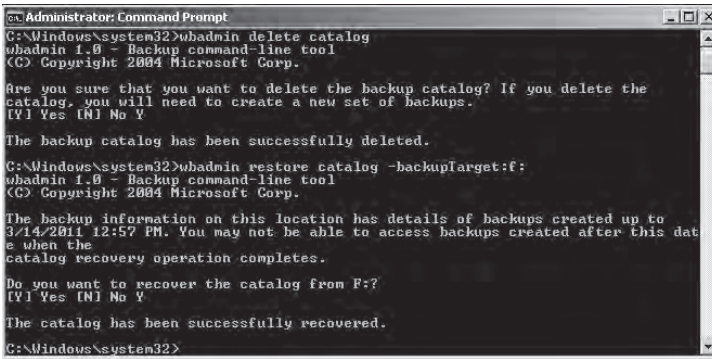
16. Введите `Restore Object "cn=Saturn,OU=Planets,dc=adatum,dc=com"` и нажмите Enter. Введите **Yes**, чтобы подтвердить восстановление.
17. Введите **Quit** два раза, чтобы завершить работу с утилитой ntdsutil. Введите **Exit** и нажмите Enter, чтобы закрыть командную строку.
18. Откройте консоль **Конфигурация системы** (System Configuration) из меню **Администрирование**. На вкладке **Загрузка** (Boot) снимите флажок **Безопасный режим** (Safe boot) и щелкните **ОК**. Когда будет предложено, щелкните **Перезагрузка** (Restart), чтобы перезагрузить сервер. В процессе восстановления сервер может перезагрузиться несколько раз.
19. Когда перезагрузка завершится, зайдите под учетной записью Kim Akers. Нажмите Enter в командной строке, чтобы подтвердить завершение восстановления состояния системы.
20. Откройте оснастку **Active Directory — пользователи и компьютеры**. Убедитесь, что подразделение Planets восстановлено и содержит учетную запись компьютера Saturn.

### Упражнение 3. Восстановление каталога архивов

В этом упражнении вы имитируете процесс удаления поврежденного каталога архивации и восстановите новый каталог из текущего набора архивов.

1. Если требуется, зайдите на VAN-DC1 под учетной записью Kim Akers. Откройте командную строку с повышенными привилегиями. Если будет предложено, щелкните **Да** в диалоговом окне службы контроля учетных записей.
2. Введите `wbadmin delete catalog` и нажмите Enter.
3. Введите **Y** и нажмите Enter, чтобы подтвердить удаление каталога. Введите `wbadmin get versions`, чтобы убедиться, что каталог удален.
4. Выполните команду `wbadmin restore catalog -backupTarget:f`, где f: — том, на котором хранятся архивы.

5. Введите **Y**, чтобы подтвердить восстановление каталога. Командная строка должна выглядеть аналогично рис. 13-26.



```
Administrator: Command Prompt
C:\Windows\system32>wbadmin delete catalog
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2004 Microsoft Corp.

Are you sure that you want to delete the backup catalog? If you delete the
catalog, you will need to create a new set of backups.
[Y] Yes [N] No Y

The backup catalog has been successfully deleted.

C:\Windows\system32>wbadmin restore catalog -backupTarget:f:
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2004 Microsoft Corp.

The backup information on this location has details of backups created up to
3/14/2011 12:57 PM. You may not be able to access backups created after this dat
e when the
catalog recovery operation completes.

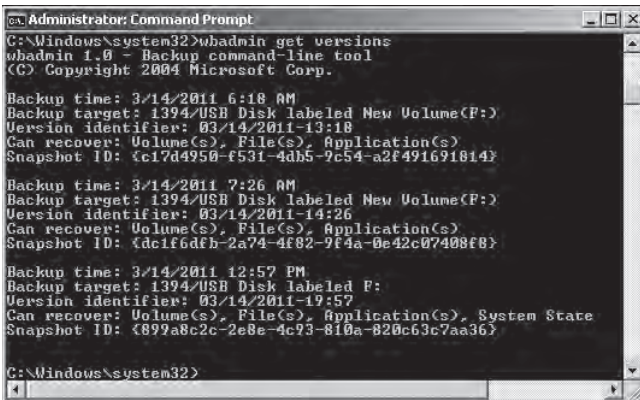
Do you want to recover the catalog from F:?
[Y] Yes [N] No Y

The catalog has been successfully recovered.

C:\Windows\system32>
```

Рис. 13-26. Удаление и восстановление каталога архивации

6. Выполните команду `wbadmin get versions`, чтобы проверить содержимое каталога (рис. 13-27).



```
Administrator: Command Prompt
C:\Windows\system32>wbadmin get versions
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2004 Microsoft Corp.

Backup time: 3/14/2011 6:18 AM
Backup target: 1394/USB Disk labeled New Volume(F:)
Version identifier: 03/14/2011-13:18
Can recover: Volume(s), File(s), Application(s)
Snapshot ID: {c17d4950-f531-4db5-7c54-a2f491691014}

Backup time: 3/14/2011 7:26 AM
Backup target: 1394/USB Disk labeled New Volume(F:)
Version identifier: 03/14/2011-14:26
Can recover: Volume(s), File(s), Application(s)
Snapshot ID: {dc1f6dfb-2a74-4f82-7f4a-0e42c07408f8}

Backup time: 3/14/2011 12:57 PM
Backup target: 1394/USB Disk labeled F:
Version identifier: 03/14/2011-19:57
Can recover: Volume(s), File(s), Application(s), System State
Snapshot ID: {897a8c2c-2e8e-4c73-810a-820c63c7aa36}

C:\Windows\system32>
```

Рис. 13-27. Просмотр восстановленного каталога архивации

## Закрепление материала главы

Чтобы попрактиковаться и закрепить знания, полученные при изучении этой главы, выполните следующее:

- прочитайте резюме главы;
- просмотрите список основных терминов, представленных в этой главе;
- выполните задания лабораторной работы, моделирующей реальные ситуации, требующие применения полученных знаний;
- выполните рекомендуемые упражнения;
- пройдите пробный тест.

## Резюме главы

- Данные, полученные в Windows Server 2008 R2 при выполнении архивации по расписанию, можно записывать на локальные и внутренние диски, тома и в сетевые папки. Данные, полученные при выполнении архивации вручную, можно записывать на внутренние и внешние диски, на DVD и в сетевые папки.
- Утилита командной строки Wbadmin.exe позволяет архивировать и восстанавливать сервер в режиме Server Core и в обычном режиме Windows Server 2008 R2.
- Для выполнения операций восстановления при помощи системы архивации данных Windows Server пользователь должен входить в группу операторов архива или администраторов или иметь соответствующие делегированные полномочия.
- Модуль Active Directory для Windows PowerShell можно использовать для восстановления объектов AD DS.
- Выполняя восстановление операционной системы или полное восстановление сервера на новом жестком диске, необходимо убедиться, что этот диск имеет не меньший объем, чем исходный диск, содержащий архивированные тома.

## Основные термины

Проверьте, знаете ли вы, что означают перечисленные ниже термины из этой главы:

- Принудительное восстановление.
- Автоматическое восстановление.
- Режим восстановления служб каталогов.
- Архив состояния системы.

## Лабораторная работа

Для выполнения заданий лабораторной работы используйте знания о резервном копировании и восстановлении, полученные из этой главы. Ответы можно найти в разделе «Ответы» в конце книги.

### Задание 1. Инфраструктура архивации в компании Wingtip Toys

Вы планируете стратегию архивации для компании Wingtip Toys, которая в скором времени собирается перевести все серверы с Windows 2000 Server на Windows Server 2008 R2. Текущая стратегия разрабатывалась с учетом специализированных средств, и одна из ваших задач — обеспечить согласованность процедур архивации. Учитывая это, ответьте на следующие вопросы:

1. 30 файловых серверов, архивация которых выполняется с использованием NTBackup и ленточных носителей, будут обновлены до Windows Server



2008 R2. Что следует сделать, чтобы ежедневную запланированную архивацию можно было выполнять с использованием системы архивации данных Windows Server?

2. Вы планируете стратегию архивации в удаленном расположении. Архивация будет выполняться при помощи системы архивации данных Windows Server. Какое оборудование следует использовать в этой стратегии?
3. В настоящее время 23% всех задач службы поддержки — восстановление документов, случайно удаленных из общих папок пользователями, работающими над ними. Как можно уменьшить нагрузку на персонал службы поддержки?

## **Задание 2. Аварийное восстановление в компании Fabrikam**

В субботу вечером, в 23:00 главный офис компании Fabrikam был уничтожен пожаром. В этом офисе находились контроллеры корневого домена леса и дочерний домен `hq.fabrikam.internal`. Лес `Fabrikam.internal` включает 15 доменов. В удаленном расположении доступны следующие архивы:

- полные архивы контроллеров корневого домена леса, полученные в пятницу;
- архивы данных состояния системы контроллеров домена `hq.fabrikam.internal`, полученные в среду;
- полные архивы контроллеров домена `hq.fabrikam.internal`, полученные в пятницу;
- полный архив файлового сервера `fileserv.hq.fabrikam.internal`, полученный в среду;
- архив всех общих папок сервера `fileserv.hq.fabrikam.internal`, полученный в пятницу при выполнении архивации вручную.

В четверг вечером из домена `hq.fabrikam.internal` во время обновления ПО были случайно удалены некоторые важные объекты Active Directory, которые были восстановлены в субботу утром до пожара. Сейчас вы находитесь в расположении, предназначенном для аварийного восстановления, и имеете серверы для замены.

- Какие контроллеры домена следует восстановить в первую очередь и почему?
- Что следует сделать, чтобы восстановить объекты, имеющиеся в Active Directory в субботу вечером, в максимально полном составе?
- Что следует сделать, чтобы восстановить файлы из общих папок на сервере `fileserv.hq.fabrikam.internal` в максимально полном составе?

## **Рекомендуемые упражнения**

Чтобы успешно справиться с экзаменационными заданиями по темам этой главы, выполните следующие упражнения.



## Удаленная архивация

- Если в вашей сети установлен рядовой сервер VAN-SRV1, используйте консоль системы архивации данных Windows Server на VAN-DC1 для выполнения полной архивации VAN-SRV1.

## Восстановление сервера

- Загрузите VAN-SRV1 при помощи установочного носителя Windows Server 2008 R2 и выполните полное восстановление сервера. Используйте для этого архив, полученный на первом практикуме.
- Удалите на VAN-DC1 подразделение с учетными записями компьютеров. Используйте модуль Active Directory для Windows PowerShell для восстановления этого подразделения и всех его дочерних объектов.

## Пробный экзамен

Тренировочные тесты на прилагаемом к книге компакт-диске позволяют проверить знания только по одной или сразу по всем темам сертификационного экзамена 70-646. Тестирование можно организовать так, чтобы оно проводилось как настоящий экзамен, а можно проходить в режиме обучения, просматривая правильные ответы и объяснения после каждого ответа.

---

### **ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ** Пробный экзамен

Подробнее о пробном экзамене рассказано во Введении.

---

# П Р И Л О Ж Е Н И Е

## Настройка компьютеров для выполнения упражнений и практикумов

Ниже приведены упражнения, содержащие инструкции по настройке компьютеров VAN-DC1, VAN-SRV1 и VAN-SRV2, используемых для выполнения практических упражнений, приведенных в конце всех глав данного руководства, кроме главы 1. Для выполнения этих упражнений установите Windows Server 2008 R2 Enterprise с конфигурацией по умолчанию, установив для учетной записи администратора пароль **Pa\$\$w0rd**.

### Упражнение 1. Подготовка компьютера для функционирования в качестве контроллера домена

1. Войдите в систему на первом компьютере с Windows Server 2008 R2, используя учетную запись администратора и пароль **Pa\$\$w0rd**.
2. Откройте командную строку с повышенными привилегиями и выполните следующую команду:  
`Netsh interface ipv4 set address «Local Area Connection» static 10.10.0.10`
3. Выполните следующую команду:  
`netdom renamecomputer %computename% /newname:VAN-DC1`
4. Перезагрузите компьютер и снова зайдите под учетной записью администратора.
5. Щелкните **Пуск**. В поле поиска введите **Dcpromo**.
6. Запустится мастер установки доменных служб Active Directory. Два раза щелкните **Далее**.
7. На странице **Выберите конфигурацию развертывания** (Choose A Deployment Configuration) установите переключатель **Создать новый домен в новом лесу** (Create A New Domain In A New Forest) и щелкните **Далее**.

8. На странице **Укажите имя корневого домена леса** (Name The Forest Root Domain) введите **Adatum.com** и щелкните **Далее**.
9. На странице **Режим работы леса** (Forest Functional Level) выберите режим работы леса Windows Server 2008 и щелкните **Далее**.
10. Убедитесь, что на странице **Задайте режим работы домена** (Set Domain Functional Level) выбран режим Windows Server 2008, и щелкните **Далее**.
11. Убедитесь, что на странице **Дополнительные параметры контроллера домена** (Additional Domain Controller Options) выбран DNS-сервер, и щелкните **Далее**. Когда появится предупреждение о том, что делегирование для DNS-сервера не может быть создано, щелкните **Да**, чтобы продолжить работу.
12. Примите предложенные по умолчанию расположения базы данных, файлов журнала и SYSVOL и щелкните **Далее**.
13. В диалоговом окне **Пароль администратора для режима восстановления служб каталогов** (Directory Services Restore Mode Administrator Password) два раза введите пароль **Pa\$\$w0rd** и щелкните **Далее**.
14. На странице со сводными данными щелкните **Далее**, чтобы начать установку доменных служб Active Directory (AD DS) на компьютере VAN-DC1. Когда мастер завершит работу, щелкните **Готово**. Когда будет предложено, перезагрузите компьютер.

## Упражнение 2. Подготовка AD DS

1. Зайдите на сервер VAN-DC1 под учетной записью администратора.
2. Используя оснастку **Active Directory — пользователи и компьютеры**, создайте учетную запись Kim\_Akers в контейнере **Пользователи** (Users) и назначьте ей пароль **Pa\$\$w0rd**. Укажите, что срок действия пароля никогда не истекает. Добавьте эту учетную запись в группы администраторов предприятия, администраторов домена и администраторов схемы.
3. Откройте консоль DNS и создайте основную зону обратного просмотра для подсети 10.10.0.x. Убедитесь, что эта зона хранится в AD DS и реплицируется на все DNS-серверы, работающие на контроллерах домена в лесу.

## Упражнение 3. Подготовка рядового сервера и его включение в домен

1. Убедитесь, что компьютер VAN-DC1 включен и подключен к сети или виртуальной сети, к которой подключен второй компьютер.
2. Зайдите в систему на втором компьютере с Windows Server 2008 R2, используя учетную запись администратора и пароль **Pa\$\$w0rd**.
3. Откройте командную строку с повышенными привилегиями и выполните следующие команды:

```
Netsh interface ipv4 set address «Local Area Connection» static 10.10.0.20
Netsh interface ipv4 set dnsservers «Local Area Connection» static
10.10.0.10 primary
```

4. Выполните следующую команду:  
`netdom renamecomputer %computername% /newname:VAN-SRV1`
5. Перезагрузите компьютер и снова зайдите под учетной записью администратора.
6. В командной строке с повышенными привилегиями выполните следующую команду:  
`netdom join VAN-SRV1 /domain:adatum`
7. Перезагрузите компьютер. Зайдите в систему под учетной записью `adatum\Administrator` и выключите компьютер.

## Упражнение 4. Подготовка второго рядового сервера и его включение в домен

1. Убедитесь, что компьютер VAN-DC1 включен и подключен к сети или виртуальной сети, к которой подключен второй компьютер.
2. Зайдите в систему на третьем компьютере с Windows Server 2008 R2, используя учетную запись администратора и пароль **Pa\$\$w0rd**.
3. Откройте командную строку с повышенными привилегиями и выполните следующие команды:  
`Netsh interface ipv4 set address «Local Area Connection» static 10.10.0.21`  
`Netsh interface ipv4 set dnsservers «Local Area Connection» static 10.10.0.10 primary`
4. Выполните следующую команду:  
`netdom renamecomputer %computername% /newname:VAN-SRV2`
5. Перезагрузите компьютер и снова зайдите под учетной записью администратора.
6. В командной строке с повышенными привилегиями выполните следующую команду:  
`netdom join VAN-SRV2 /domain:adatum`
7. Перезагрузите компьютер. Зайдите в систему под учетной записью `adatum\Administrator` и выключите компьютер.

