

Федор Зубанов

Active Directory®

подход профессионала

Издание второе, исправленное

Подробное описание
типовых методов
внедрения
и обслуживания
Active Directory

Л РУССКАЯ РЕДАКЦИЯ

Федор **Зубанов**

Active Directory

подход профессионала

Издание 2-е, исправленное

Москва 2003

 РУССКАЯ РЕДАКЦИЯ

УДК 004
ББК 32.973.81-018.2
391

Зубанов Ф. В.

391 Active Directory: подход профессионала. — 2-е изд., испр. —
М.: Издательско-торговый дом «Русская Редакция», 2003. —
544 с.: ил.

ISBN 5-7502-0118-X

В книге обобщен богатый опыт Microsoft Consulting Services в области проектирования, развертывания и эксплуатации службы каталогов Active Directory® в самых разных организациях. Основной упор сделан на методике выявления проблем в работе Active Directory® и способах их устранения. На конкретных примерах разбираются вопросы настройки сетевых служб, репликации и групповых правил. Особое внимание уделяется специфике проектирования Active Directory® в крупных и очень крупных организациях.

Книга состоит из вступления, 6 глав и словаря терминов.

Это издание адресовано системным администраторам и специалистам в области проектирования корпоративных вычислительных систем на базе Windows 2000.

УДК 004
ББК 32.973.81-018.2

Использованные в примерах и упражнениях названия компаний и продуктов, персонажи и события являются вымышленными. Любые совпадения с реальными компаниями, продуктами, людьми и событиями являются случайными.

Active Directory, ActiveX, JScript, Microsoft, Microsoft Press, MSDN, MS-DOS, PowerPoint, Visual Basic, Visual C++, Visual InterDev, Visual SourceSafe, Visual Studio, Win32, Windows и Windows NT являются либо товарными знаками, либо охраняемыми товарными знаками корпорации Microsoft в США и/или других странах. MySQL является охраняемым товарным знаком компании MySQL AB. Все другие товарные знаки являются собственностью соответствующих фирм.

ISBN 5-7502-0118-X

© Зубанов Ф. В., 2002-2003
© Издательско-торговый дом
«Русская Редакция», 2003

Оглавление

Об этой книге	XIII
Структура книги	XIV
Чего здесь нет	XVII
Принятые соглашения	XVII
Проектируем AD, или Мелочей не бывает	1
Что в имени тебе моем?	2
Бизнес определяет имена	2
Имена DNS и имена Active Directory	4
Покажем корень миру	4
Алгоритм именования DNS	6
Именованние объектов Active Directory	6
Именованние пользователей	6
Именованние компьютеров	8
Имена подразделений	9
Одоменивание	9
Один за всех	11
Критерии создания домена	11
Когда одного домена достаточно	11
Преимущества однодоменной модели	13
... все за одного	14
Преимущества многодоменной модели (дерева)	18
Посадим деревья и вырастет лес	19
Преимущества модели с несколькими деревьями	21
Преимущества модели с одним лесом	22
Модель с несколькими лесами	24
Мигрируем с доменной структуры Windows NT	26
Миграция единственного домена	26
Миграция доменной структуры с одним мастер-доменом	27
Миграция доменной структуры с несколькими мастерами	30
Миграция нескольких доменов с попарным доверием	31
Группы и стратегия их использования	32
Рекомендации по использованию универсальных групп	32
Рекомендации по использованию глобальных групп	34
Рекомендации по использованию локальных групп домена	35
Использование особых объединений	37
Административные группы	37
Если ОП создают, значит, это кому-нибудь нужно	38
Модели организационных подразделений	40
Географическая иерархия	40
Организационная иерархия	40

Объектная иерархия	40
Проектная иерархия	41
Административная иерархия	41
Так кому нужны организационные подразделения ?	43
Нужны ли подразделения пользователям?	44
Подразделения нужны администраторам!	46
Делегирование административных полномочий	46
Разбиваем на сайты	47
Так какой же все-таки критерий?	48
Сколько может быть сайтов?	49
Сколько нужно контроллеров и где их размещать	51
Менее 10 пользователей	51
От 10 до 50 пользователей	53
От 50 пользователей	54
Надежная связь между сайтами	55
Топология сетей	55
Межсайтовые связи	56
Объекты связи	59
Серверы-форпосты	59
Отказоустойчивые схемы	63
Мастера операций и Глобальный каталог. Оптимальное размещение	65
Мастер схемы	65
Мастер доменных имен	66
Имитатор PDC	67
Мастер RID	67
Мастер инфраструктуры	67
Глобальные каталоги	68
Примеры размещения	69
Конфигурация контроллеров доменов для удаленных филиалов	71
Политика изменения схемы	72
Когда и как модифицируют схему	73
Применение политики модификации схемы	73
Active Directory, межсетевые экраны и Интернет	75
Подключение доменов через VPN	75
Подключение доменов с использованием IPSec	78
Авторизация ресурсов в DMZ	80
Пример планирования	82
Постановка задачи	83
Предложенная архитектура	85
Леса	85
Домены	86
Сайты	86
Контроллеры доменов	87
Организационные подразделения	88
Группы безопасности	88
Сервер Web и доступ к нему	89
Заключение	90

Установка Active Directory	91
Что делать с DNS	91
Мой первый DNS	92
Так он работает?	94
А что если наблюдаются проблемы?	96
Выводы	98
DNS уже есть. Ну, и что с ним делать?	99
Поговорим о версиях DNS	99
DNS Windows 2000 или BIND версии лучше 8.2.2	100
BIND версии хуже 8.2.2	100
А если сервер DNS расположен за межсетевым экраном?	103
Строим лес доменов	106
Все домены в одном сайте	107
Каждый домен в своем сайте	108
Один домен разбит на несколько сайтов	110
Проблема «островов»	111
Использование «гlossких» имен корневого домена	112
DNS в крупной компании	112
Ну очень крупная компания	116
Так нужна ли служба WINS?	116
Краткий экскурс в историю NetBIOS	116
Как разрешаются имена NetBIOS	118
А нужен ли NetBIOS?	119
Краткие советы по установке серверов WINS	120
Как правильно настроить DHCP	122
Что дает авторизация	122
Зачем нужны суперобласти	123
DHCP сервер в сегментированной сети	125
Динамическая регистрация имен в DNS	125
Какие параметры определять в сети Windows	128
Последовательность применения параметров	128
Как использовать идентификатор пользовательского класса	129
Как проконтролировать работу DHCP	130
DCPROMO и все, что с этим связано	130
Требования, предъявляемые DCPROMO	131
Файлы, создаваемые при работе DCPROMO	133
Файлы базы Active Directory	133
SYSVOL	135
Журналы регистрации	136
Служба синхронизации времени	137
Автоматическая установка контроллера	138
Новое дерево в новом лесу	140
Дополнительный контроллер в домене	140
Новый дочерний домен	141
Новое дерево в лесу	141
Понижение контроллера домена до уровня сервера	142
Описание параметров и значений умолчания	142

Анализируем журналы	145
DCPromo.log	145
DCPromoUI.log	146
Netsetup.log	150
DCPromos.log	151
Как подобрать компьютер?	151
Требования к процессору	153
Требования к оперативной памяти	155
Конфигурация жестких дисков	156
Как проверить работоспособность контроллера домена	156
А если он все-таки не работает?	162
Попробуем выяснить причину	162
Некорректные параметры TCP/IP или ошибки в сети	162
Некорректная работа службы DNS	163
Проблемы с оборудованием, в первую очередь с дисковой подсистемой	163
Проблемы с репликацией Active Directory	163
Проблемы с репликацией FRS	164
Некорректная групповая политика	165
А может, все переустановить?	165
Все работает. Что делать?	166
Обновление контроллера домена Windows NT 4.0 до Windows 2000	167
Кое-что о Windows NT 4.0	167
Обеспечение безопасной миграции	168
Две стратегии миграции	168
Мигрируем домен Windows NT	171
Обновление первичного контроллера домена	171
Откат назад в случае сбоя	173
Совместная работа контроллеров разных версий	174
Алгоритмы установки контроллера домена	178
Алгоритм установки нового контроллера	178
Алгоритм обновления контроллера Windows NT 4.0	178
Заключение	178
Репликация Active Directory	179
Немного о том, как работает репликация	180
Обновления в Active Directory	182
USN	183
Штамп	184
Удаление объекта	186
Процесс репликации от А до Я	186
Создание объекта	186
Модификация объекта	187
Демпфирование распространения изменений	188
Разрешение конфликтов	192
Топология репликации	192
Какой транспорт предпочесть?	194
Синхронная и асинхронная передача	195
Внутрисайтовый транспорт	195
Особенности транспорта SMTP	196

Управление пакетом репликации	197
Автоматическая генерация топологии	198
Простая топология для одного контекста имен	198
Сложная топология для одного контекста имен	198
Топология для нескольких контекстов имен	200
КСС и его возможности	202
Генератор межсайтовой топологии	203
Репликация глобальных каталогов	208
Репликация критических событий	209
Тиражирование паролей	211
Диагностика репликации	212
Выяснение списка партнеров по репликации	214
Active Directory Sites and Services	214
Repadmin /showreps	215
Replication Monitor	218
Контроль состояния партнеров по репликации	220
DsaStat	220
Dcdiag	222
Repadmin	225
Общая информация о параметрах репликации	227
Поиск и устранение проблем репликации	232
Запрет доступа (Access Denied)	233
Вероятная причина	233
Решение	234
Неизвестная служба аутентификации (Authentication service is Unknown)	235
Контроллер домена не может установить связь репликации	235
Связь репликации существует	236
Неверное имя учетной записи цели (Target account name is incorrect)	236
Отсутствие объекта trusted Domain	237
Не совпадает набор SPN	238
Недоступен сервер RPC (RPC Server Not Available)	239
Ошибка поиска в DNS (DNS Lookup failure)	240
Служба каталогов перегружена (Directory service too busy)	240
Причина	241
Разрешение	241
Разница во времени (Ошибка LDAP 82)	242
Причина	243
Устранение	243
Внутренняя ошибка системы репликации	243
Причины	243
Устранение	244
Отсутствие конечной точки (No more end-point)	244
Ошибка LDAP 49	244
Сообщения, не являющиеся ошибками	244
Active Directory replication has been pre-empted	244
Replication posted, waiting	245
Last attempt @ ... was not successful	245
Заключение	245

Групповая политика	247
Общие сведения	247
Клиент, сервер или кто важнее	248
Типы групповых правил	250
Структура и обработка групповой политики	251
Устройство объекта групповой политики	251
Хранение параметров групповой политики	252
Версии и ревизии	255
Клиентские расширения	257
Обработка по медленным каналам связи	258
Периодическое фоновое применение	259
Применение неизменной политики	261
Параметры клиентских расширений	262
Применение групповых правил	263
Изменение последовательности	263
Блокировка наследования	263
Принудительное наследование	265
Перемычки	265
Деактивизация правил	267
Фильтрация	267
История применения правил	270
Где создавать и редактировать правила?	272
Делегирование полномочий	274
Делегирование прав на создание и модификацию ОГП	276
Делегирование полномочий на привязку ОГП к объектам Active Directory	277
Типы правил	277
Правила установки ПО для компьютеров	278
Установки Windows для компьютеров - сценарии	280
Параметры Windows для компьютеров: правила безопасности	281
Правила учетных записей	282
Локальные правила	284
Правила журнала регистрации	289
Параметры Windows для компьютеров: правила групп с ограниченным членством	290
Параметры Windows для компьютеров: правила системных служб	291
Параметры Windows для компьютеров: правила реестра	291
Параметры Windows для компьютеров: правила файловой системы	292
Параметры Windows для компьютеров: правила открытых ключей	292
Параметры Windows для компьютеров: правила IPSecurity	293
Административные шаблоны для компьютеров	294
Правила установки ПО для пользователей	296
Параметры Windows для пользователей: настройка Internet Explorer	298
Параметры Windows для пользователей: сценарии	299
Параметры Windows для пользователей: правила безопасности	300
Параметры Windows для пользователей: служба удаленной установки	300
Параметры Windows для пользователей: перенаправление папок	300
Административные шаблоны для пользователей	303
Планирование групповой политики	306

Начальство хочет, вы - желаете	307
От простого к сложному	308
Советы по применению	309
Один домен	309
Несколько доменов	312
Поиск и устранение проблем	315
Средства поиска проблем	316
GPRELUT	316
GPOTOL	322
ADDIAG	324
SECEDIT	328
FAZAM2000	328
Журналирование	329
Журнал событий приложений	330
Журналы политики для пользователей	332
Журналы установки приложений	335
Общие проблемы групповой политики	335
Зависание компьютера при регистрации пользователя или запуске компьютера	335
Определенная политика не обрабатывается полностью или частично	335
Обрабатывается не тот ОГП	336
Политика вообще не применяется	337
Заключение	337
Active Directory и файловая система	339
Служба репликации файловой системы	340
Как распространяются изменения	340
Инициация тиражирования	341
Избыточность	342
Когда удобно использовать репликацию FRS	343
Работа службы FRS в подробностях	344
Выходная репликация	345
Входная репликация	347
Таблицы службы FRS	349
Объекты Active Directory, используемые FRS	350
Настройка FRS	352
Изменение интервалов опроса Active Directory	352
Установка фильтров	353
Управление расписанием репликации	354
Рекомендации по оптимизации FRS	357
Журналирование	357
Топология репликации	358
Подготовительный каталог	359
Размер журнала NTFS	359
Использование FRS и удаленных хранилищ	360
Использование резервного копирования для начальной конфигурации реплик	360
Не превышайте	362
Поиск и устранение проблем FRS	362

Журналы	363
Журнал регистрации File Replication System	364
Журналы NTFRS	366
Связь между монитором производительности и сообщениями в журнале	370
NTFRSUTL	371
Восстановление реплицируемых файлов	373
Неавторитетное восстановление	374
Авторитетное восстановление	376
Восстановление конфигурации FRS	377
Оптимизация процессов восстановления	378
Сокращение числа серверов, создающих подготовительные файлы	379
Сокращение числа реплицируемых файлов на время выполнения процесса WV-join	380
Разрешение выполнения только одного подключения вектора версий на входном партнере	381
Распределенная файловая система	381
Немного о DFS	381
Таблица PKT	383
Взаимодействие клиента с сервером DFS	385
Репликация DFS	386
Сайты и DFS	388
Предельные возможности и ограничения	388
Ограничения доступа	390
Полезные советы	391
Работа DFS без NetBIOS	391
Резервное копирование пространства имен DFS	392
Использование DfsCmd	392
Использование DfsUtil	392
Делегирование полномочий по управлению DFS	393
Делегирование полномочий модификации конфигурации DFS	394
Делегирование полномочий настройки репликации томов DFS	395
Делегирование полномочий по управлению томами DFS и разграничению доступа	395
Поиск и устранение проблем DFS	396
DfsUtil	396
/list	397
/view	397
/pktinfo	399
Аргументы управления конфигурацией	401
Аргументы отладочного режима	402
Наиболее общие проблемы и их разрешение	403
Обновление сервера до новой версии	403
Изменение имени хоста DFS	404
Удаление последнего корня DFS	404
Перемещение хоста DFS в другой сайт	405
Проблемы доступа к пространству имен DFS	406
Невозможность администрирования DFS	406

Удаление конфигурационной информации DFS	407
Удаление доменных корней	407
Удаление корней отдельно стоящих DFS	407
Заключение	408
Поиск и устранение проблем	409
Алгоритм поиска и устранения проблем Active Directory	410
Резервное копирование Active Directory	417
Чем нужно копировать	419
Что нужно копировать	420
Кто может копировать	421
Файлы, игнорируемые при резервном копировании	421
Актуальность резервной копии	423
Никогда не ставьте время на контроллере больше текущего	424
Восстановление Active Directory	425
Восстановление через переустановку	425
Принудительное назначение мастеров операций с помощью Ntdsutil	427
Восстановление из резервной копии	429
Неавторитетное восстановление	429
Проверка восстановления с помощью Ntdsutil	432
Восстановление на другую технику	433
Если система загрузилась	434
Если система загружается только в безопасном режиме	435
Если система не загружается	435
Авторитетное восстановление	436
Авторитетное восстановление с помощью Ntdsutil	436
Обеспечение правильности авторитетного восстановления	439
Влияние авторитетного восстановления	440
Влияние на доверительные отношения и учетные записи компьютеров	440
Влияние на членство в группах	442
Восстановление Глобального каталога	444
Восстановление мастеров операций	444
Кто может быть мастером операций?	444
Восстановление мастера схемы	445
Восстановление мастера доменных имен	445
Восстановление мастера RID	446
Восстановление имитатора PDC	446
Восстановление мастера инфраструктуры	447
Проверка целостности и восстановление базы	448
«Мягкое» восстановление журналов базы	448
Проверка целостности базы	449
Семантический анализ базы	450
Ремонт базы	452
Перенос базы Active Directory	453
Выяснение местоположения файлов	453
Перенос файлов базы	453
Перенос файлов журналов	454
Если надо переустановить домен в лесу	454

Постановка задачи	455
Общая последовательность действий	456
Определение правил переноса	456
Последовательность действий с первого взгляда	457
Перенос пользователей и групп в деталях	459
Проверка результата	464
План аварийного восстановления	465
Если в лесу все перестало работать	465
Общая последовательность действий	466
Предварительные шаги	468
Документирование текущей структуры леса	468
Разработка процедуры отката назад	469
Выявление лучшего кандидата на восстановление	470
Выключение всех контроллеров доменов	472
Восстановление	472
Восстановление корневого домена	472
Восстановление остальных доменов	476
Добавление дополнительных контроллеров	478
Заключительные шаги	479
Заключение	480
Словарь терминов	481
Предметный указатель	509
Список литературы	517
Об авторе	517

Об этой книге

Скоро будет уже четыре года, как вышла система Windows 2000, а вместе с ней — служба каталогов Active Directory. Уже стихли словесные баталии о том, чем она лучше или хуже Novell NDS, уже не раздаются осторожные реплики, дескать, подождать надо, пока другие не попробуют, да сервисный пакет не выйдет, а то и два. Уже прочитана уйма литературы на эту тему, благо ее на русском языке издано предостаточно. И вот результат: крупные и средние российские компании массово стали переходить на Windows 2000 и Active Directory.

После выхода Windows Server 2003 все внимание было обращено на этот продукт. Уже сейчас компании все чаще планируют внедрение именно этой ОС, а не ее предшественницы. Возможно, открывая книгу, специалисты хотели бы видеть самую последнюю информацию об Active Directory 2003. Но для данной книги это невозможное требование, так как здесь я пишу только о том, с чем работал длительное время. Но это не означает, что книга бесполезна для таких читателей. Все концепции построения службы каталогов и ее обслуживания остались прежними. Поэтому все, что здесь описано, в полной мере относится и к Windows 2003.

С момента выхода Windows 2000 я помогал компаниям внедрять Active Directory. Шишек за это время было набито немало: в каждой организации своя специфика и свои требования, все обладают разным уровнем готовности к этому шагу. Это требовало искать обходные пути и нетривиальные решения. Но подобные процессы имели место и в других странах. В итоге в Microsoft накопился значительный опыт внедрения, учитывающий знания и достижения сотен консультантов Microsoft Consulting Services. Часть этой информации опубликована на Web-сайте Microsoft, в базе знаний Microsoft, также доступной в Интернете

и на дисках по подписке, часть — на курсах по отладке Active Directory. Ни одна самая хорошая книга не даст вам столько, сколько эти три источника. Но я и не ставил такой задачи.

Цель этой книги — научить вас пользоваться в нужное время и в нужном месте нужными источниками информации для решения сложных задач настройки и обслуживания Active Directory.

Обидно, что сотни специалистов, ознакомившись с обзорными материалами по Windows 2000, пытаются строить лес в организации и совершают при этом нелепейшие ошибки, приводящие если не к полной неработоспособности, то к «инвалидности» системы. Система «вопит» о своем «увечье», а горе-специалисты, не понимая ее мольбы о помощи, продолжают душить.

Эта книга содержит тот минимум информации, который должен знать любой администратор системы или ее проектировщик, чтобы самостоятельно поддерживать систему в добром здравии и обеспечивать не только ее бесперебойную работу, но и восстановление в случае краха.

Работая над книгой, я исходил из того, что читатель имеет общее представление о Windows 2000, Active Directory и о том, как это все работает. Поэтому здесь вы не найдете разжевывания базовых понятий службы каталогов; это все я уже объяснял в книге «Microsoft Windows 2000. Планирование, развертывание, управление» (2-е изд. М.: Русская Редакция. — 2000 г.), которую можно с полным основанием считать первой частью настоящей. Но если там акцент делался на описании новых возможностей Windows 2000 и на том, как их использовать, то здесь на том, как функции Active Directory использовать с максимальной эффективностью и бороться с возникающими проблемами. В первой книге вы знакомились со стандартными инструментами, входящими в комплект ОС, — здесь же описывается практическая работа с дополнительными программами и утилитами, поставляемыми либо в составе Windows 2000 Server Resource Kit, либо в составе Windows 2000 Support Tools.

Я постарался избегать по возможности сухой теории и специальной терминологии. Я хотел вам просто рассказать самое главное, что знаю на эту тему. Но не расслабляйтесь: за шутками порой скрывается очень важная информация, которую надо знать, как таблицу умножения. Хотя я беру за основу английскую версию ОС, употребляю я при этом русские термины. Меня коробит, когда русский человек начинает выдавать перлы вроде «бриджхед сервера» или «сайт линки». У всех терминов есть русские эквиваленты, которыми рекомендую пользоваться.

За год, прошедший с момента выхода первого издания, книга широко разошлась по стране. Для многих она стала настольной книгой

и первым источником при поиске решения каких-либо проблем. Во второе издание были **внесены** небольшие, но очень существенные изменения и дополнения в первую главу, посвященную планированию Active Directory. Эти изменения касаются вопросов построения безопасной доменной архитектуры и базируются на опыте реальных **проектов** последних двух лет. Помимо **этого**, местами введены замечания об особенностях **планирования** AD для Windows 2003. **Наконец**, были устранены замеченные мною и читателями досадные опечатки,

Структура книги

Шесть **глав**, из которых состоит книга, я намеренно не стал нумеровать: определенно сказать, какую читать первой, а какую — последней, нельзя. Главы перекликаются: из одной ссылки идут ко всем остальным. Там, где этого мало, я делаю ссылки на другие книги и в первую очередь на уже упоминавшуюся «Microsoft Windows 2000. Планирование, развертывание, управление».

Если Active Directory уже **развернута** в вашей организации, то это совсем не означает, что глава «**Проектируем Active Directory, или Мелочей не бывает**» не для вас. Во-первых, никогда не поздно **проверить**, все ли правильно у вас сделано. Возможно, есть какие-то мелочи, которым вы пока не придавали значения, но способные отравить вам жизнь в будущем. Во-вторых, компании постоянно развиваются: приобретаются и открываются новые подразделения, продаются **существующие**, происходит слияние с **конкурентами**, расширяются территории и т. п. Вот тут-то эта глава и поможет вам. Наконец, никогда не считайте полученные ранее **знания** абсолютными и неизменными. За прошедшие годы многое изменилось в принципах построения Active Directory. То, что пару лет назад казалось единственно верным, сегодня уже не представляется столь бесспорным и претерпевает изменения. То, о чем раньше даже и не **подозревали**, всплыло во время крупных проектов и теперь считается обязательным условием проектирования.

Название «**Установка Active Directory**» может сбить с **толку**. С одной стороны, те, кто ее уже установил, решат, что читать об этом незачем. Новички же, только осваивающие этот путь, могут подумать, что это для них. Не **спешите**. Эта информация станет полностью доступной только **после** того, как вы хотя бы в рамках стандартной **документации** познакомитесь с Windows 2000 DNS, DHCP, Active Directory, программой **DCPROMO**. Эта глава не о том, как из сервера сделать контроллер домена, а о том, как не допустить ошибок на предварительной стадии и как избавиться от ошибок, если они все-таки возникли при **установке**.

От правильной настройки служб DNS, WINS и DHCP зависит, как будет работать система. Способов конфигурирования так много, что выбрать

самый верный — не очень простая задача. Но вот контроллер домена установлен. Как понять, что все сделано правильно и выявить потенциальные проблемы? Ответ на этот вопрос дан в этой главе. Плюс к этому — полезные сведения о конфигурировании системы в нестандартных условиях работы.

Так же, как Active Directory немыслима без репликации, так и книга немыслима без главы **«Репликация Active Directory»**. Масса проблем с Active Directory возникает из-за некорректно работающей репликации. Чтобы их понять, надо, с одной стороны, разобраться в механизмах репликации, а с другой — знать и уметь использовать инструменты диагностики. Именно поэтому теорию данного процесса я раскрыл гораздо полнее, чем в других книгах. А изучив теорию, вы без труда справитесь с той информацией, которую предоставляют средства диагностики. А тому, с чем не справитесь, найдете объяснение в этой главе.

Но репликация службы каталогов — не единственный вид репликации в Windows 2000. Active Directory тесно связана с файловой системой: это файлы базы данных и журнала транзакций, составляющие групповых правил, хранящиеся на диске, профили пользователей и сценарии. От того, насколько эти компоненты согласованы с данными в Active Directory, зависит стабильность и защищенность системы. А согласованием занимается служба репликации файловой системы. Вот о ней и идет речь в главе **«Active Directory и файловая система»**. Как не странно, но этим вопросом многие просто пренебрегают, полагая, что «тут все ясно, оно всегда работает». Увы, это не так. Эта тема менее всего отражена в литературе, а зря! Проблемы с репликацией файлов могла причинить столько проблем, что их с лихвой хватит, чтобы омрачить радость от нормальной работы остальных служб. Поэтому основной лейтмотив этой главы — диагностика проблем.

С репликацией файловой системы неразрывно связана работа распределенной файловой системы DFS. Неискушенный администратор легко запутается, отыскивая причину недоступности тома на одном компьютере и совершенно нормальной работе на другом. Только грамотное использование средств диагностики DFS и репликации файловой системы может помочь своевременно восстановить работоспособность распределенной файловой системы. А диагностика без понимания основ — пустое занятие. Поэтому в этой главе я привел необходимый минимум теоретических сведений.

Одним из звеньев, связывающих объекты Active Directory и пользователей, является групповая политика. К сожалению, еще далеко не все представляют, как можно и нужно применять групповые правила, как применять принципы наследования и блокировки, что такое фильтры

и т. п. Этому посвящена глава «Групповая политика». Хорошо, когда политика применяется. Хуже, когда возникают проблемы. Их поиск — одна из самых неприятных и запутанных операций в Windows 2000. И даже применение инструментов диагностики требует определенной подготовки и навыка. В этом, надеюсь, вам поможет данная глава.

Глава «Поиск и устранение проблем» — не фармакологический справочник. Здесь нет списка симптомов болезни и перечня лекарств от нее. О том, как искать причины конкретной ошибки и устранять ее, рассказано в остальных главах. «А что же тогда *здесь?*» — спросите вы. А здесь — описание алгоритмов поиска источника проблем, что гораздо, по-моему, важнее. Алгоритмы ссылаются на ту или иную главу. А все вместе — дает решение.

Любая проблема подобна простуде: стоит запустить — и она перерастет в хроническую болезнь. Хорошо, если вовремя принять лекарство, а то и до скальпеля недалеко, Хирургическое вмешательство в Active Directory — дело рискованное и чревато летальным исходом. Счастье, если у вас есть резервная копия. Хорошая резервная копия, из которой можно восстановить каталог и потерянные объекты. Что такое хорошая резервная копия Active Directory, как ее сделать и как из нее восстановить информацию — вот то, что вы найдете в этой главе.

Если говорить языком *медицины*, здесь вы найдете и описание трансплантации органов (*восстановление целых доменов в дереве*), и воскрешение из *мертвых* (*восстановление погибшего каталога*).

Чего здесь нет

В этой книге вы НЕ найдете:

- описания модели безопасности Active Directory;
- описания инфраструктуры открытых ключей и ее диагностики; возможно, когда потребности в этом увеличатся, соответствующая глава будет добавлена;
- ◆ описания процесса установки Windows 2000 и конфигурирования служб, не имеющих прямого отношения к Active Directory: не стоит утяжелять книгу «сопутствующим *товаром*»;
- рекомендаций по управлению проектом внедрения Active Directory: эта тема слишком объемна и требует отдельного освещения;
- советов по организации сопровождения и поддержки корпоративной вычислительной системы на базе Active Directory: это предмет такой дисциплины, как Microsoft Operations Framework (MOF), и требует систематизированного подхода.

Короче, здесь нет ни слова о том, что не относится к Windows 2000 и Active Directory.

Принятые соглашения

Для удобства чтения в книге приняты следующие обозначения:

Любой **новый** термин, встречающийся первый раз, выделен *курсивом*. Выделение служит также подсказкой о том, что объяснение термина приведено в Словаре **терминов** в конце книги.

Ссылки на дополнительную литературу приведены в [квадратных скобках].

Тексты сценариев и листинги файлов выделены **моноширинным** шрифтом,

Описания синтаксиса команд ОС или дополнительных утилит выделены **моноширинным** шрифтом **полужирного** начертания.

Замечание Если на что-то требуется обратить особое внимание, то соответствующий абзац выделен точно так же, как и этот.

Проектируем AD, или Мелочей не бывает

Прежде чем установить Active Directory, ее нужно спроектировать. В прошлом, когда использовалась служба каталогов Windows NT, проектирование было столь же необходимо, как и сейчас. Вот только цена ошибки была гораздо ниже. Существовало четыре типовых схемы связей между доменами, которые использовались полностью либо в некоторой комбинации [9]. Если какой-то из доменов был спроектирован неверно, его можно было совершенно безболезненно для остальных «убить» и сделать по-новому. В Active Directory все домены объединены в лес. Ошиблись при проектировании корневого домена — придется переделывать весь лес, а это может обойтись дорого. Не меньше может стоить и ошибка в одном из промежуточных доменов. Я уж не говорю о том, что неверная топология репликации и планировка сайтов могут доставить вам сплошные хлопоты и неоправданные затраты на приобретение дополнительного оборудования. Разбиение на подразделения, выполненное не в соответствии с административными потребностями, а по желанию руководства, может превратить процесс администрирования в ад для технических специалистов и повлечет неоправданный рост численности технического персонала. Суммируя сказанное, можно констатировать, что неправильное планирование компонентов Active Directory чревато:

- неоправданными расходами на оборудование;
- неоправданными расходами на технических специалистов;
- повышенной трудоемкостью работ;
- нестабильной работой системы:

- ◆ потерей данных;
- ◆ утечкой конфиденциальной информации;
- ◆ вашим увольнением.

Как видите, список **серьезный**, и на вероятность любого из перечисленных в нем событий оказывает влияние масса факторов. Порой это мелочь, вырастающая в гигантскую проблему. Вот почему в этой главе мы обсудим вопросы планирования Active Directory и, в частности:

- + стратегию именования;
- ◆ стратегию и тактику деления на домены:
 - принципы построения структуры подразделений;
- ◆ правила разбиения на сайты;
- ◆ принципы размещения сетевых сервисов, Глобальных каталогов (ГК) и других служб Active Directory;
- ◆ политику модификации схемы.

Что в имени тебе моем?..

Казалось бы, какое отношение может иметь название домена к стабильности его работы или трудоемкости администрирования? Отвечая на этот вопрос, надо вспомнить, что живем мы в мире, наполненном глобальными сетями, Интернетом и всякими хакерами, способными просто из спортивного интереса «исследовать» что-то, что может представлять для них лакомый кусочек. Не забывайте, что Active Directory построена на системе именований DNS и очень тесно с ней связана, что в свою очередь предполагает понимание различий между пространством имен DNS и пространством имен Active Directory.

Кроме того, имя, которое вы даете своей структуре, в первую очередь определяется потребностями бизнеса организации и условиями его развития.

Бизнес определяет имена

Не важно, сколько доменов в вашей Active Directory. Главное, обязательно будет корневой домен — носитель имени леса доменов Active Directory. Назвав его, впоследствии ничего уже нельзя будет изменить, иначе как только переустановив все домены в Active Directory, начиная с корневого.

Замечание Для доменов Windows 2003 это не так. В состав этой операционной системы входит утилита, позволяющая переименовывать домены. Правда для этого лес должен работать в режиме естественного Windows 2003, то есть в нем не может быть доменов Windows 2000.

Критерии выбора имени леса таковы:

- ◆ отражение названия компании в доменном имени;
- ◆ присутствие организации в Интернете;
- ◆ планы по приобретению других компаний;
- ◆ сложность имени.

Первый критерий вполне очевиден. Странно было бы назвать coffesale.ru чайную компанию. Однако, называя лес Active Directory, постарайтесь учесть возможные в ближайшем будущем смены направлений деятельности или изменения имени компании, например, при ее покупке другой, более крупной компанией.

Если компания уже представлена в Интернете и имеет там зарегистрированное имя, то вполне очевидно желание использовать то же имя и внутри организации. Но даже если сейчас вы еще не вышли в Интернет, не исключено, что это будет сделано в ближайшем будущем. А раз так, выбранное имя должно быть зарегистрировано в ICANN, иначе оно может оказаться неожиданно занятым, и вам придется выбирать новое название по заданную тему.

Называя корень Active Directory, подумайте, какую долю бизнеса компании будет охватывать доменная структура. Допустим, компания занимается производством молока и соков, причем это произошло в результате слияния двух независимых компаний, и каждая имеет в значительной степени независимое управление и политику ИТ. Если в названии корневого домена будет слово «молоко», это вызовет скрытое раздражение производителей сока, и, наоборот, назвав домен «сочным» именем, вы рискуете вызвать гнев «молочников». Имя должно быть нейтральным или совмещать в себе признаки обеих организаций. Например, это может быть название совместной зарегистрированной торговой марки или объединенное имя компаний, что-то вроде milkandjuice.ru. Правда, в последнем случае есть угроза нажить себе врагов после приобретения компанией фирмы по производству газированных напитков.

Замечание Всегда можно добавить в лес новое дерево с нужным именем. Правда, у корня по-прежнему будет оригинальное имя.

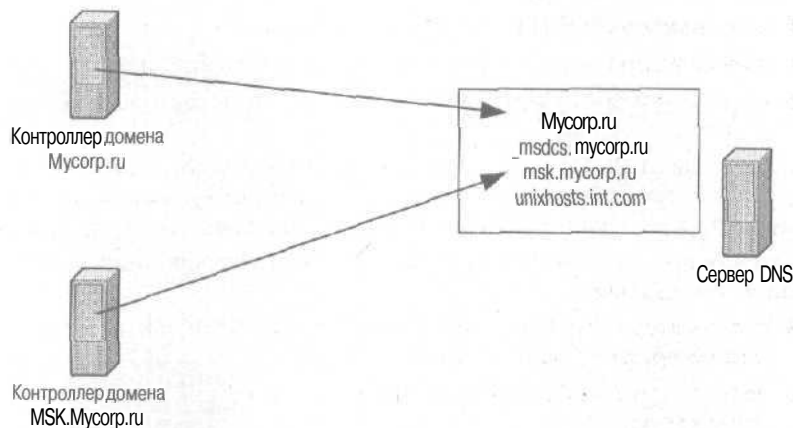
Наконец, последний критерий — сложность имени. Назвав корневой домен «Пупкин, братья и сыновья», вы ничего, кроме раздражения администраторов, не наживете. Ведь им придется для выполнения разного рода операций отладки и мониторинга писать длиннющее имя домена или контекста в Active Directory в LDAP-нотации.

Имена DNS и имена Active Directory

Давайте вспомним о разнице между именами DNS и Active Directory. Вы, конечно, знаете, что как систему именований Active Directory использует DNS. Сервер DNS хранит информацию об именах и соответствующих им адресах IP, обеспечивает разрешение этих имен по запросам от клиентов и тиражирует эту информацию между отдельными серверами согласно установленным правилам.

Active Directory хранит сведения о своих объектах (пользователях, компьютерах, подразделениях и т. п.), тиражирует их между контроллерами доменов и предоставляет своим клиентам в ответ на запросы.

Для каждого домена Active Directory есть данные (записи типа SRV, имена доменов и хостов, CNAME-записи партнеров по репликации), которые хранятся в зонах DNS. Каждому имени домена Active Directory соответствует такое же имя зоны DNS. А вот обратное — для каждой зоны DNS обязательно имеется соответствующий домен Active Directory — неверно.



Для каждого домена AD существует зона в DNS, но не наоборот

Покажем корень миру

Как упомянуто выше, к названию леса (то есть корневого домена в лесу) надо подходить чрезвычайно внимательно. Особо *остановлюсь* на ситуации с «плоским» именем корня. Практика показывает, что большинство организаций выбирает для корня имена вида xxx.yyy.zzz, то есть имя, соответствующее системе именований DNS, в котором есть по крайней мере одна точка. Это такие имена, как mybank.ru, corp.mycorp.net и пр. Однако в ряде организаций сильны традиции имен NetBIOS. Они стремятся дать корневому домену «плоское» имя, то есть

состоящее из одной части, например `mysocp` или `ad`. Свое решение специалисты этих компаний аргументируют так: «Так короче. А где сказано, что это запрещено?» И ведь в самом деле это не запрещено. Более того, в большинстве случаев это не вызывает никаких проблем, **Но...** Проблема возникает, как только контроллеры дочерних доменов или серверы-члены корневого домена **оказываются** в другой подсети, такой, что NetBIOS-имена между этими подсетями не разрешаются. Эта проблема приводит к невозможности нормального функционирования Active Directory. Именно поэтому я настоятельно рекомендую избегать таких имен. Но уж если вы **столь** упрямы, что желаете использовать их во что бы то ни стало, то обратитесь к главе «Установка Active Directory», где описано, как правильно сконфигурировать контроллеры доменов и серверы для работы с «плоскими» именами доменов.

Между именем корня леса доменов Active Directory и внешним именем DNS компании могут быть разные взаимосвязи. Все возможные варианты сводятся к трем:

- доменное имя и имя в Интернете совпадают;
- ◆ доменное имя является дочерним для имени в Интернете;
- доменное имя не имеет ничего общего с представленным в Интернете.

О настройке DNS см. главу «Установка Active Directory», здесь же я приведу только общие рекомендации. Главное, что в любом случае внутренний и внешний серверы DNS разделены межсетевым экраном.

Если имя леса Active Directory совпадает с зарегистрированным внешним именем DNS:

- ◆ пользователи осуществляют доступ как ко внешним, так и внутренним ресурсам по **одному** доменному имени;
- ◆ нельзя открывать внутренние ресурсы для внешнего мира; внешний сервер DNS не должен хранить имен, используемых Active Directory;
- ◆ для разрешения внешних имен **из** внутренней сети используйте передачу неразрешенных вызовов на внешний сервер DNS;
- ресурсы, доступные извне, должны храниться в демилитаризованной зоне (DMZ), аутентификация доступа к ним — выполняться через RADIUS-сервер, а не контроллер домена;
- ◆ на прокси-сервере надо сконфигурировать список исключений;
- ◆ при использовании протокола трансляции сетевых адресов (NAT) внутренний сервер DNS должен содержать свои записи о ресурсах, доступных как извне, так и изнутри; управление этими адресами — забота администратора.

Если имя леса Active Directory является дочерним по отношению к внешнему имени DNS:

- только внутренний сервер DNS содержит информацию об Active Directory;
- ◆ на внешнем сервере DNS создается делегирование зоны, соответствующей зоне домена Active Directory;
- пользователи применяют разные имена для доступа к внешним и внутренним ресурсам;
- ◆ для обеспечения доступа пользователей ко внешним ресурсам не требуется предпринимать дополнительных усилий;
- ◆ полные имена ресурсов *длиннее*, чем в предыдущем случае.

При различных именах леса Active Directory и внешнего имени DNS:

- ◆ управление безопасностью внутренней сети проще за счет полностью различных пространств имен;
- внутренние имена не видны снаружи;
- ◆ тиражировать информацию с внешнего сервера DNS на внутренний не обязательно;
- ◆ инфраструктура DNS может оставаться без изменений;
- ◆ внутреннее имя не обязательно регистрировать в ICAAN.

Дополнительную информацию по именованию см. в [8].

Алгоритм именования DNS

Если суммировать сказанное в этом разделе с материалами раздела, посвященного DNS главы «Установка Active Directory», можно составить такой алгоритм стратегии именования, как показано на рисунке ниже.

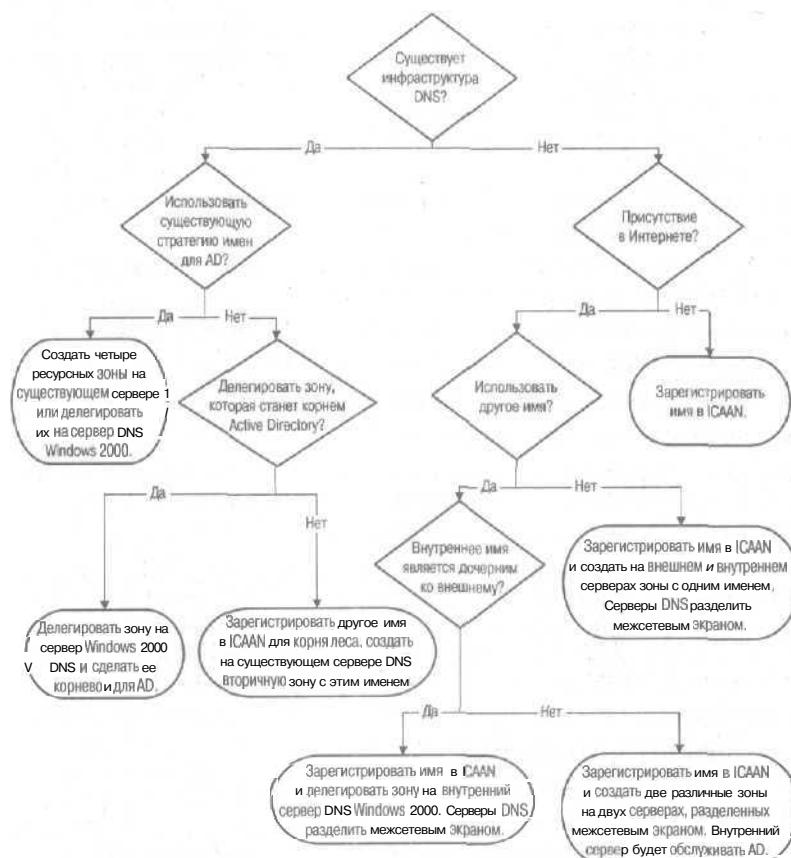
Именованние объектов Active Directory

Об именовании объектов (т. е. компьютеров, пользователей и подразделений) не часто пишут в книгах по Active Directory. Возможно, их авторы считают, что на таком тривиальном вопросе останавливаться не стоит. Мой опыт показывает, что изобретательности службы ИТ нет границ. Ниже приводятся примеры наиболее удачных типов имен.

Именованние пользователей

Когда речь идет об объектах типа User, следует отдельно говорить о таких атрибутах, как:

- ◆ Сп — общее имя;
- DisplayName — имя отображаемое в каталоге;
- ◆ SamAccountName — имя, используемое при регистрации в домене Windows NT;



Стратегия использования доменных имен DNS

- ◆ UserPrincipalName (UPN) — имя, используемое при регистрации в домене Windows 2000.