## Упражнение 5. Настройка клиентского компьютера

1. Убедитесь, что компьютер VAN-DC1 включен и подключен к сети или виртуальной сети, к которой подключен второй компьютер.
2. Зайдите в систему на первом компьютере, куда установили Windows 7 Enterprise или Ultimate, используя учетную запись администратора и пароль **Pa\$\$w0rd**.
3. Откройте командную строку с повышенными привилегиями и выполните следующие команды:

```
Netsh interface ipv4 set address «Local Area Connection» static 10.10.0.31
Netsh interface ipv4 set dnsservers «Local Area Connection» static
10.10.0.10 primary
```

4. Нажмите Windows+Break, чтобы открыть диалоговое окно свойств системы. Щелкните ссылку **Дополнительные параметры системы** (Advanced System Settings). На вкладке **Имя компьютера** (Computer Name) нажмите кнопку **Изменить** (Change). В поле **Имя компьютера** (Computer Name) введите VAN-CL1 и щелкните **ОК**.
5. Перезагрузите компьютер и снова зайдите под учетной записью администратора.
6. Нажмите Windows+Break, чтобы открыть диалоговое окно свойств системы. Щелкните ссылку **Дополнительные параметры системы** (Advanced System Settings). На вкладке **Имя компьютера** (Computer Name) нажмите кнопку **Изменить** (Change). В поле **домена** (Domain) введите ADATUM. Когда будет предложено, введите учетные данные администратора домена.
7. Перезагрузите компьютер и снова зайдите под учетной записью администратора.
8. В панели управления щелкните **Настройка общего доступа к файлам** (Set Up File Sharing). Убедитесь, что в Центре управления сетями и общим доступом настроена частная сеть и включен общий доступ к файлам.

# Ответы

## Глава 1

### Занятие 1

1. **Правильный ответ: С.**

- a. **Неправильный.** До Windows Server 2008 R2 Datacenter Edition можно обновить только Windows Server 2003 Datacenter Edition (x64).
- b. **Неправильный.** До Windows Server 2008 R2 можно обновить только Windows Server 2003 Web Server Edition.
- c. **Правильный.** Windows Server 2003 R2 Standard Edition можно обновить до Windows Server 2008 R2 Enterprise Edition, если это версия для архитектуры x64.
- d. **Неправильный.** Windows Server 2003 R2 Standard Edition (x64) нельзя обновить до Windows Server 2008 (x86) Standard Edition.
- e. **Неправильный.** Хотя Windows Server 2003 R2 Standard Edition (x64) можно обновить до Windows Server 2008 R2 Standard Edition, невозможно обновить любую версию Windows Server 2003 до Windows Server 2008 R2 в режиме Server Core.

2. **Правильный ответ: А.**

- a. **Правильный.** 32-разрядную версию Windows Server 2003 Standard Edition можно обновить только до 32-разрядной версии Windows Server 2008 Standard или Enterprise Edition.
- b. **Неправильный.** Невозможно обновить 32-разрядную версию Windows Server 2003 до Windows Server 2008 R2.
- c. **Неправильный.** Невозможно обновить 32-разрядную версию Windows Server 2003 до Windows Server 2008 Datacenter.
- d. **Неправильный.** Невозможно обновить 32-разрядную версию Windows Server 2003 до Windows Server 2008 R2.

3. **Правильный ответ: А.**

- a. **Правильный.** Компьютер с Windows Server 2008 R2 Enterprise в режиме Server Core можно настроить в качестве контроллера домена.
- b. **Неправильный.** На компьютере с Windows Server 2008 R2 Enterprise в режиме Server Core нельзя настроить роль службы управления правами Active Directory.

- c. **Неправильный.** На компьютере с Windows Server 2008 R2 Enterprise в режиме Server Core нельзя настроить роль служб федерации Active Directory.
  - d. **Неправильный.** На компьютере с Windows Server 2008 R2 Enterprise в режиме Server Core нельзя настроить роль служб WDS.
4. **Правильный ответ: С.**
- a. **Неправильный.** Windows Server 2008 R2 Enterprise Edition имеет четыре лицензии на виртуальные машины.
  - b. **Неправильный.** Windows Server 2008 R2 Enterprise Edition имеет четыре лицензии на виртуальные машины.
  - c. **Правильный.** Windows Server 2008 R2 Enterprise Edition имеет четыре лицензии на виртуальные машины.
  - d. **Неправильный.** Windows Server 2008 R2 Enterprise Edition имеет четыре лицензии на виртуальные машины.
5. **Правильный ответ: С.**
- a. **Неправильный.** Отказоустойчивые кластеры поддерживаются только в Windows Server 2008 R2 Enterprise и Datacenter.
  - b. **Неправильный.** Отказоустойчивые кластеры поддерживаются только в Windows Server 2008 R2 Enterprise и Datacenter.
  - c. **Правильный.** Отказоустойчивые кластеры поддерживаются только в Windows Server 2008 R2 Enterprise и Datacenter.
  - d. **Неправильный.** Отказоустойчивые кластеры поддерживаются только в Windows Server 2008 R2 Enterprise и Datacenter.

## Занятие 2

1. **Правильные ответы: А, В и С.**
- a. **Правильный.** Компьютер с Windows Server 2008 R2 должен входить в существующий домен AD DS, чтобы можно было развернуть WDS.
  - b. **Правильный.** Для корректного функционирования WDS в домене AD DS необходим авторизованный сервер DHCP.
  - c. **Правильный.** Для корректного функционирования WDS необходим корректно настроенный DNS-сервер.
  - d. **Неправильный.** Службы WDS не зависят от роли сервера приложений.
2. **Правильный ответ: А.**
- a. **Правильный.** Несопровождаемую установку можно инициировать из среды Windows PE.
  - b. **Неправильный.** Несопровождаемую установку нельзя инициировать с загрузочного диска Windows NT.
  - c. **Неправильный.** Несопровождаемую установку нельзя инициировать с загрузочного диска MS-DOS.
  - d. **Неправильный.** Несопровождаемую установку можно выполнить только в среде Windows PE 2.0 или в Windows Server 2003.



3. **Правильный ответ: А.**

- a. **Правильный.** При совмещении ролей DHCP и WDS необходимо убедиться, что сервер WDS не прослушивает порт 67, а DHCP-параметр 60 имеет значение PXEClient. Это выполняется на вкладке **Параметры DHCP** (DHCP Settings) диалогового окна свойств сервера WDS.
- b. **Неправильный.** В консоли DHCP-сервера нельзя настроить WDS на прослушивание альтернативного порта. По умолчанию серверы DHCP и PXE прослушивают один порт, поэтому если обе службы находятся на одном сервере, необходимо настроить сервер WDS, чтобы он прослушивал другой порт, и обновить DHCP, чтобы проинформировать клиентов PXE о том, что они должны обращаться к другому порту, настроив DHCP-параметр 60 (это можно сделать в диалоговом окне свойств сервера WDS).
- c. **Неправильный.** Проблема не в DNS-сервере, а в конфликте между серверами DHCP и WDS.
- d. **Неправильный.** Параметры клиента используются для настройки параметров несопровождаемой установки. В данном случае проблема в том, что сервер WDS не может прослушивать порт, который уже прослушивается DHCP-сервером, и должен быть настроен на прослушивание другого порта.

4. **Правильный ответ: D.**

- a. **Неправильный.** Для поддержки WDS не требуется изменять параметры DNS.
- b. **Неправильный.** Настраивать специальную DHCP-область IPv6 для клиентов PXE не обязательно.
- c. **Неправильный.** Настраивать специальную DHCP-область IPv4 для клиентов PXE не обязательно.
- d. **Правильный.** Для использования многоадресной передачи в WDS необходимы маршрутизаторы с поддержкой многоадресной передачи. В вопросе сказано, что сервер WDS и клиенты находятся в разных подсетях, что указывает на возможную проблему с маршрутизатором.

5. **Правильный ответ: С.**

- a. **Неправильный.** Хотя помещение файла несопровождаемой установки в сетевую папку — рабочий вариант, это потребует значительных трудозатрат, так как серверы потребуется загрузить в Windows PE.
- b. **Неправильный.** Параметры несопровождаемой установки настраиваются в файлах ответов, а не в свойствах многоадресной передачи.
- c. **Правильный.** Файл ответов для несопровождаемой установки можно настроить на сервере WDS.
- d. **Неправильный.** Хотя помещение файла несопровождаемой установки на съемном USB-носителе — рабочий вариант, это потребует гораздо больше трудозатрат, чем помещение такого файла на сервер WDS.

## Глава 1. Лабораторная работа

### Задание 1

1. Так как невозможно обновить систему до Windows Server 2008 R2 в режиме Server Core, придется создать резервную копию данных, выполнить чистую установку на существующее оборудование, а затем восстановить данные.
2. Если сервер будет только поддерживать веб-сайт компании, подойдет Windows Web Server 2008 R2.
3. Следует развертывать Windows Server 2008 R2 Datacenter Edition, так как эта версия имеет неограниченное число лицензий на виртуальные машины.

### Задание 2

1. Важно проверить, поддерживают ли старые маршрутизаторы многоадресную передачу.
2. При установке WDS необходимо запретить серверу WDS прослушивать порт 67 и убедиться, что для всех DHCP-областей настроен параметр 60.
3. Создать многоадресную передачу, которая будет начинаться после подключения 10 клиентов к серверу WDS.

## Глава 2

### Занятие 1

1. **Правильный ответ: В.**
  - a. **Неправильный.** Адреса локального сайта IPv6 указывают узел в пределах сайта или интрасети. Это эквивалент частных адресов IPv4, таких как 10.0.0.1.
  - b. **Правильный.** Глобальный адрес одноадресной рассылки IPv6 (или комбинированный глобальный адрес одноадресной рассылки) является эквивалентом открытого адреса одноадресной рассылки IPv4. Такие адреса глобально маршрутизируемы и доступны в Интернете IPv6.
  - c. **Неправильный.** Адреса локальной связи IPv6 автоматически конфигурируются в локальной подсети. Это эквивалент адресов APIPA IPv4, таких как 169.254.10.123.
  - d. **Неправильный.** Существует два специальных адреса IPv6. Неопределенный адрес :: указывает на отсутствие адреса и является эквивалентом неопределенного адреса IPv4 0.0.0.0. Адрес замыкания на себя ::1 указывает интерфейс замыкания на себя и эквивалентен адресу IPv4 замыкания на себя 127.0.0.1. Ни один из этих адресов не эквивалентен открытому адресу одноадресной рассылки IPv4.
2. **Правильный ответ: А.**
  - a. **Правильный.** Адрес запроса узла состоит из 104-разрядного префикса ff02::1:ff (записывается ff02::1:ff00:0/104), за которым идут последние 24 бита адреса локальной связи; в данном случае — a7:d43a.

- b. **Неправильный.** Хотя 104-разрядный префикс записывается в виде ff02::1:ff00:0/104, часть /104 указывает, что используются только первые 104 бита (ff02::1:ff). Следовательно, адресом запроса узла будет ff02::1:ffa7:d43a.
  - c. **Неправильный.** Адреса, начинающиеся с fec0, являются адресами локального сайта, а не адресами запроса узла.
  - d. **Неправильный.** Адреса, начинающиеся с fec0, являются адресами локального сайта, а не адресами запроса узла.
3. **Правильный ответ: D.**
- a. **Неправильный.** ARP — протокол, использующий широковещательные рассылки для разрешения MAC-адресов в адреса IPv4. Сообщения ICMPv6 используются протоколом ND для управления взаимодействием соседних узлов.
  - b. **Неправильный.** EUI-64 — не протокол, а стандарт для 64-разрядных аппаратных адресов.
  - c. **Неправильный.** DHCPv6 используется для настройки адресов IPv6 с ведением базы данных. Сообщения ICMPv6 используются протоколом ND для управления взаимодействием соседних узлов.
  - d. **Правильный.** Сообщения ICMPv6 используются протоколом ND для управления взаимодействием соседних узлов.
4. **Правильный ответ: A.**
- a. **Правильный.** При использовании настроенного туннелирования данные передаются по предварительно настроенному туннелю с использованием инкапсуляции. Пакет IPv6 передается внутри пакета IPv4. В точке входа в туннель создается инкапсулирующий заголовок IPv4, удаляющийся в точке выхода. Адреса конечных точек туннеля определяются по данным конфигурации.
  - b. **Неправильный.** Использование двух стеков требует, чтобы хосты и маршрутизаторы предоставляли поддержку обоих протоколов и могли отправлять пакеты IPv4 и IPv6. Туннелирование не требуется.
  - c. **Неправильный.** ISATAP соединяет хосты и маршрутизаторы IPv6 по сети, работающей на основе протокола IPv4, используя процесс, рассматривающий сеть IPv4 как канальный уровень для сети IPv6, а остальные узлы — как потенциальные хосты или маршрутизаторы IPv6. При этом автоматически создаются туннели хост-хост, хост-маршрутизатор и маршрутизатор-хост. Предварительная настройка туннелей не требуется.
  - d. **Неправильный.** Teredo — усовершенствование метода 6to4, позволяющее узлам, расположенным за устройством IPv4 NAT, использовать протокол IPv6 посредством туннелирования пакетов с помощью UDP. Teredo требует использования серверных и ретранслирующих элементов для соединения путей. Предварительно настроенные туннели не требуются.
5. **Правильный ответ: D.**
- a. **Неправильный.** Эта команда показывает конфигурацию IPv6 на всех интерфейсах. Она не позволяет вручную настраивать адреса IPv6.
  - b. **Неправильный.** Эта команда используется для добавления адреса IPv6 DNS-сервера в конфигурацию IPv6, но не для настройки адреса IPv6

вручную. Для настройки адреса IPv6 вручную используется команда `interface ipv6 set address`.

- c. **Неправильный.** Эта команда позволяет изменять свойства интерфейса IPv6, но не адрес IPv6. Для настройки адреса IPv6 вручную используется команда `interface ipv6 set address`.
- d. **Правильный.** Эта команда используется для настройки адреса IPv6 вручную.

6. **Правильные ответы: А, D, F, G.**

- a. **Правильный.** Провайдер и оборудование компании поддерживает и IPv4, и IPv6. Использование двух стеков — самая простая стратегия перехода.
- b. **Неправильный.** Инкапсуляция пакетов IPv6 в пакеты IPv4 не требуется. Настроенное туннелирование обычно используется, если протокол IPv6 недоступен.
- c. **Неправильный.** У компании не было необходимости в настройке NAT и использовании частных адресов IPv4. Вряд ли будут использоваться адреса локального сайта, являющиеся эквивалентом частных адресов.
- d. **Правильный.** В сети используются открытые адреса IPv4, поэтому в сети IPv6, скорее всего, будут использоваться глобальные адреса одноадресной рассылки.
- e. **Неправильный.** Клиенты работают под управлением Windows 7 Enterprise Edition, а серверы — под управлением Windows Server 2008 R2 Enterprise Edition. Все клиенты и серверы поддерживают протокол IPv6, устанавливаемый по умолчанию.
- f. **Правильный.** Нет гарантии, что сетевые проекторы и принтеры поддерживают IPv6, хотя они, скорее всего, поддерживают, так как компания предпочитает передовые технологии.
- g. **Правильный.** Следует проверить совместимость системы управления сетью и IPv6.
- h. **Неправильный.** Высокоуровневые приложения обычно не зависят от используемого протокола Интернета.

## Занятие 2

1. **Правильный ответ: В.**

- a. **Неправильный.** Зона интегрирована с AD DS, поэтому следует использовать параметр `/DsPrimary`. Для DNS с файловой поддержкой используется параметр `/Primary` и указывается имя файла.
- b. **Правильный.** Эта команда создает зону требуемого типа, префикс адреса указан правильно.
- c. **Неправильный.** Обозначение `in-addr.darpa` используется для зон обратного просмотра IPv4. Кроме того, тип зоны указан неправильно.
- d. **Неправильный.** Префикс адреса указывается 4-битными фрагментами в обратном порядке. Синтаксис команды `dnscmd` не допускает использования записи с разделением косой чертой.

2. **Правильный ответ: А.**

- a. **Правильный.** Нельзя получить список записей DNS при помощи команды nslookup, если не разрешить передачи зон, даже если записи находятся на том же компьютере.
- b. **Неправильный.** От имени администратора командную строку необходимо запускать для использования команд настройки, таких как dnscmd. Этого не требуется, если команда выводит информацию, ничего не изменяя.
- c. **Неправильный.** Можно ввести в командной строке nslookup ls -d adatum.internal, а можно ввести команду nslookup, а затем в приглашении nslookup> ввести ls -d adatum.internal.
- d. **Неправильный.** Большинство операций, включая nslookup, можно выполнять на сервере, выполнив вход через удаленный рабочий стол. Войти на серверы интерактивно не рекомендуется.

3. **Правильный ответ: D.**

- a. **Неправильный.** Проблем с записью хоста для веб-сервера нет. Другие пользователи могут обращаться к внутреннему веб-сайту.
- b. **Неправильный.** Нет необходимости очищать кэш DNS на DNS-сервере. Источник проблемы на клиентском компьютере.
- c. **Неправильный.** Клиентский компьютер зарегистрирован в DNS и может обращаться к другим веб-сайтам.
- d. **Правильный.** В кэше DNS на клиентском компьютере адрес URL веб-сайта помечен как неразрешаемый. Очистка кэша DNS решит проблему.

4. **Правильный ответ: В.**

- a. **Неправильный.** В централизованной топологии WINS используется одиночный централизованный высокодоступный сервер или кластер WINS.
- b. **Правильный.** Топология с полным сцеплением имеет распределенную структуру с несколькими серверами или кластерами WINS. Каждый сервер или кластер выполняет репликацию с каждым другим сервером или кластером.
- c. **Неправильный.** Кольцевая топология имеет распределенную структуру, в которой каждый сервер WINS имеет одного партнера по репликации, создавая круг.
- d. **Неправильный.** Центральная-лучевая топология имеет распределенную структуру, в которой один сервер WINS назначен главным, а остальные серверы выполняют репликацию только с центральным сервером из своего сайта.