Общее имя совпадает с именем, отображаемым в каталоге, и представляется почти так, как мы привыкли обращаться друг к другу: имя, фамилия и «кусочек» отчества. Формат общего имени такой: <имя> пробел <часть отчества> точка. пробел <фамилия>. Максимальная длина имени совместно с фамилией составляет 57 символов при отсутствии отчества и 55 — при максимальной длине отчества, равной 6 символов. Предельная длина общего имени — 64 символа. В качестве символов имени допустимы символы UNICODE, т. е. пользователей вполне можно называть по-русски.

Имя, применяемое при регистрации в домене Windows NT, обычно служит и для регистрации в домене Windows 2000. В диалоговом окне регистрации пользователь вводит именно это имя, пароль и имя домена. Если же он введет данные в формате `имя@имя.домена`, то он введет имя UPN. Первая часть UPN и имя регистрации в домене Windows NT по умолчанию совпадают, но могут быть и разными. Для простоты далее мы будем полагать, что они совпадают, и назовем их просто именем регистрации.

В качестве имени регистрации используется несколько схем. Наиболее употребительная основывается на имени и фамилии пользователя записанных латинскими буквами. В этой схеме несколько вариаций:

- ◆ <первая буква имени><фамилия><номер*>;
- ◆ <имя><первая буква фамилии><номер*>;
- ◆ <часть имени><часть фамилии>.

Звездочка означает, что номер используется в случае наличия полных тезок на предприятии. Иногда вместо номера применяется иная латинская транслитерация, например, Petrov, Petroff, Petrow.

Вторая схема встречается довольно редко. Она основывается на некотором персональном идентификаторе пользователя. Это может быть его табельный номер. К идентификатору можно добавлять дополнительную приставку, обозначающую статус сотрудника (временный сотрудник — t, сотрудник компании поставщика — v и т. п.), местонахождение или принадлежность к тому или иному подразделению. Последнее нельзя признать удачным, так как при переходе в другое подразделение имя регистрации пользователя придется менять.

Именованние компьютеров

В именовании компьютеров наблюдается полный разнбой. Одно, правда, объединяет все схемы наименований: администраторы стараются давать принципиально разные имена серверам и рабочим станциям.

В качестве примера удачного именования серверов можно привести;

`XXX-YYY-NN`

где:

- + XXX соответствует территориальному расположению сервера; это может быть код региона, записанный в Конституции РФ, аббревиатура, соответствующая определенному городу (MSK, NSK, SPB) или любой иной код, понятный администраторам;
- ◆ YYY — тип сервера, например, SRV — сервер общего назначения, DC — контроллер домена, MSG — почтовый сервер, PXY — прокси-сервер, WWW — Web-сервер и т. п.;
- ◆ NN — порядковый номер сервера данного типа в данном регионе.

Если структура Active Directory такова, что каждому региону (или каждой площадке) соответствует свой домен, то из имени можно исключить первый префикс, так как из полного имени сервера и так будет понятно, где расположен сервер.

Еще одна распространенная схема именования: присвоение серверам условных имен, например, MARS, SATURN, JUPITER и т. п. Если рассматривать неочевидность наименования как достоинство, не позволяющее **вразу** разобраться с первого взгляда, что есть что, то это же и недостаток, так как администратор вынужден держать в голове таблицу соответствия серверов выполняемым ими функциям.

Имена рабочих станций лучше всего связывать с именами пользователей, которые на них работают (если, конечно, на одной станции не работает несколько пользователей по очереди). Это удобно при поиске источника проблем или при оказании помощи пользователям.

Удачная схема именования имеет следующий формат:

XXXXXXXXNN

где:

- ◆ XXX - тип операционной системы (W2K, WXP, W98);
- ◆ YYYYYYYY — имя регистрации пользователя;
- NN — порядковый номер, если у пользователя несколько компьютеров.

Вместо номера можно применять суффиксы, указывающие на тип компьютера, например, MOB — для мобильных компьютеров.

Иногда схема именования учитывает номер комнаты и номер сетевой розетки в ней. Недостаток схемы: при перемещении сотрудника в новый офис полностью меняется имя компьютера. Достоинство: можно моментально не только вычислить злоумышленника в сети, но и оперативно отключить его от нее.

Имена подразделений

Специальных требований к именам подразделений нет. Они могут **содержать** символы UNICODE и **быть** довольно длинными — до 64 символов.

К сожалению, длина отличительного имени объекта (*distinguished name*), включающего имена всех родительских подразделений и имя домена, не воспринимается корректно некоторыми приложениями. Эта явная ошибка в приложении может доставить массу неприятностей, так как диагностика ее может быть весьма непростой.

Одоменивание

Специалисты по Windows NT считали, что создать доменную структуру очень просто: существовало четыре модели; с одним доменом, с одним **мастер-доменом**, с **несколькими мастер-доменами** и модель

полностью доверительных отношений. Выбор модели определялся в основном размерами организации и ее финансовыми возможностями, Active Directory внесла определенную смуту. Во-первых, оказалось, что прежние модели объединения более не имеют смысла. Во-вторых, наличие организационных подразделений (ОП) решает многие задачи, ранее решаемые посредством разбиения на домены. Наконец, улучшившиеся свойства доменов позволили коренным образом пересмотреть способы построения организационной структуры предприятий. Прежде чем перейти к обсуждению этих возможностей, вспомним некоторые основные определения. Итак для Windows 2000 справедливы следующие определения.

- ◆ Домен — это элемент каталога, имеющий свое собственное пространство имен. Внутри домена действуют правила безопасности, не распространяемые за его пределы.
- Доменные функции поддерживаются контроллерами доменов. Все контроллеры домена равноправны и хранят реплики каталога, доступные для внесения изменений. Изменения между контроллерами тиражируются при репликации. Тип репликации — со многими мастерами.
- Между доменами могут устанавливаться отношения доверия. Тип доверительных отношений транзитивный, т. е. если домен А доверяет домену Б, а домен Б доверяет домену В, то домен А доверяет домену В. Транзитивные доверительные отношения двунаправлены.
- Домены объединяются в деревья. Самый первый домен в дереве называется корневым. Дочерние домены наследуют пространство имен от родительского домена. Между доменами в дереве автоматически устанавливаются транзитивные доверительные отношения.
- ◆ Деревья доменов могут объединяться в леса. Самый первый домен в первом: дереве леса называется корнем леса. Каждое дерево имеет свое имя, определяемое именем корневого домена в дереве. Имя леса определяется именем корня леса. Между доменами в лесу существуют транзитивные доверительные отношения. Все домены леса используют общую схему и конфигурацию.
- ◆ Два леса характеризуются разными пространствами имен, разной конфигурацией и разной схемой. Между двумя лесами можно установить одно- или двунаправленные нетранзитивные доверительные отношения.

Замечание Между лесами Windows 2003 можно устанавливать транзитивные доверительные отношения.

Один за всех...

Как вы помните, один домен способен поддерживать до 10 миллионов объектов каталога. По крайней мере так утверждают пособия по Active Directory. Не могу не сказать, что на момент написания книги мне было известно о домене, в котором было 34 миллиона объектов. Даже если предположить, что из всех этих объектов только 1 миллион приходится на пользователей, а все остальные на компьютеры, группы, подразделения и т. п., то, повторяя небезызвестного Хрюна, так и хочется сказать: «Внушает...» А ведь и в самом деле, почему бы не остановиться на одном домене для любого предприятия? Вы можете назвать в России хоть одну организацию с миллионом сотрудников?

Увы, жизнь не столь проста, и одним доменом не всегда можно отделаться. Для начала рассмотрим критерии, по которым следует определять необходимость использования доменов.

Критерии создания домена

Первый критерий — соображения *административной политики*. Прошу не путать администрирование с управлением. Управленцы (включая президента компании, его замов, директоров и менеджеров) вообще не должны влиять на доменную структуру. Администраторы системы должны определять, как им построить систему, чтобы ею было проще управлять. Помните, что не президент компании и даже не вице-президент по информационным технологиям будут управлять политиками безопасности, распространением программ по рабочим местам и поддержкой пользователей. Они будут требовать с вас, чтобы все работало без сбоев, и именно ваша задача сделать так, чтобы доменная структура работала на вас и обеспечивала требуемую руководством функциональность с минимумом затрат и усилий.

Второй критерий — *безопасность*. Вспомните определение домена: именно в нем звучит этот термин! Домен можно рассматривать как некое государство, правительство которого проводит определенную политику по его защите. Это, например, правила работы с паролями, аутентификации (читай "паспортный режим») и т. п. Все граждане государства (пользователи) обязаны строго соблюдать установленные правила и подвергаться наказаниям при их нарушении (например, блокировка учетной записи).

Третий критерий — *размер*. Организацию с миллионом пользователей представить трудно. Но если, например, налоговики захотят создать для каждого работоспособного гражданина учетную запись в домене, то это уже десятки миллионов пользователей!

Когда одного домена достаточно

Опираясь на эти критерии, легко сообразить, когда можно обойтись одним доменом.

Пусть в компании существует некоторая организационная структура: департаменты, отделы, секторы, лаборатории и т. д. Нужно ли для каждого из этих образований создавать отдельный домен? Чтобы ответить на этот вопрос, спросите, чем отличаются в своих правах сотрудники каждого из подразделений? Можете ли вы сказать, что пользователи в разных департаментах должны применять разные политики безопасности и почему? Чем пароли в департаменте А отличаются от паролей в департаменте В?

Надо задуматься и над тем, как часто сотрудники переходят из подразделения в подразделение, как часто меняется организационная структура предприятия. Помните: домены не переименовешь, не перенесешь в новое место. Нельзя переместить домен из одного участка леса в другой. А перенос пользователей между доменами — процедура далеко не элементарная.

Не забудьте о том, как предприятие разбросано географически. Хорошо, если оно столь богато, что все площадки связаны хотя бы 10-Мбит-ными линиями связи, надежными и незагруженными. Если же это коммутируемые каналы или спутниковые линии, забитые на 70%, вы рискуете прервать репликацию между контроллерами домена на самом интересном месте. Существуют оценки максимального числа пользователей в одном глобальном домене в зависимости от пропускной способности самого медленного канала связи между сайтами. Эти оценки приведены в таблице и базируются на следующих предположениях:

- ◆ по крайней мере 10% пропускной способности канала доступно для репликации;
- ◆ все контроллеры доменов являются серверами ГК;
- в течение года добавляется 20% и увольняется 15% пользователей;
- каждому пользователю предоставлен отдельный компьютер;
- + используются зоны DNS интегрированные с Active Directory.

Зависимость размера глобального домена от пропускной способности каналов

Пропускная способность самого медленного канала (Кб/с)	Максимальное число пользователей в домене
0,6	20 000
14,4	30 000
19,2	40 000
28,8	50 000
38,4	75 000
56,0	100 000

Наконец, сколько администраторов и где они находятся? Если у вас жесткая централизованная модель управления сетью, то наличие одного

домена — это идеальное решение. Если же сеть не только распределена географически, но и администрирование децентрализовано, то стоит задуматься о потенциальных конфликтах администраторов в домене. Помните, люди весьма изобретательны, когда пытаются отстоять то, что у них пытаются отобрать.

Итак, только один домен создается, если:

- ◆ размер организации таков, что может управляться одним доменом (рекомендуется менее 1-2 миллионов пользователей);
- ◆ используется централизованная структура управления сетью с хорошо детализированной политикой;
 - допустимо применение единой политики безопасности (пароли, блокировка учетных записей, Kerberos, файловая система с шифрованием, IPSecurity, инфраструктура открытых ключей);
- 4 географическая распределенность такова, что отсутствуют некачественные или перегруженные каналы между отдельными участками;
 - предприятие стабильно и не планируется его деление на несколько новых либо слияние с другим предприятием;
- ◆ нет нужды в использовании более одного доменного имени.

Если компания соответствует этим критериям, можно говорить об однодоменной модели. Таким образом, лес предприятия будет состоять из одного дерева, в котором есть только один домен. Он же является корнем всего леса и носителем имени.

Преимущества однодоменной модели

Преимущества однодоменной модели Active Directory таковы.

- ◆ *Простота управления* Все администраторы сосредоточены в одном месте, имеют четкую специализацию. Не нужно делегировать (даже временно) избыточные административные полномочия дополнительным администраторам.
- *Более дешевое решение* Для поддержания работоспособности одного домена требуется меньше контроллеров домена. Учитывая требования к контроллерам (см. главу «Установка Active Directory»), это немалые средства.
- ◆ *Простота распределения полномочий* Полномочия администраторов распределяются по ОП внутри одного домена, а не между несколькими.
- ◆ *Меньшее число администраторов* Для управления несколькими доменами, особенно разбросанными географически, требуется больше администраторов, а значит, дополнительные расходы на их обучение и удержание.
- ◆ *Предельная емкость такая же, как у целого леса доменов* ГК может хранить не более 4 миллиардов объектов. С другой стороны,

он содержит краткие сведения обо всех объектах в лесу независимо от количества доменов в лесу. Значит, и для одного домена, и для нескольких этот предел неизменен.

... все за одного

Выяснив критерии создания одного домена, можно предположить, что прямо противоположные критерии должны определять необходимость создания нескольких доменов. Однако это не совсем так.

Начнем с размера организации. Конечно, если превышены максимальные значения, допустимые для одного домена, надо создавать несколько. Но, как я уже говорил, организаций такого размера не так много. Значит ли это, что в остальных случаях нужно использовать один домен?

Отнюдь нет. Вспомните критерии создания домена. Первым была названа **безопасность**. Если в организации существуют ОП, требования к безопасности которых существенно отличаются от остальных, то такие подразделения лучше выделить в отдельные домены. К примеру, в банке это может быть отдел пластиковых карточек, на крупном предприятии — отдел безопасности и т. п. Понятно, что у пользователей этих подразделений должны быть более стойкие пароли, их регистрация в системе и доступ к ресурсам, **возможно**, должны **осуществляться** по смарт-картам или электронным ключам, персональные данные должны быть зашифрованы без возможности их прочтения обычными администраторами сети.

Проблема безопасности тесно связана и с **полномочиями администраторов**. Если взять администраторов единственного домена (а значит, и корневого домена в лесу), то по умолчанию они включены в такие группы, как Domain Admins, Schema Admins, Enterprise Admins. Последние две наделены **огромными** полномочиями в рамках леса. Нужны ли такие всем администраторам? Ясно, нет. «**Всесильных**» админов в системе быть не должно. Чтобы не было у администратора даже возможности самостоятельно включить себя в группу с **абсолютной** властью, целесообразно создавать минимум два домена: корневой, в котором нет **пользователей**, но есть учетная запись администратора предприятия, и другой — где хранятся как учетные записи пользователей, так и все администраторы домена.

Замечание Создание пустого корневого домена для **хранения** в нем учетных записей администратора предприятия обязательно при наличии более чем одного дочернего домена или нескольких **деревьев** в лесу.

Пустой корневой домен играет и еще одну важную роль. Это своего рода «**хранитель имени**» организации. Так как корневой домен дает

имя всему лесу, то никакие изменения в нижележащей доменной структуре не отражаются в имени леса. Можно добавлять новые домены в лес при приобретении или слиянии с другими предприятиями, удалять домены при продаже части бизнеса — имя организации останется прежним.

Еще один положительный фактор наличия пустого корневого домена в том, что по самой природе в нем нет значительных нагрузок на контроллеры, и надежность их возрастает. Поэтому в этом домене можно разместить ГК и мастера схемы и инфраструктуры, которые можно будет задействовать для восстановления системы в чрезвычайной ситуации.

К недостаткам такого домена можно отнести необходимость использовать два дополнительных сервера в качестве его контроллеров. Но, по-моему, плюсы перевешивают этот минус, тем более что аппаратные требования к этим контроллерам не так уж высоки.

Второй критерий создания домена — **модель администрирования**. Если все администраторы сосредоточены в штаб-квартире или в едином центре управления сетью, неразумно добавлять к домену дополнительные домены. Дело в том, что обычно одни и те же люди администрируют все домены. Поэтому, если нет иных причин, стоит оставить один домен. Если же у вас модель децентрализованного управления, то стоит подумать о разбиении на домены — по одному на каждую группу администраторов. Однако здесь надо быть очень осторожным! Вы должны абсолютно доверять региональным администраторам. Несмотря на то, что они обладают всей полнотой власти только в своем домене, их ошибки или преднамеренные действия могут отрицательно сказаться па работе всего леса.

Очень тесно связана с этим критерием ситуация, когда региональные представительства компании относительно независимы. У них свой отдел кадров, который проводит прием персонала, в том числе и в отдел ИТ. О том, кто именно занят управлением пользователями в регионе, в центре зачастую не имеют ни малейшего представления. Где гарантия того, что внутри регионального ИТ нет внутренних конфликтов персонала с руководством, что все сотрудники имеют высокую квалификацию и опыт работы с Active Directory, что среди них нет шпионов, засланных конкурентами? А ведь у региональных администраторов есть физический доступ к контроллерам домена, что в совокупности с высокими административными полномочиями открывает большой простор для деструктивной деятельности.

Поэтому, рассматривая данный критерий создания домена, подумайте, стоит ли это делать? Может лучше все учетные записи пользователей и компьютеров в регионе разместить в организационном подразделении, а локальным администраторам делегировать определенные права по

управлению подразделением? Этот же подход следует применить и в том случае, когда домен в регионе должен быть создан в соответствии с другими критериями. Все равно не отдавайте ключи от всех дверей в доме, Управляйте таким доменом из центра, а региональным администраторам позвольте заниматься поддержкой пользователей.

Вы можете возразить, что региональные службы ИТ будут сопротивляться «урезанию» их полномочий. Будут. Еще как будут! Но помните, безопасность организации в целом должна ставиться в основу вашего решения. И тут все средства хороши: от распоряжения генерального директора до «просветительской» работы с массами. Например, стоит объяснить региональным администраторам, что у них отбирают не так уж много власти. Наглядно это демонстрирует следующая таблица.

Полномочия различных категорий администраторов¹

	Администраторы		
	леса ²	домена ³	оп ⁴
Присвоение (Take Ownership) любого объекта в Active Directory	/	—	—
Создание пользовательских учетных записей	✓	/	/
Удаление пользовательских учетных записей	/	/	/
Сброс паролей пользователей	/	/	/
Создание групп	/	✓	/
Удаление групп	/	/	✓
Изменение членства в группах	/	✓	✓
Создание объектов Типа «принтер» и управление ими	/	/	✓
Создание сетевых папок общего доступа и управление ими (на контроллерах домена)	/	/	—
Установка программного обеспечения на контроллеры домена	/	/	—
Создание учетных записей компьютеров и управление ими	/	/	✓
Создание нового домена в лесу	/	—	—
Установка контроллеров домена	/	✓	—
Резервное копирование и восстановление контроллеров домена	/	/	/
Управление Групповыми Политиками	/	/	—
Установка System Management Server	/	/	—
Настройка доверительных отношений между доменами	✓	—	—
Управление Сайтами и Подсетями	/	—	—
Создание политик Admission Control Service (ACS)	✓	—	—

см. след. стр.

	Администраторы		
	леса	домена	ОП
Авторизация сервера DHCP	/	—	—
Авторизация сервера RIS	/	—	—
Организация printer location tracking	/	—	—
Инсталляция MSMQ Routing Server	✓	—	—
Конфигурирование связей MSMQ site links	/	/	✓
Установка Удостоверяющего центра предприятия	/	—	—
Установка Подотчетного Удостоверяющего центра	✓	—	—
Установка Simple Certificate Enrollment Protocol (SCEP) Add-on для службы Certificate Services	/	—	—
Выполнение сервиса MSMQ Replication при работе MSMQ в смешанном режиме (на некоторых серверах установлены MSMQ 1.0 на Windows NT4)	/	—	—
Запуск MSMQ Upgrade wizard	/	—	—

¹ Для администраторов предприятия и домена указаны полномочия по умолчанию, для администраторов ОП — рекомендуемые.

— Область полномочий — лес.

— Область полномочий — домен.

— Область полномочий — ОП.

² Создание нового домена может быть делегировано администратору ОП. Однако это достаточно сложная процедура, требующая большого внимания и предварительной работы. В силу своей сложности она не описана в данной книге.

Хорошо видно, что те полномочия, которые делегируются на уровень подразделения, охватывают именно те работы, которые ежедневно выполняют сотрудники региональной службы ИТ. А вот «слежением за здоровьем» Active Directory и управлением ее базовыми функциями занимается центральная команда администраторов.

Еще один критерий многодоменности — разбросанность по обширной территории и **наличие ненадежных каналов связи**. Разбиение на сайты, конечно, играет важную роль, но в случае одного домена между сайтами тиражируются доменный контекст имен, контекст имен конфигурации, контекст имен схемы и данные для ПС Репликация доменного контекста имен значительно превосходит по объему остальные данные. Разместив в каждом сайте отдельный домен, вы тем самым исключаете доменный контекст имен из процесса репликации.

Существуют оценки максимального числа пользователей в одном региональном домене в зависимости от пропускной способности самого медленного канала связи между сайтами в лесу. Эти оценки приведены в таблице и основаны на следующих **предположениях**:

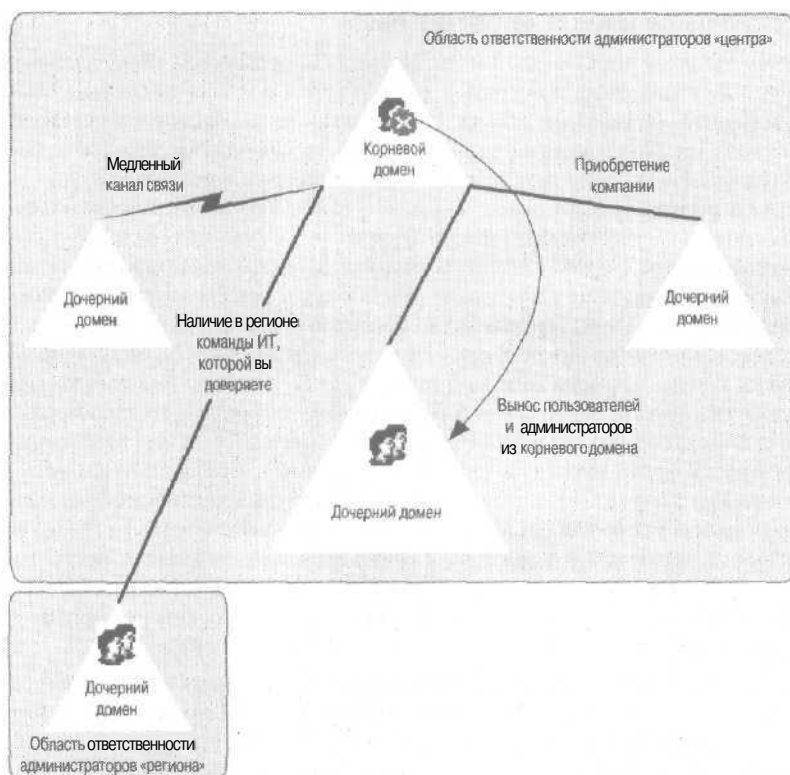
- ◆ минимум 10% пропускной способности канала доступно для репликации;
- ◆ все контроллеры доменов являются серверами ГК;
 - в течение года добавляется 20% и увольняется 15% пользователей;
- ◆ у каждого пользователя отдельный компьютер;
- ◆ используются зоны DNS интегрированные с Active Directory.

Аналогично тому, как мы это сделали для одного домена, подведем итог. Итак, несколько доменов *могут быть* созданы когда:

- ◆ размер организации таков, что не может управляться одним доменом (более 1-2 миллионов пользователей);
- ◆ используется децентрализованная структура управления сетью с несколькими ИТ-отделами, действующими достаточно независимо друг от друга;
 - необходимо исключить даже случайную возможность региональных администраторов вмешиваться в управление всей сетью;
- ◆ существуют категории пользователей для которых должна быть применена отдельная политика безопасности;
- ◆ географическая распределенность такова, что имеются некачественные или перегруженные каналы между отдельными участками;
- ◆ само предприятие нестабильно; возможна продажа отдельных направлений бизнеса либо слияние с другим предприятием.

Зависимость размера глобального домена от пропускной способности каналов

Пропускная способность самого медленного канала (Кб/с)	Максимальное число пользователей в лесу	Максимальное число пользователей в региональном домене
9,6	25 000	15 000
14,4	50 000	15 000
19,2	50 000	25 000
28,8	75 000	40 000
38,4	100 000	45 000
56,0	100 000	100 000



Критерии разбиения на несколько доменов

Преимущества многодоменной модели (дерева)

Преимущества многодоменной модели Active Directory таковы.

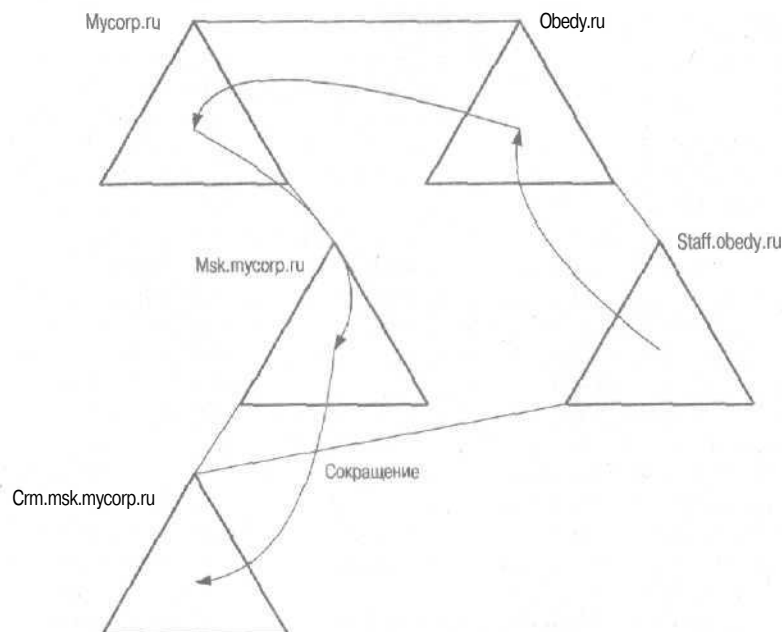
- 4 **Различные доменные политики** Так как политики учетных записей и паролей определяются на уровне домена, можно разделить пользователей по требованиям, диктуемым соображениями безопасности.
 - **Простота включения приобретенных предприятий** Если компания приобретает фирму, имеющую свой обученный технический персонал, свои правила безопасности и пр., многодоменная структура позволяет значительно легче подключать новую структуру в существующую.
 - **Пониженный трафик репликации** Междоменная репликация затрагивает только тиражирование объектов схемы и конфигурации. Объем этих данных несоизмеримо мал в сравнении с внутридоменной репликацией.

Посадим деревья и вырастет лес

Обсуждая причины создания нескольких доменов, мы полагали, что речь идет о дереве, в котором все дочерние домены наследуют имя корневого. Однако не всегда такое приемлемо. Часто организация состоит из ряда ассоциированных с ним предприятий. Каждое такое предприятие занимается независимым бизнесом, имеет свое руководство и политику. Возможно также, что имя этого предприятия известно широкому кругу лиц и безотносительно к связи с головной организацией. Так, с крупной телекоммуникационной корпорацией могут быть ассоциированы компании по доставке писем и грузов, общественного питания, строительно-монтажная и т. п. Их тесная связь с телекоммуникационной корпорацией определяется тем, что большую часть своего бизнеса они выполняют по ее заказам. Раз так, то для удобства обработки заказов и организации совместного планирования и подготовки отчетности нужно обеспечивать интеграцию информационных структур этих предприятий с предприятием-«кормильцем». Под этим подразумевается и доступ к единой системе планирования ресурсов, единая почтовая система и система документооборота, возможность доступа к определенным файловым ресурсам и т. п. Понятно, что речь не может идти о полном слиянии, так как эти компании довольно много работают и на сторонние фирмы и сохраняют свою независимость как юридические лица.

А раз так, то эти компании могут не согласиться на применение в своей сети чужого доменного имени. С другой стороны, требование единой адресной книги, основанной на Active Directory, подразумевает, что это должен быть единый лес. Именно в этом случае резонно создать отдельное дерево для каждой из таких компаний. У этого дерева будет свое уникальное в рамках леса имя, но конфигурация и схема будут общими. Кроме того, они смогут обращаться к единому ГК и осуществлять доступ ко всем предоставленным им ресурсам.

Напомню здесь о пути доверия. Дело в том, что если пользователям из одного дерева в лесу надо обратиться ресурсам, расположенным в домене другого дерева, то аутентификация такого доступа будет выполняться не напрямую, а по цепочке, путем перебора всех доменов от исходного к корневому, а затем от корневого — к домену назначения. Если необходимость в таком доступе существует регулярно, то следует организовать сокращения — доверительные отношения, связывающие эти два домена напрямую.



Для уменьшения пути доверия между деревьями используют сокращения

Преимущества модели с несколькими деревьями

Преимущества модели Active Directory с несколькими деревьями таковы.

- *Возможность использовать разные пространства имен* Имя каждого дерева уникально в рамках леса.
- *Децентрализованное управление* Ассоциированные предприятия ряда компаний обладают независимостью как юридические лица и имеют собственные ИТ-службы.
- *Простота включения новых ассоциированных предприятий* Если компания приобретает фирму с техническим персоналом, своими правилами безопасности и пр., то структура с несколькими деревьями позволяет создать для нее дерево согласно ее требованиям.
- ◆ *Использование единой схемы и ГК* Несмотря на различие, организации, входящие в разные деревья, используют единые приложения, интегрированные с Active Directory, и единую адресную книгу (например, в Microsoft Exchange 2000).

Преимущества модели с одним лесом

Рассмотренные выше модели построения доменной структуры относятся к так называемой модели Active Directory с одним лесом доменов. В 99 % случаев следует придерживаться именно этой модели. Объяснение данного факта простое; вы получаете максимум выгоды от использования Active Directory. Ниже перечислены основные преимущества этой модели.

- ◆ Как следует из определения, лес характеризуется наличием единого глобального каталога. Это означает, что для создания единой адресной книги не надо применять никаких дополнительных усилий. В случае Microsoft Exchange 2000/2003 этот каталог будет взят за основу. Для других почтовых систем он может быть указан в качестве LDAP-каталога. Любой почтовый клиент, понимающий протокол LDAP, использует существующий ГК в качестве адресной книги.
- Наличие единого глобального каталога также может быть использовано и различными серверами приложений такими, например, как IBM Web Sphere. Они могут обратиться к глобальному каталогу для авторизации пользователей. Это может стать первым шагом на пути к созданию единой точки входа в гетерогенную систему (single sign-on).
- ◆ Одним из важнейших достоинств единого леса является простота и эффективность отслеживания единой политики безопасности. Связано это как с организационными, так и с техническими причинами. Так как управление всем лесом выполняется единой командой ИТ, то не существует причин, по которым одна и та же политика была бы внедрена по-разному одними и теми же людьми. С другой стороны, высокий уровень квалификации сотрудников обеспечивает ее правильное внедрение и поддержание. Технически единство политик обеспечивается тем, что, невзирая на разные домены, к ним применяется один и тот же объект групповой политики, хранимый в Active Directory. Кроме того, неизменность данного объекта гарантируется возможностью защиты его от несанкционированного доступа средствами AD.
- ◆ В рамках единой политики безопасности легко реализуется концепция делегирования полномочий. Делегирование позволяет, с одной стороны, резко сократить число сотрудников, обладающих административными полномочиями, а с другой — централизованно контролировать зону ответственности каждого из сервисных администраторов. В такой ситуации лица, не обладающие достаточной квалификацией, не смогут получить доступ к функциям, влияющим на стабильность и безопасность всей системы.

- Наличие единого леса позволяет централизованно внедрить систему мониторинга, которая будет в реальном масштабе времени следить за контроллерами доменов и иным оборудованием. Причем такая система, как Microsoft Operations Manager (MOM 2000), позволит не только контролировать состояние обслуживаемых систем и своевременно сообщать оператору обо всех сбоях, но и автоматически отрабатывать процедуры по устранению неисправностей. Одной из особенностей MOM является возможность ведения базы знаний о возникавших проблемах. Такая база позволяет легко организовать преемственность административного персонала, когда увольнение одного не станет узким местом при разрешении проблем. Стоит упомянуть, что MOM имеет специальные наборы настроек, позволяющих интеллектуально управлять состоянием Active Directory, DNS, Windows 2000/2003 и остальных служб. При необходимости MOM может быть использован для управления и серверами приложений (SQL, Exchange и пр.), причем не только на платформе Microsoft.
- ◆ Наличие единого леса Active Directory значительно упрощает процесс внедрения корпоративных стандартов на рабочие места пользователей. Использование групповых политик в рамках леса позволяет управлять приложениями, установленными на настольных и мобильных компьютерах, выполнять своевременное их обновление, применять определенные настройки отдельных приложений, регулирующие доступ к ресурсам, централизованно управлять сценариями регистрации и пр. Так, например, групповая политика может для всех пользователей определить расположение сервера Software Update Service (SUS) в корпоративной сети предприятия, который используется для распространения всевозможных исправлений для операционной системы и связанных с ней приложений.
- Одной из задач, стоящих перед организациями, работа которых не должна прерываться при любых обстоятельствах (катастрофы, действия террористов и т. п.), является организация резервного центра управления. Резерв может быть как «горячим», так и «холодным». В том случае, когда имеется единый лес Active Directory, инфраструктура каталога может быть спроектирована таким образом, что даже в случае полного уничтожения центральной части организации вся оставшаяся часть будет продолжать функционирование без перерывов и потери функциональности. Более того, сотрудники центральной части, переехавшие в любое место в структуре предприятия, смогут незамедлительно приступить к работе, сохранив при этом доступ ко всем необходимым приложениям.

- Постоянно повышающиеся требования к защите информации предполагают использование более эффективных средств обеспечения защиты. Одним из таких средств является внедрение инфраструктуры открытых ключей (PKI) на базе сертификатов X.509 v.3. Внедрение этой инфраструктуры позволит использовать стандартизованные средства шифрования и защиты информации, сертифицированные соответствующими органами Российской Федерации. Так, в частности, и дополнение к встроенным средствам защиты можно будет использовать цифровые смарт-карты для идентификации личности на компьютерах руководителей, а также для выполнения критичных административных операций. Кроме того, станет возможно использование электронной цифровой подписи (ЭЦП) в системах документооборота и почты. Несмотря на то, что внедрение инфраструктуры PKI возможно и для нескольких лесов, в одном лесу использование системы будет наиболее прозрачным для пользователей.
- Мобильные пользователи смогут абсолютно безопасно подключаться к сети предприятия из любой точки для доступа к своей почте или иным ресурсам. Единый лес обеспечивает для них прозрачность доступа, а использование смарт-карт — безопасность.

Модель с несколькими лесами

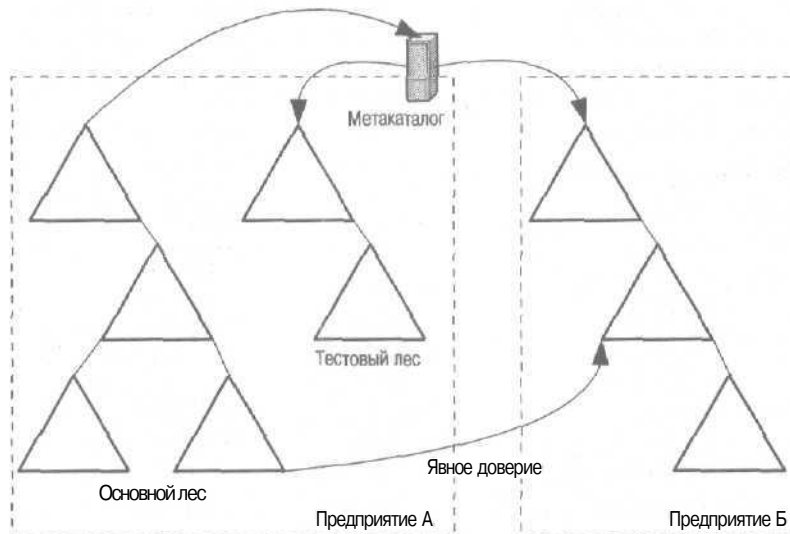
Напоследок рассмотрим модель с несколькими лесами. «Какая ж это модель? — спросите вы. — Это просто два разных каталога Active Directory». Так-то оно так. Только ведь никому в голову не приходило в Windows NT говорить о двух доменах как о несвязанных структурах. Так и тут. Раз могут существовать отдельные леса, значит, они могут взаимодействовать и использоваться для каких-либо целей.

Начнем с того, что модель с разными лесами использовать не рекомендуется. Она практически неуправляема, требует больших затрат на скоординированное администрирование и имеет ограниченное применение. Ну, например, представим, что две крупные компании, каждая из которых уже имеет свою структуру Active Directory, свое имя на рынке, свои приложения, интегрированные с AD, решили объединиться. Слить два леса нельзя. Даже если бы было можно, то как поступить со схемами? Они же разные! Единственный способ — установить прямые нетранзитивные доверительные отношения между теми доменами в каждом из предприятий, для которых нужен доступ к ресурсам друг друга.

Замечание Установить транзитивные доверительные отношения можно только между лесами, работающими в естественном режиме Windows 2003.

Отсутствие у лесов общего ГК также не позволит им использовать единую адресную книгу в почтовой системе (если, конечно, в этой системе нет собственного каталога почтовых пользователей). Единственный выход — задействовать службы синхронизации каталогов, например Microsoft Identity Integration Server (MIIS) 2003.

Кроме того, иногда без нескольких лесов не обойтись. Простейший пример — наличие в компании отдела разработок, создающего ПО, работающее с Active Directory и модифицирующее схему. Понятно, что тестовая сеть должна иметь свою службу каталогов, иначе проблемы в основной сети гарантированы. Иногда такую модель Active Directory называют моделью с лесом подписки (subscription forest).



Примеры использования нескольких лесов:

Тестовый и основной леса внутри предприятия (с лесом подписки)

Два разных предприятия

Для доступа к ресурсам используется явное нетранзитивное доверие, для синхронизации каталогов — метакаталог

Поэтому, резюмируя, обозначим причины возможного использования нескольких лесов.

- *Не требуется общая схема* Это связано либо с тестовыми разработками, либо с использованием различного ПО, интегрированного с Active Directory.
- ◆ *Не нужен единый ГК* Допустимо, когда почтовое или иное приложение использует свой каталог либо есть приложение синхронизации каталогов.

- ◆ *Отношения с партнером или контрагентом* Они не настолько близки, чтобы объединять сети, либо инфраструктуры Active Directory для *обоих* предприятий уже существуют.
- *Центральному отделу ИТ не удалось договориться с региональной службой* При *отсутствии* взаимодоверия и невозможности внедрения единой политики следует пойти на разделение лесов.

Мигрируем с доменной структуры Windows NT

Уяснив, как разбивать сеть на домены, обсудим доменную тактику и стратегию при миграции домена Windows NT. Для этого переберем все четыре модели объединения доменов Windows NT.

Прежде всего подчеркну, что *вопросы* совместимости существующих приложений с Windows 2000 мы затрагивать не будем. Дело в том, что даже после миграции домена в нем можно оставить как *серверы*, так и контроллеры, работающие и под Windows NT.

О технических аспектах миграции см. главу «Установка Active Directory».

Миграция **единственного домена**

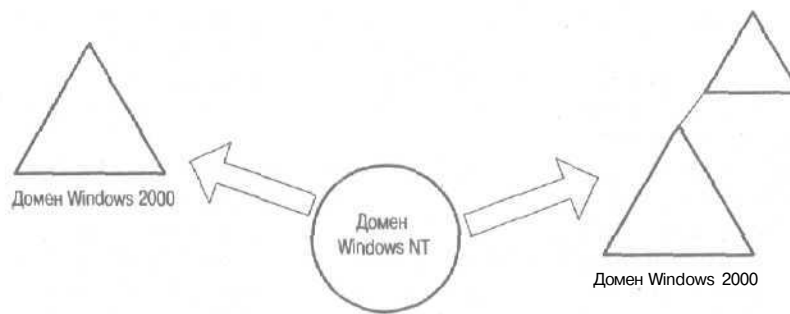
Если в организации был лишь один домен Windows NT, то потенциально есть два пути миграции:

- ◆ в один домен Windows 2000;
- ◆ в два домена Windows 2000.

Когда пойти первым? Ответ прост: см. выше критерии создания только одного домена. Очевидно, в большинстве случаев вы придете именно к решению 1 в 1. Уж если одного домена старого типа было достаточно для управления *пользователями* и ресурсами, то домена Windows 2000 хватит и подавно.

Второй путь целесообразен, когда предполагается рост предприятия и могут появиться подразделения, требующие отдельной политики безопасности либо расположенные на удаленных территориях. В этом случае рекомендуется создать корневой домен Windows 2000 — пустой хранилище *имени*, а *мигрируемый* домен сделать дочерним к нему.

В любом случае миграция, проведенная таким образом, останется *незаметной* для *пользователей*, так как они останутся в рамках домена с тем же NetBIOS-именем, а права доступа к ресурсам сохранятся.



Пути миграции одного домена

Миграция **доменной** структуры с одним мастер-доменом

Схема с одним мастер-доменом типична для большинства организаций. Разделение учетных записей и ресурсов удобно с административной точки зрения в доменах Windows NT. Доменам на базе Windows 2000 такое разделение несвойственно, хотя это возможно. С учетом сказанного можно предложить следующие варианты миграции.

- ◆ Мастер-домен Windows NT преобразуется в один домен Windows 2000. Все ресурсные домены аннулируются, а их ресурсы перемещаются в единственный домен.
- ◆ Мастер-домен преобразуется в корневой домен Active Directory. Ресурсные домены преобразуются в дочерние, по которым распределяются учетные записи пользователей.
- Создается пустой корневой домен. Мастер-домен преобразуется в дочерний. Ресурсные домены преобразуются в дочерние к нему или удаляются с переносом ресурсов в родительский домен. Учетные записи пользователей никуда не переносятся.

Наиболее распространен первый способ миграции. Он выполняется обычно в два этапа. Сначала мастер-домен обновляется до Windows 2000. Затем (это может быть сделано много позже) ресурсы из ресурсных доменов переносятся, а сами домены уничтожаются. Преимущества данного способа миграции таковы:

- **прозрачность для пользователей:** NetBIOS-имя домена может не изменяться, все ресурсы остаются постоянно доступными;
- **сокращение количества используемой техники:** на каждый ресурсный домен тратится минимум 2 контроллера домена, которые в результате миграции высвобождаются;
- **постепенность миграции:** перенос ресурсов можно выполнять длительное время.

Второй способ целесообразен в случае однозначного соответствия категорий пользователей и ресурсов, к которым они обращаются. Например, это может быть территориальное или административное разделение. Миграция выполняется в три этапа. На первом мастер-домен обновляется до корневого домена Windows 2000. Этот этап прозрачен для пользователей, так как с точки зрения аутентификации в домене, на первый взгляд, все остается по-прежнему.