## Глава 2. Лабораторная работа

### Задание 1

- 1. Адреса IPv6 локального сайта являются прямым эквивалентом частных адресов IPv4 и маршрутизируются между виртуальными сетями. Такие адреса можно использовать, но они устарели, поэтому следует дать каждому

устройству в сети комбинируемый глобальный адрес IPv6 для одноадресной рассылки. Технологии NAT и CIDR решали проблему недостатка адресов IPv4, а протокол IPv6 не имеет такой проблемы. В описанной ситуации нельзя использовать только адреса локальной связи IPv6, так как они не маршрутизируются.

2. Доступны оба стека: IPv4 и IPv6. В этом случае самой простой стратегией перехода будет использование двух стеков.
3. Как и в случае с DHCP для IPv4, следует настроить в каждой подсети сервер DHCPv6 с двумя областями. Область для локальной подсети на каждом сервере должна включать 80% всего диапазона адресов IPv6, используемых в подсети. Область для удаленной подсети на каждом сервере должна включать оставшиеся 20% адресов.

## Задание 2

1. Можно настроить безопасные динамические обновления. При этом только аутентифицированные пользователи и клиенты смогут регистрировать информацию в DNS.
2. Репликацию зон можно настроить так, чтобы она выполнялась только между DNS-серверами, имеющими запись NS и входящими в список серверов имен. Можно также указать список серверов и настроить репликацию зон вручную, чтобы зона реплицировалась только на эти серверы.
3. Если сервер Windows Server 2008 R2 настроен как контроллер домена только для чтения, он реплицирует доступную только для чтения копию всех разделов AD DS, используемых DNS, включая раздел каталога домена, ForestDNSZones и DomainDNSZones. Следовательно, информация зон DNS автоматически обновляется на контроллере домена только для чтения.
4. Создать зону обратного просмотра IPv6.

## Глава 3

### Занятие 1

1. **Правильные ответы: В, Е, F и H.**
  - a. **Неправильный.** Необходимо установить функциональный уровень леса Windows Server 2008 R2. Следовательно, вы должны установить во всех трех доменах функциональный уровень Windows Server 2008 R2. Для этого все контроллеры доменов во всех доменах должны работать под управлением Windows Server 2008 R2.
  - b. **Правильный.** Все контроллеры доменов во всех доменах должны работать под управлением Windows Server 2008 R2. Это позволит поднять функциональный уровень доменов до Windows Server 2008 R2, что, в свою очередь, позволяет поднять функциональный уровень леса до Windows Server 2008 R2.
  - c. **Неправильный.** Необходимо установить функциональный уровень леса

Windows Server 2008 R2. Следовательно, вы должны установить во всех трех доменах функциональный уровень Windows Server 2008 R2. Для этого все контроллеры доменов во всех доменах должны работать под управлением Windows Server 2008 R2.

- d. **Неправильный.** Необходимо установить функциональный уровень леса Windows Server 2008 R2. Следовательно, вы должны установить во всех трех доменах функциональный уровень Windows Server 2008 R2.
- e. **Правильный.** Установка во всех трех доменах функционального уровня Windows Server 2008 R2 позволяет повысить функциональный уровень леса до Windows Server 2008 R2.
- f. **Правильный.** Необходимо повысить функциональный уровень леса до Windows Server 2008 R2 на сервере глобального каталога в корневом домене.
- g. **Неправильный.** Повысить функциональный уровень леса до Windows Server 2008 R2 можно только один раз.
- h. **Правильный.** Установив функциональный уровень леса Windows Server 2008 R2, можно использовать командлет Enable-ADOptionalFeature для включения Корзины Active Directory.
- i. **Неправильный.** Командлет Enable-ADAccount используется для включения учетной записи Active Directory. С его помощью нельзя включить Корзину Active Directory.
- j. **Неправильный.** Когда Корзина Active Directory включена, каждый контроллер домена, не являющийся сервером глобального каталога, действует как хозяин инфраструктуры, в результате чего размещение IM FSMO не имеет значения.

## 2. Правильные ответы: А и В.

- a. **Правильный.** Обычно PSO применяется к глобальной группе безопасности.
- b. **Правильный.** PSO можно применять к доменной учетной записи пользователя, хотя лучше применять его к глобальной группе безопасности, в которую помещать учетные записи пользователей.
- c. **Неправильный.** Нельзя применить PSO непосредственно к подразделению. Если требуется применить PSO к пользователям из подразделения, нужно создать специальную группу — глобальную группу безопасности, содержащую всех пользователей из этого подразделения.
- d. **Неправильный.** Глобальные группы рассылки используются для создания почтовых списков для Exchange Server. Нельзя связать PSO с глобальной группой рассылки.
- e. **Неправильный.** Нельзя связать PSO с учетной записью компьютера.

## 3. Правильный ответ: С.

- a. **Неправильный.** Список SACL объекта позволяет указывать, для каких операций AD DS должен выполняться аудит. SACL — не утилита и не позволяет просматривать данные Active Directory, хранящиеся в моментальных снимках.



- b. **Неправильный.** Объект **PSC** по умолчанию создается в контейнере **Система** в домене и хранит объекты **PSO** для этого домена. **PSC** — не утилита и не позволяет просматривать данные **Active Directory**, хранящиеся в моментальных снимках.
  - c. **Правильный.** Средство интеллектуального анализа данных **AD DS** позволяет просматривать данные **Active Directory**, хранящиеся в моментальных снимках онлайн, сравнивать данные из моментальных снимков, полученных в разное время, и определять, какие данные следует восстановить, не перезагружая контроллер домена.
  - d. **Неправильный.** Мастер установки **AD DS** позволяет указать, какой контроллер домена устанавливается: с возможностью записи или только для чтения. Его нельзя использовать для просмотра данных **Active Directory**, хранящихся в моментальных снимках.
4. **Правильный ответ: В.**
- a. **Неправильный.** Доверие лесов устанавливается между лесами. **Windows NT 4** не использует концепцию лесов.
  - b. **Правильный.** Внешнее доверие используется для переноса ресурсов из доменов **Windows NT**. **Windows NT** не использует концепцию лесов; домен **Windows NT** — самодостаточная автономная единица. Когда требуется перенести ресурсы из домена **Windows NT** в существующий лес **Active Directory**, используется внешнее доверие.
  - c. **Неправильный.** Доверие к сфере используется для доступа к ресурсам из сферы **UNIX**. Для переноса ресурсов из домена **Windows NT** в лес **Active Directory** доверие к сфере не используется.
  - d. **Неправильный.** Если пользователям из одного дочернего домена часто требуется доступ к ресурсам из дочернего домена другого леса, можно создать сокращенное доверие между этими двумя доменами. Сокращенное доверие не используется для переноса ресурсов из домена **Windows NT** в лес **Active Directory**.
5. **Правильный ответ: D.**
- a. **Неправильный.** Чтобы настроить политику репликации паролей, следует подключить оснастку **Active Directory — пользователи и компьютеры** к контроллеру домена с возможностью записи, а не к контроллеру домена только для чтения. Коллега из филиала не имеет прав для настройки этой политики.
  - b. **Неправильный.** Политику репликации паролей нельзя настроить в Диспетчере сервера. Кроме того, не следует добавлять пользователей, не имеющих соответствующих знаний, в группу администраторов домена.
  - c. **Неправильный.** Политику репликации паролей нельзя настроить в Диспетчере сервера.
  - d. **Правильный.** Администратор домена может настроить политику репликации паролей, открыв оснастку **Active Directory — пользователи и компьютеры** и подключив ее к контроллеру домена с возможностью записи.

6. **Правильный ответ: С.**

- a. **Неправильный.** Функциональный уровень леса Windows 2000 не поддерживает доверие лесов.
- b. **Неправильный.** Смешанный режим Windows 2000 — функциональный уровень домена, а не леса, и не поддерживает доверие лесов.
- c. **Правильный.** Функциональный уровень леса Windows Server 2003 поддерживает доверие лесов.
- d. **Неправильный.** Функциональный уровень леса Windows Server 2008 поддерживает доверие лесов, но минимальный функциональный уровень леса, поддерживающий доверие лесов — Windows Server 2003.
- e. **Неправильный.** Функциональный уровень леса Windows Server 2008 R2 поддерживает доверие лесов, но минимальный функциональный уровень леса, поддерживающий доверие лесов — Windows Server 2003.

7. **Правильный ответ: С.**

- a. **Неправильный.** Функциональный уровень домена Windows Server 2008 R2 поддерживает Netdom.exe, но не поддерживает контроллеры домена, работающие под управлением Windows Server 2003 и Windows Server 2008.
- b. **Неправильный.** Функциональный уровень домена Windows Server 2008 поддерживает Netdom.exe, но не поддерживает контроллеры домена, работающие под управлением Windows Server 2003.
- c. **Правильный.** Функциональный уровень домена Windows Server 2003 поддерживает Netdom.exe и контроллеры домена, работающие под управлением Windows Server 2003, Windows Server 2008 и Windows Server 2008 R2.
- d. **Неправильный.** Функциональный уровень домена Windows Server 2000 не поддерживает Netdom.exe.
- e. **Неправильный.** Домены, работающие в смешанном режиме Windows 2000, не могут включать контроллеры домена Windows Server 2008 и Windows Server 2008 R2, и не поддерживают Netdom.exe.

## Занятие 2

1. **Правильный ответ: В.**

- a. **Неправильный.** Корневой ЦС предприятия развертывать не следует, так как в вопросе указано, что таковой уже развернут.
- b. **Правильный.** В вопросе сказано, что в головном офисе уже есть ЦС предприятия, поэтому развертывать следует подчиненный ЦС предприятия.
- c. **Неправильный.** В вопросе говорится о поддержке политик авторегистрации, поэтому необходим подчиненный ЦС предприятия.
- d. **Неправильный.** В вопросе говорится о поддержке политик авторегистрации, поэтому необходим подчиненный ЦС предприятия.

2. **Правильные ответы: А и В.**

- a. **Правильный.** Для развертывания авторегистрации необходимо включить ее в Active Directory.

- b. **Правильный.** Прежде чем можно будет автоматически регистрировать сертификаты, необходимо применить к шаблонам сертификатов разрешения авторегистрации.
  - c. **Неправильный.** Для поддержки авторегистрации не требуется изменять параметры CRL, установленные по умолчанию.
  - d. **Неправильный.** Сетевой ответчик не обязателен для развертывания авторегистрации.
  - e. **Неправильный.** Регистрация сертификатов через Интернет не требуется для развертывания авторегистрации.
3. **Правильные ответы: В, С и D.**
- a. **Неправильный.** Сертификат подписи OCSP нужно установить на сетевом ответчике, а не в ЦС.
  - b. **Правильный.** Необходимо настроить шаблон сертификатов подписи ответа OCSP в ЦС.
  - c. **Правильный.** Необходимо установить сертификат подписи ответа OCSP на сервере, который будет функционировать как сетевой ответчик.
  - d. **Правильный.** Необходимо настроить в ЦС расширение AIA с URL-адресом сетевого ответчика.
  - e. **Неправильный.** В ЦС необходимо настроить расширение AIA с URL-адресом сетевого ответчика, а не центра сертификации.
4. **Правильный ответ: D.**
- a. **Неправильный.** Установка подчиненного ЦС предприятия в офисе филиала не решит проблем, связанных с проверкой отозванных сертификатов, выполняющейся по WAN-связи.
  - b. **Неправильный.** Хотя можно публиковать данные CRL в альтернативные расположения, например, в общую папку на сервере в офисе филиала, по умолчанию подчиненный ЦС предприятия не хранит информацию из списков CRL для сертификатов, выданных ЦС, стоящими выше в иерархии PKI. С этой задачей лучше всего справятся сетевые ответчики.
  - c. **Неправильный.** Автономные подчиненные ЦС не помогут в проверке сертификатов, выданных корневым ЦС предприятия.
  - d. **Правильный.** Сетевые ответчики могут ускорить проверку сертификатов, так как хранят копию CRL и могут отвечать на запросы о состоянии отдельных сертификатов. Размещение сетевого ответчика в дополнительном офисе уменьшит трафик, проходящий через канал WAN.
5. **Правильный ответ: С.**
- a. **Неправильный.** Консоль **Центр сертификации** позволяет просматривать состояние одного активного ЦС. Для одновременного просмотра состояния всех ЦС в лесу Active Directory можно использовать оснастку **PKI предприятия**.
  - b. **Неправильный.** Эта консоль используется для управления сетевыми ответчиками. Хотя ее можно использовать для управления массивами сетевых ответчиков, сетевые ответчики не должны устанавливаться на серверы, функционирующие как центры сертификации.

- с. **Правильный.** Оснастку **РКІ предприятия** можно использовать для просмотра состояния окружения РКІ, включая все иерархии ЦС, существующие в лесу Active Directory.
- d. **Неправильный.** Оснастка **Сертификаты** позволяет просматривать сертификаты пользователей, компьютеров и служб. Ее нельзя использовать для просмотра состояния центров сертификации.

## Глава 3. Лабораторная работа

### Задание 1

1. В Windows Server 2008 появились детальные политики паролей, позволяющие назначать пользователям и группам безопасности параметры, отличные от используемых по умолчанию. Эта возможность есть и в Windows Server 2008 R2. В доменах Windows Server 2003 для применения разных политик паролей требуется создавать отдельные домены.
2. Во время этого обновления нет необходимости повышать функциональный уровень леса до Windows Server 2008 R2, поскольку функциональный уровень леса Windows Server 2003 поддерживает все новые функции. Конечный план заключается в повышении функционального уровня леса до Windows Server 2008 R2 для получения возможности использовать детальные политики паролей и Корзину Active Directory, но для этого все контроллеры домена должны работать под управлением Windows Server 2008 R2. Функциональные уровни домена и леса не влияют на рядовые серверы. Рядовой сервер под управлением Windows 2000 Server может работать в домене с функциональным уровнем домена и леса Windows Server 2008 R2.
3. В офисах филиалов можно установить RODC под управлением Windows Server 2008 R2, возможно, на тех же компьютерах, которые функционируют как дополнительные DNS-серверы. Это повысит скорость входа в систему и позволит избежать проблем с безопасностью и администрированием, связанных с размещением в этих офисах контроллеров домена, доступных для записи.

### Задание 2

1. Настроить авторегистрацию в Active Directory и в шаблоне сертификатов IPSec.
2. Развернуть сетевой ответчик.
3. Можно указать, что выданные сертификаты не должны храниться в базе данных ЦС в центрах сертификации предприятия, работающих под управлением любой версии Windows Server 2008 R2. Однако при этом следует учитывать, что становится невозможным отзыв сертификатов.

## Глава 4

### Занятие 1

#### 1. Правильные ответы: В, С, и Е.

- a. **Неправильный.** Если щелкнуть правой кнопкой мыши GPO в организационной единице, команда **Управление архивацией** не будет доступна. Необходимо щелкнуть GPO в контейнере **Объекты групповой политики**.
- b. **Правильный.** Эти действия позволяют восстановить MyGPO из резервной копии.
- c. **Правильный.** Эти действия позволяют выбрать резервную копию объекта MyGPO и восстановить этот объект.
- d. **Неправильный.** Команда **Управление архивацией** из контекстного меню контейнера **Начальные объекты групповой политики** позволяет восстановить выбранный начальный GPO из резервной копии. Она не позволяет восстанавливать обычный GPO.
- e. **Правильный.** Эти действия позволяют выбрать резервную копию объекта MyGPO и восстановить этот объект.

#### 2. Правильные ответы: В и С.

- a. **Неправильный.** Эти действия позволяют выполнить резервное копирование всех обычных GPO, но не начальных GPO.
- b. **Правильный.** Эти действия позволяют выполнить резервное копирование всех начальных GPO, включая MyStarterGPO.
- c. **Правильный.** Эти действия позволяют выполнить резервное копирование объекта MyStarterGPO.
- d. **Неправильный.** Команда **Управление архивацией** из контекстного меню контейнера **Начальные объекты групповой политики** используется для восстановления начальных GPO из резервных копий. Она не позволяет создавать резервные копии.
- e. **Неправильный.** Команда **Управление архивацией** из контекстного меню контейнера **Объекты групповой политики** используется для восстановления обычных GPO из резервных копии. Она не позволяет создавать резервные копии.

#### 3. Правильные ответы: А, С, D и Е.

- a. **Правильный.** Этот параметр включает отображение параметров политики, содержащих в комментариях указанный текст.
- b. **Неправильный.** Этот параметр не включает отображение параметров политики, содержащих в комментариях указанный текст. Следовательно, он не поможет в отображении параметров с текстом «Internet Explorer» в комментариях.
- c. **Правильный.** Чтобы искать текст в комментариях необходимо включить фильтрацию по ключевым словам.
- d. **Правильный.** Необходимо указать искомый текст. Параметр **Точное** указывает, что следует искать точное соответствие указанному тексту. Если

вместо этого выбрать **Любое** (Any), будут отображаться комментарии, содержащие любое из слов «Internet» и «Explorer».