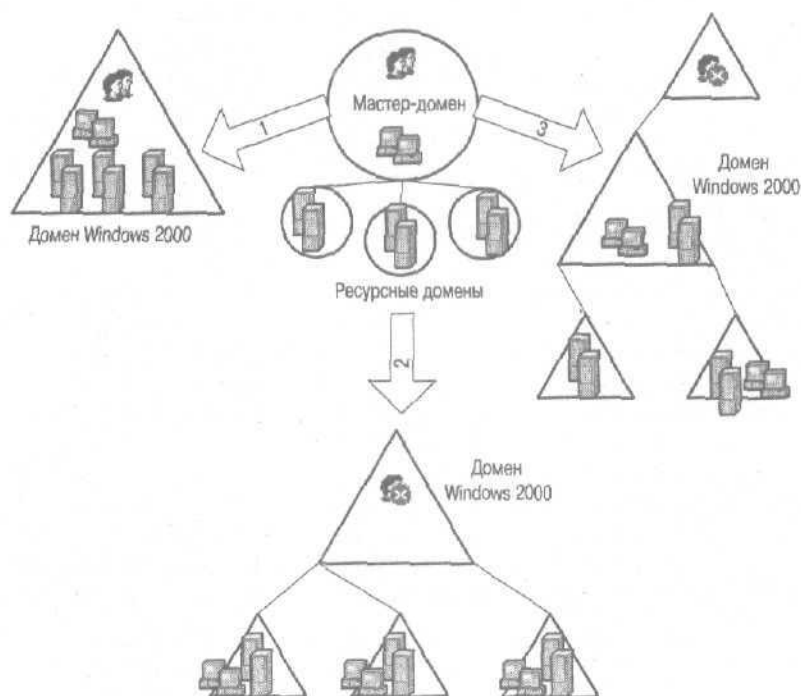
На втором ресурсные домены обновляются до доменов Windows 2000: они подключаются как дочерние домены к ранее мигрировавшему мастер-домену. Если эти домены разнесены территориально, то конфигурируются соответствующие сайты. Этот этап также прозрачен для пользователей, так как с точки зрения доступа к ресурсам они не видят никакой разницы.

На третьем этапе пользователи и их компьютеры группами выводятся из корневого домена и переносятся в дочерние. Перенос выполняется с помощью специальных утилит позволяющих сохранить историю SID пользователей (SID history) и тем самым обеспечить постоянное доступа к ресурсам. Одновременно в дочерних доменах создаются глобальные группы, куда включаются перенесенные пользователи. Эти группы включаются в соответствующие локальные группы, предоставляющие различные виды доступа к ресурсам. Это позволяет более не хранить историю SID и удалить прежние глобальные группы из корневого домена. Данный этап непрозрачен для пользователей, так как им придется переключить свой компьютер в новый домен и применять новый пароль.

Миграция кончается, когда все пользователи переносятся из корневого домена, в нем удаляются все глобальные группы, оставшиеся от старых времен, и остаются лишь административные группы предприятия (Schema Admins, Enterprise Admins) и административные группы домена.

Преимущества данного способа миграции таковы:

- ◆ **постепенность миграции:** перенос ресурсов можно выполнять в течение длительного периода времени;
- **сокращение трафика репликации;** разделение на сайты способствует этому;
- ◆ **создание границ безопасности между разными категориями пользователей:** пользователи теперь находятся в разных доменах;
- ◆ **возможность перехода на распределенную модель управления:** каждым доменом может управлять своя команда администраторов.



Возможные варианты миграции модели с одним мастер-доменом

Третий путь миграции, как это легко заметить, — комбинация первых двух. Его выбирают, когда нельзя однозначно всех пользователей отнести к разным категориям. При этом точно определить количество этапов миграции нельзя, хотя можно выделить следующие.

На первом этапе создается пустой корневой домен. Далее к нему в качестве дочернего присоединяется мигрировавший мастер-домен. Этот этап прозрачен для пользователей.

На втором могут одновременно выполняться разные действия. Например, из некоторых ресурсных доменов ресурсы переносятся в мигрировавший мастер-домен. Если это целесообразно, ресурсные домены обновляются до Windows 2000. К ним, например, можно применить специальную политику безопасности. Пользователей, работающих преимущественно с этими ресурсами, можно также перенести в эти домены. Поскольку все действия на этом этапе в значительной степени независимы, его могут выполнять разные группы специалистов в разные периоды времени.

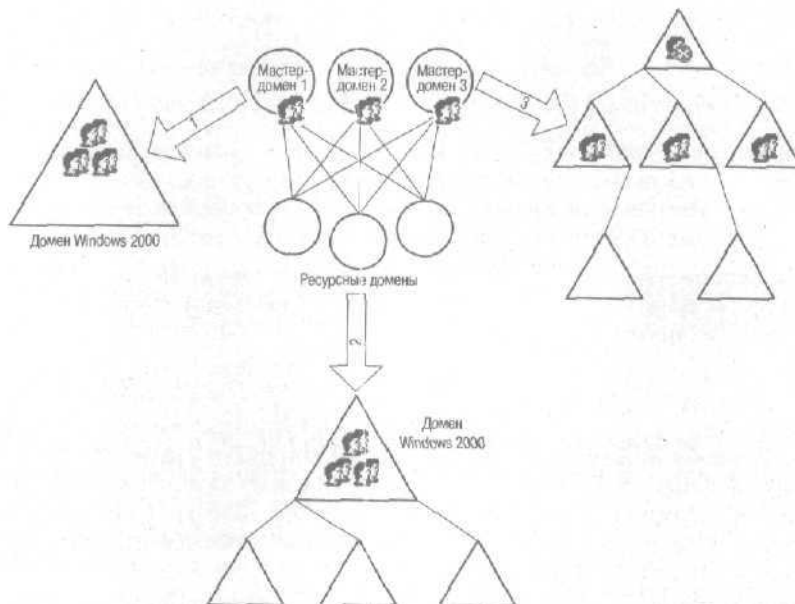
Миграция считается завершённой, когда не остается ресурсных доменов Windows NT, а в мигрировавшем мастер-домене не остается ненужных унаследованных глобальных групп.

Миграция доменной структуры с несколькими мастерами

Схема с несколькими мастерами характерна для крупных географически распределенных предприятий. Она подразумевает создание попарных доверительных отношений между ресурсными доменами и всеми мастер-доменами. Пути миграции во многом определяются теми задачами, которые миграция должна решить.

Если причиной разбиения на несколько мастер-доменов была предельная емкость домена Windows NT, то очевидно, что при миграции эти домены можно слить в один. Ресурсные домены можно уничтожить. Это самый выгодный тип миграции, при котором высвобождается большое число серверов. Для пользователей такая миграция не прозрачна. Они вынуждены переместить свои рабочие станции в новый домен и применять новые пароли. Если миграцию совместить с обновлением ОС на клиентских компьютерах, то эту смену домена выполнят технические специалисты.

Если основной задачей является сокращение числа поддерживаемых доверительных отношений и тем самым упрощения администрирования, то, выполнив миграцию ресурсных доменов и переместив в них учетные записи пользователей и клиентских компьютеров, можно подключить их в качестве дочерних к объединенному мастер-домену.



Основные варианты миграции модели с несколькими мастер-доменами

Если мастер-домены были разнесены географически, то это разделение можно оставить, сделав мигрировавшие домены дочерними к пустому корневому домену. Это позволяет использовать единое имя предприятия, снизить трафик репликации и применить различные политики в разных географических точках. Как при этом вы поступите с ресурсными доменами, зависит от ваших потребностей.

Миграция нескольких доменов с попарным доверием

Перечислить все возможные модели миграции схемы с полным доверием (или, более точно, с попарным доверием) просто невозможно: чем больше доменов, тем больше вариантов доверительных отношений между ними. Одно можно сказать вполне определенно: управляемость новой системы возрастет многократно.

Несмотря на такое многообразие, попробуем выделить основные правила рационального создания новой структуры.

1. Если все домены связаны попарно двусторонними отношениями и были созданы исключительно из-за политических соображений, важность которых сейчас не имеет значения, то все домены можно объединить в один домен Windows 2000. Выполнить это можно, либо создав новый домен и перенеся в него учетные записи пользователей, компьютеров и ресурсы, либо смигрировав самый крупный домен, а потом перенеся в него объекты из остальных.

Замечание В это может вмешаться фактор географической разобщенности. Тогда домены при миграции можно сгруппировать и преобразовать каждую группу в отдельный домен, расположенный на одной территории. Эти домены можно объединить «под крышей» пустого корневого домена либо в виде отдельных деревьев.

2. Если же политические соображения сохранили актуальность, идеальным станет решение создать пустой корневой домен и подключить к нему в качестве дочерних мигрировавшие. С точки зрения положения в дереве Active Directory, они равны, с точки зрения безопасности и политики — различны.
3. Если ключевым фактором разбиения на домены было уникальное имя, то при миграции можно сохранить этот фактор уникальности, преобразовав каждый из доменов в корень нового дерева в лесу.
4. Если доверительные отношения не двусторонние, надо проанализировать пути доверия и выделить учетные домены и ресурсные домены, а потом выбрать один из описанных выше путей миграции. Если при этом учесть географическое расположение доменов, наличие локального технического персонала, а также устойчивые долговременные связи, можно разработать весьма эффективную и управляемую структуру, что позволит сократить количество специалистов ИТ.

Группы и стратегия их использования

Прежде чем говорить о планировании групп, кратко напомним о видах групп в Windows 2000.

Универсальные группы объединяют пользователей в рамках леса и могут включать как отдельных пользователей, так и другие универсальные или глобальные группы из любого домена в лесу. Сведения о членстве в универсальных группах тиражируются на все серверы ГК.

Глобальные группы объединяют пользователей в рамках домена и могут включать как отдельных пользователей, так и другие глобальные группы из этого же домена. Сведения о членстве в глобальных группах не тиражируются на серверы ГК. Тиражируется только имя глобальной группы.

Локальные группы домена служат для предоставления доступа к ресурсам и могут включать как отдельных пользователей, так и другие универсальные или глобальные группы из любого домена в лесу. Они применяются только в списках контроля доступа локального домена. Информация о членстве в универсальных группах не тиражируется на серверы ГК.

Внимание Универсальные группы существуют только в доменах, работающих в естественном режиме. Только при этом условии возможно вложение универсальных и глобальных групп друг в друга.

Рекомендации по использованию универсальных групп

Членство в универсальных группах публикуется в ГК. Это значит, что если внести в группу или исключить пользователя, то вся информация о группе начнет реплицироваться по серверам ГК. В распределенных сетях, состоящих из большого числа сайтов, подключенных по медленным каналам, это вызовет нежелательную перегрузку канала.

Поэтому *первая рекомендация*: содержимое универсальных групп должно оставаться постоянным длительное время и меняться только в случае крайней нужды.

Возможно вы читали, что в группе не может быть более 5 000 членов. С одной стороны, это достаточно много для, скажем, типичного домена. Однако пользователей в рамках леса может быть и гораздо больше. Тиражирование большого количества членов группы может составить значительный трафик.

Отсюда *рекомендация вторая*: не включайте в универсальные группы много членов.

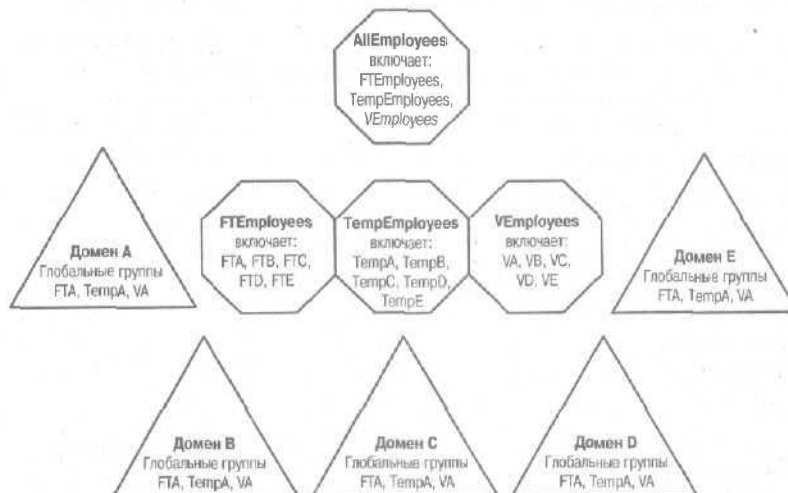
А что же, спросите вы, делать, если надо включить почти всех пользователей в универсальную группу? Мало того, что их много, так ведь они постоянно меняются: приходят, увольняются!

В таком случае *третья рекомендация*: включите в основную универсальную группу несколько дополнительных универсальных. В них в свою очередь включите глобальные группы из разных доменов. А уже в глобальные группы включите пользователей этих доменов.

Рассмотрим пример. Пусть в лесу Active Directory пять доменов и в каждом 800-1 500 пользователей. Вы планируете все учетные записи рассортировать по их статусу на предприятии: постоянные работники, подрядчики или временные сотрудники, сотрудники предприятий-партнеров. Чтобы выполнить сортировку, поступим так.

В каждом домене создаем по три глобальные группы: `FTDomainName` для постоянных сотрудников, `TempDomainName` для подрядчиков, `VDomainName` для партнеров. Далее создаем три универсальные группы: `FTEmployee`, `TempEmployee`, `VEmployee` — и включим в них соответствующие глобальные группы. Наконец, можно создать универсальную группу `AllUsers` и включить в нее три ранее созданных универсальных группы.

Несмотря на то, что в итоге в группу `AllUsers` попадет более 5 000 пользователей, она в себе содержит только 3 члена. Три другие универсальные группы содержат по 5 членов. А максимальное число членов описанных глобальных групп не превышает 1 500 человек, и то при условии, что в каком-то домене все сотрудники принадлежат только к одной категории. Очевидно, что с точки зрения универсальных групп, членство в них неизменно, поэтому репликация выполняется только при их создании и первичном наполнении другими группами.



Пример наполнения универсальных групп

Для чего могут понадобиться эти универсальные группы? Ну, например, для фильтрации групповой политики или разграничения доступа к корпоративным файловым ресурсам в масштабах всего предприятия. Правда, в последнем случае не обойтись без локальных групп домена. Но об этом чуть позже.

Рекомендации по использованию глобальных групп

Теперь поговорим о глобальных группах. Выше мы создали довольно крупные глобальные группы. Поддерживать членство в крупных группах достаточно сложно. Проще создать несколько глобальных групп меньшего размера, а их включить в глобальную группу в своем же домене.

Итак, *рекомендация первая*: создавая глобальные группы, делайте их поменьше.

По какому принципу формировать глобальные группы? Наверное, здесь уместно вспомнить, что глобальные группы будут использоваться для включения в локальные группы домена для последующего предоставления доступа к ресурсам. Все ресурсы обычно можно разделить по функциональности. Это могут быть, например, принтеры отделов и подразделений, каталоги рабочих и проектных групп, файлы руководства и т. п.

Отсюда *вторая рекомендация*: глобальные группы нужно создавать по функциональному признаку.

Рассмотрим организацию в которой есть руководство, секретариат, отдел продаж, отдел маркетинга, склад продукции, ИТ-служба и бухгалтерия. Часть сотрудников из отдела продаж, склада продукции и ИТ-службы заняты в отдельном проекте, направленном на улучшение работы склада. Исходя из этих условий, целесообразно создать 9 глобальных групп:

- ◆ MGMT для руководства;
- SECRETARY для секретариата;
- SALES для отдела продаж;
- MKTG для отдела маркетинга;
- STORE для склада;
- IT для службы ИТ;
- ACCT для бухгалтерии;
- ◆ PROJECT для тех, кто включен в проект;
- ◆ и ALL — группу, включающую в себя все перечисленные группы, кроме PROJECT.

Кстати, это необходимый минимум групп. Если при этом выяснится, что на каждом этаже есть свой принтер, можно создать и поэтажные группы. Если также обнаружится, что сотрудники даже одного отдела должны иметь доступ к разным ресурсам, то это тоже повод для разбиения их на глобальные группы. Об этом поговорим ниже.

Рекомендации по использованию локальных групп домена

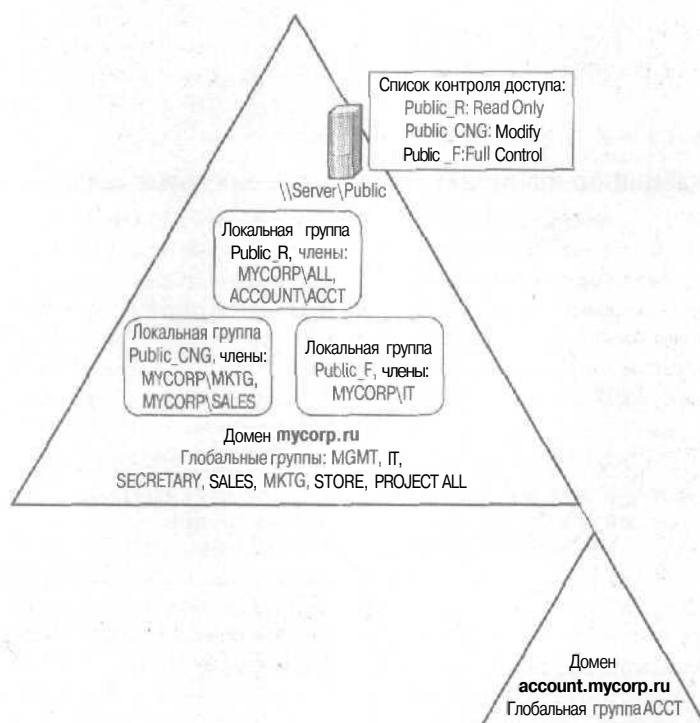
Локальные группы служат исключительно для предоставления доступа к ресурсам домена. Назначение прав доступа к принтерам, файлам, каталогам и сетевым ресурсам, предоставленным в общее пользование, должно выполняться только применительно к группам. Причина этого тривиальна. Если вы предоставили доступ отдельному пользователю, а потом он уволился, то в списке контроля доступа останется запись о несуществующем пользователе. Если же доступ ему был предоставлен через членство в группе, то при удалении из Active Directory пользователь будет удален из всех групп автоматически.

Рассматривая всевозможные виды доступа к файловым ресурсам, можно выделить три наиболее распространенных: полный доступ (F), чтение/запись+исполнение (CNG), чтение+исполнение (R). В соответствии с этой классификацией можно рекомендовать создание трех локальных групп для каждого файлового ресурса. Название группы может состоять из имени ресурса и обозначения вида доступа. Например, для каталога Public можно создать локальные группы:

- Public_F;
- Public_CNG;
- Public_R.

Теперь для предоставления доступа к такому ресурсу достаточно включить соответствующие глобальные группы в локальные с необходимым типом доступа. Допустим, в рассматриваемом выше примере все работники предприятия должны иметь доступ только на чтение, а сотрудники отделов продаж и маркетинга — еще и на запись. Полный доступ должен иметь ИТ-персонал. Тогда в группу Public_R включаем группу ALL, в Public_CNG — группы MKTG и SALES, а в Public_F — группу ИТ. Это распределение, но с одним отличием — бухгалтерия вынесена в отдельный домен, в котором и существует глобальная группа ACCT, — показано на рисунке ниже.

Рассмотренный пример довольно прост, и в реальной жизни встречаются куда более запутанные ситуации, когда нельзя всех сотрудников одного отдела однозначно включить в определенную группу доступа. Для них надо создавать специальные глобальные группы и включать их в группы доступа к ресурсам.



Пример предоставления доступа к ресурсу через членство в группах

Внимание Всякий раз, предоставляя локальной группе доступ к какому-либо ресурсу, документируйте это событие и фиксируйте имя группы, название ресурса и вид доступа. Это облегчит вам жизнь.

Кто должен заниматься включением пользователей в группы доступа? Ответ неоднозначен. Если это маленькая организация, то с такой работой могут справиться сотрудники службы ИТ. Если же это компания, в которой много отделов, обладающих своими ресурсами, то лучше всего назначить владельцев ресурсов. У каждого ресурса, предоставленного в совместное пользование, должно быть не менее двух владельцев: основной и запасной. Им должно быть делегировано право включать пользователей в «свои» группы. Причем это можно сделать через Web-интерфейс и сценарии ADSI. Если какому-то пользователю требуется доступ к ресурсу, он открывает страницу Web и запрашивает нужный доступ. Сценарий ADSI определяет ответственного и посылает ему уведомление, например по почте. Ответственный, получив письмо, заходит на сгенерированную по такому случаю страницу Web и предоставляет/запрещает доступ.

Использование особых объединений

Говоря о предоставлении доступа к ресурсам через членство в группах, нельзя не упомянуть *особые объединения* (special identities). Их можно для удобства считать группами, хотя это и не так: в них нельзя включить учетные записи пользователей, однако они включаются туда автоматически в зависимости от обстоятельств. Эти объединения не представлены в списке групп в Active Directory, но служат для разграничения доступа к ресурсам.

- В категорию **Everyone** попадают все пользователи, зарегистрировавшиеся в сети. Это могут быть даже пользователи и гости из других доменов. Главное условие включения в эту категорию — быть зарегистрированным в сети.
- ◆ **Authenticated Users** — почти то же, что и Everyone, но не содержит анонимных пользователей (гостей),
- В категорию **Network Users** входят пользователи, осуществляющие в данный момент доступ к определенному ресурсу по сети.
- В категорию **Interactive Users** входят пользователи, осуществляющие в данный момент доступ к ресурсу на том компьютере, за которым они непосредственно работают;

Для нас представляют интерес Everyone и Authenticated Users. Первую категорию надо по возможности исключать из всех списков контроля доступа. А вот вторая, наоборот, весьма полезна, так как позволяет избавиться от глобальной или универсальной группы, в которую включены все «свои» пользователи. Следовательно, при репликации трафик будет меньше.

Административные группы

Теперь о том, как лучше использовать административные группы. Начнем со встроенной локальной группы Administrators. По умолчанию в нее включены глобальные группы Domain Admins, Enterprise Admins (в естественном режиме работы домена это универсальная группа) и учетная запись Administrator. Так как это локальная группа, она служит для предоставления прав доступа к ресурсам домена. Если рассматриваемый домен не является корневым и вы не хотите, чтобы администраторы предприятия имели к вам отношение, исключите группу Enterprise Admins из локальной группы Administrators.

Внимание Не стройте иллюзий относительно своей независимости после исключения группы Enterprise Admins из группы Administrators. Если администраторам предприятия понадобится выполнить какие-то действия в вашем домене, они всегда это смогут сделать. Для этого им достаточно стать владельцами «ваших» ресурсов. При правильно настроенном аудите эта операция будет отслежена в журнале.

Группа Enterprise Admins дает практически неограниченную власть. Поэтому администраторов в ней должно быть минимум. Это же требование относится и к группе Schema Admins. Пусть ее члены и не всевластны, но последствия их действий могут стать причиной катастрофы в Active Directory. Я уже говорил, что эти две группы существуют только в корневом домене. Если в нем есть и другие учетные записи с административными полномочиями, то они могут включить себя в эти группы для выполнения несанкционированных действий в любой момент. Вот почему рекомендуется создавать пустой корневой домен, в котором нет учетных записей, кроме администратора — только он вправе включать в группы Enterprise Admins и Schema Admins пользователей из других доменов.

Замечание Пустой корневой домен должен работать в естественном режиме чтобы административные группы масштаба предприятия были универсальными.

Членство в административных группах должно жестко регламентироваться. Одним из средств регламентирования является групповое правило Restricted Groups, ограничивающее членство в указываемых группах. В политике жестко прописано, кто может быть членом группы. Если кто-то добавит себя в одну из групп с ограниченным членством, то по истечении срока обновления правил (5 минут для контроллеров домена) он будет исключен из этой группы.

Включать ли всех ИТ-сотрудников в группу администраторов, пусть даже не всего предприятия, а одного домена? Ни в коем случае. В административных группах домена должно быть минимум пользователей. Отдельные административные полномочия должны быть делегированы так, чтобы:

- обеспечивалась непрерывность администрирования;
- отсутствовали избыточные полномочия.

Таким образом, от групп мы переходим к рассмотрению организационных подразделений (ОП).

Если ОП создают, значит, это кому-нибудь нужно

Организационные подразделения — это контейнеры в Active Directory, в которых могут находиться такие объекты, как пользователи, компьютеры, группы, принтеры, совместно используемые ресурсы, приложения и другие ОП. Отличительной особенностью ОП является возможность применения к ним групповой политики (кроме политики безопасности, применяемой ко всему домену). С другой стороны, ОП — это объект Active Directory, и, как к любому объекту, к нему и ко все-

му, что в нем лежит, можно задать права доступа. Так что ОП — вещь довольно ценная.

Когда же использовать ОП? Ответов множество. Вот главные.

- **Для делегирования административных полномочий** Раз можно регламентировать права доступа к контейнеру, значит, можно назначать тех, кто имеет полный доступ, т. е. является администратором по отношению к объектам внутри контейнера.
- ◆ **Для разграничения групповой политики** Разделив пользователей и компьютеры по разным контейнерам, вы можете применять различную групповую политику.
- ◆ **Для рассортировки объектов** Можно отдельно разместить принтеры, пользователей, компьютеры и т. д.
- ◆ **Для ограничения числа объектов в контейнерах** Хотя объем контейнера не ограничен, просматривать содержимое больших ОП неудобно — проще в один ОП поместить несколько меньших по объему.
- **Для помощи в миграции** При переносе ресурсов из доменов Windows NT желательно сохранить управляемость этими ресурсами. Поэтому удобно их перемещать в отдельные ОП, для управления которыми используется делегирование.

Вы, конечно, поняли, что структура ОП планируется по определенным правилам. Вот они.

- ◆ Первый уровень ОП внутри предприятия должен следовать некоторому стандарту, т. е. в каждом домене применяется общий принцип построения ОП. Это значительно облегчит использование ОП.
- ◆ Не увлекайтесь глубиной вложения ОП. Дело тут не только в том, что навигация по глубоко вложенным подразделениям — дело достаточно занудное, а в том, что выполнение LDAP-запросов поиска по структурам с глубокой вложенностью заметно замедляется. С другой стороны, вложенность не сказывается на репликации.
- ◆ Иерархия ОП должна иметь смысл и быть понятной. Создавать ОП только ради него самого бессмысленно. Смысл же определяется ответом на вопросы: кто будет управлять и кто будет видеть ОП?
- ◆ Любой объект может находиться одновременно только в одном ОП (в отличие от групп). Следовательно, если вы хотите применять разные групповые политики к нескольким пересекающимся наборам объектов, нужно продумать иерархию ОП. При этом политики с верхних уровней будут наследоваться на нижних.

Модели организационных подразделений

Эти правила привели к разработке нескольких моделей ОП.

Географическая иерархия

Подразумевает строительство дерева ОП в соответствии с географическим положением. Однако выше мы рассматривали географическую удаленность как один из критериев разделения на домены. В чем же разница?

Пусть в крупной организации имеется три домена: производства, маркетинга и продаж. Это связано с тем, что к сотрудникам этих подразделений предъявляются разные требования безопасности. Вместе с тем предприятие разбросано по нескольким регионам: Москва, Санкт-Петербург, Нижний Новгород и Новосибирск. В каждом из городов должна применяться своя групповая политика установки приложений. Поэтому в каждом из трех доменов создаются ОП для каждой территории.

Преимущества такой модели:

- ОП первого уровня стабильны, так как существуют все время, пока предприятие ведет бизнес на указанной территории;
- администраторам легко понять, где именно находятся ресурсы.

Недостаток модели в том, что она не отражает бизнес-потребностей предприятия.

Организационная иерархия

Пользуется симпатией начальства, потому что отражает организационную структуру компании. На вершине иерархии — руководство, на втором уровне — дирекции, на третьем — отделы внутри дирекций и т. д. Всякий раз, когда руководителю требуется указать сотруднику на его место, он может открыть, скажем, Microsoft Visio, который автоматически выведет на экран графическое представление структуры Active Directory, а значит, и фактическую оргструктуру. Опять же, когда возникает ситуация из разряда «А подать сюда Ляпкина-Тяпкина!», задается поиск этого субъекта в каталоге, а из имени субъекта следует, в каком отделе он работает. Вот и причина любви! И невдомек начальству, что всякий раз, когда переименовываются отделы, создаются или сливаются подразделения, администратор вынужден все эти изменения сразу отражать и в структуре ОП. Но и это не самое плохое. Хуже, когда требуется какие-то отделы или дирекции выносить в отдельный домен по соображениям безопасности, например. И все, рушится стройная картина!

Объектная иерархия

Эту модель я бы назвал по-военному прямолинейной. Есть классы объектов, вот их и дифференцируем. Компьютеры — в одну кучу,

пользователей — в другую, принтеры — в третью и т. д. Резон для такого деления есть, и не один:

- ресурсами легче **управлять**, поскольку они все **рассортированы**;
- ◆ легче создавать общие списки контроля доступа к различным классам объектов;
- ◆ легче делегировать полномочия для различных классов объектов.

Представим структуру ОП, **построенную** на объектной модели: на первом уровне ОП Принтеры, Пользователи, Рабочие станции и Серверы, на втором идет **детализация** по какому-либо признаку, например, Принтеры 1 этажа, Принтеры 2 этажа, Пользователи 1 этажа, Пользователи 2 этажа и т. д.

Но логичнее использовать эту модель в совокупности с другими. Например, если верхние уровни определены по организационной модели, то, дойдя до нижнего уровня (например, до отделов), можно переключиться на объектную модель и для каждого отдела **разделить** пользователей, компьютеры и пр.

Вы можете усомниться в простоте использования такой **смешанной** модели и будете правы. Но только до тех пор, пока не выяснится, что учет сотрудников и техники ведется с помощью специального приложения, интегрированного с Active Directory. Если оно позволяет в графическом виде просматривать планы этажей, с легкостью перемещать сотрудников и технику между подразделениями и отслеживать инвентаризацию этой **техники**, то вам уже не придется вручную шапир по каталогу в поисках нужного объекта.

Проектная иерархия

Подразумевает, что ОП строятся с учетом проектов, исполняемых в организации. При этом легко отслеживать ресурсы и затраты для каждого из проектов. Однако проект длится определенное **время**. А значит, по его завершении структуру ОП **нужно** переработать.

А если кто-то из сотрудников вовлечен сразу **в два** проекта? Поделить его пополам и назначить две разные учетные записи? Представляете, как сложно будет следовать **этой** модели!

Поэтому она может иметь очень ограниченное применение.

Административная иерархия

Предмет любви **ИТ-сотрудников**, так как именно им она обеспечивает максимум комфорта; ОП создаются на основании того, как легче управлять **пользователями**, компьютерами и пр. Например, если известно, что все различия пользователей в домене в том, с какими приложениями они работают, то **составляются** списки пользователей каждого приложения. Из общего списка выбирается подмножество

приложений, нужных максимальному числу пользователей. Для этого приложения создаются групповая политика, назначаемая корневому ОП. Затем выбираются приложения, нужные меньшему числу пользователей, и соответствующие групповые правила применяются к ОП второго уровня. Наконец, создается ОП нижнего уровня и заполняется пользователями, которым нужны специфические приложения. Рассмотрим пример.

Согласно корпоративному стандарту организации используется почтовый клиент Microsoft Outlook, а в качестве офисных приложений – Microsoft Word и Excel. Кроме того, сотрудники бухгалтерии должны работать с 1С:Бухгалтерией и клиентской частью SAP. Последняя также требуется сотрудникам отдела кадров и аналитического отдела. Дополнительно к этому сотрудникам аналитического отдела нужны Microsoft Visio и Microsoft Project.

Вот как реализовать такую структуру ОП по административной модели:

- ◆ верхний уровень: ОП, названное SAP, в которое включены сотрудники отдела кадров;
- ◆ второй уровень: ОП 1С (сотрудники бухгалтерии) и Анализ (сотрудники аналитического отдела);
- + остальные пользователи не входят ни в какие ОП.

К домену в целом применяется офисная политика. Ко всем ОП применены соответствующие групповые политики по установке приложений. Сколь дикой ни казалась бы такая структура на первый взгляд, она обеспечивает нужную функциональность с минимумом затрачиваемых усилий.

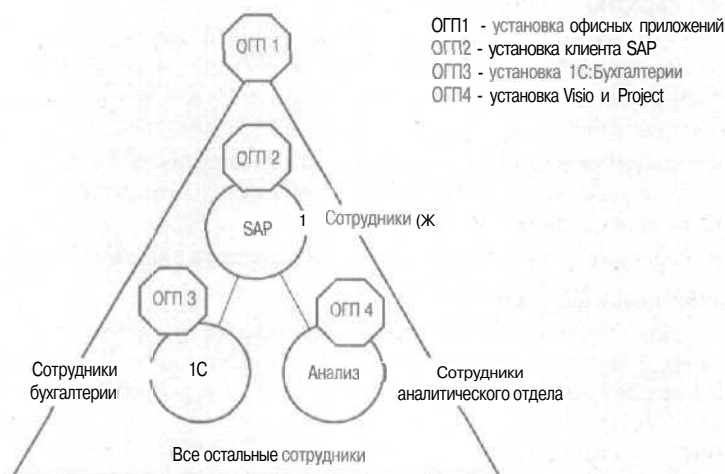
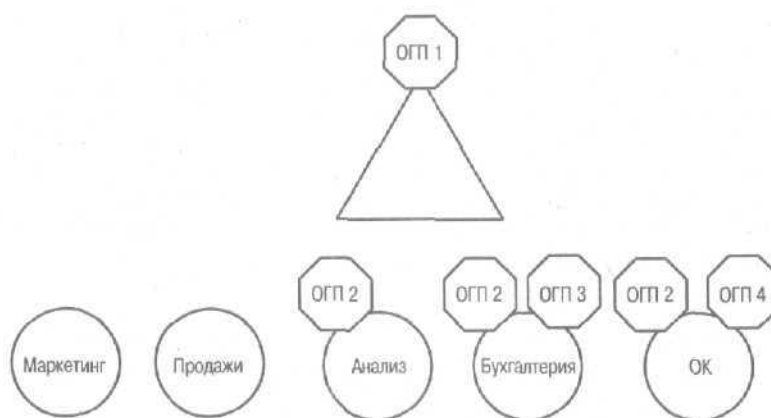


Иллюстрация примера административной модели ОП



Тот же пример, но реализованный через организационную модель

Сравним ее с другими моделями. Если следовать географической модели, то в данном случае все пользователи располагаются в одном ОП. Это значит, что для применения различных групповых правил понадобится фильтрация. Для этого будет нужно предварительно создать группы, включить в них пользователей из каждого подразделения, а затем для каждой из групповой политик (разве кроме офисной) определить фильтры.

Согласно административной модели последовательность действий такова. Вы распределяете всех пользователей по ОП. Далее создаете объекты групповой политики для установки каждого из приложений и применяете их к нужным ОП. Пока ОП мало, сложность реализации групповых правил близка к сложности административной модели. С ростом числа ОП придется распределять объекты групповой политики по все большему числу контейнеров, что затруднит их учет и анализ взаимодействия.

Так кому нужны организационные подразделения?

У каждой из пяти моделей построения ОП свои плюсы и минусы. Так что ни одна не является догмой. Можете смело комбинировать их и создавать гибрид, который вас устроит. Но в любом случае что-то одно надо выбрать за основу. Что?

Все зависит от вашего ответа на вопрос: для кого создается структура ОП? Если отбросить ответ «ни для кого», остаются такие варианты:

- ◆ для себя (т. е. для администратора);
- для начальства;
- для пользователей.

Ну, начальству структура ОП ни к чему. Увы, убедить его в этом должны вы. Сделать это трудно, но надо.

Предупреждение Выбивая деньги на развертывание Active Directory, ни в коем случае не ссылайтесь на возможность для руководства знать, кто и где находится. Иначе вам придется следовать организационной модели, даже если вы поймете, что она вам не нужна.

Нужны ли подразделения пользователям?

Пользователь повседневно работает:

- ◆ с документами (поиск, редактирование, сохранение, печать);
- ◆ с почтой (поиск в адресной книге, редактирование/чтение писем);
- со специализированными приложениями;
- ◆ с сетевыми ресурсами (поиск);
- ◆ и предоставляет локальные ресурсы в совместное использование (если разрешено).

Начнем по порядку. Прежде чем документ открыть, его надо найти. Он может храниться как на локальном компьютере, так и в сети. Чтобы его найти, пользователь выбирает команду Search в меню Start — она выводит диалоговое окно, которое по умолчанию предлагает искать файлы на локальном компьютере. Поверьте мне, для большинства пользователей это предел возможностей.

Замечание Даже этот сценарий для многих пользователей — непреодолимое препятствие. Обычно документы хранятся в папке My Documents или в некотором каталоге, подключаемом при регистрации пользователя в сети.

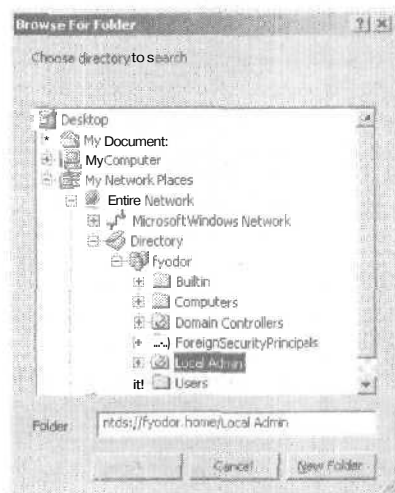
И все же допустим, что познания нашего пользователя столь глубоки, что в списке Look in он выбирает команду Browse. Но даже тогда, чтобы добраться до каталога, ему надо раскрыть My Network Places, Entire Network, Directory и найти имя своего домена! Вот только тут он впервые увидит ОП. Я уж не говорю о том, что далее ему придется отыскать в каталоге ресурс и только после этого начать поиск. Итак, считаем данное событие маловероятным.

Процесс редактирования документов не связан с доступом к каталогу и ОП в нем.

Операция сохранения документа практически идентична его открытию. Но если в первом случае поиск в каталоге еще имеет какой-то смысл, то теперь смысла нет, так как найти нужный ресурс просто невозможно! Таким образом, вероятность события равна 0.

Вывод документа на печать **невозможен без** доступа к каталогу. Но это знаете вы, технические специалисты, А пользователь об этом не знает, поэтому всегда печатает на том принтере, который к нему подключен. Если б он знал, что можно найти и другой принтер в каталоге и без проблем к нему **подключиться**, то он бы выбрал в меню **Start** команду **Search** и далее **Search for printers**. Но даже здесь знание структуры ОП ему ни к чему. Пользователь знает такие атрибуты принтера, как его месторасположение, цветной он или нет, может быть, даже имя модели. А вот в каком **ОП** он находится, ему безразлично.

Работа с почтой интересует нас потому, что здесь пользователь активно занимается поиском адресатов. Какое отношение имеет почтовая адресная книга к Active Directory? Если ваша система построена не на Microsoft Exchange 2000, то никакого. Но даже если у вас Exchange 2000, то и в этом случае структура ОП мало кого интересует. Главное — это почтовый адрес и другие атрибуты **пользователя**. Все остальные операции с почтовой программой не требуют доступа к каталогу (с точки зрения пользователя, конечно).



Расширенное окно поиска ресурсов в каталоге

Работу со специализированными приложениями мы даже рассматривать не будем: ведь они, как правило, не требуют обращения пользователя к каталогу.

Поиск сетевых ресурсов мы уже рассмотрели выше, поэтому остается последнее: предоставление своих ресурсов в совместное **использование**. Эта операция относится к разряду тех, что обычно запрещены

групповой политикой. Но так как в ряде организаций она разрешена, обсудим ее подробнее.

Предоставляя свой ресурс в совместный доступ, **пользователь** обычно не ограничивает права доступа к нему. Если же он попытается это **сделать**, то при определении списка контроля доступа он не увидит структуры ОП — только структуру доменов,

Вывод: рядовым пользователям структура ОП не нужна, а значит, вычеркнем их из списка тех, чьи интересы нужно учесть, планируя ОП.

Подразделения нужны администраторам!

Остались администраторы... А нужны ли им ОП? Еще как! Вы же заметили, что мы постоянно упоминали те операции администрирования, что без ОП невыполнимы.

Во-первых, это делегирование административных полномочий. Проще делегировать полномочия по управлению одним контейнером, чем списком различных объектов.

Во-вторых, это групповые правила, благодаря наследованию которых, в иерархии ОП можно строить гибкие управляемые системы.

В-третьих, это средство группирования ресурсов. Администраторам удобнее видеть рабочие **станции** отдельно от принтеров и пользователей. Это **позволит** эффективнее применять к ним групповые правила.

Так что, проектируя иерархию ОП, думайте только об администрировании системы. Старайтесь сделать ее такой, чтобы управление не требовало привлечения дополнительного **ИТ-персонала** для **выполнения** рутинных работ.

Делегирование административных полномочий

Стратегия делегирования полномочий может быть произвольной. И все же существует набор правил, позволяющих реализовать **успешную** стратегию делегирования. Они основаны на предположении, что ОП делятся на две категории: учетные и ресурсные. Это предположение не **конфликтует** с рассмотренными моделями ОП, так **как** в любой из них могут иметься и те и другие.

В учетных ОП хранятся учетные записи пользователей, служб, компьютеров и групп, в ресурсных — принтеры, совместно используемые ресурсы и приложения. В этом плане они чем-то напоминают учетные и ресурсные домены Windows NT. Но только в отличие от доменов вы можете жестко разграничить полномочия администраторов.

С целью делегирования полномочий записи в учетных ОП размещаются по разным вложенным ОП: Пользователи, Учетные записи **служб**, Компьютеры, Группы. Можно добавить и **другие** ОП и поместить в них, **например**, пользователей, имеющих отличные от остальных права. Для каждого вложенного, а также для самого учетного ОП создается ло-

кальная группа домена. Эти группы содержат пользователей, которым делегируется право управления соответствующими вложенными ОП. Имена этих групп удобно составлять из <имени ОП>_<выполняемой функции>. Тогда делегирование в учетном ОП сведется к назначению таких полномочий:

ОП	Имя группы	Тип доступа	Тип объекта
Родительское учетное ОП	<имя ОП>_ou_admins	Full Control	Все объекты
Дочерние ОП:			
Users	<имя ОП>_ou_user_admins	Full Control	User
Service Accounts	<имя ОП>_ou_user_admins	Full Control	User
Computers	<имя ОП>_ou_computer_admins	Full Control	Computer
Groups	<имя ОП>_ou_group_admins	Full Control	Group
Limited Admins	<имя ОП>_ou_local_admins	Full Control	User

Для ресурсных ОП в общем случае достаточно одной группы, которая владеет ОП и имеет полный доступ к объектам,

Разбиваем на сайты

Сайты Active Directory — это сегменты сети с высокой пропускной способностью. По крайней мере так гласят все определения сайтов. А для чего они? Вот основные причины, по которым Active Directory нужно разбивать на сайты.

- *Управление трафиком репликации* При тиражировании изменений в Active Directory сайты позволяют указывать, как и когда пойдет поток репликации.
- + *Минимизация трафика регистрации клиентских станций* При регистрации клиентский компьютер обращается к контроллеру домена, расположенному в том же сайте (или в ближайшем, если локального контроллера домена нет).
- ◆ *Управление трафиком репликации FRS* Так как FRS использует для репликации ту же топологию, что и репликация Active Directory, то сайты положительно влияют на трафик.
- ◆ *Управление топологией DFS* Если ресурс DFS имеет несколько реплик, то обращающийся к нему клиент будет направлен к ближайшей к нему реплике.
- ◆ *Поддержка специализированных приложений* Эти приложения, связанные с Active Directory, адресуют клиентов к своим ресурсам, расположенным в ближайшем сайте.

Главное значение разбиение на сайты имеет для репликации, поэтому в основном об этом мы и будем думать, рассуждая о топологии сайтов. О репликации Active Directory см. одноименную главу.

На репликацию огромное влияние оказывают:

- пропускная способность каналов;
- ◆ трафикрепликации;
- расположение контроллеров доменов.

Поэтому дизайн сайтов надо начинать с тщательного документирования и анализа топологии сети. Помимо фиксирования пропускной способности каналов и их числа, надо записать количество пользователей на каждой площадке и бизнес-проблемы, решаемые ими. При этом следует помнить о плюсах и минусах разбиения на сайты:

Преимущества и недостатки разбиения на сайты

Преимущества	Недостатки
Управление трафиком репликации: объем и расписание	Синхронизация изменений между контроллерами доменов в разных сайтах выполняется спустя длительное время.
Возможность использовать ненадежные каналы	Может потребоваться дополнительное оборудование, что удорожает решение
Снижение трафика регистрации Поддержка специализированных приложений	

Так какой же все-таки критерий?

Итак, первый критерий разбиения на сайты — пропускная способность каналов связи. А что считать высокой пропускной способностью и что низкой? Часто как водораздел используют значение 10 Мб/с. Всегда ли это так?

Представим сегмент сети, связанный с основной ее частью каналом с пропускной способностью 128 Кб/с. В сегменте 10 пользователей, большей частью работающих с локальными ресурсами. Канал практически свободен. Добавим к этому стабильность коллектива, т. е. скорость изменений в Active Directory низка. Понятно, что пропускная способность этого канала более чем достаточна, чтобы не выделять этот сегмент в отдельный сайт.

Теперь возьмем сегмент сети в соседней организации. Он подключен к основной территории каналом 1,5 Мб/с. На этой территории 50 работников активно используют телефон, весь трафик которого направляется по единственному каналу и занимает 50% от его пропускной способности. Кроме того, пользователи работают с электронной почтой, построенной на Microsoft Exchange 5.5. Этот трафик съедает еще 25% пропускной способности канала. Планируется и миграция на Exchange 2000. Общий размер организации невелик: 800 пользовате-

лей. но в компании текучка кадров. В такой ситуации однозначно надо говорить о создании отдельного сайта, так как трафик репликации в домене будет большим.

Итак, анализируя пропускную способность каналов, в первую очередь выделяют каналы с пропускной способностью менее 10 Мб/с. Далее рассматривают площадки, подключенные по этим каналам и анализируют потенциальный рост трафика в канале после внедрения Active Directory. Следующий шаг — анализ текущей загрузки канала и вычисление его эффективной пропускной способности. Если прогнозируемый трафик в пиковые моменты существенно ниже эффективной пропускной способности, то нет нужды создавать отдельный сайт. Если же он сравним или выше, то сайт необходим.

Замечание Анализируя эффективную пропускную способность канала, нельзя полностью полагаться на цифры, содержащиеся в договоре с провайдером линии. Провайдеры обычно делят один канал между несколькими клиентами, что может приводить к снижению эффективной пропускной способности. Поэтому лучше измерить реальную пропускную способность в разное время суток.

Второй критерий разбиения на сайты — надежность канала, под которой в первую очередь понимают его постоянную доступность. Если есть вероятность разрыва канала (даже непродолжительного), следует говорить об отдельном сайте.

Еще один критерий — возможность управления межсайтовым трафиком. Во-первых, можно составить расписание репликации. Если с 9.00 до 18.00 канал загружен на 90%, а в остальное время он практически свободен, можно сконфигурировать расписание так, что информация будет тиражироваться только в нерабочие часы. Во-вторых, можно задействовать компрессию трафика, которая включается автоматически при превышении объема тиражирования равного 50 кб. В-третьих, для ненадежных каналов можно организовывать асинхронную репликацию по протоколу SMTP.

Алгоритм разбиения на сайты выглядит так (см. след. стр.).

Сколько может быть сайтов?

Сколько может быть сайтов? Чтобы ответить на этот вопрос, подумаем, на что влияет их число. Начнем с репликации. Да, само по себе наличие сайтов влияет на трафик репликации, которая выполняется в соответствии с топологией. Топология базируется на межсайтовых соединениях. А межсайтовые соединения... создаются автоматически службой KCC (Knowledge Consistency Checker), точнее, той ее частью, что называется Генератором межсайтовой топологии (ISTG). Для меж-

сайтовой репликации служба КСС периодически проверяет доступность контроллеров домена, выполняющих роль серверов-форпостов и, если они недоступны, назначает новые серверы, т. е. перестраивает топологию репликации. Эта работа в совокупности с аналогичной деятельностью внутри сайта весьма ресурсоемка и при большом числе сайтов и доменов полностью поглощает все процессорное время компьютера, выполняющего роль КСС и ISTG.

Совет Чтобы понять, насколько КСС загружен, можно изменить в реестре значение параметра KnowledgeConsistencyChecker в ветви HKLM\System\CurrentControlSet\Services\NTDS\Diagnostics. Если установить его большим или равным 3, в журнал регистрации попадут события 1009 и 1013, сигнализирующие о начале и конце проверки топологии.

Есть формула, описывающая максимальное число сайтов и доменов при использовании автоматической генерации топологии:

$$(1+D)*S^2 \leq 100000$$

где D — число доменов, а S — число сайтов.

Так, если у вас всего один домен, максимальное число сайтов 223, если же два домена, число сайтов не может быть больше 182. И это все? А как быть с организацией, в которой 50 доменов в 50 сайтах? Это ведь далеко не запредельные значения!

Замечание В Windows 2003 алгоритм работы КСС изменен таким образом, что удалось существенно улучшить нагрузочную способность этого элемента. В приведенной выше формуле зависимость от числа сайтов стала линейной. На момент подготовки этого издания автору было известно о нормальном функционировании Active Directory с 1700 сайтами.

Вот результаты измерения времени работы КСС в разных системах с одним центральным сайтом и несколькими периферийными, выполненные на компьютере с Intel Pentium III Xeon-500 и 1 Гб ОЗУ.

Расположение	Число сайтов	Число доменов	Время (ч:м:с)	Используемая память (Кб)
Филиал	125	1	0:00:12	11 748
Центр	125	1	0:00:21	12 256
Филиал	250	1	0:00:41	45 660
Центр	250	1	0:01:05	44 820
Филиал	500	1	0:02:56	173 216
Центр	500	1	0:04:34	174 752
Филиал	1 000	1	0:15:23	685 596

см, след. стр.

Расположение	Число сайтов	Число доменов	Время (ч:м:с)	Используемая память (Кб)
Центр	1 000	1	0:17:34	688 568
Филиал	1 000	1	0:15:54	685 604
Центр	1 000	1	0:17:51	689 668
Филиал	125	10	0:00:59	58 520
Центр	125	10	0:01:19	58 536
Филиал	250	10	0:04:00	228 304
Центр	250	10	0:04:47	227 508
Филиал	500	10	0:21:32	815 916
Филиал	500	10	0:19:41	823 808
Центр	500	10	0:21:18	828 484
Филиал	125	50	0:04:49	266 088
Центр	125	50	0:05:54	264 024
Филиал	250	50	0:20:19	831 924
Центр	250	50	0:22:49	841 536

Как видите, нагрузка велика. Есть несколько вариантов решения проблемы. Не предлагаю изменить число доменов. Очевидно, если вы приняли решение создать столько доменов, то так тому и быть. Ниже я дам ряд рекомендаций, но одна из них такова: отключите ISTG и сгенерируйте топологию межсайтовой репликации вручную. При этом надо иметь в виду, что за топологией придется постоянно следить и порой перестраивать. Увы, это та цена, которую приходится платить в крупной сети. О том, как упростить себе жизнь, я расскажу в разделе «Надежная связь между сайтами».

Сколько нужно контроллеров и где их размещать

Очень часто спрашивают, сколько нужно контроллеров домена и где их размещать. То, что в домене должно быть не менее двух контроллеров, вы уже знаете. А если домен разделен на несколько сайтов? Вообще вариантов ответа — три:

- для сайтов с количеством пользователей до 10;
- для сайтов с численностью от 10 до 50 пользователей;
- для сайтов с числом пользователей от 50.

Менее 10 пользователей

Если в сайте менее 10 пользователей и они не работают с Microsoft Exchange 2000, контроллеры домена в сайте можно не устанавливать:

Преимущества и недостатки отсутствия контроллеров в сайте

Преимущества	Недостатки
Отсутствует трафик репликации Не требуется дополнительное оборудование	<p>Весь трафик регистрации направляется в канал связи</p> <p>Весь трафик LDAP-запросов к ГК направляется по каналу связи</p> <p>При недоступности канала связи нельзя получить доступ к ресурсам, в том числе к локальным. Нужны альтернативные решения</p> <p>При недоступности канала связи и работе домена в естественном режиме невозможна регистрация в сети. Нужны альтернативные решения</p>

Как видите, минусов больше, чем плюсов, но это не значит, что это решение неприемлемо. Если канал связи достаточно надежен и не сильно загружен, то нет большой беды, что трафик запросов к ГК и трафик регистрации направляются по нему. А если канал недоступен?

Как видно из таблицы, это чревато в первую очередь невозможностью обращаться к локальным ресурсам, например, файловым или принтерным. Но этот недостаток можно преодолеть.

На файловом сервере создадим локальные группы, включив их в списки контроля доступа к ресурсам наравне с локальными группами домена. На сервере же создадим локальные учетные записи для всех пользователей в сайте. Этих пользователей также включим в локальные группы сервера. Пока канал открыт, пользователи осуществляют доступ по своим доменным **учетным** записям. Если канал недоступен, применяются локальные учетные записи сервера. Очевидный недостаток этого решения — сложность администрирования: ведь приходится поддерживать второй комплект учетных записей пользователей.

Еще один способ — задействовать терминальный сервер. Пользователи осуществляют доступ к ресурсам не напрямую, а открывая терминальный сеанс. Для этого им нужно **зарегистрироваться** на терминальном сервере. Пока канал **существует**, они регистрируются согласно своим полномочиям в домене. Если канал недоступен, они все равно могут зарегистрироваться на терминальном сервере, применяя **кэшированные** полномочия. Такое решение предпочтительно при работе с локальными **приложениями** и требует гораздо меньших усилий по администрированию.

Замечание Если канал недоступен, пользователь может не зарегистрироваться, не имея доступа к контроллеру домена. Если он регистрировался ранее, то с помощью **кэшированной** на рабочей станции

информации войдет в сеть. Если же он регистрируется на конкретном компьютере впервые, то его постигнет неудача.

От 10 до 50 пользователей

Число контроллеров домена на сайтах в этом случае зависит от операций, выполняемых в сайте. Для каждого домена нужен минимум один контроллер! Если сайт принадлежит нескольким доменам, в нем должны быть контроллеры для каждого, и вот почему.

Вспомните (см. главу «Репликация Active Directory»), какие контексты имен тиражируются при репликации:

- ◆ контекст конфигурации, включающий информацию о структуре и конфигурации леса;
- контекст схемы, содержащий базовую информацию об объектах Active Directory и их атрибутах;
- доменный контекст имен, содержащий информацию как об объектах домена (пользователи, компьютеры и пр.), так и объекты групповой политики,

Контроллер в домене знает о доменном контексте имен только своего домена, но не чужих. Если сайт принадлежит нескольким доменам, то при регистрации пользователь должен обратиться к контроллеру того домена, в котором регистрируется. Если нужного контроллера в сайте нет, трафик регистрации будет направлен по каналу связи.

Приложения типа Microsoft Exchange 2000 потребуют установки ГК на одном из контроллеров, так как понадобится обслуживать большое число LDAP-запросов поиска объектов из всего леса. В противном случае эти запросы пойдут по каналу связи к серверу ГК в другом сайте.

Сервер ГК нужен в сайте, когда домен работает в естественном режиме. Дело в том, что при регистрации пользователя к ГК отправляется запрос о его членстве в универсальных группах. Если ГК недоступен, становится неясно, какие права доступа имеет пользователь, а раз так, то ему отказывают в регистрации.

Замечание Эту функциональность можно отключить на рабочей станции: в реестре изменить значение параметра `HKLM\System\CurrentControlSet\Control\LSA\IgnoreGC Failures`. Это позволит пользователю зарегистрироваться в сети, но права доступа к некоторым ресурсам будут неверными, так как членство в универсальной группе проверено не будет. В Windows 2003 от ГК в небольших сайтах можно избавиться без этого недостатка. Для этого достаточно на контроллере домена в сайте включить функцию кэширования глобальных и универсальных групп.

Наличие ГК в сайте сразу увеличивает трафик репликации по каналу. Чем больше доменов в лесу, тем выше трафик репликации ГК.

Преимущества и недостатки размещения контроллеров домена в сайте таковы.

Преимущества и недостатки размещения контроллеров в небольшом сайте

Преимущества	Недостатки
В случае недоступности канала связи пользователи могут регистрироваться в сети и осуществлять доступ к ресурсам	Канал занимается трафиком репликации. Если канал загружен в обычные часы, нужно планировать время репликации
Одни и те же серверы могут выполнять несколько функций: DNS, DHCP, WINS, ГК, файловый сервер и т. п.	Требуется размещать сервер ГК для некоторых приложений, что увеличивает трафик репликации
Можно разворачивать приложения, активно работающие с ГК	Требуется дополнительное оборудование (от 1 контроллера на домен)

От 50 пользователей

В крупных сайтах одного контроллера на домен может оказаться недостаточно. Допустим, сайт обслуживает 200 пользователей, и вы поставили только один контроллер домена.

Риск такого решения очевиден: в случае недоступности этого контроллера локально весь трафик регистрации в сети будет направлен по каналу. В пиковые моменты времени это может оказаться весьма критично, и регистрация растянется на продолжительное время.

Далее. Не очень мощный компьютер в пиковые моменты просто не справится с потоком запросов на аутентификацию, что опять же серьезно затормозит аутентификацию.

Следующая проблема не столь очевидна. Связана она с тем, что единственный контроллер домена тянет на себе слишком много: занимаясь аутентификацией, он еще играет роль сервера-форпоста, через который направляется трафик репликации. При высокой скорости изменений в Active Directory велик будет и объем тиражируемой информации. Если же топология репликации такова, что наш сайт является сайтом верхнего уровня для нескольких мелких сайтов, то загружен он будет постоянно. Добавьте к этому возможность исполнения им таких функций, как сервер ГК, сервер DNS, WINS, DHCP, и вы поймете, что это далеко не лучшее решение. Мало того, что такой компьютер будет весьма дорогим, он при этом останется единичной точкой сбоев, не имеющей резервных вариантов.

Наличие нескольких контроллеров домена в крупном сайте предоставляет поле для маневров. Два из них можно назначить выделенными серверами форпостов: один — сервером WINS, DHCP и DNS, дру-

гой — сервером ГК. Как поступить, вы решайте в каждом конкретном случае, исходя из нагрузки в сайте.

Надежная связь между сайтами

Теперь обсудим создание межсайтовых связей и мостов, а также расположение серверов-форпостов (подробнее о них см. главу «Репликация Active Directory»).

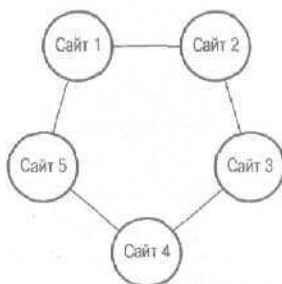
Поскольку топологию репликации можно создавать автоматически и вручную, мы уделим особое внимание ручному проектированию топологии, которое обеспечивает надежность такую же, если не выше, чем при автоматической генерации. А начнем мы с топологии сети.

Топология сетей

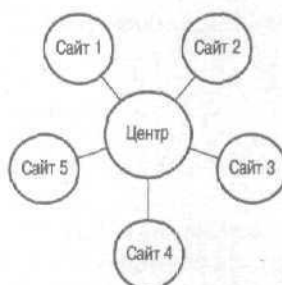
Топология межсайтовых связей зависит от топологии сети. В общем случае можно выделить три разновидности топологии сети:

- кольцо;
- звезда (иногда называют «колесом со спицами»);
- ◆ сложная.

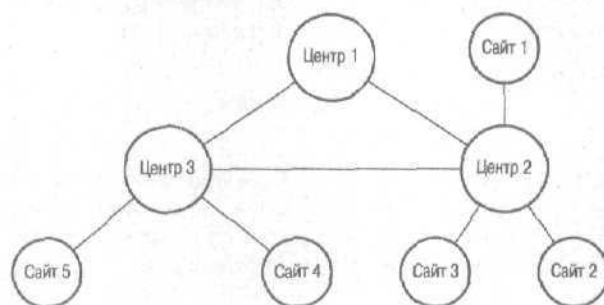
Кольцевая топология означает, что все сайты связаны между собой по очереди: первый со вторым, второй с третьим ... последний с первым. Достоинство «КОЛЬЦА» — равномерная загрузка всех сайтов, недостаток — длинный путь передачи информации между ними.



В «звезде» один центральный сайт связан со всеми остальными. При большом числе сайтов «звезда» очень напоминает ось колеса с отходящими от нее спицами. Ее достоинство — фиксированная скорость передачи информации между сайтами, недостаток — перегруженность центрального сайта. В дальнейшем центральный сайт будем называть центром, а подключенные к нему — филиалами.



Сложная (комбинированная) топология встречается чаще описанных выше и представляет собой их комбинацию, минимизирующую недостатки «КОЛЬЦА» и «ЗВЕЗДЫ».



Межсайтовые связи

Для выполнения репликации между сайтами служат специальные объекты Active Directory — межсайтовые связи. Каждый такой объект характеризуется:

- стоимостью;
- ◆ расписанием;
- ◆ интервалом;
- протоколом репликации.

Одна межсайтовая связь может использоваться между двумя и более сайтами. Поясню последнее. Например, на предыдущем рисунке между тремя центрами существуют каналы связи. Можно создать межсайтовую связь, соответствующую каждому из каналов, а можно — одну межсайтовую связь, которая будет обслуживать все три этих сайта. Если мы считаем, что все три центральных сайта расположены на магистральной сети, то нет смысла создавать несколько межсайтовых связей, так как у них будут идентичные характеристики.

Стоимость **межсайтовой** связи — это числовое значение, показывающее, насколько данная связь дороже альтернативной. Стоимость в основном **зависит** от пропускной способности канала. Следующая формула позволяет автоматически назначать стоимость и не допускать ошибок при проектировании:

$$\text{Стоимость} = \frac{1024}{\text{Log(Эффективная пропускная способность (Кб/с))}}$$

Вот значения стоимостей для типовых величин эффективной пропускной способности:

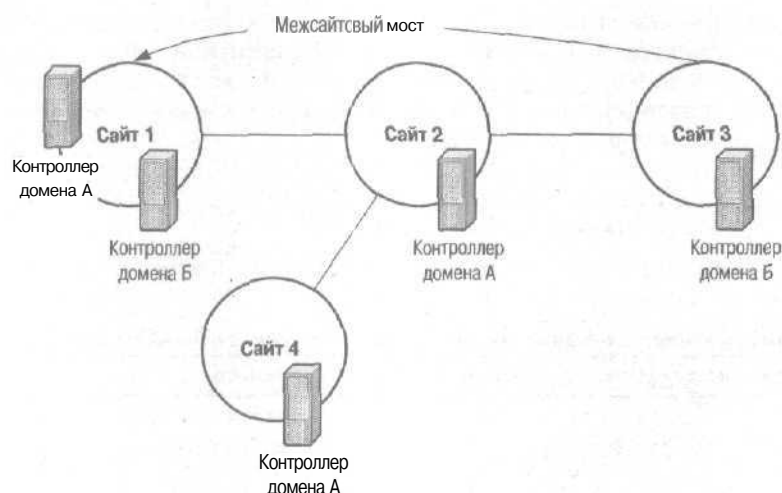
Зависимость стоимости от пропускной способности канала

Эффективная пропускная способность (Кб/с)	Стоимость
9,6	1 042
19,2	798
38,8	644
56	586
64	567
128	486
256	425
512	378
1024	340
2048	309
4096	283

Замечание Ни формула, ни таблица не являются догмой. Вы можете использовать произвольные значения.

Данная методика расчета стоимости межсайтовой связи не учитывает надежности канала. Проектируя **межсайтовые** связи, можно намеренно завысить стоимость для ненадежного канала.

Межсайтовые связи по умолчанию считаются транзитивными. Это значит, что если межсайтовые связи установлены между сайтами А и В и сайтами В и С, то существует межсайтовая связь между А и С. Транзитивность работает только в полностью маршрутизируемых сетях. Если же отдельные сегменты сети не являются полностью маршрутизируемыми, в них нужно создавать межсайтовые мосты — специальные объекты Active Directory. Необходимость в **межсайтовом** мосте возникает, когда в сегменте находится контроллер того домена, контроллеров которого нет в сегментах, непосредственно связанных с рассматриваемым. Вот пример немаршрутизируемой сети:



Пример немаршрутизируемой сети и межсайтового моста

В этой сети Сайт 2 не маршрутизирует трафик IP. Для Сайта 3 нужно создать межсайтовый мост к сайту 1, так как только в нем находится контроллер того же домена, что и в сайте 3- А вот для сайта 4 такой мост не нужен, так как контроллер его домена находится в пределах прямой досягаемости.

Теперь поговорим о расписании репликации. Расписание позволяет открывать «окна* для выполнения межсайтовой репликации. По умолчанию такое окно открыто 24 часа в сутки 7 дней в неделю. Если каналы позволяют, его можно оставить таким. Если же канал загружен в рабочее время, то на этот период окно можно закрывать. Если при этом есть незагруженный альтернативный канал, но с более высокой стоимостью межсайтовой связи, то у него можно открыть окно на то же самое время,

Замечание Если репликация началась незадолго до закрытия окна, то она завершится тиражированием всех изменений, которые должны быть переданы в сайт или из него. Окно при этом не сможет быть закрыто.

Очень тесно с расписанием связано понятие интервала репликации, т. е. времени, по истечении которого контроллеры доменов в разных сайтах обмениваются данными. По умолчанию он длится 1\$ минут, что вполне приемлемо и сравнимо с максимальным временем репликации внутри сайта.

Теперь представьте, что сайт связан с большим числом филиалов, а объем тиражируемых данных велик. В этом случае репликация, начатая в рамках одного интервала, может не закончиться до наступления следующего. Тем самым создаются предпосылки для роста очереди репликации. Поэтому интервал надо задавать таким, чтобы репликация успевала завершиться до наступления следующего интервала или до закрытия окна. Последнее связано с тем, что закрытие окна может означать загрузку канала другим трафиком, который значительно замедлит тиражирование данных.

О планировании расписания и интервалов в больших системах я расскажу далее в этой главе.

Последний параметр межсайтовой связи — протокол репликации, Протоколы мы обсудим в главе «Репликация Active Directory» — здесь лишь отмечу, что протокол SMTP используется в основном на ненадежных линиях и для него нельзя определить расписание тиражирования.

Объекты связи

Для каждой межсайтовой связи создаются объекты связи — они отвечают за передачу сведений о репликации от одного контроллера домена к другому. Объект связи характеризуется:

- направлением;
- ◆ именем;
- расписанием.

Определить пространства имен, которые будут тиражироваться тем или иным объектом связи, нельзя. Направление тиражирования встречное: для данного контроллера домена указывается, с какого контроллера созданный объект связи будет тиражировать данные.

Если в сети менее 100 сайтов, настоятельно рекомендую использовать ISTG для создания объектов связи. При большем числе сайтов лучше применять сценарии создания объектов связи. Но и в этом случае сценарий должен позволять запустить ISTG на ограниченный период времени только для того, чтобы создать объекты межсайтовой связи. Создание межсайтовых объектов связи мы обсудим в разделе «Отказоустойчивые схемы».

Объекты связи могут иметь три вида имен. У созданных ISTG имя будет безликим — <automatically generated>. Если вы измените свойства этого объекта, то его имя также изменится и станет, с точки зрения администратора, менее осмысленным. Оно превратится в GUID. Наконец, если объект связи создан вами, вам его и называть.

Серверы-форпосты

Серверы форпосты — это контроллеры домена в сайте, через которые осуществляется связь с другими сайтами. Серверы форпостов

бывают выделенными и назначаемыми автоматически. Обычно целесообразно переложить процесс выбора сервера-форпоста на плечи КСС. и вот почему. Допустим, для связи сайта А с сайтом В КСС назначил контроллер домена А в сайте А. В процессе работы контроллер стал недоступен, т. е. связь через него более невозможна. Тогда КСС выбирает иной контроллер домена в качестве сервера-форпоста и создает для него объекты связи. Таким образом, обеспечивается автоматическая отказоустойчивость системы.

Отсюда *первый вывод*: по возможности используйте автоматическое назначение серверов-форпостов.

Предположим, что такое поведение КСС вас не устраивает, так как контроллеры в домене различаются по мощности, а значит, в качестве форпоста может быть назначена слабая машина. Тогда можно назначить мощный контроллер домена сервером-форпостом принудительно. Такой сервер называется выделенным форпостом. А если он выйдет из строя? КСС знает, что вы вмешались в его деятельность и назначили выделенный сервер-форпост. Обнаружив, что он вышел из строя, КСС посмотрит, нет ли другого выделенного форпоста. Есть — КСС задействует его для репликации с удаленными сайтами, нет — КСС остановит попытки связи с другими сайтами до тех пор, пока единственный форпост не станет доступен.

Отсюда *второй вывод*: если назначается выделенный сервер-форпост и КСС работает в сайте, создайте хотя бы еще один выделенный форпост.

Если необходимо реплицировать несколько доменных контекстов, то количество серверов-форпостов должно быть равно количеству контекстов. Причем каждый из форпостов должен быть контроллером соответствующего домена.

Преимущества и недостатки разных видов форпостов таковы:

Преимущества и недостатки форпостов разных типов

Тип форпоста	Преимущества	Недостатки
Автоматический	<ol style="list-style-type: none"> 1. Отказоустойчивость обеспечивается КСС 2. Не нужно проектировать расположение форпостов 	<ol style="list-style-type: none"> 1. Может возникать перегрузка серверов-форпостов 2. Серверы назначаются без учета типа и качества их связи с сетью
Выделенный	<ol style="list-style-type: none"> 1. Можно назначить сервер, подходящий для роли форпоста наилучшим образом 2. Можно распределить нагрузку между несколькими серверами 	<ol style="list-style-type: none"> 1. Нужно проектировать расположение форпостов 2. Отказоустойчивость обеспечивается комплексом дополнительных мер

Теперь посмотрим, сколько форпостов требуется в сайте. Пусть сайт является центральным, и к нему подключено несколько филиалов. Форпост обслуживает тиражирование:

- из центра в филиалы;
- ◆ из филиалов в центры;
- SYSVOL — из центра в филиалы (предполагаем, что в филиалах не происходит изменений в сценариях или расширениях групповой политики),

При тиражировании из центра в филиалы каждый сайт филиала обращается к центральному сайту, как только открывается окно репликации. Обращение выполняется от контроллера домена в филиале к форпосту в центре. Обработка таких обращений на форпосте идет параллельно и ограничена только объемом тиражируемых данных и вычислительной мощностью форпоста в центре. Максимальное число партнеров по репликации для одного сервера-форпоста при тиражировании в филиалы рассчитывается по формуле:

$$\frac{H \cdot O}{K \cdot T} = \text{Число партнеров по репликации на один цикл}$$

где;

H — суммарное время в часах, когда может выполняться репликация в течение дня;

O — число одновременных подключений репликации за час (реалистичное значение равно 30);

K — число циклов репликации в день;

T — время выполнения репликации.

Замечание Указанное число одновременных подключений реалистично для сервера с 4 процессорами Xeop-500 и хорошей дисковой подсистемой. Примеры конфигурации см. в главе «Установка Active Directory».

Допустим, репликация возможна в течение 14 часов в день (H), число одновременных подключений максимально — 30 (O), репликация выполняется в 2 цикла (K), а время выполнения одной репликации — 1 час (T). Получим, что для рассматриваемого сервера форпоста допустимо иметь 210 партнеров по исходящей репликации.

Замечание Один контроллер домена может иметь не более 800 партнеров по репликации. Даже если расчетное значение выше, нельзя подключить более 800 партнеров в силу ограничений Active Directory. Думаю, этого ограничения вам не превысить.

Тиражирование из филиалов в центр не может выполняться параллельно. Сервер-форпост по очереди выполняет репликацию с каждым из своих партнеров. Как я уже говорил, если окно репликации закроется раньше, чем сервер закончит репликацию со всеми партнерами, репликация все равно будет продолжаться до конца списка партнеров и тем самым захватит следующее окно или вклинится в иной трафик. Поэтому число партнеров по тиражированию из филиалов рассчитывается по другой формуле:

$$\frac{R}{N} = \text{Число партнеров по репликации на один цикл}$$

где:

R — продолжительность работы окна репликации в минутах;

N — длительность тиражирования изменений с одного контроллера домена в минутах.

Оба параметра зависят от нескольких факторов. Пусть в нашем примере окно репликации открыто 60 минут, а для выполнения тиражирования изменений из каждого филиала нужно 2 минуты. Тогда один форпост не может иметь более 30 партнеров по репликации. Учтите также, что его партнерами по репликации являются контроллеры домена внутри сайта, поэтому количество сайтов, обслуживаемых одним форпостом, должно быть меньше на эту величину. Если предположить, что следующее за рассмотренным окно репликации откроется для другой группы сайтов, то число возможных партнеров по репликации удвоится. В нашем примере репликация доступна 14 часов в сутки в два интервала. Значит, в течение каждого интервала можно использовать 7 одночасовых окон. Если каждое из окон обслуживает разные группы филиалов, то наш сервер-форпост способен иметь до 210 партнеров по репликации. Предполагая, что внутри сайта у этого сервера есть два партнера, получим максимальное число внешних партнеров — 196.

Чтобы подсчитать число серверов-форпостов, надо разделить общее число филиалов на меньшее из двух рассчитанных выше значений числа партнеров для каждого форпоста.

$$\frac{B}{\text{Число партнеров по репликации на один цикл}} = \text{Мин. количество форпостов}$$

Если в нашем примере к центру подключено 390 филиалов, то минимальное число форпостов — 2.

Если расчеты покажут, что число партнеров по входящей репликации в разы отличается от числа партнеров для исходящей, подумайте, как изменить расписание репликации, чтобы выровнять эти значения.

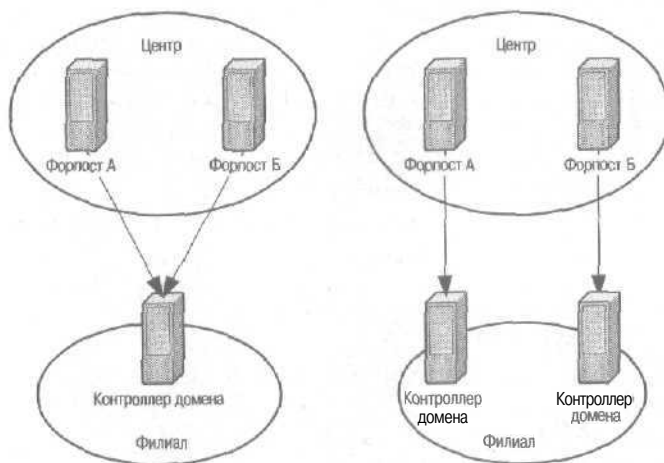
Близкие значения партнеров по репликации позволяют сократить число серверов-форпостов.

Совет Минимальное значение, вычисленное по этой формуле, нельзя назвать рекомендуемым. В случае задержек репликации или выхода из строя одного из форпостов вы рискуете не завершить репликацию. Поэтому надо использовать большее число форпостов.

Отказоустойчивые схемы

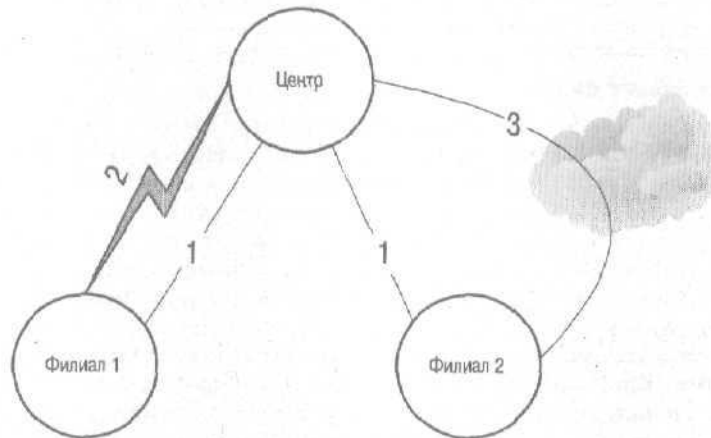
В больших и очень больших системах возникает необходимость в отключении генератора топологии межсайтовой репликации (ISTG). При этом вы берете на себя ответственность за надежную работу системы. Один из способов — создать два объекта связи для каждого из филиалов. Каждый из объектов связывает контроллер домена в филиале с разными форпостами в центре. Для большей отказоустойчивости в филиале должно быть также два форпоста. Если какой-нибудь сервер выйдет из строя, репликация будет выполнена с «оставшегося в живых».

Внимание Если используются два разных сервера в филиале, а в качестве протокола репликации — SMTP, возникает вероятность двойного тиражирования одних и тех же изменений. Во избежание этого сделайте так, чтобы репликация с контроллерами в филиале проходила в разное время, скажем, с первым по четным часам, со вторым — по нечетным.



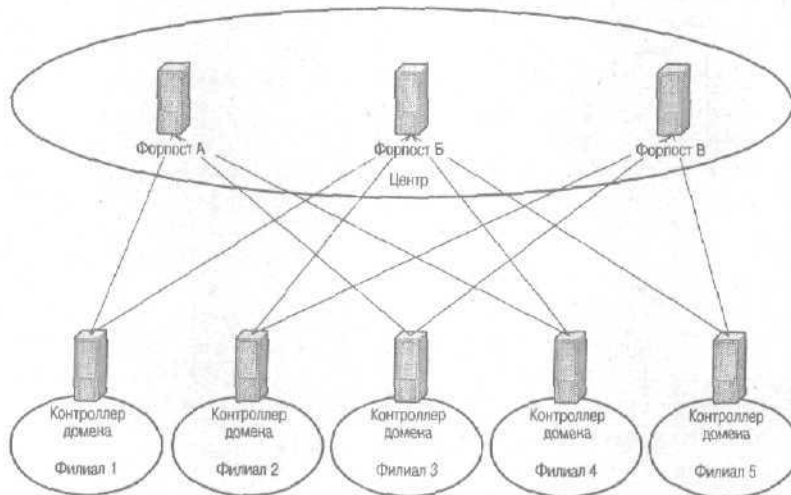
Варианты отказоустойчивого подключения филиалов

Если канал связи с филиалом ненадежен, желательно иметь резервный канал. Для него создается межсайтовая связь более высокой стоимости. При недоступности **основного** канала репликация будет перенаправлена в **запасной**. В качестве запасного канала может выступать коммутируемая линия или виртуальный канал через Интернет.



Создание резервных каналов:

1 — основной канал, 2 — коммутируемый канал,
3 — виртуальный туннель



Пример отказоустойчивого и сбалансированного подключения филиалов

Отказоустойчивость полезно интегрировать с балансировкой нагрузки. Допустим, центральный сайт связан с большим количеством филиалов. Помимо создания объекта связи для каждого из филиалов с двумя разными форпостами в центре, имеет смысл сделать «рваное» расписание репликации. Пусть контроллер домена в первом филиале связан с первым и вторым форпостами в центре, контроллер во втором филиале — со вторым и третьим форпостами, контроллер в третьем филиале — с третьим и первым и т. д. Расписание репликации составляется так, чтобы репликация с четными форпостами в центре выполнялась по четным часам, а с нечетными — по нечетным. Это позволит разгрузить форпосты и создать временной запас на тот случай, если репликация не завершится в отведенное время.

Мастера операций и Глобальный каталог.

Оптимальное размещение

Для мелких предприятий, расположенных в одном сайте, практически не важно, где именно находятся мастера операций — они и так в «прямой видимости» остальных контроллеров домена. Для крупных же, распределенных организаций доступность мастеров операций может оказаться критичной.

Мастер схемы

Как вы знаете, это единственный во всем лесу мастер операций, ответственный за внесение изменений в схему. Изменять схему может администратор с правами группы Schema Admins. Так как эта группа располагается только в корневом домене леса, то целесообразно и мастер схемы держать там же. Если используется пустой корневой домен, именно он — идеальное место для мастера схемы.

Компьютер, на котором находится мастер схемы, не несет особой нагрузки, поскольку схема модифицируется крайне редко. Так, устанавливая Microsoft Exchange 2000, можно запустить мастер подготовки, который добавит в схему нужные классы объектов и атрибуты. Его можно запустить как на самом мастере схемы, так и на любом ином контроллере. В последнем случае надо разрешить выполнять модификацию схемы на этом контроллере. Изменения в схеме будут реплицированы на остальные контроллеры, и ваша задача — сделать так, чтобы эта репликация не забила собой каналы связи. Если у вас медленные каналы и вы планируете развернуть Exchange 2000 или иное приложение, модифицирующее схему, то подготовьте Active Directory до того, как в филиалах будут развернуты контроллеры домена.

Мастер схемы по умолчанию размещается на самом первом контроллере домена в лесу. В силу его небольшой загруженности он может там и оставаться.

Мастер доменных имен

Он один на весь лес и отвечает за добавление в лес новых доменов, кроме существующих доменов из леса, и за добавление/удаление объектов перекрестных ссылок на внешние каталоги. Эти операции может выполнять только администратор с правами **Enterprise Admins**. Так как эта группа находится только в корневом домене леса, то целесообразно и мастер доменных имен держать там же. Если используется пустой корневой домен, то именно он — идеальное место для мастера доменных имен.

Мастер доменных имен отвечает за уникальность имен доменов в лесу. Когда добавляется новый домен, мастер обращается к серверу ГК в поисках такого имени. Именно поэтому он должен располагаться на одном сервере с сервером ГК. Но почему он не может обратиться к серверу ГК на другом компьютере? Теоретически может, но... Представьте, что в момент добавления нового домена сервер ГК недоступен. При этом появляется вероятность добавления домена с уже существующим в лесу именем, что неминуемо приведет к конфликтам. Поэтому ГК и должен быть на том же самом компьютере.

Компьютер, на котором располагается мастер доменных имен, не несет практически никакой нагрузки, так как домены в лес добавляются нечасто. Это позволяет разместить его на одном компьютере с мастером схемы. По умолчанию это первый контроллер доменов в лесу. Мастер доменных имен должен быть доступен из любой точки сети.

Имитатор PDC

Имитатор PDC прежде всего нужен для клиентов старого типа (ранее Windows 2000), так как с их точки зрения он играет роль главного контроллера домена. Кроме того, он является основным обозревателем домена (master browser) для приложений, ориентированных на NetBIOS. Если они используют функцию **NetGetDCName**, то она обслуживается только имитатором PDC. Если домен работает в смешанном режиме и в нем есть контроллеры домена Windows NT, то имитатор PDC для них — главный контроллер, с которого они получают реплики базы SAM,

Но даже если не используются старые клиенты и нет контроллеров домена Windows NT, роль имитатора PDC все равно важна. Он отвечает за срочное тиражирование изменений в Active Directory, таких как смена паролей или блокировка учетных записей. Он также отвечает за аутентификацию пользователей, сменивших пароль (см. главу «Репликация Active Directory»).

Планируя расположение имитатора PDC, учтите:

- ◆ для каждого домена должен быть свой имитатор PDC;
- ◆ имитатор PDC должен быть всегда доступен для других контроллеров в домене;
- ◆ в больших доменах имитатор PDC несет повышенную нагрузку, и его целесообразно размещать на отдельном сервере.

Мастер RID

О RID можно прочитать практически везде, например, в [1], [3], [6], так что описывать его не буду. Мастер относительных идентификаторов (RID):

- хранит общий пул идентификаторов домена и выдает их контроллерам по мере необходимости; при этом обеспечивается уникальность RID в домене;
- ◆ переносит объекты из одного домена в другой; дело в том, что при переносе учетной записи между доменами у нее меняется DN и SID, а вот уникальный ID остается неизменен; мастер RID следит, чтобы в домене не появилось двух объектов с одним уникальным ID.

Компьютер с мастером RID относительно не загружен и поэтому может располагаться на тех же контроллерах, где находятся другие мастера доменных операций.

Мастер инфраструктуры

Чтобы понять, как правильно расположить мастер инфраструктуры, надо знать, как он работает.

Когда объект на одном контроллере домена ссылается на отсутствующий в локальной базе объект, этот объект представляется в виде записи, содержащей GUID объекта, его SID (если это участник безопасности) и его отличительное имя DN. При перемещении этого объекта меняются его DN и SID (если он перемещается в домен), но не GUID. Мастер инфраструктуры периодически проверяет такие ссылки в доступной ему реплике базы Active Directory. Для этого он обращается к ГК и проверяет, не изменились ли у объекта с данным GUID его DN и SID. Если да, то соответствующие изменения вносятся в локальную реплику и тиражируются на остальные контроллеры в домене.

Если мастер инфраструктуры находится на том же компьютере, что и ГК, то он не функционирует (о чем и сообщает в журнале регистрации событий). Дело в том, что компьютер, выполняющий роль ГК, хранит реплики всех объектов в лесу, т. е. на нем присутствуют (пусть и в урезанном виде) все объекты Active Directory, а следовательно, нет ссылок на отсутствующие объекты. Если все контроллеры в домене

являются ГК, то надобности в мастере инфраструктуры нет, и он может не работать.

Таким образом, размещая мастер инфраструктуры помните, что он:

- ◆ должен быть один в каждом домене;
- ◆ не должен располагаться на сервере ГК;
- + является слабо загруженным и может располагаться на одном сервере с другими мастерами в домене.

Глобальные каталоги

Рекомендации по расположению серверов ГК несколько различны для одно- и многодоменной структур.

Когда в лесу только один домен, то надобности в ГК вообще-то нет. Все контроллеры домена имеют информацию обо всех объектах в лесу. Может, и отказаться от него? Не стоит. Во-первых, для работы ряда программ требуется обращение именно к серверу ГК. Во-вторых, всегда есть вероятность расширения Active Directory и добавления новых доменов или деревьев. А тут уж без ГК уже не обойтись.