- e. **Правильный.** Этот параметр позволяет искать текст, указанный в поле **Комментарий**.
  - f. **Неправильный.** Эти параметры позволяют искать текст в заголовке параметров политики и тексте справки, но не в комментариях. По условиям вопроса необходимо искать текст в поле **Комментарий**.
4. **Правильный ответ: D.**
- a. **Неправильный.** Элемент Policies содержит определения отдельных параметров политики. Он не содержит номера версий и сведения о кодировке.
  - b. **Неправильный.** Элемент SupportedOn указывает ссылки на локализованные строки текста, определяющие операционные системы или приложения, на которые влияет определенный параметр политики. Он не содержит номера версий и сведения о кодировке.
  - c. **Неправильный.** Элемент PolicyNamespaces определяет уникальное пространство имен для файла ADMX. Он не содержит номера версий и сведения о кодировке.
  - d. **Правильный.** Декларация XML подтверждает, что файл является файлом XML. Она содержит номера версий и сведения о кодировке.
5. **Правильный ответ: B.**
- a. **Неправильный.** Элемент Categories указывает категории редактора управления групповыми политиками, в которых будет отображаться параметр политики, содержащийся в файле. Этот элемент не указывает ссылки на локализованные текстовые строки, определяющие операционные системы или приложения.
  - b. **Правильный.** Элемент SupportedOn указывает ссылки на локализованные текстовые строки, определяющие операционные системы или приложения, к которым применяется параметр политики. Этот элемент не содержит номера версий и сведения о кодировке.
  - c. **Неправильный.** Элемент PolicyNamespaces определяет уникальное пространство имен для файла ADMX. Он не указывает ссылки на локализованные текстовые строки, определяющие операционные системы или приложения.
  - d. **Неправильный.** Элемент Resources указывает требования к языковым ресурсам, такие как минимальная требуемая версия связанного файла .adml. Он не указывает ссылки на локализованные текстовые строки, определяющие операционные системы или приложения.

## Занятие 2

### 1. Правильные ответы: А и Е.

- a. **Правильный.** Параметр **Диагностика диска: Настроить уровень выполнения** из конфигурации компьютера требует установки компонента **Воз-**

**возможности рабочего стола.** Этот параметр определяет уровень выполнения для диагностик на основе SMART.

- b. **Неправильный.** Параметр **Не разрешать перенаправление буфера обмена** из конфигурации пользователя определяет, запрещается ли совместное использование содержимого буфера обмена удаленным и клиентским компьютерами в сеансе служб терминалов или служб удаленных рабочих столов. Этот параметр не требует установки компонента **Возможности рабочего стола.**
- c. **Неправильный.** Параметр **Принудительная отмена фонового рисунка удаленного рабочего стола** из конфигурации пользователя определяет, будет ли фоновый рисунок рабочего стола отображаться на удаленных клиентах, подключающихся через службы терминалов или службы удаленных рабочих столов. Этот параметр не требует установки компонента **Возможности рабочего стола.**
- d. **Неправильный.** Параметр **Set The Map Update Interval For NIS Subordinate Servers** (Установить интервал обновления карт для подчиненных серверов NIS) из конфигурации компьютера определяет интервал обновления для передачи карт NIS на подчиненные серверы NIS. Этот параметр не требует установки компонента **Возможности рабочего стола.**
- e. **Правильный.** Параметр **Диагностика диска: Настроить пользовательский текст предупреждения** из конфигурации компьютера требует установки компонента **Возможности рабочего стола.** Этот параметр подставляет пользовательский текст предупреждения в сообщения диагностики диска, появляющиеся при обнаружении ошибки SMART.

2. **Правильные ответы: А, С и D.**

- a. **Правильный.** Параметр **Разрешить перенаправление часового пояса** из конфигурации пользователя определяет, перенаправляются ли параметры часового пояса клиента в сеанс служб терминалов или служб удаленных рабочих столов.
- b. **Неправильный.** Параметр **Диагностика диска: Настроить уровень выполнения** из конфигурации компьютера определяет уровень выполнения для диагностик диска, выполняемых на основе SMART. Он не относится к службам терминалов или службам удаленных рабочих столов.
- c. **Правильный.** Параметр **Не разрешать перенаправление буфера обмена** из конфигурации пользователя определяет, будет ли совместно использоваться содержимое буфера обмена (перенаправление буфера обмена) удаленным и клиентским компьютерами в сеансе служб терминалов или служб удаленных рабочих столов.
- d. **Правильный.** Параметр **Принудительная отмена фонового рисунка удаленного рабочего стола** из конфигурации пользователя определяет, будет ли отображаться фоновый рисунок рабочего стола на удаленных клиентах, подключающихся через службы терминалов или службы удаленных рабочих столов.



- e. **Неправильный.** Параметр **Turn On Extensive Logging For Active Directory Domain Services Domain Controllers That Are Running Server For NIS** (Включить расширенные функции журнала для контроллеров домена Active Directory, выполняющих функцию сервера для NIS) из конфигурации компьютера позволяет управлять расширенными функциями журнала на контроллерах домена SNIS. Он не относится к службам терминалов или службам удаленных рабочих столов.

3. **Правильные ответы: В, С и Е.**

- a. **Неправильный.** Хотя создание слишком большого числа GPO (часто имеющих одинаковые параметры) является ошибкой, ошибкой будет и слишком малое число. Если объект GPO имеет много настроенных параметров политики, может быть сложно понять, для чего служит этот объект, и дать ему содержательное имя. Связывание GPO с подразделениями из разных сайтов может замедлить репликацию и увеличить трафик, передаваемый по медленным подключениям глобальной сети.
- b. **Правильный.** Если ADMX-файлы поместить в центральное хранилище на контроллере домена, их можно реплицировать на другие контроллеры домена. Редактор управления групповыми политиками не копирует AMDX-файлы в каждый редактируемый GPO, а считывает их из расположения, единого для домена, или центрального хранилища. Это ускоряет обработку и снижает сетевой трафик. Кроме того, если создать собственные ADMX-файлы, их можно поместить в центральное хранилище и открывать в редакторе управления групповыми политиками.
- c. **Правильный.** Объектам GPO и подразделениям следует давать содержательные имена. Создавая объект GPO06, вы знаете, для чего он нужен, но будете ли помнить об этом через три месяца? Если, например, дать ему имя Kiosk Policy, его предназначение будет намного понятнее. Аналогично, имя подразделения Human Resources понятнее, чем OU23.
- d. **Неправильный.** Перечисленные функции могут быть полезны в определенных ситуациях, но они усложняют структуру групповой политики и затрудняют ее понимание. Эти функции следует использовать только в том случае, если они дают конкретные преимущества.
- e. **Правильный.** Даже если изменения в GPO были реплицированы в домене, они не применяются до следующего обновления групповой политики. Команда Gpupdate форсирует обновление политики. Она выполняется на контроллере домена, любом рядовом сервере или клиенте домена, на котором требуется незамедлительное вступление изменений в силу.

4. **Правильный ответ: В.**

- a. **Неправильный.** Утилита GPREsult.exe показывает все параметры политики, применяемые к определенному пользователю или компьютеру. Она не проверяет согласованность объектов GPO на контроллерах домена.
- b. **Правильный.** Утилита GPOTool.exe, входящая в состав Windows Server 2003 Resource Kit, проверяет согласованность GPO на всех контроллерах домена, определяет действительность политик и показывает подробную информацию о реплицированных GPO.

- c. **Неправильный.** Функция создания отчетов GPMC позволяет получать отчеты, по которым можно определять, например, указаны ли применяемые объекты GPO в результатах групповой политики. Эта функция не проверяет согласованность GPO на всех контроллерах домена.
  - d. **Неправильный.** Утилита Gpupdate.exe форсирует обновление политики и применяется после изменения параметров групповой политики. Эта утилита не проверяет согласованность GPO на контроллерах домена.
5. **Правильный ответ: А.**
- a. **Правильный.** Эти действия приведут к созданию отчета о результирующем наборе политик для пользователя, вошедшего в систему на локальном контроллере домена.
  - b. **Неправильный.** Моделирование групповой политики позволяет пользователю эмулировать развертывание политики, применяемой к пользователям и компьютерам, до ее фактического применения. Отчет о моделировании групповой политики иногда называют отчетом RSoP в режиме планирования, но это не отчет RSoP.
  - c. **Неправильный.** Моделирование групповой политики позволяет пользователю эмулировать развертывание политики, применяемой к пользователям и компьютерам, до ее фактического применения. Отчет о моделировании групповой политики иногда называют отчетом RSoP в режиме планирования, но это не отчет RSoP.
  - d. **Неправильный.** Эти действия приведут к созданию и сохранению отчета GPO, а не отчета RSoP.

## Глава 4. Лабораторная работа

### Задание 1

1. Если в конфигурации компьютера нет настроенных политик, можно отключить конфигурацию компьютера в объекте GPO. Это ускорит обработку GPO.
2. Начальные GPO архивируются отдельно от обычных GPO, желательно, в отдельном контейнере. Дон должен щелкнуть свой начальный GPO правой кнопкой мыши и выбрать команду **Архивировать** (Back Up) или щелкнуть правой кнопкой мыши контейнер **Начальные объекты групповой политики** (Starter GPOs) и выбрать команду **Архивировать все** (Back Up All).

### Задание 2

1. В первую очередь следует проверить, должен ли пользователь иметь доступ к этим функциям. Коллеги, о которых он говорит, могут работать в другом отделе. Затем следует получить список результирующих политик для этого пользователя. Это можно сделать при помощи GPMC или утилиты GPRresult.exe. Наконец, выясните, не задерживается ли применение изменений политик для этого пользователя. Например, политика могла измениться недавно, и пользователь должен выйти из системы и войти снова, или требуется выполнить на компьютере пользователя команду Gpupdate.

2. Если проблемы связаны с компьютером, а не с пользователем, в первую очередь следует проверить сетевую инфраструктуру. Подключен ли компьютер к сети? Запущены ли службы? Получил ли компьютер необходимую конфигурацию через DHCP? Есть ли проблемы с DNS? Затем следует проверить, входит ли компьютер в нужное подразделение. Если параметры групповой политики недавно изменялись, выполните на компьютере команду Groupdate.
3. Показаны ли в результирующей политике применяемые GPO? Показан ли нужный параметр в отчете о результирующей политике? Входит ли GPO в список запрещенных?

## Глава 5

### Занятие 1

1. **Правильные ответы: А, D и E.**
  - a. **Правильный.** RSAT можно установить на компьютеры под управлением Windows Vista Business, Enterprise и Ultimate, Windows Server 2008 и 2008 R2, Windows 7 Professional, Enterprise и Ultimate.
  - b. **Неправильный.** RSAT нельзя использовать в Windows XP.
  - c. **Неправильный.** RSAT нельзя использовать в версиях Windows Vista и Windows 7, не имеющих возможности подключения к домену AD DS.
  - d. **Правильный.** RSAT можно установить на компьютеры под управлением Windows Vista Business, Enterprise и Ultimate, Windows Server 2008 и 2008 R2, Windows 7 Professional, Enterprise и Ultimate.
  - e. **Правильный.** RSAT можно установить на компьютеры под управлением Windows Vista Business, Enterprise и Ultimate, Windows Server 2008 и 2008 R2, Windows 7 Professional, Enterprise и Ultimate.
2. **Правильные ответы: А и В.**
  - a. **Правильный.** По умолчанию члены группы администраторов могут подключаться к автономному компьютеру под управлением Windows Server 2008 через удаленный рабочий стол.
  - b. **Правильный.** Члены группы **Пользователи удаленного рабочего стола** могут подключаться к автономному компьютеру под управлением Windows Server 2008 через удаленный рабочий стол.
  - c. **Неправильный.** По умолчанию члены группы **Опытные пользователи** не имеют возможности заходить на автономный компьютер под управлением Windows Server 2008.
  - d. **Неправильный.** По умолчанию члены группы **Операторы печати** не имеют возможности заходить на автономный компьютер под управлением Windows Server 2008.
  - e. **Неправильный.** По умолчанию члены группы **Операторы архива** не имеют возможности заходить на автономный компьютер под управлением Windows Server 2008.

### 3. Правильный ответ: С.

- a. **Неправильный.** Нельзя подключиться к компьютеру через удаленный рабочий стол, если сетевой адаптер вышел из строя.
- b. **Неправильный.** Нельзя подключиться к компьютеру через Telnet, если сетевой адаптер вышел из строя.
- c. **Правильный.** При помощи EMS можно отключить компьютер, даже если его видеокарта и сетевой адаптер не функционируют. Подключения EMS можно выполнять через последовательный порт или порт USB.
- d. **Неправильный.** Так как информации на экране не видно, нельзя использовать PowerShell для выполнения задачи, описанной в вопросе.

### 4. Правильный ответ: А.

- a. **Правильный.** Серверы шлюзов удаленного рабочего стола позволяют туннелировать сеансы удаленного рабочего стола через порт 443 брандмауэра. Размещение такого сервера в офисе дочерней компании позволит подключаться к находящимся там серверам с Windows Server 2008 для выполнения административных задач.
- b. **Неправильный.** Не следует размещать сервер шлюза удаленного рабочего стола в локальном офисе, так как это не предоставит доступа к серверам из удаленного офиса.
- c. **Неправильный.** Порт 25 не используется протоколом RDP.
- d. **Неправильный.** Порт 25 не используется протоколом RDP. Даже если вы сможете использовать этот порт, диапазон частных IP-адресов главного офиса не будет соответствовать конфигурации брандмауэра.

### 5. Правильный ответ: В.

- a. **Неправильный.** Фильтры необходимо создавать каждый раз перед использованием. Настраиваемые представления можно сохранять и повторно использовать.
- b. **Правильный.** Настраиваемые представления можно сохранять. Это позволяет автоматически просматривать критические события из журнала **Перенаправленные события**, произошедшие за последние 24 часа.
- c. **Неправильный.** Хотя подписки можно настроить для извлечения данных о критических событиях, по условиям задания требуется просматривать только критические события, а не собирать только критические события. Разница в том, что при помощи подписки можно собирать события всех типов, а затем применять настраиваемое представление, чтобы просматривать отдельные события.
- d. **Неправильный.** Политику WSRM настраивать не следует, т.к. она не имеет отношения к журналам событий.

## Занятие 2

### 1. Правильный ответ: А.

- a. **Правильный.** Делегирование полномочий на глобальном уровне возможно только после входа под встроенной учетной записью администратора или при ее вызове через команду `runas`.

- b. **Неправильный.** Делегирование полномочий на глобальном уровне возможно только с использованием встроенной учетной записи администратора. Невозможно выполнить делегирование полномочий на управление IIS на глобальном уровне, используя учетную запись, входящую в локальную группу администраторов, но не являющуюся встроенной учетной записью администратора.
    - c. **Неправильный.** Делегирование полномочий на глобальном уровне возможно только с использованием встроенной учетной записи администратора. Добавление доменной учетной записи в группу администраторов домена ничем не поможет.
    - d. **Неправильный.** Добавление локальной учетной записи в локальную группу администраторов не решит проблему, поскольку единственный способ выполнить делегирование на глобальном уровне — использовать встроенную учетную запись администратора.
  2. **Правильный ответ: D.**
    - a. **Неправильный.** Делегирование возможности управлять группами не даст доверенным пользователям возможности изменять пароли.
    - b. **Неправильный.** Делегирование возможности создавать учетные записи даст пользователям больше прав, чем необходимо для работы, но не позволит изменять пароли.
    - c. **Неправильный.** Разрешение доверенным пользователям в офисах филиалов читать пользовательскую информацию не даст возможности изменять пароли.
    - d. **Правильный.** Делегирование этой задачи доверенным пользователям в офисах филиалов позволит им выполнять базовые задачи по управлению паролями без предоставления лишних привилегий.
  3. **Правильный ответ: D.**
    - a. **Неправильный.** Хотя технически это решит задачу, пользователь получит возможность управлять всеми группами из подразделения, а не только группой Interns. Это нарушает принцип наименьших привилегий, который предписывает назначение только тех прав, которые необходимы.
    - b. **Неправильный.** Мастер делегирования управления нельзя выполнять напрямую для групп безопасности.
    - c. **Неправильный.** Мастер делегирования управления нельзя выполнять напрямую для групп безопасности.
    - d. **Правильный.** Менеджер группы, указанный на вкладке **Управляется** (Managed By), имеет возможность изменять список членов группы.
  4. **Правильные ответы: A и B.**
    - a. **Правильный.** Команда dscls, выполненная для соответствующего подразделения с параметром /resetDefaultDACL, вернет разрешения по умолчанию.
    - b. **Правильный.** Кнопка **Восстановить умолчания** в диалоговом окне дополнительных параметров безопасности для делегирования вернет исходные разрешения подразделения.