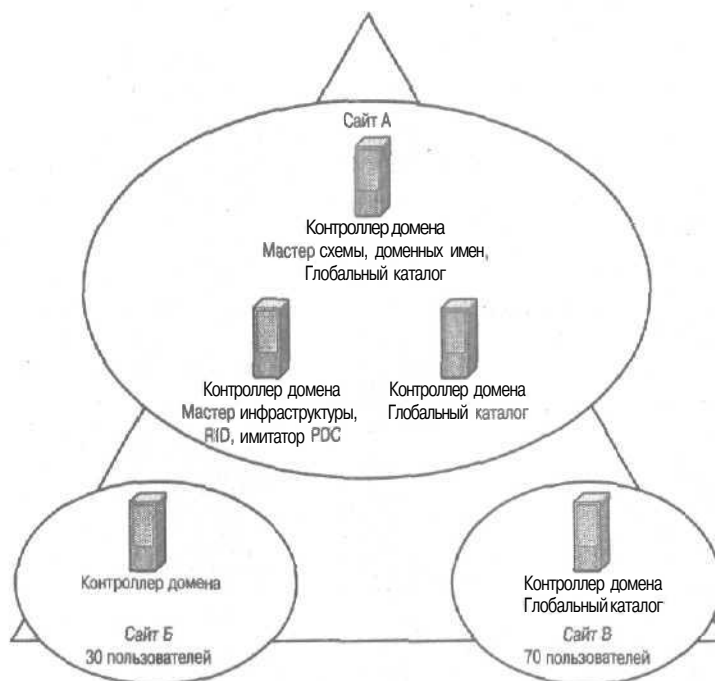
Поэтому рассмотрим две ситуации: весь домен в одном сайте и домен «размыт» по сайтам. В первом случае достаточно иметь один ГК. С целью его резервирования можно создать второй. Для распределенного домена ГК надо размещать в удаленных сайтах. Необходимость ГК в сайте возникает при числе пользователей от 50 человек.

Совет Серверы ГК можно поместить на всех контроллерах домена, кроме мастера инфраструктуры.

В случае нескольких доменов в лесу рекомендации по размещению ГК во многом совпадают с описанными выше. Однако теперь придется подумать о трафике репликации. Чем больше доменов в лесу и объектов в доменах, тем выше трафик репликации ГК. Если удаленные сайты связаны медленными каналами, то трафик может стать критичным. С другой стороны, наличие ГК в филиале просто необходимо, так как иначе возрастет трафик регистрации через канал. Оптимальным считается создание двух ГК в центре и по одному в сайтах с числом пользователей от 50 человек. Если структура связи сайтов сложная, то в крупных сайтах, можно иметь по 2 ГК.

Примеры размещения

Итак, вы познакомились с общими рекомендациями по размещению мастеров операций и ГК — рассмотрим пару примеров оптимального размещения.



Пример распределения ролей в одном домене

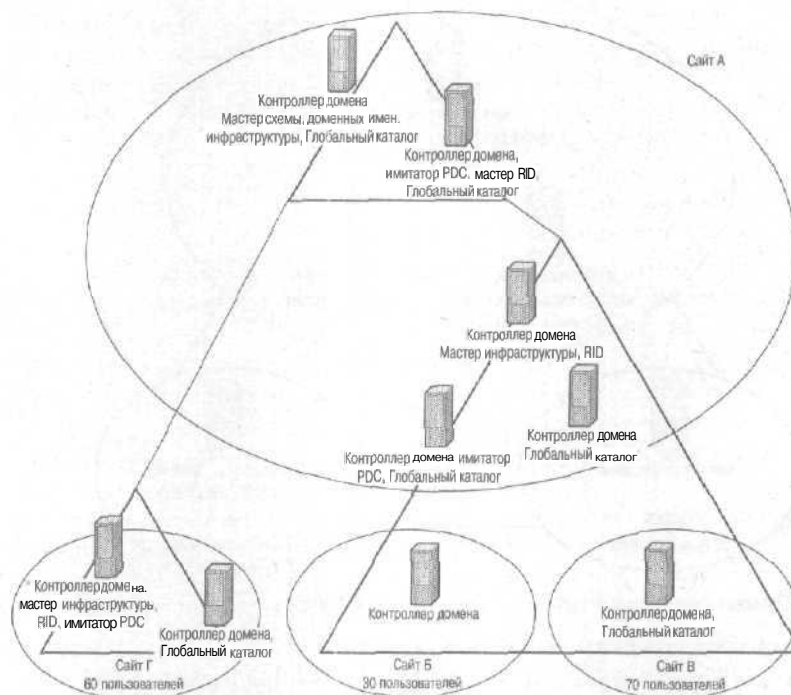
Вариант для одного домена в лесу:

- ◆ все контроллеры домена в сайте А, кроме одного, являются серверами ГК;
- ◆ мастера, имеющие отношение ко всему лесу, отделены от мастеров, относящихся к домену;
 - сайт Б не очень крупный, поэтому в нем нет ГК;
- ◆ сайт В крупный, и в нем присутствует ГК.

Вариант для нескольких доменов в лесу:

- ◆ все контроллеры корневого домена в сайте А являются серверами ГК;
- мастера, имеющие отношение ко всему лесу, расположены в корневом домене;
- ◆ мастера, имеющие отношение к доменам, располагаются в каждом из доменов;
- ◆ сайт Б не очень крупный, поэтому в нем нет ГК;

- ◆ сайт В крупный, и в нем присутствует ГК;
- ◆ сайт Г содержит домен, поэтому в нем присутствуют как ГК, так и все доменные мастера операций.



Пример размещения мастеров в лесу доменов

Конфигурация контроллеров доменов для удаленных филиалов

Эта тема может показаться довольно странной в главе по планированию Active Directory, но только показаться. Обычно чем меньше или удаленнее сайт (УГ центра, тем меньше в нем квалифицированных специалистов, способных настроить DNS, установить контроллер домена и подключиться к общему дереву Active Directory. Но даже если специалисты готовы приехать из центра, чтобы выполнить эту работу, медленные каналы связи заметно замедляют разворачивание Active Directory, особенно в крупных системах с большим количеством пользователей и доменов. Поэтому в таких случаях целесообразно создавать подготовительные сайты, обеспечивающие имитацию условий в удаленных сайтах.

Подготовительный сайт надо расположить в центре, вблизи от корневого домена и квалифицированных специалистов. Рассмотрим предъявляемые к нему требования.

1. Если филиалы подключены по медленным каналам связи, то и подготовительный сайт тоже должен быть подключен по каналу с такой же пропускной способностью. Однако канал для подготовительного сайта должен быть постоянным и всегда доступным для репликации.
2. В подготовительном сайте должен постоянно присутствовать контроллер домена, служащий источником репликации для создаваемых контроллеров. Он должен быть сервером ГК.
3. Подготовительный сайт должен обеспечивать надежный доступ к корневому домену и к серверу DNS в нем, а также мастерам RID, доменных имен и инфраструктуры.
4. Подсеть в этом сайте должна обеспечивать легкость конфигурирования, с тем чтобы адреса и маска совпадали с теми, что будут в создаваемом сайте.
5. KCC в подготовительном сайте должен быть отключен. Все соединения надо создавать вручную. Дело в том, что при автоматической генерации объектов связи будут созданы объекты в основном сайте, о которых вы не будете и подозревать. Это приведет к тому, что после переноса контроллеров на их постоянное место репликация пойдет с прежними партнерами по медленным каналам.
6. Должно быть достаточно мест для компьютеров, чтобы сконфигурированные компьютеры длительное время были подключены к сети для поддержания на них актуальной информации и предупреждения рассинхронизации паролей.

Политика изменения схемы

Это важный компонент планирования Active Directory. Схема — скелет, который удерживает в нужном положении остальные органы: объекты, права доступа к ним, атрибуты и взаимоотношения между объектами. Повредите скелет, и стройный организм зачахнет, а то и умрет. Но хватит аллегорий — посмотрим, что в схеме есть такого, что требует планирования ее модификации.

Схема представляет собой набор классов объектов и атрибутов, из которых создаются экземпляры объектов Active Directory. По умолчанию она содержит более 140 классов и 850 атрибутов. Такого количества с лихвой хватает для выполнения всех операций с Active Directory. И все же довольно часто схему приходится модифицировать. Например, вы не представляете работу без некоторого атрибута у пользователей

либо устанавливаете приложение, **которое модифицирует схему** и заносит в нее классы **своих объектов**.

Поскольку репликация схемы работает с одним мастером, а репликация Active Directory — с несколькими, могут возникать конфликтные **ситуации**, когда вы пытаетесь создать объект с новым атрибутом на том контроллере домена, до которого еще не дошли соответствующие изменения в схеме. И хотя обычно **такая** ситуация разрешается без вашего участия, сетевые проблемы могут серьезно помешать нормальному течению процесса.

Безобидная, казалось, модификация схемы порой вызывает **важные** последствия. Допустим, вы хотите, чтобы некий атрибут реплицировался на серверы ГК. Вы указываете это в оснастке диспетчера схемы и... Все серверы ГК устанавливают свой USN в 0. Результат — полная репликация абсолютно всех объектов в ГК и перегрузка в сети.

Замечание При установке Microsoft Exchange 2000 в ГК добавляются **атрибуты**. Следовательно, выполнять это надо **так**, чтобы репликация не шла по медленным каналам.

Еще большие проблемы возникают, когда вы понимаете, что все ваши модификации схемы больше не нужны. Active Directory не позволяет удалять что-либо из схемы. Вы можете только **деактивизировать** классы объектов или атрибутов. Деактивизация какого-либо класса не приводит к удалению экземпляров объектов, использующих **деактивизированный** класс. Они по-прежнему будут присутствовать в Active Directory. Правда, нельзя будет создавать новые экземпляры **этих** объектов. Для удаления «**нехороших**» объектов нужно организовать их поиск по всему каталогу.

Сказанное демонстрирует необходимость понимания того, когда и как именно схему надо модифицировать.

Когда и как модифицируют **схему**

Ниже перечислены случаи, в которых нужно выполнять модификацию схемы, а также способы того, как это лучше сделать.

Способы модификации схемы

Ситуация	Решение
Ни один из существующих классов не отвечает вашим требованиям	Создайте новый класс.
Существующий класс в целом подходит, но у него нет нужных атрибутов	Создайте: ◆ новые атрибуты и добавьте их к существующему классу ;

Ситуация	Решение
Вам нужен набор новых уникальных атрибутов, но не нужен новый класс	или: ◆ новый класс па базе существующего и добавьте новые атрибуты к созданному классу. ИЛИ: ◆ вспомогательный класс, который содержит только недостающие атрибуты, и добавьте вспомогательный класс к существующему
Созданные классы или атрибуты больше не нужны	Создайте вспомогательный класс, который содержит только необходимые атрибуты Деактивизируйте класс или атрибут. При необходимости найдите и удалите все объекты этого класса или содержащие деактивизированные атрибуты
Вы собираетесь установить приложение, которое модифицирует схему	Установку рекомендуется выполнять в 2 этапа и только после тщательного тестирования в отдельном лесу: ◆ пользователь с правами Schema Admins готовит схему и добавляет нужные классы и атрибуты; ◆ после репликации всех изменений по сети любой пользователь с правом установки приложений устанавливает приложения

Замечание Не все классы и атрибуты могут быть изменены. Подробнее см. [3], [6].

Применение политики модификации схемы

Один из ключевых моментов в **политике** модификации схемы — создание специальной комиссии. В нее надо включить **специалистов, знающих**, к чему могут привести изменения в схеме и можно ли их избежать. На этой комиссии будет лежать ответственность за последствия модификации схемы.

Вот правила политики модификации схемы.

- ◆ Инициализация процесса модификации схемы:
 - передача списка предлагаемых изменений на рассмотрение специальной комиссии;
 - проверка необходимости в изменениях;
 - определение потенциального воздействия на существующие объекты, сетевой трафик;
 - разработка процесса модификации;
 - получение действительного идентификатора объекта;
 - получение разрешения от комиссии.

- Тестирование модифицированной схемы;
 - тестирование предлагаемого решения в тестовой зоне в отдельном лесу;
 - определение соответствия выполненных изменений требуемым спецификациям;
 - разработка эффективного плана восстановления оригинальной схемы;
 - получение разрешения на выполнение изменения в рабочей сети.
- Выполнение модификации:
 - ограничение членства в группе Schema Admins;
 - разрешение выполнения записи на мастере схемы;
 - проверка того, что все контроллеры доменов получили новую версию схемы;
 - перевод мастера схемы в режим только для чтения.

Данная политика должна быть разработана и применена в обязательном порядке. При модификации схемы:

- ◆ семь раз убедитесь в том, что без изменения не обойтись;
- прежде чем выполнить изменения, тщательно все спланируйте и протестируйте;
- постарайтесь начать с самого простого решения;
- ◆ используйте понятные названия для классов и атрибутов; помните, что вас уже может и не быть в организации, а другим придется расхлебывать то, что вы натворили;
- тщательно документируйте все сделанные изменения;
- следите за тем, кто входит в группу Schema Admins, и за разрешением записи на мастере схемы.

Active Directory) межсетевые экраны и Интернет

Все, о чем мы рассуждали выше, относится к внутренним частям корпоративной сети. Внутри корпорации обычно не ставят препоны в виде межсетевых экранов. Доверие между отдельными частями сети если не полное, то достаточное, чтобы обойтись границами безопасности, предоставляемых доменами. Однако доступ в сеть некоторых отделов защищают межсетевым экраном. Во многих распределенных системах отдаленные филиалы подключаются либо по каналам, предоставляемым третьей стороной, либо вообще через Интернет. Для защиты от несанкционированного проникновения из этих незащищенных каналов зачастую также применяют межсетевые экраны и шифрование трафика. Внедряя Active Directory, вы стараетесь вклю-

чить в нее все объекты корпорации независимо от того, где они находятся: за сетевым экраном или нет. Следовательно, надо знать, как это сделать с минимальным риском для безопасности.

Довольно часто также требуется обеспечить доступ авторизованных пользователей к внутренним ресурсам в сети из Интернета. Как авторизовать пользователя, где разместить контроллеры домена — вот вопросы, которые при этом возникают.

Ниже показан общий подход к решению этих проблем. Вот наиболее типичные случаи:

- **подключение домена к дереву через VPN:** характерно для филиалов, связанных с основной частью сети предприятия через частные сети или через Интернет;
- ◆ **подключение домена к дереву с использованием IPSec:** чаще всего такой вариант рассматривают для связи с внутренними подразделениями, находящимися за межсетевым экраном;
- ◆ **авторизация ресурсов в демилитаризованной зоне (DMZ):** вариант применяется при авторизованном доступе к Web-серверу, почтовому серверу и пр.

Подключение доменов через VPN

Связь филиалов с центром или между собой через Интернет дает значительную экономию по сравнению с арендой выделенных каналов. Этому способствует и то, что выход в Интернет все равно нужен, хотя бы для обмена почтой. Надо лишь заключить договор с провайдером Интернета, получить от него пул адресов и настроить DNS.

Я забыл сказать про межсетевой экран. Естественно, он позволит исключить нежелательный доступ из столь агрессивной среды, как Интернет. Межсетевой экран настраивается так, чтобы пропускать только нужный трафик. Например, если для пользователей внутренней сети предоставляется доступ к ресурсам Web, необходимо открыть трафик HTTP и HTTPS.

Как вы понимаете, контроллеры домена обмениваются между собой по совершенно иным протоколам. Нужно открывать трафик DNS, RPC (с огромным числом портов), LDAP, SMB, при необходимости — NetBIOS и др.). Взгляните на список служб и протоколов, используемых при взаимодействии контроллеров домена.

Перечень протоколов и портов, используемых службами Windows 2000

Служба	Порт/протокол
RPC	135/tcp, 135/udp
NetBIOS (служба имен)	137/tcp, 137/udp

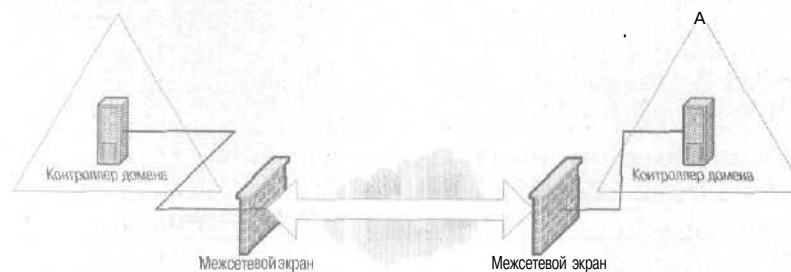
Служба	Порт/протокол
NetBIOS (датаграммы)	138/udp
NetBIOS (сеансы)	139/tcp
RPC динамические порты	1024-65535/tcp
SMB поверх <i>\P</i>	445/tcp, 445/udp
Lightweight Directory Access Protocol (LDAP)	389/tcp
LDAP через SSL	636/tcp
ГК LDAP	3268/tcp
ГК LDAP через SSL	3269/tcp
Kerberos	88/tcp, 88/udp
Domain Name Service (DNS)	53/tcp, 53/udp
Windows Internet Naming Service (WINS)	1512/tcp, 1512/udp
Репликация WINS (если надо)	42/tcp, 42/udp

Разрешив этот трафик через межсетевой экран, вы оголите сеть. Фактически это то же, что убрать экран вообще.

Еще одна проблема — адресация. В корпоративной сети обычно используют адреса, не маршрутизируемые в Интернете. А значит, требуется механизм трансляции адресов вроде NAT. Но при этом для двусторонней связи нужно обеспечить однозначное назначение компьютеру во внутренней сети еще и адреса из интернетовского пула, что опять же практически *выставляет* этот компьютер наружу. Если он к тому же контроллер домена, то все «потроха» Active Directory будут напоказ.

Именно поэтому применяется туннелирование. Главное при этом — обеспечить правильную настройку межсетевых экранов, DNS и контроллеров домена. Схематично такое подключение изображено на рисунке. Начнем с первого межсетевого экрана. Пусть оба межсетевых экрана выполнены на Microsoft ISA Server. Если у вас иные средства защиты, вы сможете адаптировать параметры. Эти же компьютеры будут выполнять роль серверов удаленного доступа.

Итак, в качестве протокола используем PPTP.



Связь двух доменов через VPN

Замечание Если у вас развернута инфраструктура PKI, можно использовать L2TP/IPSec.

- Разрешаем двустороннюю передачу и указываем, что соединение может инициировать как этот сервер, так и удаленный.
- ◆ В качестве источника второго конца туннеля указываем адрес удаленного межсетевого экрана.
- ◆ Указываем адреса компьютеров, которым разрешено использовать туннель.
- ◆ Сохраняем конфигурационную информацию в файле.

В результате будут созданы и сконфигурированы как VPN-интерфейс, так и 4 пакетных фильтра доступа.

Конфигурировать второй ISA-сервер проще, так как для этого программе конфигурации достаточно предложить использовать конфигурационный файл первого межсетевого экрана.

Далее, находясь в удаленном офисе, надо убедиться, что доменные имена в центральном офисе разрешаются без проблем. Особое внимание — к параметрам DNS (см. главу «Установка Active Directory»). Помните: 90% успеха зависит от правильной конфигурации DNS на сервере, который станет контроллером домена.

Убедитесь также, что и из центрального офиса разрешаются имена в филиале.

Если все прошло гладко, можно создать и подключить домен.

Теперь несколько советов по расположению мастеров операций и сетевых служб. Как вы помните, межсетевые экраны конфигурируют так, что не все клиенты могут использовать туннель. Это условие необязательное, но довольно распространенное. В силу этого обычные клиенты в филиале могут и не иметь доступа в туннель. Раз так, то в филиале должен быть контроллер домена, а лучше — два независимо от числа пользователей. Этот контроллер должен выполнять функции всех мастеров операций и быть сервером ГК (если у вас два контроллера, функции мастера инфраструктуры и ГК должны быть на разных компьютерах). Кроме того, нужен локальный сервер DNS, обслуживающий домен Active Directory. Желательно, чтобы на нем была вторичная зона `_msdcs.<имя_леса>`. Это особенно актуально, если у филиала есть собственные филиалы с отдельными доменами.

Филиал нужно выделить в отдельный сайт независимо от качества канала, предоставленного вашим поставщиком услуг Интернета.

Подключение доменов с использованием IPSec

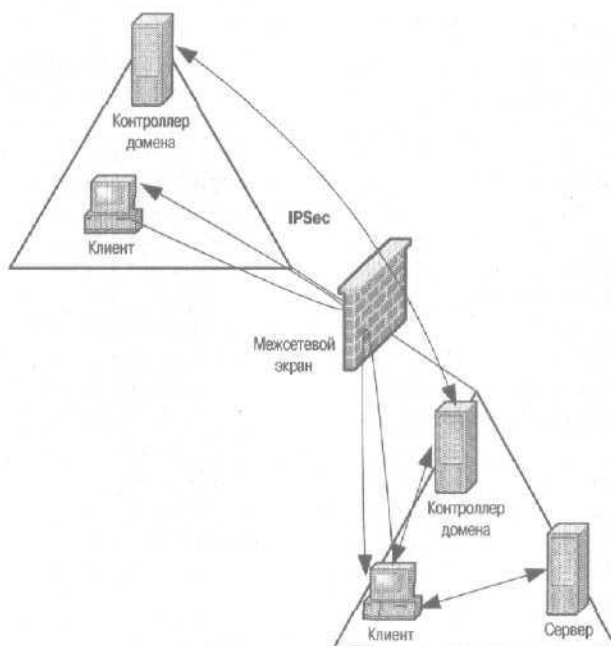
Внутри сайта могут существовать области, доступ к которым надо жестко ограничить для основной массы пользователей. Обычно их отделяют от остальной сети межсетевыми экранами. Начиная разворачивать Active Directory, вы можете столкнуться с необходимостью разместить контроллеры домена или новые домены в этих защищенных областях. Список портов, которые надо открыть для обеспечения взаимодействия контроллеров, см. в предыдущем разделе. Ни один здравомыслящий сотрудник службы безопасности не разрешит их открыть. Особенно впечатляют порты, динамически используемые службой удаленного вызова процедур (RPC). Способы ограничения числа этих динамических портов есть, но это вряд ли выход из положения. Можно, конечно, организовать туннель, но вряд ли это оптимальное решение. Лучше всего использовать протокол IPSec. Не стану вдаваться в подробности насчет его работы. Думаю, вы это и сами знаете, а если нет, то прочитайте в [4]. Основной эффект от IPSec в том, что число портов, которые надо открыть на межсетевом экране, резко сокращается. Вот они.

Перечень портов, используемых IPSec

Служба	Протокол/Порт
DNS	53/tcp, 53/udp
Kerberos	88/tcp, 88/udp
IKE, Internet Key Exchange	500/udp
IPSec ESP. encapsulated security payload	IP protocol 50
IPSec AH. authenticated header	IP protocol 51

Заметьте: все эти порты следует открыть, только если политика IPSec сконфигурирована для контроллеров домена, а серверы DNS располагаются раздельно. Если же все серверы DNS расположены на контроллерах, порт 53 можно закрыть.

Еще дальше можно пойти, если внедрить инфраструктуру PKI. Тогда для установления связи IPSec можно использовать сертификаты, а не Kerberos. Такой подход позволит закрыть порт 88.



Связь двух доменов через межсетевой экран с использованием IPSec

К какому результату приведет такое решение?

1. Любой пользователь из внешней сети, для которого не определена соответствующая политика IPSec, не получит доступа в защищенную зону.
2. Репликация между контроллерами домена в защищенной зоне и вне ее будет выполняться только между теми контроллерами домена, для которых сконфигурирована политика IPSec. Пример политики для этого случая см. в главе "Групповая политика".
3. Любой пользователь в защищенной сети может быть аутентифицирован в домене, но при этом может не иметь доступа за пределы своей закрытой зоны.

Не стану описывать точную конфигурацию контроллеров домена и параметров межсетевого экрана, так как это выходит за рамки данной главы. Если вам это интересно, обратитесь к Microsoft Technet, книга *Top IT Tasks, Active Directory replication over firewalls*.

Совет Будьте внимательны при создании политик IPSec. Нужно четко представлять, какие категории пользователей и какие компьютеры могут взаимодействовать, а какие — нет.

Авторизация ресурсов в DMZ

Одна из распространенных задач — предоставление авторизованным пользователям предприятия доступа к ресурсам из Интернета. Подчеркну: речь идет именно об авторизованных пользователях, т. е. тех, кто со своего рабочего места имеет доступ к почте, серверам Web и другим приложениям. Задача в том, чтобы предоставить им доступ к тем же ресурсам извне и сделать это так, чтобы не нарушить безопасность сети и не усложнить процедуру доступа. Если с первым требованием все понятно, второе требует пояснения. Обычно доступ из Интернета к внутренним ресурсам нужен мобильным пользователям на выезде. Реалии нашей жизни таковы, что ими, как правило, являются большие шишки, для которых ввод пароля при регистрации — уже стресс. Если же их заставить вводить пароль дважды, трижды, да еще и разные, то уровень их удовлетворенности резко понизится.

Типовое решение — разместить такие ресурсы в демилитаризованной зоне (DMZ), отделенной и от Интернета, и от внутренней сети межсетевыми экранами. При правильной настройке экранов проблему безопасности решить довольно легко. Трафик организуется так, что к ресурсам в DMZ можно пройти либо из внутренней сети, либо из Интернета, но пройти DMZ насквозь нельзя.

Авторизация же подразумевает, что пользователь, прежде чем получить доступ к ресурсу, должен обратиться к центру авторизации, получить у него сеансовый билет, а потом, предъявив его серверу, на котором лежат нужные ресурсы, получить к ним доступ. Так как сквозной проход через DMZ закрыт, то, на первый взгляд, центр авторизации может находиться только внутри DMZ. Исходя из этого, возможны три варианта его размещения:

- каждый сервер сам авторизует доступ к своим ресурсам;
- в DMZ помещается домен, не входящий в дерево Active Directory внутренней сети; между этим доменом и внутренним деревом устанавливаются односторонние нетранзитивные отношения;
- в DMZ помещается контроллер домена и ГК основного дерева, который и выполняет авторизацию доступа.

Преимущества и недостатки каждого из этих способов таковы.

Преимущества и недостатки различных способов авторизации в DMZ

Тип авторизации	Преимущества	Недостатки
На каждом сервере	Нет компрометации базы пользователей внутренней сети	Сложность администрирования: каждый сервер содержит свой комплект учетных записей и групп

си. след. стр.

Тип авторизации	Преимущества	Недостатки
Отдельный домен	Нет компрометации базы пользователей внутренней сети Доступ из внутренней сети возможен в силу односторонних доверительных отношений	Неудобный доступ из внутренней сети: надо регистрироваться на каждом сервере. Неудобный доступ из внешней сети: надо регистрироваться на каждом сервере
Контроллер внутреннего домена вынесен в DMZ	Простота администрирования Простота доступа из внутренней сети Простота доступа из внешней сети	Двойное администрирование. Надо содержать базу внешних пользователей без синхронизации паролей Неудобство доступа из внешней сети: надо регистрироваться в этом домене Учетные записи Active Directory подвергаются высокой опасности быть скомпрометированными

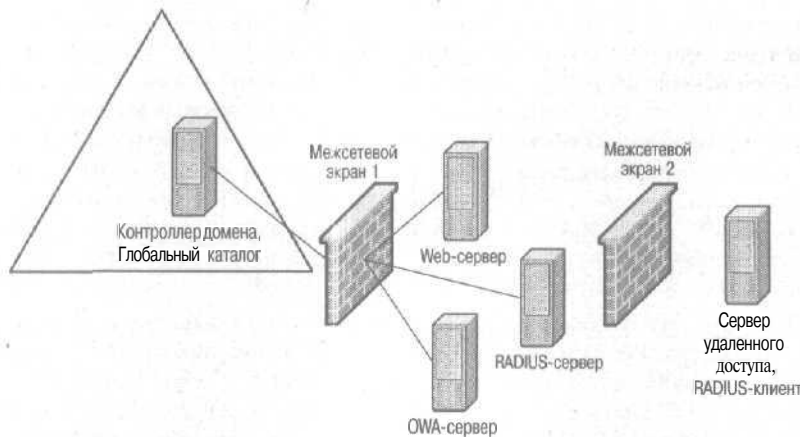
Как видите, все три варианта потенциально опасны или неудобны. Больше всего преимуществ у последнего, однако его недостаток способен перекрыть все преимущества. Сеть DMZ потенциально уязвима. Никто не даст 100% гарантии того, что хакер не проникнет в DMZ. А раз так, нельзя считать эту сеть надежной и размещать в ней критически важные серверы. Контроллер домена с ГК относится к самым критическим элементам Active Directory, так как на нем хранится информация обо всех пользователях сети. Выходит, данный вариант отпадает по соображениям безопасности. Первые два просто неудобны. Я знаю компании, использующие их, но они были бы рады от них избавиться.

Выходит, сделать так, чтобы и волки были сыты, и овцы целы, нельзя? Отнюдь нет. Решение есть: это сервер аутентификации RADIUS. (В Windows 2000 это Internet Authentication Server — IAS.) О его работе см. [2]. В DMZ размещается RADIUS-сервер, который по IPsec связан через межсетевой экран с контроллером домена во внутренней сети. Так как на этом сервере нет компонентов Active Directory, то компрометация учетных записей исключена.

Каждый клиент, приходящий в DMZ из Интернета, может использовать два способа доступа: прямо на сервер или через виртуальный туннель. К категории удаленных пользователей можно также отнести и тех, кто дозванивается на пул модемов компании. Если используется туннель, сервер доступа выполняет роль клиента RADIUS. В остальных случаях сами клиентские компьютеры являются клиентами RADIUS. Как бы там ни было, клиент RADIUS находится вне DMZ, до внешнего межсетевого экрана.

Клиент RADIUS обращается к серверу RADIUS в DMZ с запросом об авторизации от имени пользователя, установившего соединение. Сервер RADIUS обращается через внутренний межсетевой экран к контроллеру домена во внутренней сети. Получив от него положительный или отрицательный ответ, он его транслирует клиенту запрашившему доступ. Если доступ разрешен, устанавливается соединение, и пользователь получает доступ ко внутренним ресурсам, расположенным на серверах — членах домена. Если доступ не разрешен, соединение не устанавливается. Особенно удобна данная схема для управления внешним межсетевым экраном.

Наиболее предпочтителен вариант с туннельным доступом, так как обеспечивает наивысшую степень безопасности, защищая трафик, проходящий от клиента к серверу удаленного доступа через Интернет. Туннель может работать как по протоколу PPTP, так и по L2TP/IPSec. Добавьте сюда аутентификацию пользователя по смарт-карте (по протоколу EAP) и получите сытых волков (руководство довольно, что пароли не надо вводить вообще) и целых овец (объекты Active Directory надежно защищены).



Авторизация ресурсов в DMZ

Пример планирования

В заключение рассмотрим пример проекта Active Directory. Я поборол в себе искушение привести пример реальной российской организации. Причин тут несколько. Во-первых, хочется показать планирование комплексной структуры со сложными взаимосвязями. Я, увы, не слышал о таких российских организациях. Во-вторых, есть риск, что в иной организации, увидев нечто похожее на свою структуру,

могут взять да и перенести рекомендации, приводимые в примере, на свой проект. А это чревато... Ну, не будем о грустном.

Поэтому я и выдумал организацию, которая меньше всего похожа на те, что существуют на наших бескрайних просторах. В то же время при всей фантазмагоричности вымышленной компании отдельные части ее могут послужить примером для других организаций. Короче, имеющий уши да слышит.

Постановка задачи

Компания ГлобРосТур (ГРТ) недавно вышла на российский рынок с предложением услуг в области туризма. Руководство ГРТ считает Россию перспективной с точки зрения туризма, в частности горнолыжного. Специалисты компании уверены, что их предложения будут привлекательны не только для россиян, но и для жителей Европы.

Штаб-квартира ГРТ в Москве. В окрестностях столицы приобретены земельные участки, на которых сооружаются круглогодичные базы отдыха: зимой предлагаются искусственные горные склоны с подъемниками и трассы для катания на снегоходах, летом — верховая езда, бассейны, пэйнтбол и пр. Каждая база будет иметь свою гостиницу.

Сооружение подобных баз проектируется близ Санкт-Петербурга, в Карелии, на Среднем Урале и на Алтае. Ведутся переговоры с компанией ДальТур о слиянии, в результате которого появятся аналогичные базы отдыха на Дальнем Востоке и на Камчатке.

Для привлечения иностранных туристов планируется создать подобные базы в Польше, Чехии, Германии, Болгарии и Хорватии через 3 года. Потенциал системы по оценке специалистов ГРТ — 400-500 тысяч отдыхающих в год.

Отличительной особенностью отдыха на базах ГРТ должна стать полная интеллектуальность сервиса. Так, любой клиент, заказав отдых на какой-либо из баз, получит карточку постоянного клиента ГРТ. Карточка является бесконтактной смарт-картой, в которой записана информация о клиенте, его семье (если он пожелает отдыхать с семьей), его фотография и иные персональные данные. В дальнейшем он сможет заказывать туры через Web по своей карточке.

По прибытии на базу отдыха карточка становится его обязательным спутником: это и ключ от номера гостиницы, и плата за ресторан, за услуги проката, подъемник и пр. Карточка также предоставляет доступ к голосовой почте, доступ к Интернету и пр. Карточка действует на любой базе отдыха и служит для накопления скидки.

Каждая база отдыха является независимым юридическим лицом, Учет персонала осуществляется разными приложениями, интегрированными

ми с Active Directory. Информация об основных фондах базы отдыха также хранится в Active Directory. Часть персонала каждой базы должна иметь доступ в локальную сеть для выполнения таких обязанностей, как выдача и учет инвентаря, заказ оборудования и пр.

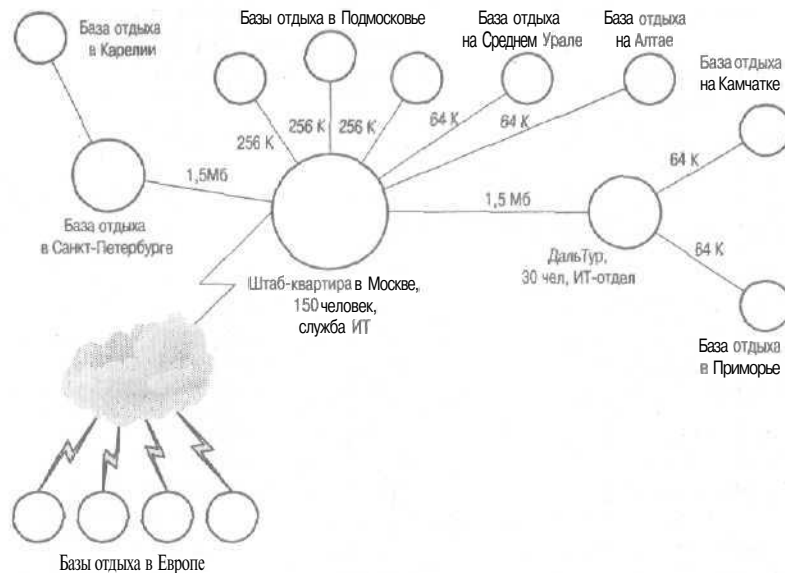
В штаб-квартире ДальТур развернута сеть на основе Active Directory, включающая в себя и две имеющиеся базы отдыха.

В штаб-квартире ГРТ находится ИТ-центр, который занимается поддержкой локальной сети, но будет отвечать и за работу общей сети. Здесь же будет расположен центр авторизации клиентов. Каждая база отдыха имеет 1-2 сотрудников, ответственных за поддержание работоспособности локальной сети, установку новых версий приложений и развитие системы. В штаб-квартире ДальТур также имеется ИТ-отдел, полностью ответственный за работу сети.

Штаб квартира имеет каналы связи со всеми базами отдыха в Московской области. Пропускная способность каналов — 256 кб/с. 50% трафика по этим каналам используется для передачи телефонных сигналов. Канал между базой в Санкт-Петербурге и штаб-квартирой имеет полосу пропускания 1,5 Мбит/с. База отдыха в Карелии связана только с базой в Санкт-Петербурге. Планируется, что базы на Среднем Урале и Алтае будут иметь спутниковые каналы 64 кб с Москвой. Дальневосточные базы связаны пока со штаб-квартирой ДальТур во Владивостоке. Все каналы спутниковые 64 кб/с. Планируется, что между Московской штаб-квартирой и штаб-квартирой ДальТур будет канал 1,5 Мб/с. Связь с европейскими базами отдыха будет осуществляться по виртуальным выделенным каналам через Интернет. Штаб-квартира имеет канал в Интернет с полосой 1,5 Мбит/с, но его пропускную способность планируется увеличить до 10 Мбит/с.

Численность персонала в московской штаб-квартире — 150, в штаб-квартире ДальТур — 30 человек. На каждой базе отдыха число сотрудников варьируется, но число пользователей невелико — 15–20.

В качестве ОС выбрана Windows 2000, в качестве службы каталогов — Active Directory. Нужно спланировать архитектуру Active Directory. Описанная топология сети такова:



Планируемая топология общей сети компании ГРТ

Предложенная архитектура

Беглый анализ задачи позволяет выделить две разные категории пользователей: клиенты баз отдыха и обслуживающий персонал. В то время как клиенты должны авторизоваться на любой базе, персонал не выходит за пределы своей базы. Более того, нет нужды в том, чтобы персонал авторизовался где-либо еще. Фраза о том, что на каждой из баз используются свои приложения учета персонала, интегрированные с Active Directory, означает, что схемы Active Directory различны для разных баз отдыха.

Леса

Можно сделать вывод о том, что данной организации требуется несколько лесов доменов:

- один лес — для клиентов;
- остальные — для каждой из баз отдыха и штаб-квартиры.

Небольшое исключение придется сделать для дальневосточной штаб-квартиры, так как там уже развернут лес Active Directory, объединяющий и штаб-квартиру, и базы отдыха.

Между корнями лесов сотрудников баз отдыха установлены двусторонние нетранзитивные отношения. Это сделано, во-первых, затем.

чтобы администраторы штаб-квартиры могли помочь ИТ-персоналу на базах отдыха, а во-вторых, чтобы сотрудники имели доступ к ресурсам штаб-квартиры для заказа инвентаря и оборудования, а также для пересылки отчетности.

Между корнями леса клиентов и леса штаб-квартиры установлены односторонние нетранзитивные доверительные отношения так, что домен клиентов доверяет домену штаб-квартиры. Это сделано для того, чтобы ИТ-сотрудники могли управлять лесом клиентов,

Домены

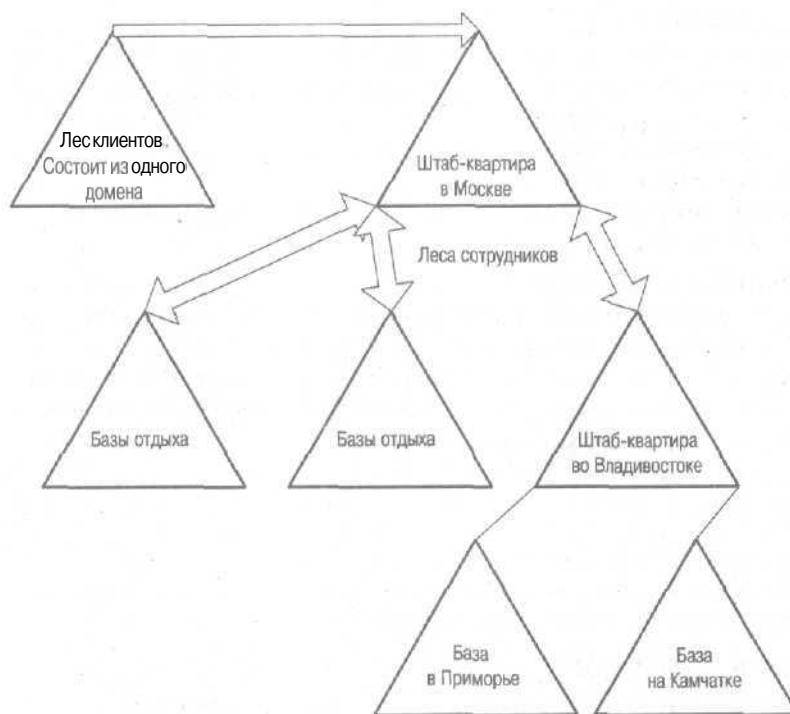
Итак, очевидно, каждая из баз отдыха представляет собой один домен в лесу. В силу сделанного ранее исключения для дальневосточных баз предположим, что доменная структура для них содержит 3 домена: корневой — для штаб-квартиры ДальТур и дочерние — для баз отдыха.

Ответ на вопрос о количестве доменов в лесу клиентов не так очевиден. С одной стороны, все клиенты равны, и к ним применяются общие требования безопасности. С другой — разделение на домены для каждой из баз позволит сократить трафик внутридоменной репликации. Критично в данном случае количество баз отдыха. Оно не маленькое и со временем будет только расти. А значит, будут расти объем ГК и трафик его репликации. Кроме того, клиент, зарегистрировавшийся на одной базе, не должен испытывать неудобств по приезду на другую (а в случае разных доменов он обязательно испытает неудобства из-за длительного времени аутентификации). Все говорит за то, что лес клиентов также состоит из одного домена. В итоге получаем такую топологию, как показано на рисунке.

Сайты

Говорить о сайтах имеет смысл только применительно к лесу клиентов и к лесу ДальТур. Все остальные леса располагаются в отдельных сайтах.

Лес клиентов разбит на столько сайтов, сколько существует баз отдыха. Это следует из анализа пропускной способности каналов. То, что скорость доступа штаб-квартиры в Интернет составит 10 Мбит/с, значения не имеет, так как полагаем связь по виртуальному каналу через Интернет ненадежной, а значит, требующей создания удаленных сайтов. Дополнительный сайт сделан в московской штаб-квартире. Именно здесь находится тот Web-сервер, через который клиенты могут бронировать места в гостиницах и планировать заезды на базы. В сайте ДальТур нет надобности, так как клиенты не имеют доступа в офис ДальТур.



Топология лесов и доменов

Контроллеры **доменов**

В каждом сайте клиентского леса размещается по два контроллера домена, каждый из которых является сервером ГК. Контроллеры домена в московском сайте также исполняют роли мастеров схемы, доменных имен, инфраструктуры, RID, имитатора PDC. Эти же контроллеры являются выделенными серверами-форпостами, и на них созданы межсайтовые связи. Для надежности для каждого сайта создано по две связи. Расписание репликации по ним сконфигурировано так, что по четным часам выполняется репликация с первым контроллером домена в удаленном сайте, а по нечетным — со вторым.

Лес **ДальТур** разбит на три сайта. Это определяется пропускной способностью каналов. В центральном сайте расположены два контроллера домена. В сайтах баз отдыха — по одному контроллеру. Ни один из серверов не является выделенным сервером-форпостом.

Во всех остальных лесах сотрудников баз отдыха стоит по два контроллера домена, выполняющих все роли и являющихся ГК.

Организационные подразделения

Домен клиентов содержит следующие ОП.

- ◆ **ОП для каждой из баз отдыха** После регистрации на любой из баз отдыха учетная запись клиента перемещается в соответствующее ОП, чтобы предоставить доступ к услугам, специфическим для конкретной базы отдыха.
- **ОП администраторов** Здесь находятся учетные записи сотрудников службы ИТ.
- ◆ **ОП штаб-квартиры** Здесь размещаются приложения и серверы, используемые для обслуживания клиентов. К ним относится, например, сервер Web.

Домены сотрудников баз отдыха могут не содержать ОП, так как по условиям задачи мы ничего не знаем о специальных требованиях.

В штаб-квартире в Москве должны быть ОП:

- службы ИТ;
- финансового отдела;
- службы безопасности,

О последних двух в условиях задачи ничего не сказано, но они скорее всего есть, и к ним применяются иные политики.

Группы безопасности

В домене клиентов должны быть такие группы безопасности:

- администраторов домена;
- ◆ администраторов схемы;
- администраторов каждого из ОП; этим группам делегируются права управления соответствующими ОП;
- администраторов сервера Web

В доменах баз отдыха должны быть:

- группа администраторов домена;
- группа администраторов схемы;
- ◆ глобальная группа доступа к отчетам на просмотр;
- ◆ глобальная группа доступа к отчетам на запись;
- ◆ глобальная группа доступа к инвентарной информации на просмотр;
- глобальная группа доступа к инвентарной информации на запись;
- ◆ локальная группа доступа к отчетам на просмотр;
- ◆ локальная группа доступа к отчетам на запись;
- локальная группа доступа к инвентарной информации на просмотр;

- локальная группа доступа к инвентарной информации на запись.

В домене московской штаб-квартиры должны быть:

- группа администраторов своего домена;
- группа администраторов своей схемы;
- глобальная группа администраторов домена клиентов;
- глобальная группа администраторов схемы леса клиентов;
- глобальная группа доступа к отчетам на просмотр;
- глобальная группа доступа к инвентарной информации на просмотр;
- ◆ локальная группа доступа к отчетам на просмотр;
- локальная группа доступа к инвентарной информации на просмотр.

Могут быть и иные группы для отделов в штаб-квартире.

Сервер Web и доступ к нему

У сервера Web две основные функции;

- ◆ являться лицом компании ГРТ в Интернете;
- служить средством бронирования туров для зарегистрированных пользователей.

В соответствии с этим на сервере должны существовать две зоны: открытая для всех желающих и открытая только для зарегистрированных пользователей. Поскольку доступ к Web будет организован по смарт-картам, предлагается использовать следующий алгоритм регистрации клиентов.

Узнав об услугах, предоставляемых ГРТ, и решив обратиться в компанию, потенциальный клиент заполняет форму на Web-странице и отправляет ее. Затем представитель ГРТ связывается с ним по телефону, обговаривает условия оплаты и доставки. Приехав на заказанную базу отдыха, клиент получает бесконтактную смарт-карту и инструкции по ее использованию. Также он получает USB-устройство для считывания смарт-карт и необходимое ПО на компакт-диске. В следующий раз для заказа тура клиент уже использует смарт-карту, что откроет ему доступ на сервере Web к страницам, предназначенным только для зарегистрированных пользователей. Здесь он сможет заказать новый тур уже без вызова агента по продажам.

Для реализации этой функциональности Web-сервер размещается в DMZ в московской штаб-квартире. Сервер является членом домена клиентов. Когда клиент оплатит первый тур, его учетная запись создается в домене клиентов в том ОП, которое соответствует заказанной базе отдыха. Одновременно с этим запрашивается сертификат пользователя.

Замечание Использование сертификатов нуждается в инфраструктуре открытых ключей, описание которой выходит за рамки данной книги.

Закрытый ключ пользователя записывается в смарт-карту с другой персональной информацией.

Если смарт-карта применяется на базе отдыха для регистрации в домене (скажем, для доступа к голосовой почте), то происходит обыкновенная авторизация пользователя по протоколу Kerberos.

Если пользователь обращается к серверу Web через Интернет по смарт-карте, то предоставленное ему ПО организует виртуальный канал и обеспечивает аутентификацию RADIUS. Это гарантирует защищенное подключение к домену клиентов и доступ к нужным ресурсам. Заказ тура в автоматическом режиме приводит к тому, что сценарий определяет наличие свободных мест, бронирование, выполняет проверку оплаты и переносит учетную запись пользователя в соответствующее ОП.

Вот мы и создали структуру Active Directory эффективного туристического агентства.

Заключение

Прочитав эту главу, вы, надеюсь, поняли, насколько серьезно надо подходить к планированию. Из опыта известно, что от начала проектирования до внедрения проходит минимум 5-6 месяцев в зависимости от объема организации. И все это время вы занимаетесь тем, о чем написано в этой главе!

Рассмотренные вопросы проектирования Active Directory охватывают такие области, как оценка нужного количества лесов, критерии разбиения на домены и ОП, общие рекомендации по применению групп безопасности, размещение мастеров операций и ГК, но очень слабо затрагивают планирование групповой политики. Чтобы составить полную картину, обратитесь к главе "Групповая политика". Если же вы не до конца разобрались в том, почему выбираются те или иные модели, советую почитать главы «Устанавливаем Active Directory» и «Репликация Active Directory».

Установка Active Directory

В любом учебнике или книге по Active Directory или Windows 2000 Server вы прочтете, что установить службу каталогов очень просто — достаточно выполнить команду `DCPROMO`. Уны, на практике установка проходит гладко далеко не всегда. И виноваты в этом не Microsoft и не Windows 2000 — мы сами. Корень всех проблем либо в недостаточном знании сетевых сервисов Windows 2000, либо в излишней самоуверенности. Поясню последнее. Допустим, вы большой специалист по сетям и работали преимущественно в UNIX-системах. Вы считаете, что ваше знание, скажем, DNS является исчерпывающим. Может, это и так, однако, приступая к установке Active Directory, вы не ознакомились со специфическими требованиями к DNS, а в результате — неудачная установка службы каталогов.

С чего же начинать установку? С планирования. Этой важной задаче посвящена предыдущая глава, а также написано немало книг, и я не стану повторяться. Если вы еще ничего не читали, то обратитесь к [8]. Допустим, вы спланировали структуру Active Directory (или для вас это сделал кто-то иной) и собираетесь приступить к тестированию. (Заметьте: я пишу «к тестированию», а не «к разворачиванию в боевых условиях».) Не торопитесь — прочтите советы, приведенные ниже. Лишними они не будут.

Что делать с DNS

Служба DNS — одна из основных служб Windows 2000, на которую опирается Active Directory. От правильности ее настройки зависит работа службы каталогов в целом. Обычно меньше всего проблем

возникает при использовании службы DNS, встроенной в Windows 2000. Однако это не значит, что нельзя использовать другие службы, например BIND. Откройте любую книгу по Active Directory и найдите требования к DNS — везде будет написано, что сервер DNS должен быть BIND версии не ниже 8.2.2, т. е. среди прочего он должен поддерживать:

- записи типа SRV;
- ◆ символ «_»;
- ◆ динамические обновления;
- ◆ расширенный набор символов (опционно).

Однако только первые два требования обязательны. Без динамических обновлений, строго говоря, можно обойтись, однако это прибавит вам массу хлопот.

Советы по настройке различаются в зависимости от того, какая конфигурация каталога и какие службы DNS уже имеются в сети. Вот четыре наиболее типичных случая:

- ◆ нет ни одного сервера DNS — это может быть новая сеть либо сеть на базе Windows NT или Novell Netware;
- ◆ сервер DNS уже существует — возможно, он служит для доступа пользователей в Интернет или для разрешения имен хостов UNIX;
- создается много доменов Active Directory — при этом существует масса способов организации DNS;
- ◆ создается лес доменов Active Directory — ситуация похожа на предыдущую, но имеет некоторые особенности.

Что ж, начнем по порядку — с самого простого случая.

Мой первый DNS

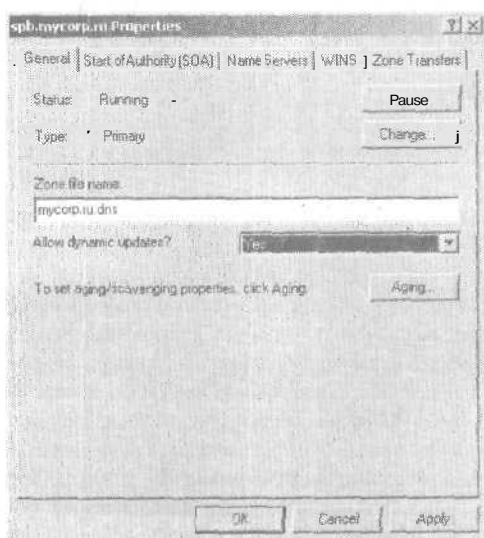
Итак, вы приступаете к созданию первого домена Windows 2000. Не имеет никакого значения, устанавливаете ли вы контроллер «с нуля» или выполняете обновление контроллера домена Windows NT, — сервер DNS необходим.

Если вы устанавливаете новый контроллер для первого домена, то последовательность действий такова.

- Установите ОС Windows 2000 Server или Advanced Server.
- Установите необходимые драйверы устройств и убедитесь, что система работает нормально.
- ◆ Проверьте параметры сетевого интерфейса. Адрес IP должен быть назначен статически. В качестве адреса сервера DNS укажите адрес этого же компьютера.

- Далее можно **либо** установить и сконфигурировать сервис DNS самостоятельно, либо приступить сразу к установке контроллера домена. Если раньше вы никогда не **конфигурировали DNS**, лучше всего доверить мастеру установки службы каталогов Active Directory сделать это за вас. По крайней мере так вы застрахуетесь от неудачи при первой установке, а также позволит ознакомиться с правильными записями и параметрами DNS.
- ◆ Если вы все же хотите сконфигурировать сервис **DNS** сами:
 - установите службу DNS через консоль управления;
 - откройте оснастку DNS;
 - создайте Forward lookup zone с тем **именем**, которое вы хотите дать своему домену Active Directory; эта зона должна быть первичной; созданием зоны занимается программа-мастер;
 - когда зона будет создана, откройте окно свойств зоны и убедитесь, что она **позволяет** выполнять динамические обновления.

Внимание Зона, созданная мастером, по умолчанию не разрешает выполнять динамические обновления. И это правильно, так как диктуется требованиями безопасности. И все же для работы с Active Directory зона должна быть динамически обновляемой, поэтому обеспечьте безопасную работу хотя бы до окончания установки контроллера домена.



Свойства зоны DNS. Обратите внимание на поле *Allow dynamic updates*

После этого вас и поджидают первые мелкие неприятности. Итак, запускаем DCPROMO. На вопросы мастера отвечаем, что это новый домен в новом дереве в новом лесу. Вводим имя домена (полностью совпадающее с именем ранее созданной зоны DNS) и... получаем сообщение о том, что программа не может определить, поддерживает ли сервер DNS динамические обновления. Такое сообщение выводится в 90% случаев. Программа не только предупреждает вас об этом, но и **предлагает** автоматически сконфигурировать сервер DNS. Если вы уверены, что сконфигурировали зону правильно, не поддавайтесь искушению согласиться с этим предложением. Кстати, программа все равно не сможет сконфигурировать **зону**, так как вы ее уже создали. Вот если бы вы с самого начала не морочили себе голову и не конфигурировали сервер DNS, то мастер установки Active Directory сконфигурировал бы зону без проблем.

Итак, отказываемся от услуг мастера по конфигурированию DNS и продолжаем установку Active Directory.

Если вы обновляете контроллер домена Windows NT, не забудьте в процессе установки сказать, что требуется установить сервер DNS. Больше у вас не будет возможности его сконфигурировать. Программа обновления сделает это сама.

Замечание Все, что рассказано выше, относится только к случаю отсутствия каких-либо серверов DNS в сети. Если же они нами используются, то процедура установки и конфигурирования иная.

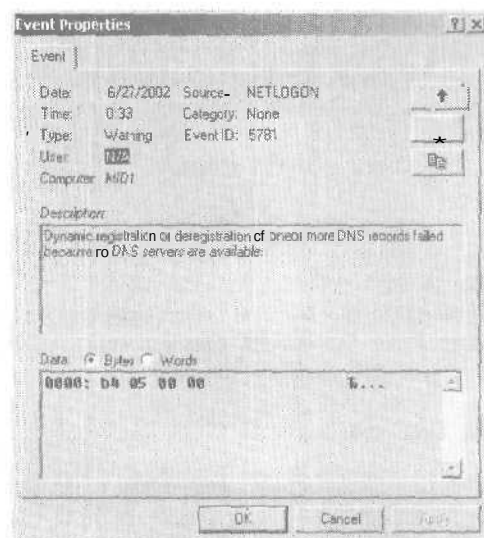
Так он работает?

По завершении работы мастера установки Active Directory и перезагрузки компьютера вы **сможете оценить**, все ли сделано правильно. На наличие каких-либо проблем вам укажет подозрительно долгая загрузка системы.

Понимаю, что не все **однозначно воспримут слова** «подозрительно долгая загрузка», поэтому выделю те моменты, на которые стоит обратить внимание. Во-первых, загрузка контроллера домена выполняется немного дольше загрузки сервера, что определяется большим числом служб, запускаемых при старте системы. Во-вторых, самая **первая** загрузка контроллера домена выполняется еще дольше, и степень задержки определяется исключительно быстродействием жесткого диска. В-третьих, после перехода процесса загрузки в графический режим выполняется применение **групповых правил** к компьютеру и запуск каталога, о чем дают знать сообщения «Starting Networking» и «Applying group policy». Компьютер, надолго задумавшийся на этапе запуска сетевых служб, — первый сигнал о том, что не все в порядке с парамет-

рами. В таком случае загрузка компьютера до появления приглашения аутентификации занимает десятки минут и сопровождается сообщением о том, что одна или несколько служб не были запущены. В наихудших случаях даже после ввода вашего имени и пароля проходит несколько десятков минут до появления привычного Windows Explorer. Я. может, и сгущаю краски, рассказывая о достаточно редких ситуациях, возникающих, как правило, из-за сбоев компьютера в процессе установки Active Directory, и все же надо знать, что такое случается, и не суетиться, нажимая кнопку Reset. В любом случае надо дождаться загрузки и аутентификации для выяснения причины сбоя.

Поскольку служба DNS — ключевая в работе Active Directory, то именно ее сбои в первую очередь приводят к подобным катастрофам. Для обнаружения сбоев откройте журнал регистрации событий. Одним из часто встречаемых и достаточно безобидным в рассматриваемой ситуации является событие 5781. Оно сообщает о том, что динамическое обновление записей в DNS не выполнено.



Вот так вы можете узнать, что не все записи о домене были записаны в DNS

Так как DNS у вас только один и стоит на том же компьютере, что контроллер домена, то причину надо искать здесь же. Если вы разрешили динамическое обновление зоны, то почти наверняка причина в том, что DNS запускается на 1-3 секунды позже службы Netlogon. Виноват в этом только ваш компьютер. Скорее всего быстрое действие

системы в целом не соответствует требованиям, предъявляемым к серверам. Чтобы исправить положение и внести нужные записи в DNS, перезапустите службу Netlogon:

```
Net stop netlogon
```

```
Net start netlogon
```

Можно и проигнорировать запись об этой ошибке, так как через 5 минут служба Netlogon вновь попытается обновить информацию в DNS. Следующие попытки обновления будут выполнены через 10, 40 и 60 минут, а затем регулярно с интервалом в 1 час.

А что если наблюдаются проблемы?

Откройте консоль DNS и убедитесь, что все необходимые записи занесены. Как, вы еще не знаете, какие записи там должны появиться? Ну, это совсем просто. Вы их все увидите, открыв файл %sysdir%\config\netlogon.dns. Они могут выглядеть, например, так:

```
fyodor.home. 600 IN A 10.1.1.111
_ldap._tcp.fyodor.home. 600 IN SRV 0 100 389 ETA.fyodor.home.
_ldap._tcp.5fc937ce-ba70-481d-aeb7-f30bce70ebaf.
domains._msdcs.fyodor.home. 600 IN SRV 0 100 389 ETA.fyodor.home.
1615c0e3-c2e8-4996-92b3-fba6d73d79c8._msdcs.fyodor.home. 600 IN CNAME
ETA.fyodor.home.
_kerberos._tcp.dc._msdcs.fyodor.home. 600 IN SRV 0 100 88
ETA.fyodor.home.
_ldap._tcp.dc._msdcs.fyodor.home. 600 IN SRV 0 100 389 ETA.fyodor.home.
_kerberos._tcp.fyodor.home. 600 IN SRV 0 100 88 ETA.fyodor.home.
_kerberos._udp.fyodor.home. 600 IN SRV 0 100 88 ETA.fyodor.home.
_kpasswd._tcp.fyodor.home. 600 IN SRV 0 100 464 ETA.fyodor.home.
_kpasswd._udp.fyodor.home. 600 IN SRV 0 100 464 ETA.fyodor.home.
_ldap._tcp.Site-2._sites.fyodor.home. 600 IN SRV 0 100 389
ETA.fyodor.home.
_ldap._tcp.Site-1._sites.fyodor.home. 600 IN SRV 0 100 389
ETA.fyodor.home.
_kerberos._tcp.Site-2._sites.dc._msdcs.fyodor.home. 600 IN SRV 0 100 88
ETA.fyodor.home.
_kerberos._tcp.Site-1._sites.dc._msdcs.fyodor.home. 600 IN SRV 0 100 88
ETA.fyodor.home.
_ldap._tcp.Site-2._sites.dc._msdcs.fyodor.home. 600 IN SRV 0 100 389
ETA.fyodor.home.
_ldap._tcp.Site-1._sites.dc._msdcs.fyodor.home. 600 IN SRV 0 100 389
ETA.fyodor.home.
_kerberos._tcp.Site-2._sites.fyodor.home. 600 IN SRV 0 100 88
ETA.fyodor.home.
_kerberos._tcp.Site-1._sites.fyodor.home. 600 IN SRV 0 100 88
ETA.fyodor.home.
```

```
_ldap._tcp.gc._msdcs.fyodor.home. 600 IN SRV 0 100 3268
    ETA.fyodor.home.
gc._msdcs.fyodor.home. 600 IN A 10.1.1.111
_gc._tcp.fyodor.home. 600 IN SRV 0 100 3268 ETA.fyodor.home.
_ldap._tcp.Site-1._sites.gc._msdcs.fyodor.home. 600 IN SRV 0 100 3268
    ETA.fyodor.home.
_gc._tcp.Site-1._sites.fyodor.home. 600 IN SRV 0 100 3268
    ETA.fyodor.home.
_ldap._tcp.Site-2._sites.gc._msdcs.fyodor.home. 600 IN SRV 0 100 3268
    ETA.fyodor.home.
_gc._tcp.Site-2._sites.fyodor.home. 600 IN SRV 0 100 3268
    ETA.fyodor.home.
_ldap._tcp.pdc._msdcs.fyodor.home. 600 IN SRV 0 100 389
    ETA.fyodor.home.
```

Не думаю, что этот листинг нуждается в комментариях. Хорошо видно, что речь идет о добавлении в домен `fyodor.home` контроллера домена `ETA`. Кстати, если вы сделали зону не обновляемой динамически по забывчивости или умышленно, то данный файл можно импортировать в DNS, что позволит создать нужные для работы записи.

Если же зона сконфигурирована как обновляемая динамически, то отсутствие указанных записей свидетельствует о проблемах с настройкой DNS. Чтобы их выявить, попробуйте выполнить команду `NSLOOKUP <полное.имя.домена>`. Ответ должен быть примерно таким:

```
Server: dc01.fyodor.home
Address: 10.1.1.3
Name: fyodor.home
Addresses: 10.1.1.3
```

Если вместо этого появится сообщение о том, что сервер не найден, проверьте параметры сетевого интерфейса.

Одним из средств анализа проблем регистрации в DNS записей, выполняемых службой `Netlogon`, является просмотр файла `%systemroot%\netlogon.log`. Предварительно нужно модифицировать в ветви реестра `HKLM\System\CurrentControlSet\Services\Netlogon\Parameters` значение параметра `DbFlag` и установить его в `2000FFFF`.

Еще одна из причин возникновения ошибки `5781` — различие между именем домена и суффиксом в имени компьютера. Эта ошибка наиболее вероятна при обновлении контроллера домена Windows NT 4 до Windows 2000. В этом случае флажок в диалоговом окне свойств компьютера «*Change primary DNS suffix when domain membership changes*» оказывается сброшенным, что и приводит к расхождению имени домена и суффикса. Чтобы решить эту проблему, запустите `DSPROMO`, верните контроллер домена в состояние сервера, а затем

снова сделайте его контроллером домена, предварительно отметив указанный флажок.

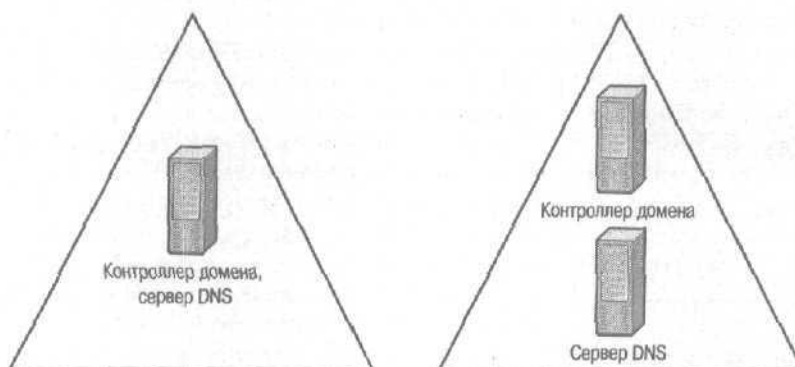
Замечание Если установка Windows 2000 производилась со «sleep-stream» дистрибутива, т. е. такого, к которому применен пакет обслуживания SPI и выше, подобного не случается.

Если в журнале регистрации все еще появляются сообщения об ошибках в работе службы DNS, обратитесь к статье «Windows 2000 DNS Event Messages 1 Through 1614*» в Microsoft [Technet](#).

Выводы

Подведем первые итоги.

Если вы доверили установку и конфигурирование службы DNS программе DCPROMO, то сервер будет сконфигурирован на контроллере домена, а на нем будут созданы две зоны: с именем, совпадающим с именем созданного домена, и корневая зона — «.». Обе будут интегрированы с Active Directory, что для вас автоматически решит проблему тиражирования информации между различными серверами DNS. Наличие корневой зоны подразумевает, что передача запросов на разрешение имен с данного сервера DNS на другие невозможна. Поэтому, если в дальнейшем вы захотите использовать внешний DNS для разрешения имен Интернета, то корневую зону на вашем сервере надо будет удалить. Другая особенность зон, интегрированных с Active Directory, в том, что они поддерживают только защищенные динамические обновления. Под этим подразумевают возможность установления списка контроля доступа к зонной информации так, что только те клиенты, которым такое обновление разрешено, смогут вносить изменения.



Два варианта расположения первого сервера DNS

Конфигурируя сервер DNS самостоятельно, вы можете разместить его как на контроллере домена, так и на отдельном сервере. В первом случае зоны можно будет интегрировать с Active Directory, во втором — нет. Однако второй вариант позволяет использовать не только сервер DNS Windows 2000, но и любой другой, удовлетворяющий определенным требованиям, речь о которых пойдет далее. Кроме того, при расположении сервера DNS на компьютере отличном от того, на котором находится контроллер домена, вы избавляетесь от ошибки, связанной с поздним стартом службы DNS.

DNS уже есть. Ну, и что с ним делать?

Рассмотренный выше случай скорее подходит для небольшой сети, построенной на базе Windows NT или ранних версий Novell Netware. Обычно DNS в той или иной степени используется для предоставления доступа к UNIX-хостам или разрешения имен Интернета. В такой ситуации к действующему серверу DNS надо подходить крайне осторожно. При этом есть несколько вариантов развития событий, зависящих как от версии существующего сервера DNS, так и от желания администратора что-либо изменять в нем.

Сервер DNS, поддерживающий свойства, необходимые Active Directory, можно использовать для создания домена, если его администратор согласен и если это не повредит безопасности. Но не будем спешить: сначала вспомним, какие свойства DNS должны поддерживаться.

Поговорим о версиях DNS

К серверу DNS предъявляется ряд обязательных (например, поддержка записей типа SRV) и факультативных (например, поддержка динамических обновлений) требований, необходимых для поддержки Active Directory. В настоящее время существует несколько реализаций службы DNS, среди которых можно выделить службу DNS Windows 2000, службу DNS Windows NT 4.0, а также самые разные реализации серверов BIND. Взгляните на сравнение разных реализаций в плане поддержки функций, требуемых для работы Active Directory:

Сравнение свойств различных реализаций DNS

Свойство	Windows 2000	Windows NT 4.0	Bind		
			8.2.2	8.2.1	4.9.7
SRV	Да	Да (с SP 4)	Да	Да	Да
Динамические обновления	Да	Нет	Да	Да	Нет
Защищенные динамические обновления	Да	Нет	Нет	Нет	Нет
WINS / WINS-R	Да	Да	Нет	Нет	Нет
Быстрая передача	Да	Да	Да	Да	Да
Инкрементная передача	Да	Нет	Да	Нет	Нет
UTF-8	Да	Нет	Нет	Нет	Нет

Полагая, что поддержка защищенных динамических обновлений, разрешения NetBIOS-имен компьютеров путем интеграции со службой WINS, поддержка UTF-8 являются факультативными функциями, видим, что для работы Active Directory полностью подходят только службы DNS Windows 2000 (что и понятно) и BIND версии 8.2.2 и выше.

Теперь рассмотрим варианты использования существующего сервера DNS. Начнем с ситуации, когда версия этой службы позволяет использовать ее для поддержки Active Directory.

DNS Windows 2000 или BIND версии лучше 8.2.2

Это простейший случай. Вряд ли стоит говорить об использовании сервера DNS Windows 2000, Это «родной» для Active Directory сервер, и проблем с ним быть не должно. (Хотя, как мы уже видели, они все-таки бывают.)

Замечание Использование для построения Active Directory сервера DNS, расположенного в незащищенном участке сети, например в демилитаризованной зоне, крайне нежелательно.

Использование сервера BIND версии 8.2.2 и выше должно быть оправданно. Например, сеть построена так, что сетевая инфраструктура (службы DHCP и DNS) реализована на базе Optivity NetID от фирмы Nortel. Архитектура данной реализации такова, что на центральном сервере работает «движок», осуществляющий доступ к центральной СУБД (например, Oracle) и управляемый с отдельной консоли. С «движком» связаны агенты, расположенные в различных частях сети и исполняющие роль серверов DNS/DHCP. Агентами нельзя управлять иначе, нежели через центральную консоль, что предопределяет жесткую централизацию управления. С другой стороны, единая база гарантирует надежную выдачу уникальных адресов и их регистрацию. Развертывание такой службы весьма дорого, так как приходится платить не только за лицензию на СУБД, но и за количество обслуживаемых адресов. Если вы не используете совместимый тип СУБД, то экономически выгоднее служба DNS Windows 2000.

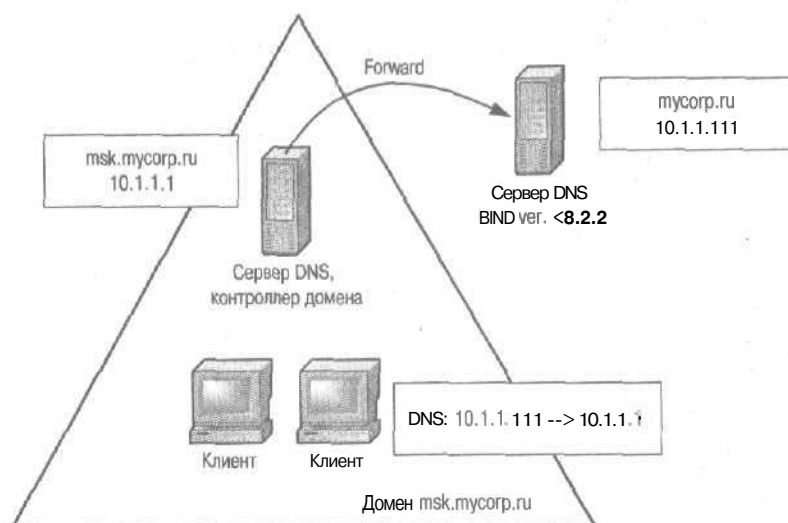
BIND версии хуже 8.2.2

Если же в настоящее время в сети имеется сервер DNS версии ниже 8.2.2, то могу предложить несколько сценариев его использования. Первый, конечно же, — обновление его до нужной версии. Но этот способ мы отвергаем, предполагая, что на то имеются важные причины. Тогда два основных варианта:

- для поддержки Active Directory устанавливается новый сервер DNS;
- в конфигурацию имеющегося сервера вносятся небольшие изменения, и дополнительно устанавливается новый сервер DNS.

Оба варианта рассматриваются в предположении того, что имя домена Active Directory не совпадает с именем существующей зоны. Если же это не так, то решение несколько сложнее, Имя существующей зоны пусть будет mycorp.ru.

Первый вариант тривиально прост. На любом из серверов в сети устанавливается дополнительный сервер DNS, скажем, тот, что входит в Windows 2000. На нем создается дочерняя зона, например msk.mycorp.ru, для которой разрешены динамические обновления. Сам сервер конфигурируется так, что все неразрешенные запросы перенаправляются на существующий сервер DNS. На всех клиентских компьютерах в качестве первичного сервера DNS указываем адрес нового сервера. И устанавливаем Active Directory.



Для поддержки Active Directory устанавливается новый независимый сервер DNS

Недостаток такого решения — необходимость смены адреса первичного сервера DNS на всех клиентах в сети. Однако служба DHCP значительно упрощает решение этой задачи.

Второй вариант посложнее. Как и в предыдущем случае для поддержки Active Directory создается отдельный сервер DNS. На нем конфигурируется соответствующая зона, например msk.mycorp.ru, и устанавливается одноименный домен Active Directory. Затем на сервере DNS, поддерживающем зону mycorp.ru, создается делегирование зоны msk.mycorp.ru на новый сервер DNS. На всех клиентах параметры TCP/IP не изменяются, но они все же получают возможность полноценной регистрации и поиска в домене.



Существующий сервер делегирует управление зоной на новый сервер

Совсем иное дело, когда имена зоны существующего сервера DNS и домена Active Directory совпадают. Так как мы рассматриваем случай сервера DNS, не совместимого с Active Directory, то его нельзя использовать для построения домена. А надо бы... Что ж, попробуем!

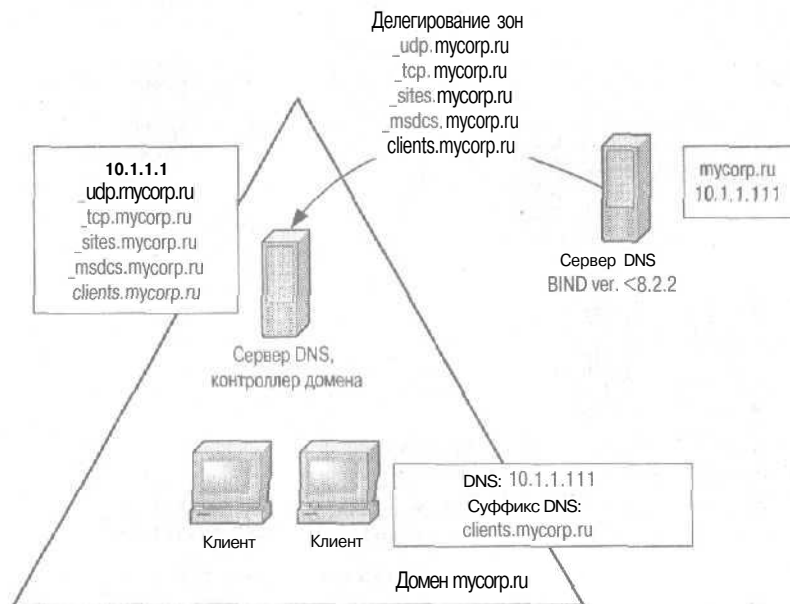
- ◆ Установите новый сервер DNS, совместимый с Active Directory. Создайте на нем зоны:
 - _udp.mycorp.ru;
 - _tcp.mycorp.ru;
 - _sites.mycorp.ru;
 - _msdcs.mycorp.ru.
- Разрешите динамическое обновление этих зон.
- На старом сервере DNS делегируйте перечисленные выше зоны на новый сервер. Это позволит контроллерам домена динамически обновлять информацию в записях типа SRV.

Чтобы клиенты смогли динамически регистрироваться в DNS:

- на новом сервере DNS создайте специальную зону, например clients.mycorp.ru, разрешите для нее динамические обновления;
 - ◆ на старом сервере делегируйте эту зону на новый сервер;
 - ◆ на всех клиентах в качестве первичного суффикса укажите clients.mycorp.ru и сбросьте флажок Change primary DNS suffix when domain membership changes в свойствах компьютера; после перезагрузки клиенты зарегистрируют себя в новой зоне.

Однако это не все. Дело в том, что контроллеры домена регистрируют не только записи типа `SRV`, но и записи типа `A` для всех сетевых интерфейсов и для всех сетевых интерфейсов глобального каталога (ГК). Так как описанный выше трюк не пройдет, придется внести соответствующие записи в зону на «старом» сервере DNS вручную. Эти записи можно взять из файла `netlogon.dns`.

Выше я упомянул о том, что служба `netlogon` периодически обновляет записи в DNS. В нашем случае всякий раз при попытке обновления записей типа `A` в журнал регистрации будет заноситься ошибка 5773 — «The DNS server for this DC does not support dynamic DNS. Add the DNS records from the file '%SystemRoot%\System32\Config\netlogon.dns to the DNS server serving the domain referenced in that file». Чтобы исключить ее появление, запретите службе Netlogon обновление этих записей: в ветви реестра `HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters` установите параметр `RegisterDnsARecords` в 0.



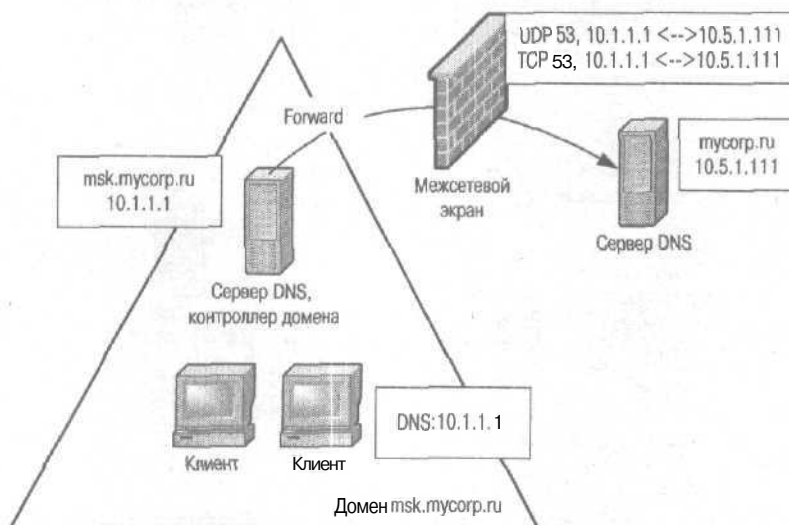
При совпадении имен существующей зоны с именем домена используют более сложное решение

А если сервер DNS расположен за межсетевым экраном?

Рассмотрим еще одну распространенную ситуацию: сервер DNS расположен за межсетевым экраном в демилитаризованной зоне (DMZ) и используется для разрешения имен Интернета.

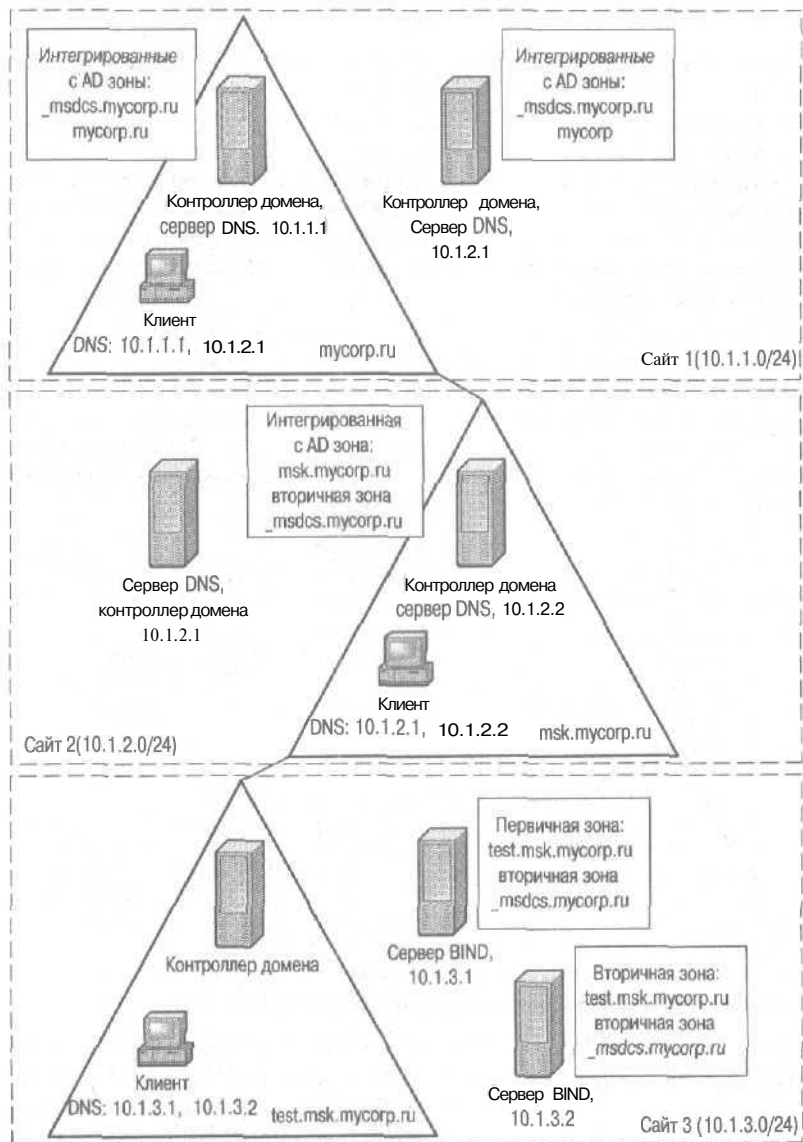
Независимо от того, совместим ли он с Active Directory, использовать данный сервер для хранения зон Active Directory не рекомендуется. Этим вы серьезно компрометируете безопасность сети. А раз так, то целесообразнее всего установить новый сервер DNS во внутренней сети, создать на нем зоны для домена Active Directory и передать все неразрешенные запросы на внешний сервер DNS через межсетевой экран. Для этого на межсетевом экране надо открыть порты UDP 53 и TCP 53 для пропуска трафика между двумя серверами DNS. На всех клиентах в качестве адреса первичного сервера DNS указывается адрес нового сервера.

Дополнительный плюс такого решения в том, что на межсетевом экране порты открываются лишь для одного определенного компьютера во внутренней сети, а не для всех клиентов.



Если сервер DNS расположен за межсетевым экраном, надо открыть соответствующие порты между серверами DNS

Описанное решение годится для случая, когда имя домена Active Directory не совпадает с именем зоны на сервере DNS в DMZ. А теперь представьте себе организацию с зарегистрированным в Интернете именем myscorp.ru. Принято решение использовать его в качестве имени корневого домена Active Directory. Допустим также, что сотрудники должны иметь доступ к корпоративному Web-серверу www.myscorp.ru, расположенному в DMZ, и к своей почте, используя Outlook Web Access (OWA) как изнутри, так и извне, т. е. из Интернета.

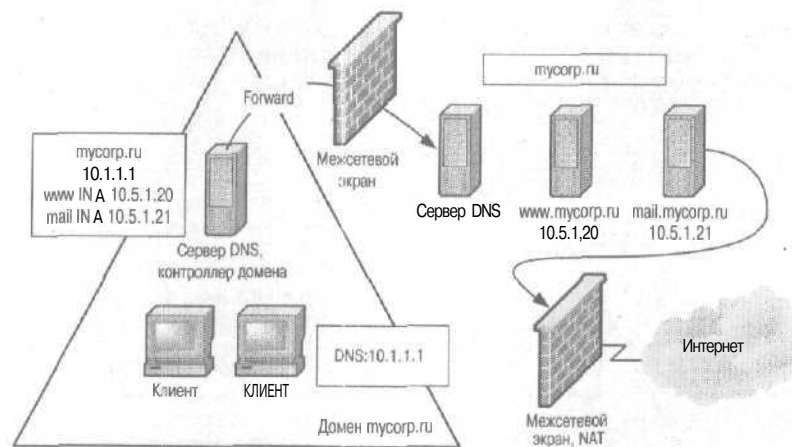


Пример реализации структуры DNS при размещении доменов в отдельных сайтах

Я уже говорил, что размещать информацию о зонах Active Directory за межсетевым экраном недопустимо, поэтому описанное ранее решение невозможно. И все же решение есть.

Итак, сначала во внутренней сети устанавливаем сервер DNS для работы Active Directory. На нем создается зона `myscorp.ru`, для которой разрешены динамические обновления. В этой же зоне статически создаются записи типа A для серверов, расположенных в DMZ. (Возможно и создание записей типа CNAME.) Неразрешенные запросы переадресуются на сервер DNS в DMZ. На межсетевом экране открываются порты для обмена между серверами DNS, и для всех пользователей открываются нужные порты для доступа к серверу Web и OWA. На всех клиентах в качестве адреса основного сервера DNS указывается адрес внутреннего сервера.

Доступ из Интернета осуществляется через межсетевой экран и NAT (Network Address Translation). Сервер DNS в DMZ содержит записи о сервере Web и OWA, но адресация для них указана внешняя, т. е. та, по которой они доступны извне через NAT.



Для обеспечения доступа к серверам в DMZ необходимо статически прописать их адреса на внутреннем сервере

Строим лес доменов

Строительство дерева доменов можно вести по-разному в зависимости от конкретных условий. Главное влияние на структуру DNS оказывает разбросанность дерева по сайтам, т. е. по участкам сети, связанным между собой относительно медленными каналами связи.

Допустим, что структура дерева состоит из трех доменов: корневого myscorp.ru, дочернего к нему msk.myscorp.ru и домена test.msk.myscorp.ru, дочернего ко второму. Мы рассмотрим следующие варианты:

- все домены расположены в одном сайте;
- каждый из доменов располагается в отдельном сайте;
- + один из доменов разбит на несколько сайтов.

Все домены в одном сайте

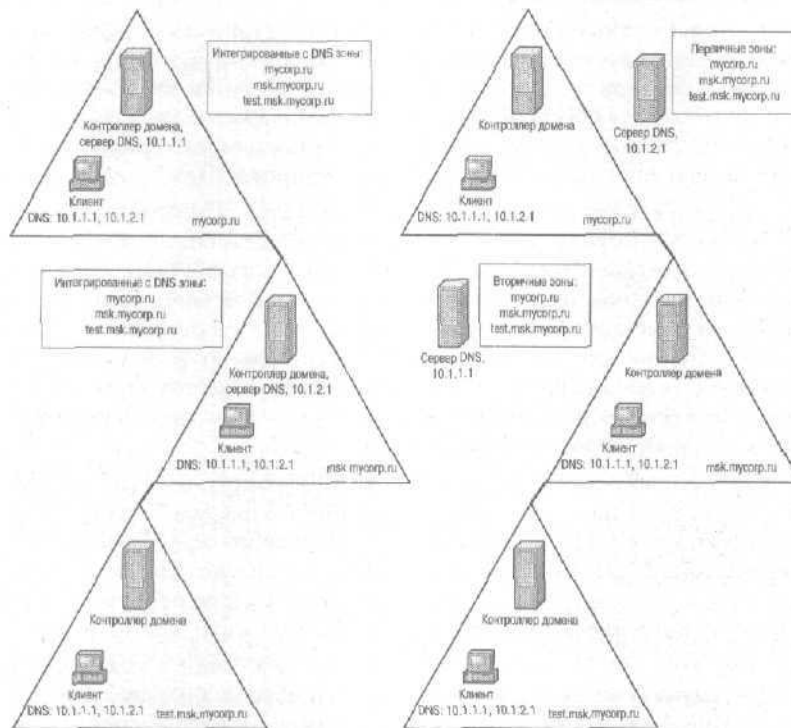
Этот вариант самый простой, так как связь внутри сайта предполагается высокого качества, а значит, любой клиент может иметь доступ к любому серверу DNS. Однако есть повод поразмышлять. Во-первых, сколько серверов DNS конфигурировать? Во-вторых, какого типа зоны создавать: стандартные первичные, вторичные или интегрированные с Active Directory? В-третьих, как конфигурировать DNS и клиенты?