- c. **Неправильный.** Вкладка **Управляется** (Managed By) в диалоговом окне свойств подразделения предоставляет информацию для ознакомления, а не для администрирования.
- d. **Неправильный.** Вкладка **Управляется** (Managed By) в диалоговом окне свойств подразделения предоставляет информацию для ознакомления, а не для администрирования.
- e. **Неправильный.** Команда `dsquery` только предоставляет информацию об объектах в AD DS. Ее нельзя использовать для сброса неверных параметров делегирования.

## Глава 5. Лабораторная работа

### Задание 1

1. Убедитесь, что служба сборщика событий Windows запускается автоматически. Настройте на компьютере-сборщике подписку, инициируемую компьютером-источником.
2. Используйте групповую политику, чтобы настроить 30 серверов для пересылки событий на компьютер, настроенный как сборщик.
3. Прикрепите задачу к событию, используя средство просмотра журналов событий, и укажите в качестве этой задачи созданный вами сценарий PowerShell.

### Задание 2

1. Разделите учетные записи пользователей, создав структуру подразделений, отражающую существующее разделение на отделы. После добавления учетных записей в новые подразделения можно использовать мастер делегирования управления, чтобы предоставить помощникам администратора право на изменение паролей.
2. Хотя руководители групп должны иметь возможность изменять список членов группы, нет причин предоставлять им права на создание и удаление групп. Создайте необходимые группы и на вкладке **Управляется** (Managed By) окна свойств каждой из них укажите соответствующую учетную запись менеджера группы.

## Глава 6

### Занятие 1

1. **Правильный ответ: А.**
  - a. **Правильный.** Политика WSRM Equal\_Per\_User гарантирует, что пользователь, имеющий два сеанса на сервере узла сеансов удаленных рабочих столов, получит столько же ресурсов, сколько пользователь с одним сеансом.
  - b. **Неправильный.** Политика WSRM Equal\_Per\_Session обеспечивает равное выделение ресурсов каждому сеансу на сервере узла сеансов удаленных

рабочих столов. Когда применена эта политика, пользователь с двумя сеансами получит больше системных ресурсов, чем пользователь с одним сеансом.

- c. **Неправильный.** Параметры выделения ресурсов нельзя настроить, изменив свойства сервера в консоли управления сервером узла сеансов удаленных рабочих столов. Выделением ресурсов можно управлять только через WSRM.
- d. **Неправильный.** Параметры выделения ресурсов нельзя настроить, изменив свойства RDP-Тср. Выделением ресурсов можно управлять только через WSRM.

2. **Правильный ответ: А.**

- a. **Правильный.** Если областью обнаружения сервера лицензирования является домен, запрашивать клиентские лицензии у этого сервера смогут только компьютеры из локального домена.
- b. **Неправильный.** Если областью обнаружения сервера лицензирования является лес, клиенты из других доменов этого леса смогут получать лицензии у этого сервера, даже если есть более близкий к ним сервер, например, если у локального сервера кончатся лицензии.
- c. **Неправильный.** Сервер лицензирования, расположенный в корневом домене и имеющий область обнаружения Лес, будет выдавать клиентские лицензии компьютерам в лесу, но такой способ не удовлетворяет требованиям задания.
- d. **Неправильный.** Сервер лицензирования, расположенный в корневом домене и имеющий область обнаружения Домен, будет выдавать клиентские лицензии только компьютерам из корневого домена, а не из определенных офисов, как требуется в задании.

3. **Правильные ответы: А и С.**

- a. **Правильный.** Необходимо установить область обнаружения сервера, прежде чем устанавливать клиентские лицензии на сервер лицензирования удаленных рабочих столов.
- b. **Неправильный.** Для установки лицензий на сервер лицензирования удаленных рабочих столов не требуется устанавливать функциональный уровень домена Windows Server 2008 R2.
- c. **Правильный.** Перед установкой клиентских лицензий необходимо активировать сервер лицензирования удаленных рабочих столов.
- d. **Неправильный.** Серверы лицензирования удаленных рабочих столов могут выдавать и лицензии «на устройство», и лицензии «на пользователя».

4. **Правильный ответ: D.**

- a. **Неправильный.** Использование политик WSRM не дает возможности наращивать ресурсы сервера при необходимости.
- b. **Неправильный.** Hyper-V не подойдет в качестве решения, поскольку существует верхний предел ресурсов процессора на виртуальном хосте. Это решение требует возможности наращивать ресурсы процессора при необходимости.



- c. **Неправильный.** Хотя серверы узлов сеансов удаленных рабочих столов позволяют наращивать ресурсы, они требуют перенастройки клиентов.
  - d. **Правильный.** Развертывание фермы серверов узлов сеансов удаленных рабочих столов позволит добавлять и удалять серверы из фермы при необходимости, не изменяя конфигурацию клиентов.
5. **Правильный ответ: С.**
- a. **Неправильный.** Forefront Endpoint Protection и другие антивирусные решения позволяют выполнять проверку на вирусы и вредоносное ПО после установки клиентского подключения, но не будут предотвращать подключение нестабильных клиентов.
  - b. **Неправильный.** Посредник подключений к удаленному рабочему столу используется для управления сеансами, подключающимися к фермам серверов узлов сеансов удаленных рабочих столов. Его нельзя использовать для проверки работоспособности подключающихся клиентов.
  - c. **Правильный.** Сервер шлюза служб терминалов можно использовать в сочетании с NAP, чтобы запрещать компьютерам, не прошедшим проверку, подключение к серверу узла сеансов удаленных рабочих столов.
  - d. **Неправильный.** ISA Server 2006 нельзя использовать для блокирования клиентов, подключающихся к серверу узла сеансов удаленных рабочих столов, если они не проходят проверку работоспособности. Совместно с ISA Server 2006 можно использовать NAP, но не для блокирования доступа клиентов служб удаленных рабочих столов.

## Занятие 2

1. **Правильные ответы: А, В и С.**
- a. **Правильный.** Можно обращаться к приложениям RemoteApp через веб-страницы и развертывать ссылки на такие веб-страницы через групповую политику.
  - b. **Правильный.** Можно создавать пакеты установщика Windows для приложений RemoteApp и развертывать эти пакеты через групповую политику.
  - c. **Правильный.** Можно создавать ярлыки для файлов RDP и помещать их в общие папки, чтобы пользователи могли обращаться к приложениям RemoteApp.
  - d. **Неправильный.** Приложения RemoteApp не будут работать, если запускать их из общих папок; их требуется запускать на сервере узла сеансов удаленных рабочих столов. Приложения можно развертывать при помощи страниц веб-доступа к удаленным рабочим столам, пакетов установщика Windows и ярлыков RDP.
2. **Правильный ответ: С.**
- a. **Неправильный.** Следует использовать App-V. Приложения RemoteApp служб терминалов не решают проблему с приложениями, конфликтующими при установке на одном сервере узла сеансов удаленных рабочих столов.

- b. **Неправильный.** Следует использовать App-V. Сервер шлюза служб терминалов не решает проблему с приложениями, конфликтующими при установке на одном сервере узла сеансов удаленных рабочих столов.
  - c. **Правильный.** App-V позволяет развертывать на одном сервере узла сеансов служб терминалов приложения, конфликтующие при обычных условиях, включая разные версии одного приложения.
  - d. **Неправильный.** Следует использовать App-V. Веб-доступ к удаленным рабочим столам не решает проблему с приложениями, конфликтующими при установке на одном сервере узла сеансов удаленных рабочих столов.
3. **Правильный ответ: С.**
- a. **Неправильный.** Проблема в том, что не установлена последняя версия клиента удаленных рабочих столов. Установка Internet Explorer 6.0 не решит эту проблему.
  - b. **Неправильный.** Отключение брандмауэра Windows XP не решит проблему. Необходимо установить последнюю версию клиента удаленных рабочих столов, входящую в пакет обновлений Windows XP SP3.
  - c. **Правильный.** Для подключения к приложениям RemoteApp с помощью веб-доступа компьютерам с Windows XP требуется версия клиента удаленных рабочих столов, входящая в пакет обновлений SP3.
  - d. **Неправильный.** Установка Защитника Windows не решит проблему. Необходимо установить последнюю версию клиента удаленных рабочих столов, входящую в пакет обновлений Windows XP SP3.
4. **Правильные ответы: В и D.**
- a. **Неправильный.** Установка DFS потребует открытия портов, относящихся к протоколу SMB, на брандмауэре между внутренней сетью и периметром.
  - b. **Правильный.** Хотя FTP 7.5 поддерживает только базовую аутентификацию, можно обезопасить аутентификацию и передачу данных из внутренней сети при помощи SSL.
  - c. **Неправильный.** Настройка общей папки потребует открытия портов, относящихся к протоколу SMB, на брандмауэре между внутренней сетью и периметром.
  - d. **Правильный.** WebDAV поддерживает методы безопасной аутентификации. Данные, передающиеся из внутренней сети, можно защитить при помощи SSL.

## Глава 6. Лабораторная работа

### Задание 1

1. Разверните сервер лицензирования удаленных рабочих столов в каждом офисе. В качестве области обнаружения выберите домен.
2. Создайте ферму служб терминалов и используйте посредник подключений к службам терминалов.

3. Для обращения к приложениям RemoteApp через веб-доступ необходимо обновить клиенты под управлением Windows Vista, установив пакет обновлений SP1, и клиенты под управлением Windows XP, установив пакет обновлений SP3. В качестве альтернативы можно обновить все клиенты до Windows 7.

## Задание 2

1. Чтобы предоставить пользователям возможность запуска разных версий одного приложения, используйте App-V.
2. Создайте файлы установщика Windows для приложений RemoteApp и настройте параметры установщика так, чтобы документы были связаны с соответствующими приложениями RemoteApp.
3. При подготовке файлов установщика можно настроить параметры шлюза удаленного рабочего стола. При запуске приложение проверяет, в какой сети находится компьютер: во внутренней или во внешней. Если компьютер находится во внешней сети, он обратится к серверу шлюза удаленного рабочего стола, чтобы установить подключение.

## Глава 7

### Занятие 1

1. **Правильный ответ: D.**
  - a. **Неправильный.** Оснастку **Управление печатью** можно использовать для изменения портов принтера на удаленном сервере. Однако это можно было выполнять и раньше, так что эта возможность не относится к новым.
  - b. **Неправильный.** Оснастку **Управление печатью** можно использовать для просмотра состояния принтера на удаленном сервере. Однако это можно было выполнять и раньше, так что эта возможность не относится к новым.
  - c. **Неправильный.** Оснастку **Управление печатью** можно использовать для добавления и изменения форм принтера на удаленном сервере. Однако это можно было выполнять и раньше, так что эта возможность не относится к новым.
  - d. **Правильный.** Настраиваемые фильтры позволяют администраторам просматривать и управлять принтерами, выбранными по принадлежности к узлу, правам и ролям. Это новая возможность оснастки **Управление печатью**.
2. **Правильный ответ: B.**
  - a. **Неправильный.** Разрешение **Печать** по умолчанию назначается группе **Все**. Пользователь может подключаться к принтеру и отправлять документы, но не может приостанавливать, перезапускать и отменять печать или изменять порядок документов, отправленных другими пользователями.

- b. **Правильный.** Разрешение **Управление документами** по умолчанию назначается группе создателей-владельцев. Оно позволяет приостанавливать, возобновлять и отменять печать и изменять порядок документов, отправленных другими пользователями, но не дает возможности отправлять документы на печать и управлять состоянием принтера.
- c. **Неправильный.** Разрешение **Управление принтерами** по умолчанию назначается администраторам, операторам печати и операторам сервера. Оно позволяет выполнять задачи, связанные с разрешением **Печать** и дает полный административный контроль над принтером. Пользователь с этим разрешением может отправлять документы на принтер и управлять состоянием принтера.
- d. **Неправильный.** Разрешение **Управление сервером** позволяет создавать и удалять очереди печати (с уже установленными драйверами), добавлять и удалять порты и формы. По умолчанию это разрешение имеют администраторы, операторы сервера и операторы печати. Это разрешение на доступ к серверу, и оно не дает возможности приостанавливать, возобновлять и отменять печать и изменять порядок документов, отправленных другими пользователями.

3. **Правильный ответ: А.**

- a. **Правильный.** Разрешение **Управление сервером** позволяет создавать и удалять очереди печати (с уже установленными драйверами), добавлять и удалять порты и формы. Обычный пользователь, имеющий это разрешение, является администратором делегированной печати.
- b. **Неправильный.** Разрешение **Просмотр сервера** позволяет просматривать сервер печати. Без этого разрешения пользователь не сможет видеть принтеры сервера, поэтому оно предоставляется членам группы **Все**. Это разрешение не делает пользователя администратором делегированной печати.
- c. **Неправильный.** Разрешение **Управление документами** позволяет приостанавливать, возобновлять, перезапускать и отменять печать и изменять порядок документов, отправленных другими пользователями. Оно не дает возможности администрировать порты и формы, и его предоставление не делает пользователя администратором делегированной печати.
- d. **Неправильный.** Разрешение **Управление принтерами** позволяет выполнять задачи, связанные с разрешением **Печать** и дает полный административный контроль над принтером. Это разрешение не следует давать обычным пользователям.

4. **Правильные ответы: С и Е.**

- a. **Неправильный.** Эта политика определяет, будут ли устанавливаться на локальный компьютер драйверы, работающие в режиме ядра. Она не влияет на публикацию принтера, к которому открыт общий доступ.
- b. **Неправильный.** Эта политика применяется, когда печать выполняется через сервер печати. Она определяет, самостоятельно ли клиент обрабатывает задания печати или передает их на сервер, и не влияет на публикацию принтера.

- c. **Правильный.** Если эта политика включена, принтер будет автоматически публиковаться в Active Directory при открытии к нему общего доступа, если публикация принтеров разрешена.
- d. **Неправильный.** Эта политика включает физическое отслеживание принтеров Windows. Она не влияет на публикацию принтера.
- e. **Правильный.** Эта политика разрешает публикацию принтеров. Если публикация разрешена, политика **Автоматическая публикация новых принтеров в Active Directory** определяет, будет ли принтер, к которому открывается общий доступ, автоматически публиковаться в Active Directory.

## Занятие 2

### 1. Правильный ответ: А.

- a. **Правильный.** Мастер подготовки общих папок можно запустить из оснастки **Управление общими ресурсами и хранилищами**.
- b. **Неправильный.** Мастер создания нового пространства имен запускается из оснастки **Управление DFS**.
- c. **Неправильный.** Для создания квот не используется мастер. Диалоговое окно **Создание квоты (Create Quota)** можно запустить из диспетчера ресурсов файлового сервера.
- d. **Неправильный.** Для создания фильтров блокировки файлов не используется мастер. Диалоговое окно **Создание фильтра блокировки файлов (Create File Screen)** можно запустить из диспетчера ресурсов файлового сервера.

### 2. Правильные ответы: А, В и D.

- a. **Правильный.** Мастер подготовки общих папок позволяет открыть общий доступ к существующей папке.
- b. **Правильный.** Мастер подготовки общих папок позволяет создать папку и открыть общий доступ к ней.
- c. **Неправильный.** Службы для NFS не установлены, поэтому доступен только протокол SMB, и выбрать протокол нельзя.
- d. **Правильный.** Если общий ресурс находится на томе, отформатированном в NTFS, или является таким томом, то мастер подготовки общих папок можно использовать для настройки локальных разрешений NTFS.
- e. **Неправильный.** Роль сервера DFS не установлена, поэтому нельзя опубликовать общий ресурс в пространстве имен DFS.

### 3. Правильный ответ: С.

- a. **Неправильный.** В Windows Server 2008 и 2008 R2 квоты применяются к томам и общим папкам. В предыдущих версиях Windows Server их можно было применять только к томам. Шаблон **Предел 100 МБ** создает жесткую квоту (которую нельзя превысить), применяемую и к томам, и к общим папкам.
- b. **Неправильный.** В Windows Server 2008 и 2008 R2 квоты применяются к томам и общим папкам. В предыдущих версиях Windows Server их мож-

но было применять только к томам. Шаблон **Предел 200 МБ с уведомлением пользователя** создает жесткую квоту (которую нельзя превысить), применяемую и к томам, и к общим папкам.

- c. **Правильный.** В Windows Server 2008 и 2008 R2 квоты применяются к томам и общим папкам. В предыдущих версиях Windows Server их можно было применять только к томам. Однако шаблон **Наблюдение за томом 200 ГБ** создает мягкую квоту (которую можно превысить), используемую для мониторинга, которую можно применять только к томам.
- d. **Неправильный.** В Windows Server 2008 и 2008 R2 квоты применяются к томам и общим папкам. В предыдущих версиях Windows Server их можно было применять только к томам. Однако шаблон **Наблюдение за общим ресурсом размером 500 МБ** создает мягкую квоту (которую можно превысить), используемую для мониторинга, которую можно применять только к общим папкам.

4. **Правильный ответ: D.**

- a. **Неправильный.** Диспетчер ресурсов файлового сервера используется для управления квотами, фильтрами блокировки файлов и отчетами хранилища. Он не создает файловое хранилище в филиалах и не имеет режима размещенного кэша.
- b. **Неправильный.** Диспетчер ресурсов файлового сервера используется для управления квотами, фильтрами блокировки файлов и отчетами хранилища. Он не создает файловое хранилище в филиалах и не имеет режима распределенного кэша.
- c. **Неправильный.** Режим распределенного кэша компонента BranchCache для сетевых файлов в Windows 7 обычно используется в филиалах с числом пользователей меньше 50. В режиме распределенного кэша локальный клиент, работающий под управлением Windows 7, хранит копию содержимого и делает ее доступной другим авторизованным клиентам.
- d. **Правильный.** В режиме распределенного кэша BranchCache для сетевых файлов в филиале разворачивается компьютер под управлением Windows Server 2008 R2, выполняющий функцию хоста.

## Глава 7. Лабораторная работа

### Задание 1

1. На компьютере под управлением Windows Server 2008 R2 можно установить службу роли BranchCache для сетевых файлов, входящую в состав роли сервера **Файловый сервер**. Эта служба роли кэширует данные в сети филиала, создавая копию содержимого, полученного с файлового или веб-сервера из центрального офиса. Если другой клиент из филиала запросит то же содержимое, он сможет получить его из своей локальной сети, не загружая по WAN-каналу.
2. Если служба роли BranchCache для сетевых файлов установлена и включена на исходном сервере в центральном офисе, можно использовать ее в ре-

жиме распределенного кэша. В этом режиме локальный клиент под управлением Windows 7 хранит копию содержимого и делает ее доступной другим авторизованным клиентам. Это избавляет от необходимости развертывания в филиале сервера под управлением Windows Server 2008 R2. Режим распределенного кэша лучше всего подходит для небольших филиалов, все компьютеры которых находятся в одной подсети.

3. Инфраструктура классификации файлов в Windows Sever 2008 R2 предоставляет встроенное решение для классификации на основе ценности данных для организации, позволяющее автоматизировать процессы, ранее выполнявшиеся вручную. Встроенная функциональность службы роли диспетчера ресурсов файлового сервера позволяет классифицировать файлы по содержанию и расположению, что обеспечивает более эффективную защиту и управление на основе ценности данных.
4. Улучшенная оснастка **Управление печатью**, входящая в состав Windows Server 2008 R2, включает мастер установки сетевых принтеров, облегчающий добавление сетевых принтеров. Этот мастер автоматически находит принтеры и устанавливает соответствующие драйверы.

## Глава 8

### Занятие 1

#### 1. Правильный ответ: А.

- a. **Правильный.** Политика **Аудит событий входа учетной записи** позволяет записывать события входа, когда проверка подлинности выполняется контроллером домена. Пересылка этих событий со всех контроллеров домена позволит получить полную информацию о входах учетных записей в пределах сайта.
- b. **Неправильный.** Политика **Аудит управления учетными записями** связана с созданием и изменением учетных записей пользователей и групп. Она не имеет отношения к событиям проверки подлинности в домене.
- c. **Неправильный.** Политика **Аудит событий входа** позволяет записывать только локальные события входа. Такие записи, полученные с контроллера домена, позволят узнать, кто входил в систему на этом контроллере домена, а не кто проходил на нем проверку подлинности для входа на другой компьютер в домене.
- d. **Неправильный.** Политика **Аудит доступа к службе каталогов** используется для аудита доступа к объектам Active Directory, к которым применены списки SACL.

#### 2. Правильный ответ: С.

- a. **Неправильный.** Хотя общие папки можно защищать при помощи BitLocker, эта технология шифрует целые тома и не позволяет предоставлять доступ отдельным учетным записям.
- b. **Неправильный.** EFS работает только с учетными записями пользователей. Учетным записям групп нельзя назначать сертификаты EFS.



- c. **Правильный.** EFS позволяет шифровать конфиденциальные данные, используя сертификаты EFS каждого из пяти бухгалтеров.
- d. **Неправильный.** Хотя общие папки можно защищать при помощи BitLocker, эта технология шифрует целые тома и не позволяет предоставлять доступ отдельным учетным записям.

3. **Правильные ответы: В, С, Е и F.**

- a. **Неправильный.** Всегда полезно знать, кто предпринял атаку, но эту информацию редко удастся получить. Цель криминалистического анализа — определить время проведения, серьезность и последствия атаки и выяснить, какие системы были скомпрометированы. При криминалистическом анализе обычно не записываются идентификационные данные злоумышленника.
- b. **Правильный.** Цель криминалистического анализа — определить время проведения, серьезность и последствия атаки и выяснить, какие системы были скомпрометированы.
- c. **Правильный.** Цель криминалистического анализа — определить время проведения, серьезность и последствия атаки и выяснить, какие системы были скомпрометированы. Следовательно, длительность атаки должна записываться.
- d. **Неправильный.** Всегда полезно знать, с какого компьютера была проведена атака, но эту информацию не всегда удастся получить. Если атака внешняя, идентификационные данные сети, из которой исходила угроза, и компьютер-источник почти невозможно определить. Цель криминалистического анализа — определить время проведения, серьезность и последствия атаки и выяснить, какие системы были скомпрометированы. При криминалистическом анализе обычно не записываются идентификационные данные компьютера, с которого проведена атака.
- e. **Правильный.** Цель криминалистического анализа — определить время проведения, серьезность и последствия атаки и выяснить, какие системы были скомпрометированы. Следовательно, должны записываться идентификационные данные компьютеров, пострадавших от атаки.
- f. **Правильный.** Цель криминалистического анализа — определить время проведения, серьезность и последствия атаки и выяснить, какие системы были скомпрометированы. Следовательно, должны записываться изменения, произошедшие в сети в результате атаки.

4. **Правильный ответ: D.**

- a. **Неправильный.** Эта категория позволяет выполнять аудит событий, связанных с доступом к службе каталогов, репликацией службы каталогов и изменением объектов AD DS. Она не позволяет следить за созданием и удалением групп безопасности.
- b. **Неправильный.** Эта категория позволяет выполнять аудит событий, сгенерированных при отправке запросов на шифрование и дешифровку DPAPI, при создании, запуске или завершении процесса или при установке входящего подключения RPC. Она не позволяет следить за созданием и удалением групп безопасности.

- c. **Неправильный.** Эта категория позволяет выполнять аудит различных событий доступа и событий, относящихся к операциям. Сюда входит доступ к реестру, сетевым ресурсам и хранящимся в них файлах и папках, объектам файловой системы, объектам COM+, объектам SAM и объектам ядра. Эта категория не позволяет следить за созданием и удалением групп безопасности.
  - d. **Правильный.** Эта категория позволяет выполнять аудит создания, удаления и изменения групп приложений, рассылки и безопасности, а также учетных записей компьютеров и пользователей.
5. **Правильный ответ: С.**
- a. **Неправильный.** 21 день — типичный срок хранения информации в онлайн-базах данных, позволяющих быстро просматривать недавние события.
  - b. **Неправильный.** 180 дней — типичный срок хранения информации в резервных копиях. Большинству организаций этого достаточно.
  - c. **Правильный.** Обычно организации, работающие в регулируемых законодательством секторах, должны хранить информацию в течение семи лет.
  - d. **Неправильный.** Бессрочно должны храниться данные, имеющие отношение к национальной безопасности. К другим данным такое требование не предъявляется.

## Занятие 2

1. **Правильные ответы: В и С.**
- a. **Неправильный.** NLB используется только для балансировки нагрузки между серверами WSUS. Настройка NLB не поможет клиентам использовать локальный сервер WSUS в любом филиале.
  - b. **Правильный.** Включение циклического обслуживания DNS с расстановкой по адресу позволит клиентам получать IP-адрес ближайшего сервера WSUS.
  - c. **Правильный.** Чтобы использовать способ с настройкой циклического обслуживания DNS с расстановкой по адресу, все клиенты должны обращаться к серверу WSUS по одному полному доменному имени. Это позволит DNS-серверу возвращать адрес ближайшего к клиенту сервера.
  - d. **Неправильный.** Дополнительные серверы BIND позволяют DNS-серверам, работающим под управлением других операционных систем, размещать данные зон, полученные от DNS-серверов Windows. Это никак не связано с развертыванием WSUS.
  - e. **Неправильный.** Настройка файла хостов не решит проблему. Запросы к файлам хостов не возвращают результаты с учетом IP-адреса запрашивающего хоста.
2. **Правильный ответ: С.**

- a. **Неправильный.** Каждый факультет должен иметь возможность одобрять обновления, поэтому подчиненные серверы не следует настраивать как реплики.
  - b. **Неправильный.** Серверы в режиме реплики не позволяют локальным администраторам одобрять обновления.
  - c. **Правильный.** Один вышестоящий сервер, получающий обновления из Интернета, и пять подчиненных автономных серверов, по одному для каждого факультета, удовлетворяют условиям вопроса. Это позволяет минимизировать интернет-трафик и дает каждому факультету возможность одобрять или отклонять обновления.
  - d. **Неправильный.** Хотя пять автономных серверов позволят факультетам независимо одобрять обновления, трафик между университетом и службой обновлений Microsoft не будет минимизирован.
3. **Правильные ответы: А и С.**
  - a. **Правильный.** Следует создать группы компьютеров на сервере WSUS и включить в них клиентов, используя групповую политику, примененную к подразделениям департаментов.
  - b. **Неправильный.** GPO следует связывать с подразделениями, а не с доменом.
  - c. **Правильный.** Следует создать группы компьютеров на сервере WSUS и включить в них клиентов, используя групповую политику, примененную к подразделениям департаментов.
  - d. **Неправильный.** Нет необходимости создавать группы безопасности. Требуется создать группу компьютеров WSUS.
  - e. **Неправильный.** Нет необходимости создавать группы безопасности. Требуется создать группу компьютеров WSUS.
4. **Правильный ответ: С.**
  - a. **Неправильный.** Хотя это возможно, если приложить много усилий, создание запланированной задачи — не лучший способ развертывания обновлений при помощи WSUS. Следует создать правило автоматического одобрения, указав в качестве целевой группу компьютеров WSUS **Patch-Test**.
  - b. **Неправильный.** Если для правила автоматического одобрения в качестве целевой указать группу **Все компьютеры**, обновления будут развертываться на всех компьютерах, а не только на компьютерах из группы **PatchTest**.
  - c. **Правильный.** Правила автоматического одобрения используют группы компьютеров WSUS в качестве целевых.
  - d. **Неправильный.** Правила автоматического одобрения в качестве целевых групп используют группы компьютеров WSUS, а не группы безопасности.
5. **Правильный ответ: С.**
  - a. **Неправильный.** Этот отчет показывает число компьютеров, на которые не установлено обновление, но не предоставляет подробной информации об отдельных компьютерах.

- b. **Неправильный.** Этот отчет содержит сводную информацию о компьютерах и обновлениях, но не предоставляет подробной информации об отдельных компьютерах.
- c. **Правильный.** Этот отчет предоставляет информацию о каждом обновлении, включая список компьютеров и состояние обновления. На странице с информацией о проблемах с обновлениями можно быстро найти нужные компьютеры.
- d. **Неправильный.** Этот отчет предоставляет информацию о состоянии обновлений, по одной странице на компьютер. Хотя можно изучить каждую страницу такого отчета, чтобы решить поставленную задачу, проще и быстрее создать детальный отчет о состоянии обновлений.

## Глава 8. Лабораторная работа

### Задание 1

1. Следует настроить политики аудита системы, расположенные в разделе групповой политики **Конфигурация компьютера | Политики | Параметры Windows | Параметры безопасности | Конфигурация расширенной политики аудита** (Computer Configuration | Policies | Windows Settings | Advanced Audit Policy Configuration). Для настройки этих политик используйте редактор управления групповой политикой, а для просмотра результата аудита — средство просмотра событий.
2. Данные, имеющие отношение к национальной безопасности, нельзя удалять, они должны храниться бессрочно. К таким данным относится и криминалистическая информация об атаках и попытках доступа к таким данным.
3. Веб-серверы в периферийной сети — наиболее вероятные цели для DoS-атак, а потому требуют особой защиты, например, при помощи IP-фильтрации и черных списков.

### Задание 2

1. Учетную запись технического директора следует добавить в локальную группу **Создатели отчетов WSUS**. Это позволит создавать отчеты без предоставления лишних административных привилегий.
2. Подчиненные серверы WSUS в дополнительных офисах следует настроить как реплики WSUS. При этом одобрения обновлений и группы компьютеров, настроенные на сервере WSUS в главном офисе, автоматически будут наследоваться подчиненными серверами.
3. Следует создать детальный отчет о состоянии обновлений и найти в нем страницу со списком компьютеров, на которые не удалось установить обновления.

## Глава 9

### Занятие 1

1. **Правильный ответ: В.**

- a. **Неправильный.** L2TP/IPsec использует порт 1701, и по условиям задания трафик будет блокироваться.
- b. **Правильный.** SSTP использует порт 443, и по условиям задания трафик будет разрешен.
- c. **Неправильный.** PPTP использует порт 1723, и по условиям задания трафик будет блокироваться.
- d. **Неправильный.** IKEv2 использует порт UDP 500, и по условиям задания трафик будет блокироваться.

2. **Правильный ответ: D.**

- a. **Неправильный.** Протокол L2TP/IPsec не поддерживает автоматическое переподключение после выхода из режима гибернации. При повторной установке подключения VPN с использованием этого протокола придется заново проходить проверку подлинности.
- b. **Неправильный.** Протокол SSTP не поддерживает автоматическое переподключение после выхода из режима гибернации. При повторной установке подключения VPN с использованием этого протокола придется заново проходить проверку подлинности.
- c. **Неправильный.** Протокол PPTP не поддерживает автоматическое переподключение после выхода из режима гибернации. При повторной установке подключения VPN с использованием этого протокола придется заново проходить проверку подлинности.
- d. **Правильный.** Протокол IKEv2 поддерживает автоматическое переподключение в течение 8 часов после установки исходного подключения.

3. **Правильные ответы: А и В.**

- a. **Правильный.** К VPN-серверу SSTP под управлением Windows Server 2008 R2 могут подключаться компьютеры под управлением Windows Vista с пакетом обновлений 1 и Windows 7.
- b. **Правильный.** К VPN-серверу SSTP под управлением Windows Server 2008 R2 могут подключаться компьютеры под управлением Windows Vista с пакетом обновлений 1 и Windows 7.
- c. **Неправильный.** Компьютеры под управлением Windows XP Professional не могут подключаться к VPN-серверу SSTP под управлением Windows Server 2008 R2.
- d. **Неправильный.** Компьютеры под управлением Windows 2000 с пакетом обновлений 2 не могут подключаться к VPN-серверу SSTP под управлением Windows Server 2008 R2.

4. **Правильный ответ: D.**

- a. **Неправильный.** Данные учета NPS создаются на сервере NPS, который является также сервером RADIUS, а не на клиенте RADIUS.

- b. **Неправильный.** Данные учета NPS создаются на сервере NPS, который является также сервером RADIUS, а не на клиенте RADIUS.
  - c. **Неправильный.** Компьютер, на котором работает SQL Server, не пересылает данные учета RADIUS на сервер NPS; наоборот, сервер NPS пересылает данные учета RADIUS в базу данных SQL Server.
  - d. **Правильный.** В консоли NPS можно указать, что все данные учета NPS должны записываться в базу данных SQL Server, а не в локальные файлы журнала.
5. **Правильный ответ: С.**
- a. **Неправильный.** Технология DirectAccess доступна только в Windows 7 Enterprise и Ultimate.
  - b. **Неправильный.** Нельзя использовать DirectAccess в Windows Vista Enterprise. Эта технология доступна только в Windows 7 Enterprise и Ultimate.
  - c. **Правильный.** Технология DirectAccess доступна только в Windows 7 Enterprise и Ultimate.
  - d. **Неправильный.** Нельзя использовать DirectAccess в Windows 7 Home Premium. Эта технология доступна только в Windows 7 Enterprise и Ultimate.

## Занятие 2

1. **Правильный ответ: А.**

- a. **Правильный.** Принудительная защита IPsec позволяет разрешать и запрещать доступ к определенным портам. Значит, можно разрешать доступ к порту RDP только работоспособным компьютерам, а доступ к портам HTTP и HTTPS — всем компьютерам.
- b. **Неправильный.** 802.1X распределяет клиентов по разным VLAN в зависимости от работоспособности. Работоспособные и неработоспособные клиенты будут направлены в разные VLAN. Коммутаторы, работающие на втором уровне OSI, нельзя настроить так, чтобы они блокировали отдельные порты TCP/UDP (но некоторые коммутаторы могут отдавать приоритет определенному трафику), хотя в будущем это может измениться. В общем случае, термин *порт* для коммутатора означает интерфейс.
- c. **Неправильный.** Принудительная защита DHCP распределяет клиентов по разным IP-сетям в зависимости от работоспособности. Ее нельзя настроить для разрешения доступа к одному порту и запрета к другому.
- d. **Неправильный.** Принудительная защита VPN применяется для удаленных клиентов и не работает во внутренней сети, так как не влияет на клиентов, не являющихся удаленными.

2. **Правильные ответы: А и D.**

- a. **Правильный.** Использование операционной системы в качестве условия позволит применять разные правила к клиентам под управлением Windows XP и Windows Vista.