Количество серверов DNS в сайте определяется объемом хранимой информации, загруженностью сервера и требованиями отказоустойчивости. Исходя из последнего, серверов DNS должно быть минимум два. Если на одном располагаются стандартные первичные зоны для всех трех доменов, то на втором — стандартные вторичные зоны для тех же доменов. Клиентские компьютеры сконфигурированы так, что в качестве адреса первичного сервера DNS указывается адрес сервера, на котором установлены первичные зоны, в качестве альтернативного — сервер со вторичными зонами.

Если же эти зоны интегрированы с Active Directory, то серверы DNS располагаются на контроллерах доменов и содержат одинаковую информацию. Клиентам безразлично, адрес какого сервера указан как первичный, а какого — как альтернативный. Но вот для самих контроллеров домена это важно. В их параметрах адрес основного сервера DNS должен указывать на другой сервер, а адрес альтернативного — на себя. Почему это так, я расскажу в разделе «Проблема островов».

Когда нагрузка на серверы DNS велика, требуется больше серверов DNS. Например, можно создать по два сервера DNS для каждого домена Active Directory. Если используются стандартные зоны, то один из таких серверов содержит стандартную первичную зону, а второй — стандартную вторичную. При этом целесообразно в корневом домене делегировать все дочерние зоны на соответствующие серверы DNS, а на всех клиентах указать в качестве первичного и альтернативного серверов DNS адреса серверов в корневом домене. Можно поступить и иначе: каждый из дочерних серверов DNS пересылает неразрешенные запросы к родительскому, а клиенты в каждом домене указывают в качестве серверов DNS адреса серверов в «своем» домене. Однако тогда надо позаботиться о правильной автоматической конфигурации этих адресов через DHCP или сконфигурировать их вручную.

Если зоны интегрированы с Active Directory, дополнительная настройка не нужна. Надо лишь, чтобы первый контроллер в корневом домене в качестве адреса первичного сервера DNS не указывал сам на себя. Если домены содержат огромное число контроллеров, потребуется дополнительная настройка (см. раздел «Ну очень большая компания»). А теперь — прямо противоположный пример: каждый домен располагается в своем сайте.



Вариант расположения серверов DNS для зон, интегрированных с Active Directory и для стандартных зон

Каждый домен в своем сайте

На первый взгляд, решение здесь просто развивает представленное выше. В каждом домене (а значит, и в сайте) по 2 сервера DNS. Если они расположены на контроллерах домена и все зоны интегрированы с Active Directory, то этого вполне достаточно. Репликация автоматически будет тиражировать изменения между серверами. На клиентских компьютерах прописывается по два адреса серверов DNS:

расположенного в том же сайте, что и клиент, и расположенного в ближайшем сайте. При этом надо обратить внимание на пропускную способность каналов. Если сайт связан одновременно с двумя другими, но полоса пропускания канала с первым — 64 кб, а со вторым — 256 кб, предпочтение надо отдать второму.

Если служба DNS организована посредством серверов BIND либо вы не хотите использовать зоны, интегрированные с Active Directory, то для отказоустойчивости желательно иметь по два сервера DNS в каждом сайте. На первом будет первичная зона для домена данного сайта. В ней должно быть прописано делегирование остальных зон на соответствующие серверы DNS в других сайтах. Второй содержит вторичную зону для локального домена. На клиентах прописаны адреса серверов DNS «своего» сайта. Если нужно обеспечить разрешение других имен, например хостов в Интернете, каждый из серверов DNS должен иметь настроенную пересылку неразрешенных запросов (forwarding) к внешнему серверу DNS.

В теории ясно, а вот как на практике? Есть тут одна тонкость, которую надо учесть. Каждый контроллер домена регистрирует в DNS два набора записей: один, касающийся своего домена, второй — леса в целом. Первый заносится в зону, соответствующую имени домена, например, в нашем случае — для домена msk.mycorp.ru, а второй — в зону _msdcs.mycorp.ru. Последняя существует только в корневом домене, т. е. в mycorp.ru.

Внимание Записи, заносимые в зону _msdcs.<имя леса>, весьма важны для Active Directory. Это, например, адреса глобальных каталогов или имена партнеров по репликации.

В случае расположения всех доменов в одном сайте, доступ с контроллера любого домена всегда возможен к зоне _msdcs.mycorp.ru. Однако если домены разнесены по сайтам, есть вероятность прерывания канала связи и отсутствия доступа к рассматриваемой зоне. Для решения этой проблемы в DNS корневого домена надо создать отдельную зону _msdcs.<имя леса> (_msdcs.mycorp.ru в нашем примере) и тиражировать ее на все серверы DNS в лесу. Если эта зона интегрирована с Active Directory в корневом домене, то на всех остальных DNS в других доменах надо создать вторичные зоны с тем же названием и растиражировать содержимое.

Описанный подход решает еще одну проблему. Допустим, в нашем примере домен test.msk.mycorp.ru расположен в сайте, связанном с остальными коммутируемой линией. В этом случае всякий раз, когда понадобится разрешение имени из зоны _msdcs.<имя леса>, будет генерироваться трафик по коммутируемой линии. Разместив эту

зону на локальных серверах DNS, мы избавимся от этого трафика, а значит, и от лишнего дозвона по коммутируемой линии.

«Да, но тиражирование этой зоны по всем серверам DNS в сайте избыточно,» — возразите вы и... и будете неправы. Пусть на некотором сервере DNS в сайте нет описываемой зоны, и он к тому же не сконфигурирован для передачи неразрешенных запросов на другие серверы. Тогда для поиска имени в этой зоне он должен использовать рекурсию. Для этого он должен обратиться к корневому серверу DNS для зоны, а затем проследовать по делегируемым зонам до нахождения нужной. Если корневой сервер — за пределами сайта, а связь сайта с другими прервана, то он никогда не найдет требуемой зоны, даже если она будет находиться на соседнем сервере DNS в сайте.

Мораль проста: при расположении доменов в отдельных сайтах в каждом сайте должно быть минимум два сервера DNS. Сервер DNS корневого домена должен содержать;

- ◆ первичную (или интегрированную с Active Directory) зону для своего домена, реплицируемую как минимум на еще один сервер DNS в сайте;
- ◆ первичную (или интегрированную с Active Directory) зону `_msdcs.<имя леса>`, реплицируемую на все сервера DNS во всех сайтах;
- делегирование для зон `всех` дочерних доменов.

Каждый из серверов DNS в дочерних доменах должен иметь:

- первичную (или интегрированную с Active Directory) зону для своего домена, реплицируемую как минимум на еще один сервер DNS в сайте;
- ◆ вторичную зону `_msdcs.<имя леса>`;
- переадресацию запросов на сервер DNS в корневом домене и/или делегирование для зон `всех` дочерних доменов.

Один домен разбит на несколько сайтов

Данный случай почти не отличается от описанного выше. Однако надо особо рассмотреть домен, разбитый на два (или в общем случае — на большее число сайтов). Из нескольких возможных вариантов рассмотрим самые интересные:

- один из сайтов в домене подключен по медленному, но выделенному каналу связи и содержит не более 20 пользователей;
- один из сайтов в домене подключен по достаточно быстрому и незагруженному каналу и содержит большое число пользователей;
- ◆ один из сайтов подключен по медленному, но выделенному каналу связи и содержит более 20 пользователей;
- один из сайтов подключен по коммутируемому каналу

Используя информацию, приведенную выше, делаем выводы:

Характеристики сайта	Организация DNS
Подключение по медленному выделенному каналу, не более 20 пользователей ИЛИ	Можно обойтись без сервера DNS в сайте. Все клиенты в качестве адреса DNS-сервера используют адреса в других сайтах, связанных с рассматриваемым
Подключение по быстрому незагруженному каналу, большое число пользователей	Минимум один DNS-сервер, имеющий зону для домена, предпочтительно интегрированную с Active Directory, либо вторичную зону. Также имеет вторичную зону <code>_msdcs.<имя леса></code>
Подключение по медленному выделенному каналу, более 20 пользователей ИЛИ	
Подключение по выделенному каналу	

Проблема «островов»

Речь пойдет не о взаимоотношениях Японии с Россией, а о довольно распространенной ошибке, допускаемой администраторами при конфигурировании DNS.

Рассмотрим случай, когда на контроллере домена, являющимся также сервером DNS, в параметрах TCP/IP в качестве адреса сервера DNS, содержащего зону `_msdcs.<имя леса>`, указан собственный адрес. Это справедливо, например, для контроллера корневого домена, являющегося сервером DNS с зоной, интегрированной с Active Directory. Как я уже говорил, зона `_msdcs.<имя леса>` содержит записи о партнерах по репликации. (Это записи типа CNAME, которые связывают GUID контроллера домена с его именем.) Пусть у контроллера домена изменился IP-адрес. Так как первичным сервером DNS для него является он сам, то он внесет соответствующее изменение в запись CNAME в собственный сервер DNS. Любой другой контроллер домена, настроенный аналогично, не сможет реплицировать эти изменения, так как в «его» сервере DNS записан старый адрес контроллера домена, на котором произошло изменение. Таким образом, контроллер домена окажется в изоляции, или «на острове», поскольку ни одно из изменений, вносимых на нем в Active Directory, не будет тиражироваться на другие контроллеры домена.

Избежать проблемы «островов» несложно: на любом контроллере домена нельзя в качестве первичного сервера DNS указывать собственный сервер. Как первичный надо указать адрес сервера DNS на другом контроллере домена, а как альтернативный — свой.

Как это сделать? Пусть в домене мусопр.ру сервер DNS установлен на контроллере rootl.мусопр.ру. Соответствующая зона интегрирована с Active Directory. Вы устанавливаете дополнительный контроллер

домена root2, на котором также установлен, но еще не сконфигурирован сервер DNS. Перед запуском DCPROMO в качестве адреса основного сервера DNS укажем адрес сервера root1, а в качестве альтернативного — собственный. По окончании работы DCPROMO, но до перезагрузки компьютера надо на сервере root1 указать как адрес первичного сервера DNS адрес сервера root2, а как альтернативный — собственный. После перезагрузки все будет работать.

Использование «плоских» имен корневого домена

«Плоским» именем домена называется такое, в котором нет ни одной точки. Как указывалось в предыдущей главе, не рекомендуется использовать «плоские» имена корневого домена поскольку:

- ♦ в домене «плоским» именем по умолчанию клиенты не могут использовать DNS для поиска контроллеров домена;

- * для контроллеров домена с «плоским» именем динамическая регистрация записей в DNS по умолчанию невозможна.

Тем не менее в случае острой необходимости поддержку плоских имен можно включить. Для этого надо выполнить следующее.

1. Для того чтобы члены домена с «плоским» именем могли находить контроллеры в домене, можно либо соответствующим образом настроить разрешение имен NetBIOS (допустим, сконфигурировав службу WINS), либо на всех клиентах установить в реестре значение параметра AllowSingleLabelDnsDomain в ветви HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters равным 1.
2. Для того чтобы клиентские компьютеры на базе Windows XP Professional или Windows 2000 SP4 могли динамически регистрировать записи в DNS, следует установить в реестре значение параметра UpdateTopLevelDomainZones в ветви HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DnsCache\Parameters равным 1. Этот же параметр для клиентов на базе Windows Server 2003 расположен в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient.

DNS в крупной компании

При развертывании Active Directory в крупных организациях чрезвычайно важно избежать ошибок, связанных с неправильной конфигурацией DNS.

Допустим, в организации существует дерево доменов mусогр.ru. Все в этом дереве работает нормально. И тут принимается решение о создании нового дерева в лее доменов, в которое нужно включить пока только один домен — int.filial.ru. Подключение этого домена в виде отдельного дерева обусловлено административными причинами. Из сообра-

жений безопасности выдвигается требование: никто из этого домена не должен иметь административных прав в основном дереве, а лучше даже ограничить доступ на уровне сети. С другой стороны, администраторы основного дерева **могут** иметь доступ к новому домену.

Исходя из этого системный администратор:

- ◆ устанавливает новый сервер Windows 2000;
- устанавливает на нем сервер DNS, конфигурирует первичную зону `int.filial.ru`, указывает необходимость пересылки неразрешенных запросов на внешний сервер DNS `filial.ru`, обслуживающий запросы на доступ в Интернет;
- ◆ указывает в качестве адреса основного сервера DNS собственный адрес, а в качестве альтернативного — адрес сервера DNS в корневом домене основного дерева;
- ◆ запускает `DCPROMO` и конфигурирует контроллер домена `int.filial.ru`;
- на всех клиентских компьютерах указывает в качестве адреса сервера DNS адрес нового контроллера домена.

После перезагрузки все работает нормально. Пользователи домена `int.filial.ru` входят в домен без проблем. Окрыленный успехом администратор решает установить второй контроллер в домене `int.filial.ru`. Он повторяет практически те же шаги за исключением того, что сервер DNS автоматически конфигурирует программой `DCPROMO`, а после перезагрузки указывает адрес первого контроллера в домене как адрес первичного сервера DNS, а как альтернативный — свой.

Заглянув потом в журнал регистрации, он обнаруживает, что там с завидной периодичностью появляется сообщение об ошибке динамической регистрации записи в домене... `filial.ru`.

Если вы внимательно читали эту главу, то поняли, что контроллер домена периодически пытается обновить записи в зоне `_msdcs.mycorp.ru`. Не найдя их на своем сервере DNS, он обращается к серверу, поддерживающему зону `filial.ru`, но и там нет нужной зоны. Не смертельно, но неприятно.

Что делать? Правильно. Создать вторичную зону `_msdcs.mycorp.ru` на обоих контроллерах домена и синхронизировать ее с основной.

А теперь рассмотрим вариант оптимизации работы DNS для случая, когда несколько сайтов подключены к одному центральному. Это типичная ситуация для организации с большим числом филиалов. Обычно при этом пользователи одного филиала не должны иметь доступа к ресурсам в другом филиале. С другой стороны, крайне желательно, чтобы пользователи могли найти контроллеры домена только в своем сайте, либо при отсутствии контроллеров в сайте — контроллер в центральном сайте.

Для реализации такого решения служба Netlogon на контроллерах доменов в филиалах должна регистрировать в DNS только записи, относящиеся к сайту. При этом клиенты, у которых в качестве адреса первичного сервера DNS прописан сервер своего сайта будут видеть адреса контроллеров доменов только внутри сайта. В случае недоступности внутреннего сервера DNS клиенты будут обращаться к DNS родительского сайта и получать информацию о контроллерах домена только этого сайта.

Внимание Возможность конфигурирования типа записей, регистрируемых службой Netlogon в DNS, появилась в Windows 2000 SP2.

Чтобы запретить регистрацию службой Netlogon определенных записей, надо изменить параметр DnsAvoidRegisterRecords в ветви реестра HKLM\System\CurrentControlSet\Services\Netlogon\Parameters. Это параметр типа REG_MULTI_SZ, т. е. хранит в себе строку с несколькими значениями. Если строка пуста, то разрешается поведение по умолчанию, т. е. регистрация всех типов записей. В таблице приведен перечень значений, допустимых для рассматриваемого параметра, а также записи в DNS, соответствующие каждому из значений.

В нашем примере на всех контроллерах домена в филиалах нужно указать среди параметров все значения, в имени которых нет окончания AtSite.

Перечень значений параметра DnsAvoidRegisterRecords

Значение	Тип	Запись в DNS
DC	SRV	_ldap._tcp.dc._msdcs.<ИмяДомена>
DcAtSite	SRV	_ldap._tcp.<ИмяСайта>._sites.dc._msdcs.<ИмяДомена>
DcByGuid	SRV	_ldap._tcp.<DomainGuid>.domains._msdcs.<ИмяЛеса>
Pdc	SRV	_ldap._tcp.pdc._msdcs.<ИмяДомена>
Gc	SRV	_ldap._tcp.gc._msdcs.<ИмяЛеса>
GcAtSite	SRV	_ldap._tcp.<ИмяСайта>._sites.gc._msdcs.<ИмяЛеса>
GenericGc	SRV	_gc._tcp.<ИмяЛеса>
GenericGcAtSite	SRV	_gc._tcp.<ИмяСайта>._sites.<ИмяЛеса>
GcIpAddress	A	_gc._msdcs.<ИмяЛеса>
DsaCname	CNAME	<DsaGuid>._msdcs.<ИмяЛеса>
Kdc	SRV	_kerberos._tcp.dc._msdcs.<ИмяДомена>
KdcAtSite	SRV	_kerberos._tcp.dc._msdcs.<ИмяСайта>._sites.<ИмяДомена>
Ldap	SRV	_ldap._tcp.<ИмяДомена>
LdapAtSite	SRV	_ldap._tcp.<ИмяСайта>._sites.<ИмяДомена>

см. след. стр.

Значение	Тип	Запись в DNS
LdapIpAddress	A	<ИмяДомена>
Rfc1510Kdc	SRV	_kerberos. tcp.<ИмяДомена>
Rfc1510KdcAtSite	SRV	_kerberos. tcp.<ИмяСайта>. sites.<ИмяДомена>
Rfc1510UdpKdc	SRV	_kerberos. udp.<ИмяДомена>
Rfc1510Kpwd	SRV	_kpasswd. tcp.<ИмяДомена>
Rfc1510UdpKpwd	SRV	_kpasswd. udp.<ИмяДомена>

Как частный случай рассмотрим ситуацию, когда в сайте нет контроллера домена. В Windows 2000 встроена функция *AutoSiteCoverage*, позволяющая клиенту выбирать ближайший (т. е. наиболее доступный) контроллер домена в другом сайте. *AutoSiteCoverage* указывает контроллеру домена, может ли он обслуживать клиенты в других сайтах. Если да, то список обслуживаемых сайтов формируется динамически на основании следующих метрик (в порядке приоритета):

- ◆ **стоимость подключения** — имеется в виду стоимость подключения, с точки зрения топологии сети (см. главу «Репликация Active Directory»)
- ◆ **количество контроллеров в сайте** — чем больше контроллеров, тем лучше;
- ◆ **порядок по алфавиту** — тот сайт, имя которого стоит по алфавиту раньше, получит приоритет при прочих равных.

Как видим, в нашем примере данный критерий теоретически позволяет клиенту из одного сайта филиала подключиться к контроллеру домена в сайте другого, что, как мы знаем, крайне нежелательно.

Дабы исключить такую возможность, на всех контроллерах домена надо отключить функцию *AutoSiteCoverage*, задав нулевое значение параметру *AutoSiteCoverage* в ветви реестра `HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters`.

Замечание По умолчанию в реестре данного параметра нет.

Можно также **сконфигурировать** список сайтов, обслуживаемых контроллером домена. Для этого в ветви реестра `HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters` надо изменить значения параметров *SiteCoverage* и *GcSiteCoverage*. В первом перечисляются сайты, обслуживаемые данным контроллером домена, во втором — обслуживаемые сервером ГК.

Ну очень крупная компания

Наверняка вам интересно знать, есть ли **практические** ограничения DNS Windows 2000? Конечно, но в нашей стране они относятся к разряду скорее гипотетических. Чтобы с ними столкнуться, надо **выполнить** одновременно минимум три условия:

- ♦ организация (или большая ее часть) сосредоточена в одном домене;
- контроллеров домена **больше** 850;
- вся информация хранится в зоне **DNS** интегрированной с Active Directory.

Сочетание просто редкостное. И все же выясним, с чем **связано** ограничение. Дело в том, что зонные записи хранятся в атрибутах с **несвязанными множественными значениями** (в отличие от **групп**, **членство** в которых записывается в атрибуты со связанными множественными значениями). Для таких атрибутов существует ограничение в 850 значений. Так что, если вы планируете для **огромной**, территориально разбросанной организации поместить все в один домен, то во избежание превышения **установленного** предела воспользуйтесь советами из предыдущего раздела и перенесите нагрузку на сайты. Тогда в домене останется совсем немного записей в DNS.

Так нужна ли служба WINS?

Этот вопрос я слышу довольно часто. Бывает, администраторы, **прочитав** в Windows 2000 Resource Kit фразу о том, что Windows 2000 может обходиться без WINS, не устанавливают его в своей сети. Хорошо это или плохо? Давайте разберемся. Но начнем с NetBIOS.

Краткий экскурс в историю NetBIOS

NetBIOS — это интерфейс **сеансового** уровня, используемый сетевыми приложениями для взаимодействия через совместимый транспорт. Он позволяет устанавливать в сети логические имена, сеансы между двумя логическими **именами**, а также поддерживать надежное соединение между ними. Имена NetBIOS являются плоскими в противоположность полностью определенным именам DNS. Длина имени не может превышать **15 символов** (плюс 1 служебный символ). Имена автоматически регистрируются при старте компьютера и регистрации пользователя. Имена делятся на **уникальные**, т. е. соответствующие одному адресу, и групповые, которым соответствует несколько адресов. Если вы выполните на компьютере с ОС Windows команду nbtstat -n, то получите результат, аналогичный этому:

```
Local Area Connection:  
Node IpAddress: [10.1.1.3] Scope Id: []
```

NetBIOS Local Name Table

Name		Type	Status
DC01	<00>	UNIQUE	Registered
DC01	<20>	UNIQUE	Registered
MYCORP	<00>	GROUP	Registered
MYCORP	<1C>	GROUP	Registered
HYCORP	<1B>	UNIQUE	Registered
Inet~Services	<1C>	GROUP	Registered
MYCORP	<1E>	GROUP	Registered
IS~DC01	<00>	UNIQUE	Registered
MYCORP	<1D>	UNIQUE	Registered
.._MSBROWSE_	<01>	GROUP	Registered
DC01	<03>	UNIQUE	Registered
FYODORZ	<03>	UNIQUE	Registered

В этой таблице имя DC01 соответствует имени контроллера домена. Для него определены NetBIOS имена:

- ◆ 00 (Имя регистрируемое службой workstation);
- 03 (служба Messenger);
- ◆ 20 (служба Server).

Имя Mycorp соответствует имени домена и для него определены имена:

- ◆ 00 (экземпляр доменного имени, зарегистрированный службой Workstation для использования в сети LAN Manager);
- ◆ 1B (экземпляр имени, зарегистрированный службой Server и используемый при просмотре содержимого домена);
- ◆ 1C (групповое имя, может содержать до 25 адресов; первый адрес соответствует первичному контроллеру домена, все остальные — вторичным);
- 1D [уникальное имя указывающее на адрес главного браузера (master browser)].

Имя .._MSBROWSE_ используется для широковещательных рассылок и приема доменных оповещений в локальной подсети. Благодаря этому имени, главные браузеры в доменах узнают о существовании друг друга и других доменов.

Имя Fyodorz соответствует учетной записи пользователя. Служба Server регистрирует его, чтобы пользователь мог получать сообщения, посылаемые командой Net Send.

Я не случайно так подробно перечислил эти имена. В дальнейшем будет легче понять роль сервера WINS или результаты отсутствия поддержки NetBIOS.

Как разрешаются имена NetBIOS

Думаю, ни для кого не секрет, что в сетях Microsoft могут применяться три механизма разрешения имен NetBIOS:

- ◆ поиск в файле LMHOSTS;
- широковещательные рассылки;
- сервер WINS.

Первый механизм можно назвать архаичным и неудобным. Подобно тому, как в сервере DNS, имеющем только статические зоны, все записи надо добавлять вручную, так и поддержание актуальной информации в файле LMHOSTS — обязанность администратора. Я уж не говорю о проблемах, связанных с безопасностью, возникающих при работе с централизованными файлами LMHOSTS. Допустим, на каждом клиентском компьютере *есть* свой файл LMHOSTS такими строками;

```
10.1.1.3 SERVER #PRE
#include \\SERVER\PUBLIC\LMHOSTS
```

Очевидно, что *первая* определяет адрес сервера SERVER, а вторая позволяет загрузить централизованный файл LMHOSTS, хранящийся на этом сервере. Знаете ли вы, что надо предпринять, чтобы это работало? Одно из условий — предоставить группе Everyone доступ Change к ресурсу \\Server\public! Просто лафа злоумышленникам!

Широковещательные рассылки, как показывает опыт, — довольно распространенный способ разрешения имен NetBIOS. Для маленьких сетей он еще приемлем, но для средних и больших совершенно не годится. Во-первых, генерируется значительный *трафик* в сети. И чем больше компьютеров, тем больше трафик. Во-вторых, *широковещательные* рассылки, как правило, не передаются между сегментами сети. Ну, и в-третьих, так как каждый компьютер должен откликнуться на каждую рассылку, это его дополнительно загружает.

Поэтому лучший способ разрешения NetBIOS-имен — применить сервер WINS: вы *избавитесь* от *широковещательных* рассылок, сможете использовать в больших сегментированных сетях и легко контролировать зарегистрированные имена и разрешать конфликты.

При этом есть 4 способа разрешения имен клиентскими компьютерами: b-node, p-node, m-node и h-node. Первый предполагает только широковещательные *рассылки*, второй — только серверы *имен* WINS. Третий и четвертый являются комбинацией первого и второго *способов*, но если в режиме m-node сначала рассылаются широковещательные сообщения, а потом идет обращение к серверу WINS, то в режиме h-node все выполняется с точностью до наоборот. С точки зрения нагрузки на сеть, более предпочтителен режим h-node.

Замечание Все эти режимы в случае неудачи обращаются сначала к файлу `LMHOSTS` (если это разрешено на клиенте), а потом — к серверу `DNS`.

Теперь выясните, как разрешаются `NetBIOS`-имена в вашей сети. Для этого выполните команду `nbtstat -g`. Не удивляйтесь, если вы используете `WINS`, а число имен, разрешенных с помощью широковещательных рассылок, весьма велико. Посмотрите на имена компьютеров, разрешенных таким способом. Скорее всего они просто не являются клиентами `WINS`.

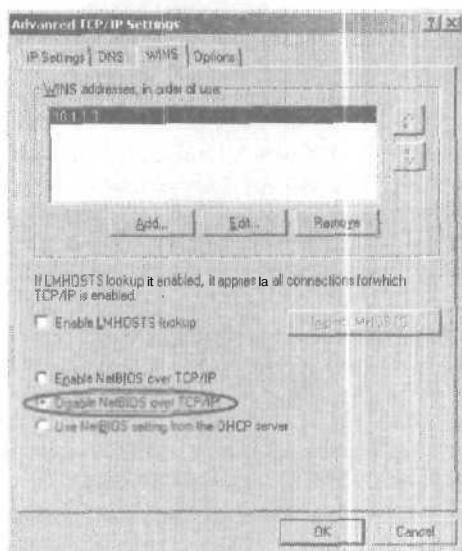
Так что приходим к выводу: уж коли используется `NetBIOS`, то без `WINS` не обойтись. Тогда зададимся другим вопросом.

А нужен ли **NetBIOS**?

В самом деле, может, не его? Удалим, и дело с концом. И широковещательных рассылок не будет, и сервер `WINS` ставить не надо, а?

Из документации известно, что для работы Windows 2000 интерфейс `NetBIOS` больше не нужен, если используется только среда Windows 2000. То есть в сети нет больше других клиентов Windows (или NT). Проверим это, Советую провести простой опыт. Запретите на двух компьютерах с Windows 2000 (или Windows XP) `NetBIOS`, а потом на одном из них зайдите в Сетевое окружение и просмотрите содержимое домена (или рабочей группы), в котором расположены данные компьютеры. Много увидели? Ага: НИЧЕГО. А все потому, что нет больше главного браузера и нет механизма, который бы позволил просмотреть содержимое домена. Помните, мы выписывали имена для них? Попробуйте выполнить команду `nbtstat -n` на любом из этих компьютеров. Никаких записей вы больше не увидите,

Так что, все пропало и больше ничего не работает? Отнюдь нет. Пошлите сообщение с одного компьютера на другой командой `net send`. Сообщения передаются. В строке `Run` наберите `\\имя_любого_компьютера\`. Вы увидите, как в списке появятся все ресурсы данного компьютера, предоставленные в совместное пользование. Выполните другие сетевые операции. Все они будут работать.



Отключение поддержки NetBIOS

Итак, отказываемся от NetBIOS!.. Пойдите, а вы проверили приложения? Как они обойдутся без этого интерфейса? **Помните**, в начале этого раздела я сказал, что NetBIOS «используется приложениями для взаимодействия». Так вот, составьте список ваших программ и протестируйте их на работоспособность. Microsoft SMS 2.0 можно не тестировать: он работать не будет.

Если окажется, что приложений, которые пока не могут обойтись без NetBIOS, у вас хватает (или даже одно, но очень важное, и заменить его нечем), придется оставить NetBIOS до лучших времен и заняться конфигурированием серверов WINS.

Краткие советы по установке серверов WINS

Нет смысла подробно описывать конфигурирование серверов WINS — все это уже сделано в разных книгах, в первую очередь в [4]. Поэтому ограничусь только самыми главными советами.

Сервер WINS рассчитан на высокую нагрузочную способность и может один обслуживать компанию с 10–15 тысячами компьютеров. Однако из соображений надежности и постоянной доступности этой службы нужно иметь не менее 2 серверов WINS. Оба должны быть push-pull партнерами по репликации.

Внимание При настройке параметров TCP/IP на серверах WINS нельзя в качестве адреса сервера WINS указывать свой адрес. Это должны быть адреса партнеров по репликации.

Если ваша сеть разбита на несколько сайтов, то целесообразность размещения серверов WINS внутри сайта определяется количеством компьютеров в сайте, а также установленной на них ОС. Если на всех компьютерах Windows 2000 или Windows XP нет приложений, для работы которых требуется NetBIOS, его можно вообще не использовать. В противном случае обращаем внимание как на количество компьютеров, так и на необходимость для пользователей обращаться по NetBIOS к ресурсам на других сайтах. Если компьютеров мало (10-20) и нет нужды просматривать ресурсы вне сайта, можно обойтись без сервера WINS и применять широковещательные рассылки для разрешения имен. Если же просмотр внешних для сайта ресурсов все-таки нужен, то компьютеры конфигурируются как клиенты WINS в другом сайте, а маршрутизатор должен пересылать запросы к WINS, т. е. выступать в роли WINS проху. Если это невозможно, то на одной из машин с Windows 2000 нужно сконфигурировать WINS проху. Если в сайте много компьютеров, установите локальный сервер WINS и сконфигурируйте его в качестве партнера по репликации для серверов WINS в родительском сайте.

Обычно серверы WINS можно размещать на контроллерах домена. Например, если вы спланировали Active Directory так, что у вас имеется корневой домен, не содержащий пользователей и применяемый лишь как держатель имени домена и административных групп, то его контроллеры домена не очень загружены и могут выполнять дополнительные функции. Но будьте внимательны. Если топология Active Directory такова, что с центральным сайтом связаны десятки (или даже сотни) других сайтов, то серверы-форпосты в центральном сайте будут чрезвычайно загружены, и размещать на них дополнительные службы, такие как WINS, категорически не рекомендуется.

И последнее. Вы, наверное, знаете, что сервер WINS можно задействовать совместно с сервером DNS для разрешения имен NetBIOS. Для этого на сервере DNS используются записи типа WINS. В сетях на базе Windows NT 4.0 это было удобно, так как служба DNS в Windows NT не поддерживает динамических обновлений. Актуально ли это для Windows 2000/XP? Теоретически эту функцию можно использовать. Особый смысл она имеет, когда клиенты (не Windows 2000/XP) не используют службу DHCP для получения адресов IP. В противном же случае лучше применять службу DHCP для регистрации клиентов в DNS. Вот мы и подошли к рассмотрению особенностей использования этой службы в Windows 2000.

Как правильно настроить DHCP

Служба DHCP существует в Windows уже довольно давно и, казалось бы, не должна вызывать проблем или вопросов. Однако многие, даже довольно опытные администраторы порой не знают некоторых свойств DHCP, что приводит к возникновению проблем в сети, по крайней мере к недоумениям. Конечно, разобравшись в источнике проблем, так и хочется ударить себя по лбу и сказать что-то типа «Семен Семен ыч!..», но лучше заранее побеспокоиться и предотвратить появление нежелательных ситуаций.

Среди тем, незнание или неполное понимание которых обычно приводит к нештатным ситуациям, отмечу такие:

- ◆ авторизация сервера DHCP;
- ◆ суперобласти и плоская сеть;
- ◆ размещение сервера DHCP в сегментированной сети;
 - параметры, определяемые для сервера, областей и исключений и порядок их назначения;
 - работа с пользовательскими идентификаторами;
- ◆ динамическая регистрация имен в DNS;
 - ◆ разрешение конфликтных ситуаций.

Что дает авторизация

Тот, кто работал с Windows NT, знает, что наличие двух серверов DHCP в сети может при определенных условиях привести к ее частичной и даже полной неработоспособности. Рассмотрим пример. В сегменте сети установлен сервер DHCP, на котором определена область с диапазоном адресов 137.45-45.1 — 137.45.45.254. Некто в исследовательских целях устанавливает собственный сервер DHCP и активизирует на нем область с диапазоном 10.1.1.1 — 10.1.1.50. Ясно, что спустя некоторое время многие машины потеряют доступ к ресурсам сети. (Кому это не ясно, обратитесь к [4].) Подобное было возможно из-за того, что практически любой мог активизировать свой сервер DHCP.

Появившаяся в Windows 2000 авторизация серверов в Active Directory вселила надежду, что с этим покончено. И правда, как написано в упомянутой выше книге, для того, чтобы служба DHCP стартовала и обслуживала пользователей, она должна быть авторизована в Active Directory. А такую операцию можно проделать, только имея полномочия Enterprise Admins. Но, увы, радость была преждевременна.

Во-первых, если в сети, где развернут домен Active Directory, установить сервер Windows NT 4.0, не входящий в указанный домен, то служба DHCP на нем может быть поднята без каких-либо помех, а значит, он окажет свое пагубное влияние на сеть.

Во-вторых, если в той же сети установить контроллер домена Windows 2000, не принадлежащего существующему лесу, и на этом контроллере домена установить службу DHCP, ее можно будет активизировать, а значит, продолжить свою вредоносную деятельность.

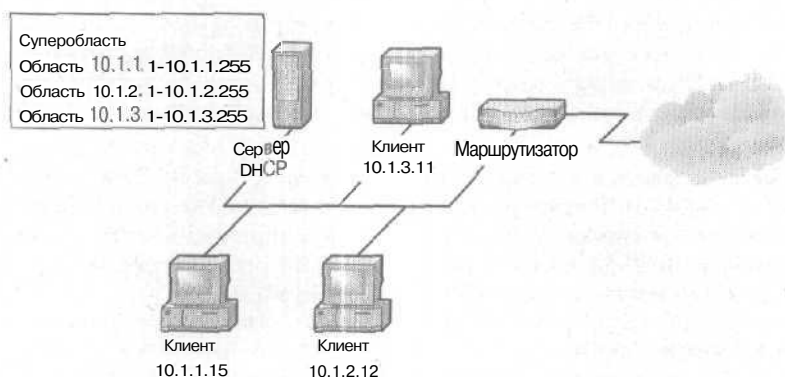
И лишь только для тех серверов, которые входят в основной домен, такая подрывная деятельность будет запрещена. При попытке запустить службу DHCP происходит обращение к Active Directory, где просматривается список адресов IP для всех авторизованных в домене серверов DHCP. Если адреса рассматриваемого сервера нет, то служба DHCP будет автоматически на нем терминирована.

Замечание До выхода Windows 2000 SP2 в Active Directory могло храниться не более 852 адресов авторизованных серверов DHCP.

Зачем нужны суперобласти

Предположим, в сегменте сети используются мультисети, т. е. несколько логических подсетей. Пусть это 10.1.1.0/22, 10.1.2.0/22 и 10.1.3.0/22. Чтобы один сервер DHCP мог обслуживать эти мультисети, на нем нужно создать три соответствующие области и объединить их в суперобласть.

А если этот сегмент сети обслуживается не одним, а тремя серверами DHCP, каждый из которых отвечает только за одну область? Допустим, у клиентского компьютера был адрес 10.1.1.15, выданный первым сервером DHCP. После перезагрузки клиент посылает запрос DHCPREQUEST без указания идентификатора сервера. Если этот запрос первым получит сервер, на котором не определена нужная область, он ответит клиенту сигналом DHCPNACK, что переведет его в режим поиска нужного сервера DHCP. Клиент разошлет широковещательное сообщение DHCPDISCOVER. Пусть первым откликнется сервер, на котором определена область 10.1.2.0/22. Тогда клиент пошлет ему запрос DHCPREQUEST, на что тот ответит DHCPACK и предоставит адрес из своего диапазона. Таким образом, клиент окажется в другой мультисети. Но это не самое страшное — хуже, что выданные данному клиенту адреса, заняты как на первом сервере DHCP, так и на втором. При следующей перезагрузке клиента он может получить адрес с третьего сервера. Если подобное поведение распространить на все оставшиеся клиенты, станет понятно, что очень скоро доступные адреса в областях будут исчерпаны, так как каждый клиент резервирует по 3 адреса. Такое возможно, когда серверы DHCP ничего не знают друг о друге.

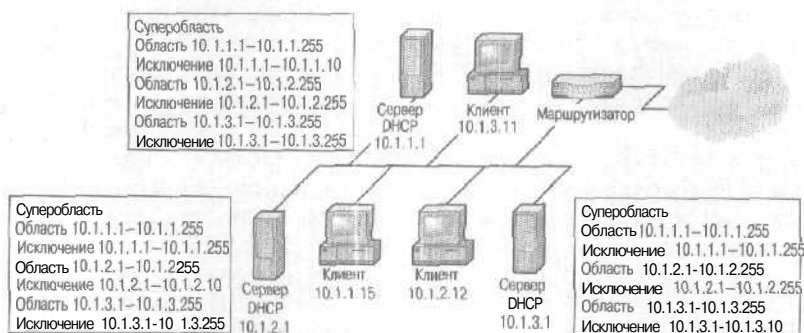


Создание суперобласти для поддержки мультисети

Дабы исключить такую ситуацию:

- ◆ на каждом сервере DHCP создадим области для каждой из подсетей;
- ◆ эти области включим в суперобласть;
- на каждом из серверов определим по две области исключений.

Например, на первом сервере в нашем примере для областей 10.1.2.0 и 10.1.3.0 формируются исключения на весь диапазон их адресов. На втором — исключения формируются для областей 10.1.1.0 и 10.1.3.0, а на третьем — для областей 10.1.1.0 и 10.1.2.0. Тогда второй сервер не откликнется на DHCPREQUEST сообщением DHCPNACK, так как увидит, что за запрашиваемую область отвечает другой сервер.



Конфигурирование суперобластей для недопущения неправильной выдачи адресов

DHCP сервер в сегментированной сети

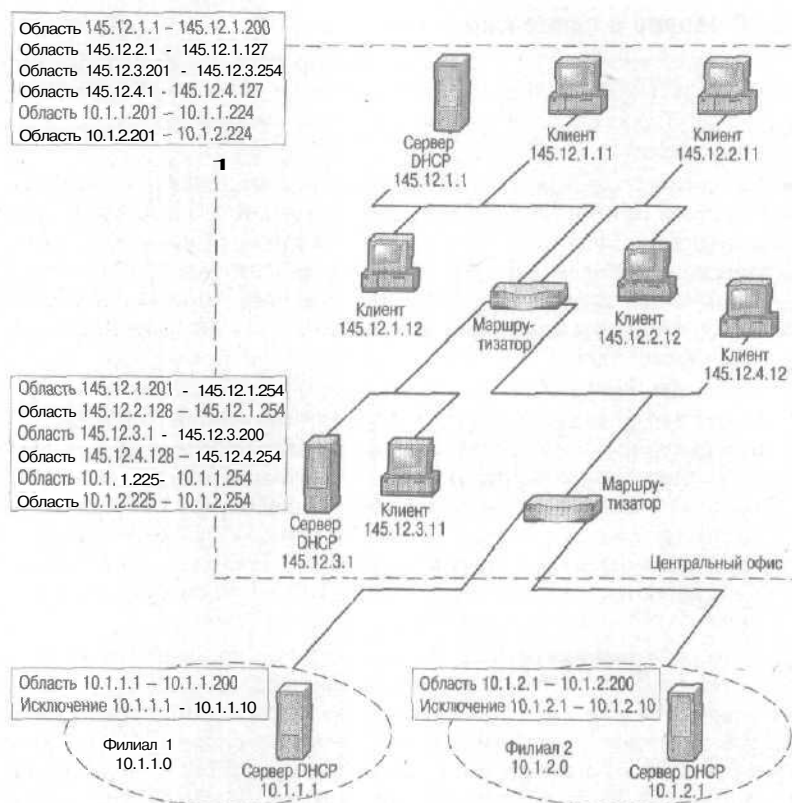
Если сеть не является плоской, а сегментирована, то использование DHCP практически ничем не отличается от того, как это было в Windows NT. В связи с этим напомним два основных правила развёртывания серверов DHCP.

- Маршрутизатор между сегментами должен выполнять роль агента передачи BOOTP (BOOTP relay agent) или DHCP, когда один сервер DHCP обслуживает несколько сегментов. В качестве агента передачи DHCP может выступать сервер Windows 2000, на котором сконфигурирована служба RRAS (Routing and Remote Access Server). При этом данный компьютер может заодно выполнять роль маршрутизатора.
- ◆ Если в двух сегментах сети свой сервер DHCP, а маршрутизатор выполняет роль агента передачи BOOTP, то серверы DHCP можно сконфигурировать так, чтобы выступать в качестве резерва друг для друга. При этом руководствуются известным правилом 80/20: на каждом из серверов создаются области для каждой из подсетей, но так, что область, в которую входит сам сервер DHCP, содержит 80% доступных адресов, а зона для другого сегмента — только 20%. Тогда при отказе «своего» сервера DHCP клиенты смогут запросить адреса у резервного сервера в соседнем сегменте.

Рассмотрим типичный пример. Несколько филиалов компании (в каждом от 50 до 200 чел.) связаны с центральным офисом (1 000 чел.) выделенными линиями с относительно небольшой пропускной способностью. У каждого сотрудника свой компьютер. Сеть в центральном офисе разбита на 4 сегмента: 145.12.1.0/24, 145.12.2.0/24, 145.12.3.0/24 и 145.12.4.0/24. Для филиалов выделены подсети 10.1.x.0/24. В центральном офисе планируется установить два сервера DHCP, а в каждом филиале — по одному. Нетрудно сообразить, что для обеспечения отказоустойчивости филиальные серверы должны содержать по 80% адресов своей подсети, а остальные 20% — отдать серверам DHCP в центре. Те в свою очередь должны поделить эти адреса между собой пополам. Кроме того, они должны разделить пополам адреса для тех сегментов, к которым они не принадлежат, а адреса для «своих» сегментов — разделить в соотношении 80/20.