- b. **Неправильный.** Не следует создавать VLAN. Следует создать политику с операционной системой в качестве условия.
  - c. **Неправильный.** Проверку должны пропускать клиенты под управлением Windows XP, а не Windows Vista.
  - d. **Правильный.** Если настроить политику, разрешающую клиентам под управлением Windows XP пропускать проверку, клиенты с Windows Vista все равно будут проверяться.
3. **Правильный ответ: С.**
- a. **Неправильный.** Контроллер домена, работающий под управлением Windows Server 2003, не требуется обновлять для поддержки NAP для DHCP.
  - b. **Неправильный.** DNS-сервер не требуется обновлять для поддержки NAP для DHCP.
  - c. **Правильный.** Клиент безопасности DHCP имеется только в Windows Server 2008 и 2008 R2. Для поддержки NAP для DHCP необходимо обновить Windows Server 2003 до Windows Server 2008 или 2008 R2.
  - d. **Неправильный.** Сервер NPS не требуется обновлять для поддержки NAP для DHCP.
4. **Правильные ответы: А и В.**
- a. **Правильный.** Для использования принудительной защиты для IPsec требуется центр регистрации работоспособности и центр сертификации под управлением Windows Server 2008.
  - b. **Правильный.** Для использования принудительной защиты для IPsec требуется центр регистрации работоспособности и центр сертификации под управлением Windows Server 2008.
  - c. **Неправильный.** Для использования принудительной защиты для IPsec не требуется DHCP-сервер, так как можно статически настроить адреса.
  - d. **Неправильный.** Серверы HCAP используются совместно с Cisco Network Access Control и не применяются для принудительной защиты IPsec.
5. **Правильные ответы: А и С.**
- a. **Правильный.** Роль сервера NPS в среде, где разворачивается принудительная защита 802.1X, должна размещаться на компьютере под управлением Windows Server 2008.
  - b. **Неправильный.** Прокси-сервер RADIUS для принудительной защиты 802.1X не требуется.
  - c. **Правильный.** Для разворачивания принудительной защиты 802.1X клиентские компьютеры должны иметь клиент безопасности EAPHost.
  - d. **Неправильный.** HCAP требуется только при использовании клиентов Cisco Network Access Control. Хотя в сети могут использоваться коммутаторы Cisco, для принудительной защиты 802.1X установка роли сервера HCAP не требуется.



## Глава 9. Лабораторная работа

### Задание 1

1. В Сиднее следует использовать RD-CAP.
2. Следует использовать SSTP, так как открыт порт 443, используемый этим протоколом.
3. В Мельбурне следует использовать принудительную защиту доступа к сети для VPN.

### Задание 2

1. Поскольку некоторые устаревшие серверы компании не поддерживают IPsec, следует использовать принудительную защиту DHCP, пока пилотная программа не будет успешно завершена.
2. Когда пилотная программа будет успешно завершена, следует использовать принудительную защиту 802.1X. Это соответствует требованию ограничения доступа на уровне коммутатора для компьютеров, не соответствующим политике работоспособности.
3. Создайте группу серверов обновлений. После развертывания принудительной защиты 802.1X создайте отдельную VLAN, разрешающую доступ к серверам обновлений, но блокирующую доступ к производственной сети.

## Глава 10

### Занятие 1

1. **Правильный ответ: В.**
  - a. **Неправильный.** Массив RAID 0 (чередование дисков) не обеспечивает отказоустойчивость.
  - b. **Правильный.** Если есть два диска, и отказоустойчивость приоритетнее производительности, следует создать массив RAID 1 (зеркальное отражение).
  - c. **Неправильный.** Для создания массива RAID 5 требуется минимум три диска. По условиям задания доступно только два диска.
  - d. **Неправильный.** В Windows Server 2008 R2 нельзя создать программный массив RAID 1+0.
2. **Правильный ответ: В.**
  - a. **Неправильный.** Имя для обращения к доменному пространству имен имеет формат `\\домен\пространство_имен`.
  - b. **Правильный.** Имя для обращения к доменному пространству имен имеет формат `\\домен\пространство_имен`.
  - c. **Неправильный.** Имя для обращения к доменному пространству имен имеет формат `\\домен\пространство_имен`.

- d. **Неправильный.** Имя для обращения к доменному пространству имен имеет формат `\\домен\пространство_имен`.

3. **Правильный ответ: D.**

- a. **Неправильный.** Диспетчер ресурсов файлового сервера используется для создания фильтров блокировки файлов, квот и срока действия файлов. Этот диспетчер не имеет отношения к организации совместной работы и поддержке версий файлов.
- b. **Неправильный.** DFS, изолированная или доменная, не предоставляет функций для совместной работы с файлами и поддержки версий.
- c. **Неправильный.** DFS, изолированная или доменная, не предоставляет функций для совместной работы с файлами и поддержки версий.
- d. **Правильный.** SharePoint Foundation 2010 позволяет совместно работать с файлами и обеспечивает поддержку версий.

4. **Правильный ответ: D.**

- a. **Неправильный.** Переопределение сортировки ссылок позволяет изменить приоритет конечных объектов. Оно не позволяет ограничить просмотр файлов и папок в пространстве имен DFS.
- b. **Неправильный.** Автономные файлы позволяют использовать содержимое специальным образом настроенных общих ресурсов без доступа к сети. Они не позволяют ограничить просмотр файлов и папок в пространстве имен DFS.
- c. **Неправильный.** Компонент BranchCache повышает доступность файлов в офисах филиалов. Он не позволяет ограничить просмотр файлов и папок в пространстве имен DFS.
- d. **Правильный.** Перечисление на основе доступа позволяет настроить пространство имен DFS так, чтобы пользователи видели только те файлы и папки, к которым имеют доступ.

5. **Правильные ответы: C и D.**

- a. **Неправильный.** В этом случае пользователь должен выбрать файлы, которые будут доступны в автономном режиме. Это не гарантирует, что при следующем запуске исполняемого файла он будет взят из кэша, а не из общего ресурса.
- b. **Неправильный.** Этот переключатель запрещает кэширование файлов.
- c. **Правильный.** Чтобы при следующем запуске исполняемый файл извлекался из кэша, а не общего ресурса на сервере, следует установить переключатель **Все открываемые пользователем файлы и программы доступны в автономном режиме** и установить флажок **Оптимизировать производительность**.
- d. **Правильный.** Чтобы при следующем запуске исполняемый файл извлекался из кэша, а не общего ресурса на сервере, следует установить переключатель **Все открываемые пользователем файлы и программы доступны в автономном режиме** и установить флажок **Оптимизировать производительность**.

## Занятие 2

### 1. Правильный ответ: С.

- a. **Неправильный.** Удаленное разностное сжатие используется для передачи данных с минимальным расходом трафика. Напрямую к устройствам Fibre Channel оно не относится.
- b. **Неправильный.** UDDI используется веб-службами и не имеет отношения к Fibre Channel.
- c. **Правильный.** Если сервер будет обращаться к LUN через несколько портов Fibre Channel или адаптеров инициатора iSCSI.
- d. **Неправильный.** RPC через прокси HTTP не имеет прямого отношения к устройствам хранения Fibre Channel.

### 2. Правильный ответ: D.

- a. **Неправильный.** Составной LUN не повышает производительность ввода-вывода и не обеспечивает отказоустойчивость.
- b. **Неправильный.** Чередующийся LUN обладает большей производительностью, чем простой LUN, но не обеспечивает отказоустойчивости.
- c. **Неправильный.** Простой LUN не повышает производительность ввода-вывода и не обеспечивает отказоустойчивость.
- d. **Правильный.** Чередующийся LUN с контролем четности (RAID 5) обеспечивает отказоустойчивость и более высокую производительность ввода-вывода по сравнению с простыми, составными и зеркальными LUN.

### 3. Правильный ответ: В.

- a. **Неправильный.** Восстановление размещения — политика MPIO, использующая предпочтительный путь, передавая трафик по альтернативному пути, только когда предпочтительный выйдет из строя.
- b. **Правильный.** Циклический перебор — политика MPIO, использующая все доступные пути между сервером и массивом SAN.
- c. **Неправильный.** Взвешенный путь — политика MPIO, направляющая ввод-вывод по пути, которому администратор назначил наименьший вес.
- d. **Неправильный.** Динамическая наименьшая глубина очереди — политика MPIO, направляющая ввод-вывод по пути с наименьшим числом запросов. Она не распределяет запросы равномерно по всем путям, а направляет запросы с учетом текущей нагрузки на путь.

### 4. Правильный ответ: А.

- a. **Правильный.** Диспетчер хранилищ для сетей SAN используется для создания LUN.
- b. **Неправильный.** Проводник хранилищ используется для управления структурами Fabric Fibre Channel и iSCSI. С его помощью нельзя создавать LUN в массивах хранилищ.
- c. **Неправильный.** Диспетчер устройств не позволяет создавать LUN в массивах Fibre Channel.

- d. **Неправильный.** Оснастка «Управление дисками» не позволяет создавать LUN в массивах Fibre Channel.

## Глава 10. Лабораторная работа

### Задание 1

1. На всех серверах, размещающих реплику, требуется установить службу DFSR.
2. В каждом сайте настройте сервер, содержащий копию пространства имен DFS.
3. Настройте репликацию с топологией «полная сетка».

### Задание 2

1. SharePoint Foundation 2010 или SharePoint Server 2010.
2. Чтобы пользователи имели доступ к общим папкам из дома, следует включить автономные файлы.
3. RAID 1 или RAID 5.

## Глава 11

### Занятие 1

1. **Правильный ответ: А.**
  - a. **Правильный.** Если включена расстановка по адресу, то, когда клиент запрашивает имя хоста, связанное с несколькими IP-адресами, сервер проверяет, существует ли для этого хоста запись в зоне, связанной с подсетью запрашивающего клиента.
  - b. **Неправильный.** Настройка дополнительной зоны DNS не гарантирует, что клиент получит адрес хоста из своей подсети, если циклическое обслуживание DNS может предоставить таковой.
  - c. **Неправильный.** Настройка зоны-заглушки DNS не гарантирует, что клиент получит адрес хоста из своей подсети, если циклическое обслуживание DNS может предоставить таковой.
  - d. **Неправильный.** Настройка параметров сходства не гарантирует, что клиент получит адрес хоста из своей подсети, если циклическое обслуживание DNS может предоставить таковой.
2. **Правильный ответ: А.**
  - a. **Правильный.** Следует настроить режим фильтрации одного узла и убедиться, что весь трафик порта 25 направляется в тот узел, где установлен сервер SMTP.
  - b. **Неправильный.** Не следует настраивать правило фильтрации с отключением диапазона портов. Следует использовать режим фильтрации одного узла.

- c. **Неправильный.** Не следует настраивать правило фильтрации нескольких узлов, так как весь трафик должен направлять на один узел NLB.
  - d. **Неправильный.** Не следует настраивать правило фильтрации нескольких узлов, так как весь трафик должен направляться на один узел NLB.
3. **Правильный ответ: С.**
- a. **Неправильный.** В этом режиме клиенты будут направляться к определенному хосту, а не узлу NLB из локальной подсети.
  - b. **Неправильный.** В этом режиме клиенты не будут направляться к узлу NLB из локальной подсети.
  - c. **Правильный.** В этом режиме клиенты будут направляться к узлу кластера NLB из локальной подсети.
  - d. **Неправильный.** В этом режиме клиенты не будут направляться к узлу NLB из локальной подсети.
4. **Правильный ответ: С.**
- a. **Неправильный.** Команда **Остановить** завершает существующие сеансы и блокирует новые.
  - b. **Неправильный.** Команда **Запустить** используется для возобновления работы узла после его остановки. Она не запрещает создание новых сеансов.
  - c. **Правильный.** Команда **Остановить сток** блокирует создание новых сеансов, но не завершает существующие.
  - d. **Неправильный.** Команда **Приостановить** приостанавливает работу узла кластера, завершая существующие сеансы и запрещая создание новых.

## Занятие 2

1. **Правильные ответы: В и С.**
- a. **Неправильный.** Эта модель используется для кластеров с четным числом узлов.
  - b. **Правильный.** Эта модель используется для кластеров с нечетным числом узлов.
  - c. **Правильный.** Хотя Microsoft не рекомендует использовать эту модель, она подходит для кластеров с нечетным числом узлов.
  - d. **Неправильный.** Эта модель используется для кластеров с четным числом узлов.
2. **Правильный ответ: А.**
- a. **Правильный.** В режиме «Большинство узлов и общих ресурсов» для хранения данных конфигурации используется общий ресурс, и кластер может продолжать работу, если половина узлов выйдет из строя.
  - b. **Неправильный.** Диск-свидетель хранится в общем ресурсе.
  - c. **Неправильный.** При использовании общего ресурса данные конфигурации кластера остаются доступными в этом ресурсе, а значит, этот ответ неправильный.
  - d. **Неправильный.** Эта модель кворума позволяет кластеру работать при выходе из строя половины узлов.

3. **Правильные ответы: С и D.**

- a. **Неправильный.** Windows Server 2008 R2 Foundation не поддерживает отказоустойчивую кластеризацию. Такую поддержку имеют только версии Datacenter и Enterprise.
- b. **Неправильный.** Windows Server 2008 R2 Standard не поддерживает отказоустойчивую кластеризацию. Такую поддержку имеют только версии Datacenter и Enterprise.
- c. **Правильный.** Поддержку отказоустойчивой кластеризации имеют версии Windows Server 2008 R2 Datacenter и Enterprise.
- d. **Правильный.** Поддержку отказоустойчивой кластеризации имеют версии Windows Server 2008 R2 Datacenter и Enterprise.

4. **Правильный ответ: D.**

- a. **Неправильный.** Кластер с моделью кворума «Большинство узлов и дисков» продолжает работать, если доступна хотя бы половина узлов. Это значит, что по условиям задания из строя должны выйти пять узлов.
- b. **Неправильный.** Кластер с моделью кворума «Большинство узлов и дисков» продолжает работать, если доступна хотя бы половина узлов. Это значит, что по условиям задания из строя должны выйти пять узлов.
- c. **Неправильный.** Кластер с моделью кворума «Большинство узлов и дисков» продолжает работать, если доступна хотя бы половина узлов. Это значит, что по условиям задания из строя должны выйти пять узлов.
- d. **Правильный.** Кластер с моделью кворума «Большинство узлов и дисков» продолжает работать, если доступна хотя бы половина узлов. Это значит, что по условиям задания из строя должны выйти пять узлов.

## Глава 11. Лабораторная работа

1. Доступность базы данных SQL Server можно повысить при помощи отказоустойчивой кластеризации. SQL Server 2008 R2 поддерживает кластеризацию, и единственный способ обеспечить доступность СУБД в случае выхода сервера из строя — создать отказоустойчивый кластер. Исходя из условий задания, можно сделать вывод, что основной веб-сайт работает на одном сервере. Следует добавить еще один сервер и использовать NLB, чтобы веб-приложение могло работать в случае выхода сервера из строя. Для веб-приложения, работающего на сервере Linux, следует использовать циклическое обслуживание DNS, так как NLB Windows использовать нельзя.
2. Настройте отказоустойчивый кластер, использующий общее хранилище в SAN. После создания отказоустойчивого кластера можно развернуть в нем SQL Server и перенести туда базу данных.
3. Наиболее подходящая модель кворума — «Большинство узлов и общих ресурсов», так как в ней диск-свидетель хранится в общем ресурсе. Так как в задании речь идет только о двух серверах, лучше хранить диск-свидетель отдельно.

## Глава 12

### Занятие 1

#### 1. Правильный ответ: С.

- a. **Неправильный.** Если выбрать для службы тип запуска **Автоматически**, она будет запускаться во время загрузки компьютера. Скорее всего, служба, описанная в задании, имеет такой тип запуска, что приводит к замедлению загрузки. Служба не должна запускаться сразу после включения компьютера, поэтому этот тип запуска не требуется.
- b. **Неправильный.** Тип запуска **Вручную** позволяет операционной системе запускать службу при необходимости. Службу с таким типом запуска может запускать также администратор или оператор сервера. Запуск вручную не удовлетворяет условию задания, по которому служба должна запускаться автоматически.
- c. **Правильный.** Служба с типом запуска **Автоматически (отложенный запуск)** запускается сразу после завершения загрузки компьютера. Выбор такого типа запуска для описанной службы ускорит процесс загрузки и позволит службе запускаться автоматически.
- d. **Неправильный.** Если выбрать тип запуска **Отключена**, служба не будет запускаться, даже когда требуется. Это противоречит условиям задания.

#### 2. Правильный ответ: А.

- a. **Правильный.** Монитор стабильности системы отслеживает установку приложений. Он позволяет определить, установлено ли приложение, и если да, то когда именно.
- b. **Неправильный.** Центр поддержки может предупреждать о том, что драйвер или приложение не работает должным образом. Он не дает информации о времени установки приложений.
- c. **Неправильный.** Группы DCS собирают информацию о текущей производительности и конфигурации. Они не дают информации о времени установки приложений.
- d. **Неправильный.** Системный монитор используется для просмотра счетчиков производительности в реальном времени и для анализа данных из групп DCS. Он не дает информации о времени установки приложений.

#### 3. Правильные ответы: А, В, С и Е.

- a. **Правильный.** Монитор стабильности системы записывает данные о сбоях приложений.
- b. **Правильный.** Монитор стабильности системы записывает данные об ошибках Windows.
- c. **Правильный.** Монитор стабильности системы записывает данные об установке и удалении приложений.
- d. **Неправильный.** Сведения о запуске и остановке служб записываются в журнал событий, а не в монитор стабильности системы.



- е. **Правильный.** Монитор стабильности системы не записывает данные о сбоях драйверов устройств.
4. **Правильный ответ: А.**
- а. **Правильный.** Для настройки службы сборщика событий используется команда Wecutil.
  - б. **Неправильный.** Команда Winrm используется для настройки службы WinRM. Обычно она выполняется на компьютере-источнике. Можно выполнить ее на компьютере-сборщике, если настраивается подписка, инициированная источником, но это не соответствует условиям задания, поскольку сервер VAN-SRV1 собирает события с сервера VAN-DC1. В любом случае, эта команда не используется для настройки службы сборщика событий.
  - с. **Неправильный.** Команда Winrm используется для настройки службы WinRM. С параметром -q она запускается в тихом режиме. Эта команда не используется для настройки службы сборщика событий.
  - д. **Неправильный.** Эта команда запускает оснастку управления групповой политикой. Групповую политику можно использовать для добавления компьютеров-источников в подписку, инициированную источником, но это не относится к условиям задания. В любом случае, эта команда не используется для настройки службы сборщика событий.
5. **Правильный ответ: В.**
- а. **Неправильный.** На вкладке **Общие** можно указать, как часто будет обновляться диаграмма, и сколько данных будет в ней отображаться, прежде чем системный монитор начнет перезаписывать данные в левой части диаграммы. Можно также указать, какие элементы диаграммы будут отображаться, и какие значения будут отображаться в режиме отчета и гистограммы. Здесь нельзя настроить отображение текущей активности в реальном времени или просмотр данных, собранных группами DCS.
  - б. **Правильный.** На вкладке **Источник** можно выбрать отображение текущей активности в реальном времени или просмотр данных, собранных группами DCS. Если просматриваются данные групп DCS, можно определить временной диапазон, который будет отображаться в системном мониторе.
  - с. **Неправильный.** На вкладке **Данные** можно настроить отображение определенных счетчиков. В списке счетчиков можно выбрать счетчик, который требуется настроить, и изменить цвет, ширину и стиль линии. Здесь нельзя настроить отображение текущей активности в реальном времени или просмотр данных, собранных группами DCS.
  - д. **Неправильный.** На вкладке **График** можно выбрать тип прокрутки и тип диаграммы. Здесь нельзя настроить отображение текущей активности в реальном времени или просмотр данных, собранных группами DCS.
  - е. **Неправильный.** Если открыто несколько окон системного монитора одновременно, на вкладке **Оформление** можно изменить цвет фона и других элементов, чтобы было проще различать окна. Здесь нельзя настроить отображение текущей активности в реальном времени или просмотр данных, собранных группами DCS.

## Глава 12. Лабораторная работа

### Задание 1

1. Использовать группы DCS для записи базовых показателей производительности, когда сервер нормально работает. Затем вручную запустить те же группы DCS, когда возникнет проблема с производительностью. Если эта проблема возникает в определенное время дня, можно запланировать запись данных в это время. Затем следует использовать системный монитор для анализа результатов, их сравнения с базовыми показателями и определения факторов, являющихся источником проблемы.
2. Следует обратиться к серверу DEN\_FS1 с сервера DEN\_SPARE через удаленный рабочий стол и запустить монитор стабильности системы. Это позволит выяснить, когда были установлены или обновлены приложения на сервере.
3. Использовать пересылку событий для сбора событий, связанный с нехваткой места на диске, на сервере DEN\_SPARE, который должен быть настроен как компьютер-сборщик. Затем выполнять мониторинг журнала событий на сервере DEN\_SPARE, чтобы выявлять компьютеры, на которых заканчивается свободное дисковое пространство, привязав задачу с оповещением к соответствующему событию.

### Задание 2

1. Следует использовать инструмент **Отчеты** из консоли **Системный монитор** для создания регулярных отчетов диагностики системы на каждом сервере. Отчет диагностики системы предоставляет информацию о состоянии аппаратных ресурсов, времени ответов системы и процессах на локальном компьютере, а также системную информацию и данные конфигурации.
2. Следует использовать **Монитор ресурсов**. Этот инструмент позволяет просматривать требуемую информацию в реальном времени и фильтровать результаты, а также управлять процессами и службами для решения проблем с зависшими приложениями.
3. Process Explorer можно настроить так, чтобы он загружался вместо диспетчера задач.

## Глава 13

### Занятие 1

1. **Правильный ответ: В.**
  - a. **Неправильный.** Члены группы «Опытные пользователи» не могут выполнять архивацию вручную.
  - b. **Правильный.** Члены группы «Операторы архива» не могут настраивать расписание архивации, но могут выполнять архивацию вручную на компьютерах под управлением Windows Server 2008.

- c. **Неправильный.** Хотя локальные администраторы могут выполнять архивацию вручную, добавление пользователя в эту группу предоставит ему лишние административные привилегии.
  - d. **Неправильный.** Члены группы «Пользователи удаленного рабочего стола» не могут выполнять архивацию вручную.
2. **Правильные ответы: А и С.**
- a. **Правильный.** Сценарий будет выполняться с учетными данными локального администратора, поэтому необходимо указать дополнительные учетные данные для доступа к удаленной сетевой папке. Параметр `-include` позволяет указать папку, которую требуется архивировать.
  - b. **Неправильный.** Учетные данные локального администратора не позволят получить доступ к удаленной сетевой папке (если только локальный администратор на удаленном компьютере не имеет такой же пароль).
  - c. **Правильный.** Сценарий необходимо выполнять от имени локального администратора, поскольку утилита Wbadmin.exe может работать только с повышенными привилегиями.
  - d. **Неправильный.** Сценарий необходимо запускать с учетными данными администратора, поскольку утилита Wbadmin.exe может работать только с повышенными привилегиями.
  - e. **Неправильный.** В задании указано, что задание должно выполняться каждые три часа.
3. **Правильные ответы: А, В, С и Е.**
- a. **Правильный.** Система архивации данных Windows Server может записывать данные, полученные при архивации по расписанию, на локальные внешние диски USB 2.0.
  - b. **Правильный.** Система архивации данных Windows Server может записывать данные, полученные при архивации по расписанию, на локальные внешние диски IEEE 1394.
  - c. **Правильный.** Система архивации данных Windows Server может записывать данные, полученные при архивации по расписанию, на внутренние диски IDE.
  - d. **Неправильный.** Система архивации данных Windows Server не может записывать данные, полученные при архивации по расписанию, на устройства SAN iSCSI.
  - e. **Правильный.** Система архивации данных Windows Server может записывать данные, полученные при архивации по расписанию, на тома или внешние диски.
  - f. **Неправильный.** Система архивации данных Windows Server не может записывать на DVD данные, полученные при архивации по расписанию.
4. **Правильный ответ: С.**
- a. **Неправильный.** Если выбрать этот параметр, время, затраченное на архивацию, будет прямо пропорционально объему архивируемых данных. Производительность сервера не снижается. Нельзя настроить разные тома для выполнения полной и добавочной архивации.

- b. **Неправильный.** Если выбрать этот параметр, скорость архивации увеличится за счет отслеживания изменений между последним и текущим архивами. Производительность сервера может значительно снижаться во время архивации. Нельзя настроить разные тома для выполнения полной и добавочной архивации.
  - c. **Правильный.** Если отдельные тома интенсивно используются, можно настроить выборочную архивацию. Это позволит настроить разные тома для выполнения полной и добавочной архивации.
  - d. **Неправильный.** Полную архивацию VSS следует выбирать, когда для архивации хоста не используются другие программы резервного копирования. Если выбрать этот параметр, будут обновлены атрибуты архивации всех файлов и очищены журналы приложений. Это параметр конфигурации архивации, а не оптимизации производительности.
  - e. **Неправильный.** Копировать архив VSS следует, когда для архивации приложений, расположенных на томах текущего архива, используются дополнительные программы. Если выбрать такой тип архивации, журналы приложений сохраняются. Это параметр конфигурации архивации, а не оптимизации производительности.
5. **Правильные ответы: А, В и С.**
- a. **Правильный.** Выполняя однократную архивацию данных состояния системы на контроллере домена под управлением Windows Server 2008 R2, можно записывать данные в сетевую папку.
  - b. **Правильный.** Выполняя однократную архивацию данных состояния системы на контроллере домена под управлением Windows Server 2008 R2, можно записывать данные на DVD. Если размер архива превышает размер одного DVD, будет предложено вставить дополнительные диски.
  - c. **Правильный.** Выполняя однократную архивацию данных состояния системы на контроллере домена под управлением Windows Server 2008 R2, можно записывать данные на внешний диск USB 2.0.
  - d. **Неправильный.** Выполняя архивацию состояния системы вручную, нельзя записывать данные на устройство SAN iSCSI.

## Занятие 2

1. **Правильный ответ: С.**
- a. **Неправильный.** Эта команда восстанавливает объект Solar, расположенный в подразделении Pluto.
  - b. **Неправильный.** Для восстановления объекта, будь то учетная запись пользователя или компьютера, необходимо использовать команду Restore Object.
  - c. **Правильный.** Для восстановления учетной записи компьютера Pluto из подразделения Solar следует выполнить команду Restore Object "cn=Pluto,OU=Solar,dc=Contoso,dc=internal".

- d. **Неправильный.** Для восстановления объекта, будь то учетная запись пользователя или компьютера, необходимо использовать команду Restore Object.

2. **Правильный ответ: С.**

- a. **Неправильный.** Члены группы «Опытные пользователи» не могут восстанавливать данные из архивов.
- b. **Неправильный.** Члены группы «Опытные пользователи» не могут восстанавливать данные из архивов.
- c. **Правильный.** Выполнять восстановление могут пользователи, входящие в группу администраторов или операторов архива на сервере, где будет выполняться восстановление. Следует использовать группу «Операторы архива», так как члены этой группы имеют меньше привилегий, чем администраторы.
- d. **Неправильный.** Хотя администраторы могут выполнять восстановление файлов и папок, эту задачу могут выполнять и операторы архива. Операторы архива имеют меньше привилегий, чем администраторы, поэтому в соответствии с принципом наименьших привилегий следует использовать группу «Операторы архива».

3. **Правильный ответ: D.**

- a. **Неправильный.** Сначала требуется восстановить объект-контейнер AD DS, а затем выполнить вторую команду для восстановления его содержимого.
- b. **Неправильный.** Подразделение называется Australia, а не Melbourne, поэтому в коде ошибка.
- c. **Неправильный.** Необходимо направить выходные данные командлета Get-ADObject в командлет Restore-ADObject, а не наоборот.
- d. **Правильный.** Эта команда восстанавливает учетную запись компьютера Melbourne и все остальные дочерние объекты подразделения Australia.

4. **Правильный ответ: С.**

- a. **Неправильный.** Автоматическое восстановление выполнять не следует, так как при этом с сервера будет удалена существующая операционная система и все данные.
- b. **Неправильный.** Подключать архивные образы как тома не следует, так как это не приведет к восстановлению функциональности сервера.
- c. **Правильный.** Восстановление архивных образов на виртуальной машине Hyper-V позволит поддерживать функциональность служб до восстановления физического сервера.
- d. **Неправильный.** Восстановление данных состояния системы с одного сервера на другом не решит проблему и может привести к нестабильности системы.

## Глава 13. Лабораторная работа

### Задание 1

1. Для записи данных, полученных при запланированной архивации, к серверу должен быть подключен внутренний или внешний диск USB 2.0 или IEEE 1394. Запись можно также вести на внутренние жесткие диски или в сетевые папки, но жесткие диски, скорее всего, будут использоваться для записи организационных архивов.
2. Система архивации данных Windows Server позволяет записывать данные, полученные при запланированной архивации, только на локальные или внешние жесткие диски, тома и сетевые папки. Для выполнения архивации в удаленном расположении носитель для записи архивов требуется доставить в это удаленное расположение. Это значит, что следует использовать внешние устройства, которые легко транспортировать, например, диски USB 2.0 и IEEE 1394.
3. Настройте теневые копии для каждой общей папки и проинструктируйте пользователей, как обращаться к ним. Это даст пользователям возможность восстанавливать свои файлы и уменьшит нагрузку на персонал службы поддержки.

### Задание 2

1. Первыми следует восстановить контроллеры корневого домена леса, так как они необходимы для выполнения некоторых операций в остальных доменах леса.
2. Восстановите контроллеры домена, используя полные архивы серверов, полученные в пятницу. Выполните принудительное восстановление объектов, удаленных в четверг, используя архивы состояния системы, полученные в среду.
3. Чтобы восстановить данные на сервере `filesolve.hq.fabrikam.internal` в максимально полном составе, восстановите полный архив сервера, а затем восстановите архив общих папок, полученный вручную.

# Об авторах

**Йен Маклин** (Ian Mclean), MCSE, MCTS, MCITP, MCT, имеет более 40 лет опыта работы в компьютерной индустрии, включая коммерцию и обучение. Карьеру начал как инженер-электронщик, затем стал заниматься дистанционным обучением и преподаванием в университете в качестве профессора. В настоящий момент управляет собственной консалтинговой компанией. Йен написал более 20 книг и много технических статей. Работает с серверными операционными системами Microsoft с 1997 г.

**Орин Томас** (Orin Thomas), MCITP, MCT, MVP, тренер, лектор, автор более десятка книг, выпущенных в издательстве Microsoft Press. Обладает сертификационными статусами MCITP Server Administrator и Enterprise Administrator. Член группы Melbourne Security and Infrastructure Group и участник программы Microsoft vTSP. Последние книги Орина посвящены Windows 7 и Exchange Server 2010. Можете следить за ним в Твиттере: @orinthomas.



Томас Орин, Маклин Йен

# **Администрирование Windows Server® 2008**

## **Учебный курс Microsoft**

Подготовлено к печати издательством «Русская редакция»  
125362, Москва, ул. Свободы, д. 17, а/я 14. Тел.: (495) 638-5-638,  
[www.ITbook.ru](http://www.ITbook.ru), [www.rusedit.com](http://www.rusedit.com)

 **РУССКАЯ РЕДАКЦИЯ**

Подписано в печать 21.07.2013 г. Формат 70х100/16.  
Усл. физ. л. 43. Тираж 1000 экз. Заказ №

Отпечатано с готовых диапозитивов в ГУП «Типография «Наука»  
199034, Санкт-Петербург, 9 линия, 12

# Администрирование Windows Server® 2008

2-е издание, дополненное

Учебный  
курс  
Microsoft®

## MCITP

Экзамен **70-646**

### Официальное пособие для самоподготовки

Полностью обновленный курс для новой операционной системы Windows Server 2008 R2! Освоив материалы этого курса, вы изучите все возможности администрирования операционной системы Windows Server 2008 R2. Кроме того, вы подготовитесь к сдаче экзамена 70-646 по программе сертификации MCITP (Microsoft Certified IT Professional).

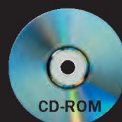
#### В этой книге:

- планирование установки и обновления Windows Server 2008 R2;
- настройка DNS и IPv6;
- планирование структуры Active Directory, приложений и служб сертификации;
- планирование стратегии управления сервером, групповой политики, служб удаленных рабочих столов и делегирования;
- подготовка приложений, данных, служб файлов и печати;
- внедрение решений для обеспечения высокой доступности, хранения, архивации и восстановления данных;
- управление системой безопасности и обновлениями;
- мониторинг и оптимизация производительности сервера.

#### Об авторах:

*Орин Томас (Orin Thomas)* — MCITP, MCT, MVP, IT-консультант, тренер и автор нескольких книг, выпущенных в издательстве Microsoft Press. Обладатель статусов MCITP Windows Server Enterprise Administrator и Server Administrator.

*Йен Маклин (Ian McLean)* — MCITP, MCSE, MCT, имеет более чем сорокалетний опыт работы в компьютерной индустрии, включая коммерцию и обучение. Автор многочисленных учебных пособий, более десяти лет работает с серверными технологиями Microsoft.



#### На прилагаемом компакт-диске:

- демонстрационная версия экзаменационных тестов с автоматическим подсчетом результатов и разъяснением верных и неверных ответов;
- более 200 заданий и вопросов для самопроверки;
- упражнения, которые позволят вам на практике закрепить полученные знания;
- электронные книги на английском языке.

 Windows Server 2008

Издательство  
**Русская редакция**  
Москва,  
ул. Свободы, д. 17, а/я 14  
E-mail: [info@rusedit.com](mailto:info@rusedit.com)  
Internet: [www.rusedit.com](http://www.rusedit.com)  
Тел.: (495) 638-5-638

ISBN 978-5-7502-0427-4



9 785750 204274

 РУССКАЯ РЕДАКЦИЯ