Динамическая регистрация имен в DNS

Теперь обсудим динамическую регистрацию имен клиентов в DNS через службу DHCP. Известно, что клиенты Windows 2000/XP могут динамически регистрировать свое имя в DNS Windows 2000. Если отмечен соответствующий флажок в параметрах TCP/IP, то всякий раз при загрузке клиента в DNS будет обновляться запись типа A. Однако справедливости ради стоит отметить, что запись типа PTR при этом не обновляется.



Пример распределения областей по серверам DHCP в многосегментной сети

С другой стороны, в корпоративной сети применяются и иные клиенты, например Windows 9x или NT, которые не умеют обновлять свои записи в DNS, а значит, компьютер становится недоступен по имени. К счастью, сервер DHCP Windows 2000 снабжен функцией динамической регистрации записей в DNS от имени клиентов. Администратор может выбрать несколько вариантов регистрации на вкладке DNS диалогового окна свойств области DHCP. Несмотря на простоту этих возможностей, администраторы порой теряются и на всякий случай отмечают все подряд. Хорошо, что это не приводит к неприятным последствиям, но все же желательно понимать, для чего используется каждый флажок.

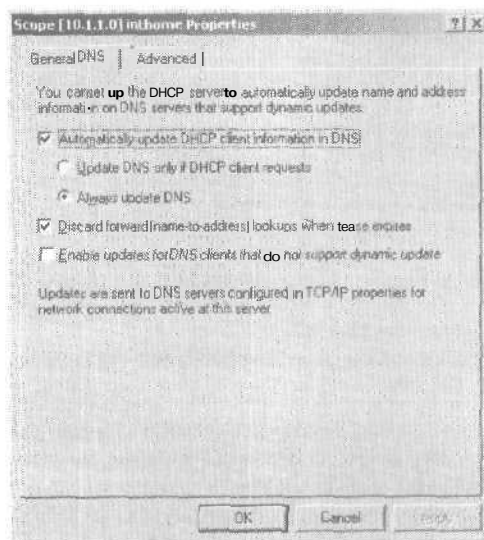
Итак, если флажок *Automatically update DHCP client information in DNS* снят, то DHCP не обновляет записи DNS. В случае с клиентами

Windows 2000/XP это значит, что они обновляют только записи типа A, да и то если это установлено в их параметрах. Для всех остальных клиентов это означает, что информация о них не заносится в DNS.

Замечание Если клиенты DHCP являются одновременно клиентами WINS, а сервер DNS сконфигурирован для разрешения имен через WINS, будет выполняться обновление записей типа A.

Если этот флажок установлен, то дальнейшее поведение зависит от положения переключателя. Если это Update DNS only if DHCP client requests, то обновления будут выполняться только для клиентов Windows 2000/XP, да и то, только если необходимость обновлений на них задана. В отличие от самостоятельного режима обновлений в режиме обновлений через DHCP в DNS заносятся записи как типа A, так и PTR. Для всех остальных клиентов все остается без изменений.

Если переключатель в положении Always update DNS, то сервер DHCP будет обновлять записи как типа A, так и PTR абсолютно для всех своих клиентов Windows 2000/XP независимо от того, хотят они этого или нет.



*Управление режимами обновления записей в DNS
посредством сервера DHCP*

Флажок Discard forward (name-to-address) lookups when lease expires задает удаление из DNS записей типа A о клиентах, для которых истек срок аренды адреса. Если флажок не установлен, удаляются только записи типа PTR.

Флажок **Enable updates for DNS clients** that do not support dynamic update предписывает динамически обновлять информацию в DNS о любых клиентах DHCP, включая такие, как сетевые принтеры.

Внимание Если сетевой принтер является клиентом DHCP и принтеру не было присвоено имя, то в DNS для него будет зарегистрирован его IP-адрес вместо имени. Причем октеты адреса будут интерпретированы как субдомены. Так, для принтера с адресом 10.1.12.133 в домене `mysogp.ru` в DNS будет занесена запись типа А для хоста «10» в зоне `1.12.133.mysogp.ru`. Чтобы этого не случилось, надо присвоить принтеру имя согласно инструкции.

Какие параметры определять в сети Windows

Неожиданно часто администраторы задумываются над тем, какие параметры определять для сервера или областей. Обилие возможностей вносит смуту в умы и подталкивает к конфигурированию того, что клиентами Windows просто игнорируется. Вот параметры, воспринимаемые клиентами Windows.

Параметр	Назначение
003 Router	Указывается адрес маршрутизатора, устанавливаемый по умолчанию, а также адреса остальных маршрутизаторов, о которых надо знать клиенту
006 DNS Servers	Перечисляются адреса серверов DNS, необходимых для работы клиента
015 DNS Domain Name	Суффикс домена. Можно указать только суффикс основного домена, но нельзя указать перечень возможных суффиксов для поиска. Это ограничение протокола DHCP
044 WINS/NBNS Servers	Адреса серверов WINS
046 WINS/NBT Node Type	Способ разрешения NetBIOS-имен. Подробнее см, раздел, посвященный WINS

Дополнительно можно запретить использование NetBIOS для клиентов Windows 2000/XP: в диалоговом окне конфигурирования свойств области откройте вкладку **Advanced**, в списке **Vendor Options** щелкните **Microsoft**, выберите параметр **001** и установите его в **1**,

Последовательность применения параметров

Вы наверняка уже обратили внимание, что параметры можно определить для сервера DHCP в целом, для областей и для каждого исключения в отдельности. Кроме того, есть параметры, определяемые для клиентов различных производителей (отличаются идентификатором **Vendor ID**) и для клиентов с разными пользовательскими идентифи-

каторами (User class ID). Несомненно, должно быть правило применения всех этих параметров к клиентам. Вот оно:

- ◆ первыми применяются параметры, определенные для сервера DHCP в целом;
- ◆ затем применяются параметры для клиентов с различными Vendor ID и User Class ID, определенные для всего сервера;
- ◆ за ними применяются параметры, определенные для той области, в которой находится клиент;
- ◆ далее, естественно, применяются параметры для клиентов с различными Vendor ID и User Class ID, определенные для области;
- наконец, если конкретный адрес попадает под исключения, то к нему применяются параметры, определенные для этого исключения, а также соответствующие параметры для клиентов с различными Vendor ID и User Class ID.

Как использовать идентификатор пользовательского класса

Как видим, возможностей немало. Но есть еще одно свойство, которое позволит сделать назначение параметров более целенаправленным. Рассмотрим сеть, в которой один из сайтов связан с центральным сайтом медленным каналом так, что в нем используется та же самая подсеть, что и в центральном сайте. В этом филиале работает 5-7 человек, и у них нет своего сервера DHCP и WINS. Для аренды адресов IP они используют сервер DHCP в центральном сайте. Доступ к ресурсам центрального сайта им нужен крайне редко. Все клиенты работают под Windows 98. Ясно, конечно, что обращения к серверу WINS в центральном офисе, мягко говоря, неуместны — проще использовать широковещательные рассылки.

Можно каждый из компьютеров сконфигурировать вручную и настроить TCP/IP. Но лучше, однако, сделать иначе. На сервере DHCP в центральном офисе надо определить свой User Class ID и сконфигурировать для него параметр 046 равный 4 (M-node). Затем на всех клиентах в удаленном сайте выполнить команду `ipconfig /setclassid <имя сетевого интерфейса> <идентификатор пользовательского класса>`. Теперь, получив запрос на аренду адреса от клиента из удаленного сайта, сервер DHCP обнаружит, что данному клиенту присвоен определенный User Class ID. Сравнив его со списком идентификаторов, определенных для сервера, и обнаружив идентичность, сервер передаст на клиент параметр 046 равный 4, а не 8, как это имеет место для всех остальных клиентов.

Как проконтролировать работу DHCP

Контролировать работу сервера DHCP особо не требуется. Если он не работает или работает не так, как это должно быть, вы сразу поймете. Однако вот общие способы контроля.

1. Загрузите клиентский компьютер и с помощью команды `ipconfig /all` проверьте правильность параметров, полученных от сервера DHCP. Здесь же вы увидите, какой именно сервер выдал адрес в аренду. Если параметры не соответствуют ожидаемым, выясните причину, устраните ее и выполните подряд команды `ipconfig /release` и `ipconfig /renew`.
2. Запустите консоль сервера DHCP. Выберите нужную область и посмотрите, какие адреса и каким компьютерам выданы. Для каждой области можно посмотреть статистику: каков процент свободных адресов в их распоряжении. Если адресов осталось мало, выясните причину их утечки. Возможно, имеет смысл сократить срок аренды адресов.
3. Если вы запустили административную консоль DHCP, а в ней нет команды Authorise, значит, вы используете учетную запись, не обладающую правами Enterprise Admins.

Замечание Часто нужно авторизовать сервер DHCP, расположенный в удаленном филиале. Если этот филиал расположен в отдельном домене, управляемом локальными администраторами, то по умолчанию они не смогут авторизовать сервер. Чтобы предоставить им соответствующее право, надо изменить права доступа к объекту `CN=Dhcp-Root,CN=NetServices,CN=Services,CN=Configuration,<имя леса>` и к контейнеру `CN=NetServices,CN=Services,CN=Configuration,<имя леса>`.

4. Если сервер, исполнявший роль сервера DHCP, был некорректно удален из сети, используйте команду `Netsh a dhcp a delete` для удаления его имени из Active Directory.
5. Регулярно просматривайте журнал регистрации системных событий.

DCPROMO и все, что с этим связано

Как вы хорошо знаете, для перевода сервера в статус контроллера домена служит программа DCPROMO, расположенная в каталоге `%SYSTEMROOT%\System32`. Вот что она делает.

- Изменяет функциональность сервера так, что он перестает использовать хранимые в реестре учетные записи SAM и переключается на каталог, основанный на ESE (Extensible Storage Engine).

Замечание Если вы обновляете контроллер домена Windows NT 4.0, то DCPROMO запустится автоматически и перенесет учетные записи из SAM в Active Directory.

- Если вы устанавливаете новый контроллер домена в новом лесу, то база Active Directory создается на основе шаблона NTDS.DIT, хранящегося в каталоге %SYSTEMROOT%\System32. Если это дополнительный контроллер в домене, то в качестве шаблона используется информация, взятая с другого контроллера.
- Создается новая учетная запись администратора и ее идентификатор безопасности (SID). Старая учетная запись, равно как и ее SID, уничтожается. Кроме того, создается целый набор встроенных учетных записей пользователей и групп.
- На локальном диске создается иерархия каталогов SYSVOL, а также общедоступные ресурсы SYSVOL и NETLOGON. При обновлении контроллера домена Windows NT 4.0 все содержимое ресурса NETLOGON (REPL\EXPORT\SCRIPTS) переносится в одноименный ресурс в иерархии SYSVOL.
- Изменяются стартовые параметры некоторых служб. Они переходят из разряда Manual в разряд Automatic.
- Служба Windows 2000 Win32 Time выполняет синхронизацию времени с внешним источником эталонного времени.

Как видим, перечень выполняемых действий обширен и затрагивает важнейшие функции Windows 2000. Если соблюсти все предварительные требования, то процесс превращения сервера в контроллер домена проходит без сучка и задоринки. Рассмотрим эти требования.

Требования, предъявляемые DCPROMO

Что нужно знать перед запуском DCPROMO? Главное — хорошо понимать, что именно вы собираетесь сделать. Более того, если с одним и тем же компьютером вы экспериментируете не первый раз (без переустановки ОС), то надо *знать*, что вы сделали в прошлый раз не так и к чему это могло привести. Возможно, после некоторых ваших действий все попытки установить контроллер домена будут неудачны. Но не будем о грустном — рассмотрим все по порядку.

Во-первых, надо четко понимать, где расположен данный контроллер домена в Active Directory. Если вы создаете самый первый контроллер домена в лесу, позаботьтесь, чтобы компьютер обладал высокой надежностью. Предусмотрите на нем средства резервного копирования, обеспечьте его постоянную доступность в сети. Помните: первое время он

будет выполнять роли всех мастеров операций да плюс ко всему будет ГК. Неожданная утрата такого компьютера приведет фактически к неработоспособности всего леса доменов.

Во-вторых, убедитесь, что параметры TCP/IP заданы верно. Проверьте, что нужные серверы доступны (см. раздел «Что делать с DNS?»). Возможно, придется проверить сеть на физическом уровне. Ведь если вы устанавливаете контроллер домена в удаленном филиале, должна существовать связь с компьютером, выполняющим роль мастера имен доменов (domain naming master), расположенным скорее всего в центральном офисе.

В-третьих, на компьютере должен иметься минимум один дисковый раздел, отформатированный как NTFS5, с необходимым объемом свободного места. И хотя этого достаточно для установки Active Directory, лучше последовать рекомендациям, приведенным далее при конфигурировании дисковой подсистемы.

В-четвертых, вам нужны соответствующие административные права. Если вы создаете новый лес доменов, то достаточно быть администратором на сервере, переводимом в разряд контроллера. Если же вы включаете контроллер в существующий лес, то нужно либо знать учетную запись и пароль с правами Enterprise Admins, либо вам должны быть делегированы права на включение контроллера домена в лес.

В-пятых, стоит понимать последствия выбора в одном из диалоговых окон DCPROMO одного из двух значений:

Permissions compatible with pre-Windows 2000 servers

или:

Permissions compatible only with Windows 2000 servers

Когда Active Directory будет установлена, в списки контроля доступа ко всем объектам каталога будет добавлена встроенная группа Pre-Windows 2000 Compatible Access. Если при установке контроллера вы указали первую возможность в рассматриваемом диалоговом окне (а она предлагается по умолчанию), то в группу Pre-Windows 2000 Compatible Access будет включена группа Everyone. Это значит, что не только аутентифицированные в домене пользователи получают доступ к объектам Active Directory, но и анонимные пользователи. Но не спешите переключать домен в режим Permissions compatible only with Windows 2000 servers. Возможно, в домене есть серверы Windows NT 4.0, на которых исполняются нужные вам приложения, требующие анонимного доступа к каталогу. Тогда придется оставить значение, по умолчанию. В последующем вы всегда можете добавить в группу Pre-Windows 2000 Compatible Access или исключить из нее группу Everyone.

Замечание Группу Even-one нельзя добавить (или исключить) в группу Pre-Windows 2000 Compatible Access через оснастку Active Directory Users and Computers. Используйте команду `net localgroup «Pre-Windows 2000 Compatible Access» everyone /add` для добавления и `net localgroup «Pre-Windows 2000 Compatible Access» everyone /remove` для удаления.

Наконец, вы должны представлять, какими ограничениями обладает Active Directory. Например, полное имя домена не может превышать 64 символов UTF-8. Скажем, вы хотите создать домен с именем (не улыбайтесь — чудак на свете полно):

```
Ust.uripinsk.filial.vostok.refinery.oil.windows2000.krasnoyarsk.mycorp.ru  
123456789012345678901234567890123456789012345678901234567890123
```

Для удобства снизу отмерено 64 символа. Понятно, что такое имя создать не удастся,

Но само по себе имя может и не быть очень длинным, но его длины хватит, чтобы для какого-либо ресурса превысить значение MAX_PATH, установленное равным 260 символам. Например, для доступа к хранилищу групповой политики используется путь:

```
\\имя_домена\sysvol\<имя_филиала>\Policies\<GUID>\<Машинное_имя_пользователя>\  
<путь_к_клиентскому_расширению_групповой_политики>
```

Чувствуете? Тут есть где развернуться.

Файлы, создаваемые при работе DCPROMO

Итак, как я уже говорил, при работе DCPROMO создается ряд файлов на локальных жестких дисках. Это файлы, обеспечивающие работу Active Directory, файлы и каталоги, обеспечивающие инфраструктуру и расположенные в иерархии SYSVOL, а также файлы журналов регистрации событий, возникающих при работе программы DCPROMO.

Файлы базы Active Directory

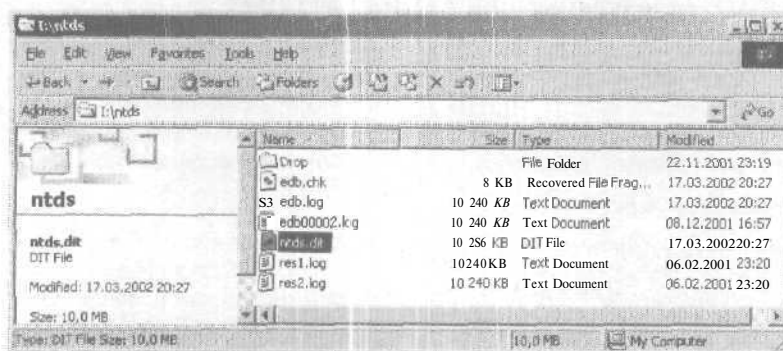
Файлы Active Directory по умолчанию предлагается хранить в каталоге WINNT\NTDS. Прямо скажем, не очень удачное место, но об этом потом. Сейчас же нас больше интересует, какие файлы там размещаются. Во-первых, это файл базы ActiveDirectory NTDS.DIT. Именно здесь хранится вся информация Active Directory. Если вы создаете новое дерево доменов, то его размер — 10 Мб. Обратите внимание и на файлы res1.log и res2.log. Пусть вас не вводит в заблуждение их расширение. К файлам журналов регистрации они не имеют никакого отношения. Они «оккупируют» место на жестком диске на тот случай, если файл Active Directory увеличится, а на диске не окажется свободного места. Тогда один из «оккупантов» будет удален, а NTDS.DIT вырастет

на его величину. Кстати, в журнал регистрации событий будет занесено соответствующее предупреждение. Размер этих двух файлов также равен 10 Мб, что дает запас 20 Мб для роста базы Active Directory.

Замечание Если обновляется контроллер домена Windows NT 4.0, то файл NTDS.DIT будет в несколько раз больше файла SAM. Ориентировочно можно полагать разницу в 10 раз.

Теперь займемся файлом `edb.log`. Это журнал транзакций Active Directory. Сюда заносятся все операции в базе. Его размер тоже 10 Мб. Если журнал переполняется, то он переименовывается в `edb00001.log`, а транзакции записываются в файл `edb.log`. Регистрация транзакций — весьма ответственный процесс. Очевидно, что выполнять запись в отложенном режиме рискованно, так как в случае непредвиденного краха системы информация о транзакциях будет потеряна. Именно поэтому при старте контроллера домена принудительно отключается кэширование записи для того диска, на котором расположены журналы транзакций. Речь идет о физическом (а не логическом диске). Если ОС или пользовательские файлы хранятся на том же физическом диске, что и журналы транзакций Active Directory, то производительность заметно снизится.

Замечание Снижение производительности на современных серверных системах наблюдается лишь при значительном числе пользователей.



Файлы, используемые при работе Active Directory

И еще один файл — `edb.chk`. Сюда заносятся контрольные точки БД. Они нужны для того, чтобы при необходимости повторно воспроизводить транзакции, занесенные в журнал. Допустим, произошел сбой системы. После перезагрузки происходит обращение к файлу `edb.chk` за информацией о последней контрольной точке, т. е. о последней

подтвержденной транзакции. Далее начинается повторение транзакций записанных в журнал сразу за контрольной точкой. Если бы контрольной точки не было, пришлось бы повторять все транзакции, сведения о которых занесены в журнал.

Обновление контрольной точки выполняется, если:

- накапливается необходимое количество изменений в базе, таких что не указывают назад на контрольную точку;
- завершается восстановление **базы**;
- выполняется корректный выход из системы.

Возможно, вы сталкивались с ситуацией, когда после аварийного завершения работы контроллера домена последующая загрузка выполняется гораздо дольше обычного. Это связано с тем, что система повторяет все транзакции от последней контрольной точки.

SYSVOL

Другой группой **файлов**, которые создаются в результате работы DCPROMO, является иерархическая структура SYSVOL. Подробнее об этой структуре мы поговорим в главах, посвященных репликации и групповой политике, а пока лишь коротко опишем структуру, так как по **правильности** ее создания можно оценить корректность установки контроллера домена.

Итак, на втором уровне иерархии располагаются четыре папки.

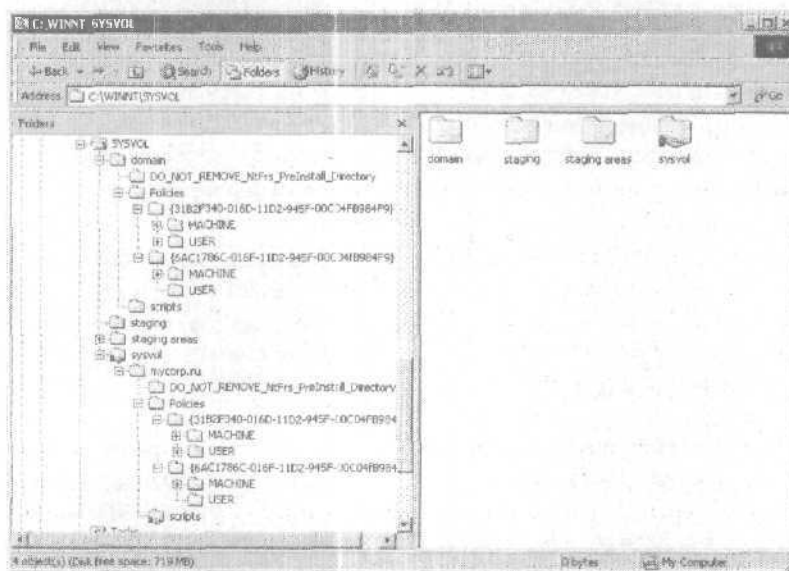
- ◆ Domain — здесь хранится **шаблон** структуры sysvol.
- Staging.
- ◆ Staging areas — как и предыдущая, требуется механизму репликации FRS (о них см. главу «Active Directory и файловая **система**»).
- ◆ Sysvol — предоставлена в совместное использование, содержит папку, соответствующую **домену**, которому принадлежит контроллер. В последней находятся следующие папки.
 - DO_NOT_REMOVE_NtFrs_PreInstall_Directory. (см. главу «Active Directory и файловая **система**».)
 - Policies. Здесь хранятся объекты групповых политик. Каждая политика хранится в виде папки с именем своего GUID, например {31B2F340-016D-11D2-945F-00C04FB984F9}. Сразу после установки нового контроллера домена создаются минимум две папки политик: для домена и для контроллеров домена. Если выполняется подключение к **домену**, в котором определено несколько дополнительных политик, то для каждой из них будут созданы свои папки.
 - Каждая папка политики содержит не менее двух папок. Обязательными являются MACHINE и USER, что, как ясно из их

названий, относится к правилам для компьютеров и пользователей. Дополнительно могут быть другие папки, например, Adm — место хранения административных шаблонов, используемых политиками.

- Scripts. Содержит файлы сценариев, используемых компьютерами пользователей. Эта папка также предоставлена в совместное использование.

Приведенная на рисунке структура SYSVOL соответствует первому контроллеру в домене. Если же вы добавляете контроллер к существующему домену, то структура может отличаться, но обязательно соответствовать структуре на остальных контроллерах.

Замечание При добавлении контроллера в домен структура SYSVOL появится не сразу, а лишь по завершении репликации. Обычно на это нужно около 10 минут, однако может продлиться дольше. Подробнее об этом см. статью Q250545 в Microsoft Knowledge base.



Структура SYSVOL

Журналы регистрации

Последними после работы DCPROMO появляются файлы регистрации выполнения этой программы и связанных с ней служб:

- DCPromoUI.log;
- DCPromo.log;
- Netsetup.log;
- DCPromos.log.

Все они находятся в каталоге %systemroot%\Debug. См. о них раздел «Анализируем журналы».

Служба синхронизации времени

Синхронизация по времени чрезвычайно важна для работы протокола аутентификации Kerberos. По умолчанию разница во времени между клиентом и сервером, превышающая 5 минут, делает аутентификацию невозможной. Именно поэтому в Windows 2000 реализована служба синхронизации времени (W32Time). Она полностью совместима с протоколом Simple Network Time Protocol (SNTP). Работает она так.

Для каждого компьютера есть свой эталон, с которым он сравнивает локальное время.

- ◆ Если при загрузке клиент обнаруживает, что его локальное время «отстает» от времени на эталоне, то его часы синхронизируются с часами эталона. Если же локальное время на клиенте опережает время на эталоне менее, чем на 2 минуты, то в течение последующих 20 минут локальные часы замедляются, а если опережение превышает 2 минуты, показания часов выравниваются сразу.
- ◆ Во время последующей работы выполняются периодические сверки времени с эталоном. Начальный интервал сверки составляет 8 часов. Если при сверке обнаруживается разница, превышающая 2 секунды, продолжительность интервала сокращается вдвое. Процесс повторяется при следующей сверке до тех пор, пока:
 - разница локального и эталонного времени не станет меньше 2 секунд

или:

- интервал сверки не уменьшится до своего минимального значения в 45 минут.

Если измеренная разница во времени меньше 2 секунд, интервал сверки увеличивается в двое. Максимальное значение интервала — 8 часов. Такое поведение установлено по умолчанию, но вы можете изменить его, используя параметры ветви реестра HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Parameters. Например, величину интервала сверки определяет параметр Period. Он может быть одного из двух типов: REG_DWORD или REG_SZ. Строковые переменные способны принимать только следующие значения:

Устанавливаемые интервалы сверки времени

Число	Строка	Описание
0		Раз в день
65535	BiDaily	Раз в два дня
65534	Tridaily	Раз в три дня
65533	Weekly	Раз в неделю
65532	SpecialSkew	Каждые 45 минут до достижения 3 последовательных удачных синхронизаций, затем каждые 8 часов
65531	DailySpecialSkew	Каждые 45 минут до достижения 1 удачной синхронизации, затем каждый день
число		Указанное число раз в день

Описание других параметров, влияющих на работу службы синхронизации времени, см. в Microsoft Knowledge Base в статье Q223184.

В рамках Active Directory существует однозначная иерархия, в соответствии с которой все компьютеры синхронизируют время. На нижней ступени — все клиентские настольные компьютеры. Для синхронизации своих часов они обращаются к тому контроллеру домена, на котором они авторизованы. Если в процессе работы выясняется, что данный контроллер домена больше недоступен, то выбирается новый контроллер. На этой же ступени в иерархии находятся и все серверы-члены домена.

Все контроллеры в домене синхронизируют свое время с тем контроллером, который выполняет роль имитатора главного контроллера домена (PDC).

В рамках всего леса доменов каждый из контроллеров, выполняющих роль имитатора главного контроллера, сверяет свое время с тем имитатором PDC, что стоит выше него в иерархии доменов Active Directory.

Главный авторитет — имитатор PDC в корневом домене. Он может сверять свое время с какой-либо эталонной службой либо сам с собой. Указать ему, с кем сверять время, позволяет команда:

```
Net time /setsntp:список серверов точного времени
```

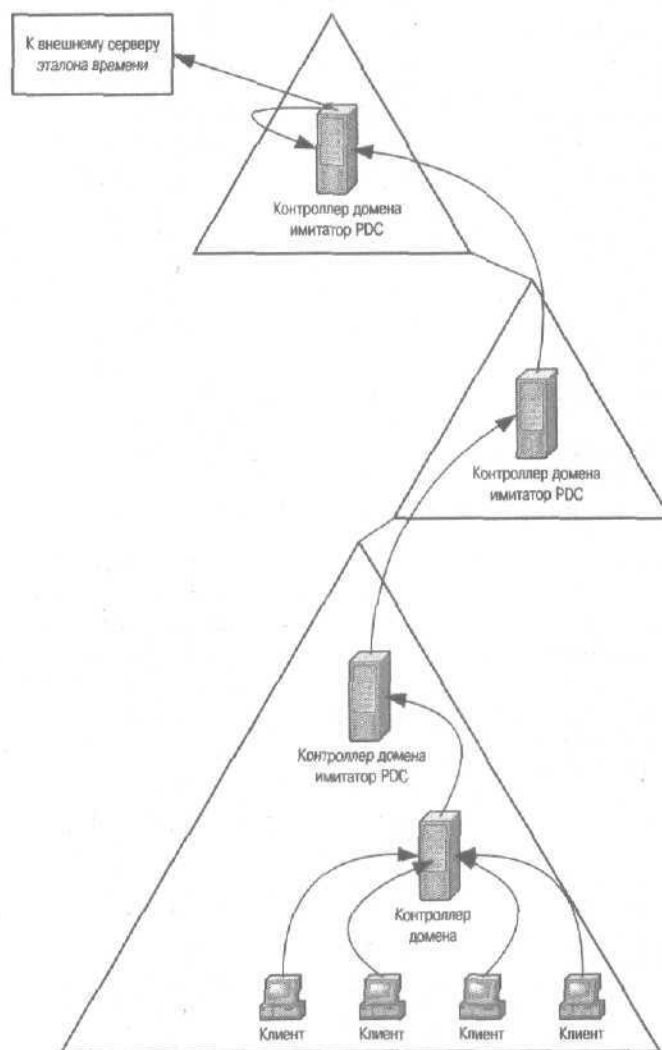
Можно, однако, установить имя сервера точного времени через реестр: в приведенной выше ветви измените значение параметра NtpServer. Не забудьте при этом в DNS указать запись для этого имени.

В качестве серверов точного времени можно использовать, например, серверы: ntp2.usno.navy.mil (192.5.41.209) или tock.usno.navy.mil (192.5.41.41).

Автоматическая установка контроллера

Не секрет, что контроллер домена можно установить, не только запустив DCPROMO в интерактивном режиме, требующем ответа на все

задаваемые вопросы, но и в автоматическом — когда ответы на все вопросы записаны в файле ответов. Этот способ удобен при установке большого числа контроллеров в домене, а также при выполнении автоматического обновления контроллеров домена Windows NT.



Иерархия службы синхронизации времени

Запускает программу в таком режиме команда:

```
Dcprmo /answer: имя_файла_ответов
```

В зависимости от типа контроллера домена [новое дерево в новом лесу, новый контроллер домена в существующем домене (или обновление контроллера Windows NT), новый дочерний домен, новое дерево в лесу], а также при понижении контроллера домена до статуса сервера в файле ответов используются различные параметры. Все они должны входить в секцию файла [DCINSTALL]. Рассмотрим эти параметры для каждого из типов установки контроллера. Если какой-то параметр не определен, то используются его значения по умолчанию (см. далее таблицу).

Новое дерево в новом лесу

```
[DCINSTALL]
ReplicaOrNewDomain=Domain
TreeOrChild=Tree
CreateOrJoin=Create
NewDomainDNSName=<полное имя домена (например мусогр.ru) >
DNSOnNetwork=yes
DomainNetbiosName=<Netbios имя домена>
AutoConfigDNS=yes
SiteName=[имя сайта Active Directory (факультативно)];
AllowAnonymousAccess=no
DatabasePath=%systemroot%\ntds (или иное место размещения файла
NTDS.DIT)
LogPath=%systemroot%\ntds (или иное место размещения файла EDB.LOG)
SYSVOLPath=%systemroot%\sysvol (или иное место размещения корня
SYSVOL)
SafeModeAdminPassword=<пароль администратора для входа в режим
остановления Active Directory>
CriticalReplicationOnly=No
RebootOnSuccess=yes
```

Дополнительный контроллер в домене

```
[DCINSTALL]
UserName=<учетная запись администратора в домене>
Password=<пароль>
UserDomain=<имя домена>
DatabasePath=%systemroot%\ntds (или иное место размещения файла
NTDS.DIT)
LogPath=%systemroot%\ntds (или иное место размещения файла EDB.LOG)
SYSVOLPath=%systemroot%\sysvol (или иное место размещения корня
SYSVOL)
SafeModeAdminPassword=<пароль администратора для входа в режим
восстановления Active Directory>
```

```

CriticalReplicationOnly=no
ReplicaOrNewDomain=Replica
ReplicaDomainDNSName=<полное имя домена Active Directory>
ReplicationSourceDC=<имя домена-источника репликации>
RebootOnSuccess=yes

```

Новый дочерний домен

```

[DCINSTALL]
UserName
Password
UserDomain
DatabasePath
LogPath
SYSVOLPath
SafeModeAdminPassword=<пароль администратора для входа в
    режим восстановления Active Directory>
CriticalReplicationOnly=no
ReplicaOrNewDomain=Domain
TreeOrChild=Child
ParentDomainDNSName
ChildName
DomainNetbiosName
AutoConfigDNS
AllowAnonymousAccess
RebootOnSuccess=yes

```

Новое дерево в лесу

```

[DCINSTALL]
UserName
Password
UserDomain
DatabasePath
LogPath
SYSVOLPath
SiteName
SafeModeAdminPassword=<пароль администратора для входа в режим
    восстановления Active Directory>
CriticalReplicationOnly=no
ReplicaOrNewDomain=Domain
TreeOrChild=Tree
NewDomainDNSName
DomainNetbiosName
AutoConfigDNS
AllowAnonymousAccess
RebootOnSuccess=yes

```

Понижение контроллера домена до уровня сервера

```
[DCINSTALL]
UserName
Password
UserDomain
AdministratorPassword
IsLastDCInDomain
RebootOnSuccess=yes
```

Описание параметров и значений умолчания

В таблице описаны параметры **используемые** в файле ответов, и значения, присваиваемые им по умолчанию.

Параметр	Возможные значения (умолчание выделено)	Описание
AllowAnonymousAccess	Yes/No	Разрешен ли анонимный доступ к объектам Active Directory. См. «Требования, предъявляемые DCPromo»
AdministratorPassword	Нет умолчания	Пароль локального администратора, устанавливаемый при понижении статуса контроллера до сервера
AutoConfigDNS	Yes/No	Указывает, конфигурировать ли сервер DNS на локальном компьютере
CbildName	Нет умолчания	Имя дочернего домена, подключаемого к родительскому. Указывается только короткое имя (до точки)
CreateOrJoin	Create/Join	Create используется при создании нового леса, Join — при создании нового дерева в существующем лесу
CriticalReplicationOnly	Yes/	Yes — репликация критичных параметров выполняется до перезагрузки компьютера. Если ничего не указано, она выполняется после перезагрузки
DatabasePath	%systemroot%\ntds	Имя каталога, в котором размещается файл базы Active Directory. См. «Файлы базы Active Directory». Имя должно быть полностью определенным <i>не</i> в стандарте UNC

см. след. стр.

Параметр	Возможные значения (умолчание выделено)	Описание
DomainNetbiosName	Нет умолчания	NetBIOS-имя домена, используемое клиентами прежних версий Windows или DOS
DNSOnNetwork	Yes/No	Yes подразумевает, что клиент DNS может быть сконфигурирован и допускается автоконфигурация.
IsLastDCInDomain	Yes/No	Указывает, является ли данный контроллер последним в домене при понижении статуса до сервера
LogPath	%systemroot%\ntds	Имя каталога, в котором размещаются файлы журнала транзакций Active Directory. См. «Файлы базы Active Directory». Имя должно быть полностью определено не в стандарте UNC
NewDomainDNSName	Нет умолчания	Имя домена при создании нового леса или нового дерева
Password	Нет умолчания	Пароль учетной записи, используемой для создания контроллера домена. Всякий раз по завершении работы DCPROMO пароль удаляется из файла ответов
ParentDomainDNSName	Нет умолчания	Имя родительского домена при создании дочернего.
RcbootOnSuccess	Yes/No	Yes указывает на необходимость перезагрузки компьютера в случае удачного завершения работы DCPROMO
ReplicaDomainDNSName	Нет умолчания	Имя домена, из которого должна выполняться репликация при установке дополнительного контроллера или обновлении домена Windows NT
ReplicaOrMember	Replica Member	Replica используется при обновлении контроллера домена Windows NT до Windows 2000, Member - при понижении статуса контроллера до сервера <i>см. след. стр.</i>

Параметр	Возможные значения (умолчение выделено)	Описание
ReplicaOrMember	Replica Member	Replica используется при обновлении контроллера домена Windows NT до Windows 2000, Member - при понижении статуса контроллера до сервера
ReplicaOrNewDomain	Domain Replica	Domain используется при создании нового домена, Replica — при добавлении контроллера в существующий домен
ReplicationSourceDC	Нет умолчания	Указывается имя контроллера домена, с которого должна тиражироваться реплика. Если ничего не указано, используется ближайший контроллер в домене
SafeModeAdminPassword	Нет умолчания	Устанавливает пароль администратора для входа в режим восстановления Active Directory
SiteName	Default-First-Site	Имя сайта, в который будет включен контроллер домена. Если ничего не указано, сайт будет подобран, исходя из конфигурации сайтов и подсетей. Если же это новый лес, создается сайт с именем по умолчанию
SYSVOLPath	%systemroot%\ SYSVOL	Путь к каталогу SYSVOL. См. «Файлы базы Active Directory». Путь должен быть полностью определен не в стандарте UNC
TreeOrChild	Tree Child	Tree указывает на создание нового дерева. Child — на создание дочернего домена
UserDomain	См. описание	Имя учетной записи для выполнения операции. Если это создание леса, значений по умолчанию нет. Если это добавление новой дерева, по умолчанию используется имя леса. Если это создание дочернего домена или добавление

см. след. стр.

Параметр	Возможные значения (умолчание выделено)	Описание
UserName	Нет умолчания	контроллера в существующий домен, это имя домена, к которому присоединяются Имя учетной записи, используемой для выполнения операции

Анализируем журналы

Программа DCPROMO создает отчет о своей работе в виде целого набора журналов. Поскольку в случае нештатной ситуации при установке контроллера домена придется воспользоваться ими для выявления причин, ознакомимся с их содержанием.

DCPromo.log

Файл DCPromo.log содержит информацию о параметрах, выбранных пользователем в процессе работы мастера, а также сведения о его работе. Взгляните на выдержку из этого файла:

```
03/22 13:25:55 [INFO] Promotion request for domain controller of new domain
03/22 13:25:55 [INFO] DnsDomainName msk.mycorp.ru
03/22 13:25:55 [INFO] FlatDomainName MSK
03/22 13:25:55 [INFO] SiteName (NULL)
03/22 13:25:55 [INFO] SystemVolumeRootPath C:\WINNT\SYSVOL
03/22 13:25:55 [INFO] DsDatabasePath C:\WINNT\NTDS, DsLogPath
C:\WINNT\NTDS
03/22 13:25:55 [INFO] ParentDnsDomainName mycorp.ru
03/22 13:25:55 [INFO] ParentServer (NULL)
03/22 13:25:55 [INFO] Account mycorp.ru\administrator
03/22 13:25:55 [INFO] Options 196
03/22 13:25:55 [INFO] Validate supplied paths
03/22 13:25:55 [INFO] Validating path C:\WINNT\NTDS.
03/22 13:25:55 [INFO] Path is a directory
03/22 13:25:55 [INFO] Path is on a fixed disk drive,
03/22 13:25:55 [INFO] Validating path C:\WINNT\NTDS.
03/22 13:25:55 [INFO] Path is a directory
03/22 13:25:55 [INFO] Path is on a fixed disk drive.
03/22 13:25:55 [INFO] Validating path C:\WINNT\SYSVOL.
03/22 13:25:55 [INFO] Path is on a fixed disk drive.
03/22 13:25:55 [INFO] Path is on an NTFS volume
03/22 13:25:55 [INFO] Child domain creation - check the new domain name
is child of parent domain name.
03/22 13:25:55 [INFO] Domain Creation - check that the flat name is unique.
03/22 13:26:03 [INFO] Start the worker task
```

```
03/22 13:26:03 [INFO] Request for promotion returning 0
03/22 13:26:03 [INFO] No source DC or no site name specified. Searching
                        for dc in domain mycorp.ru: { DS_REQUIRED | WRITABLE }
03/22 13:26:03 [INFO] Searching for a domain controller for the domain
                        mycorp.ru
03/22 13:26:03 [INFO] Located domain controller mycorp.ru for domain (null)
03/22 13:26:03 [INFO] No user specified source DC
03/22 13:26:03 [INFO] No user specified site
03/22 13:26:03 [INFO] Using site Default-First-Site-Name for server
                        mycorp.ru
03/22 13:26:03 [INFO] Forcing a time synch with \\ROOT1.mycorp.ru
03/22 13:26:05 [INFO] Reading domain policy from the domain controller
                        \\ROOT1.mycorp.ru
03/22 13:26:05 [INFO] Stopping service NETLOGON
03/22 13:26:05 [INFO] Stopping service NETLOGON
03/22 13:26:05 [INFO] Configuring service NETLOGON to 1 returned 0
03/22 13:26:05 [INFO] Creating the System Volume C:\WINNT\SYSVOL
03/22 13:26:05 [INFO] Deleting current sysvol path C:\WINNT\SYSVOL
03/22 13:26:06 [INFO] Preparing for system volume replication using
                        root C:\WINNT\SYSVOL
03/22 13:26:06 [INFO] Copying initial Directory Service database file
                        C:\WINNT\system32\ntds.dit to C:\WINNT\NTDS\ntds.dit
03/22 13:26:09 [INFO] Installing the Directory Service
```

Записи предельно лаконичны. На мой взгляд, именно этот файл следует использовать в первую очередь при возникновении проблем.

Совет Если среди строк в этом журнале вы обнаружите что-то вроде [INFO] NtdsInstall for msk.mycorp.ru returned 1396, то дайте команду net helpmsg <номер> (к рассматриваемом примере 1396) для получения подробных сведений об ошибке.

Если приводимой в этом файле информации окажется недостаточно для выявления проблемы, можно обратиться к файлу DCPromoUI.log.

DCPromoUI.log

В файле DCPromoUI.log приведен подробнейший отчет обо всех действиях пользователя в DCPROMO, а также все действия этой программы. Запись начинается сразу после старта мастера и заканчивается по завершении. Если работа мастера завершилась неудачей, дается подробное описание сообщений об ошибках, приведших к неудаче. О степени подробности регистрации вы можете судить по выдержкам из этого файла.

Вот так регистрируется начало работы программы:

```

dcpromoui t:0x42C 00000 opening log file C:\WINNT\debug\dcpromoui.log
dcpromoui t:0x42C 00001 03/22/2002 13:24:14.0787
dcpromoui t:0x42C 00002 running Windows NT 5.0 build 2195 Service Pack 2
dcpromoui t:0x42C 00003 logging mask 0038
dcpromoui t:0x42C 00004 no options specified
dcpromoui t:0x42C 00005 Enter Computer::Initialize MID1
dcpromoui t:0x42C 00006 Enter MyDsRoleGetPrimaryDomainInformation
dcpromoui t:0x42C 00007 Enter yDsRoleGetPrimaryDomainInformationHelper
dcpromoui t:0x42C 00008 Calling DsRoleGetPrimaryDomainInformation
dcpromoui t:0x42C 00009 lpServer : (null)
dcpromoui t:0x42C 00010 InfoLevel : 0x1
                        (DsRolePrimaryDomainInfoBasic)
dcpromoui t:0x42C 00011 Error 0x0 (10 => error)
dcpromoui t:0x42C 00012 Exit MyDsRoleGetPrimaryDomainInformationHelper
dcpromoui t:0x42C 00013 MachineRole : 0x2
dcpromoui t:0x42C 00014 Flags : 0x0
dcpromoui t:0x42C 00015 DomainNameFlat: WORKGROUP
dcpromoui t:0x42C 00016 DomainNameDns : (null)
dcpromoui t:0x42C 00017 DomainForestName: (null)
dcpromoui t:0x42C 00018 Exit MyDsRoleGetPrimaryDomainInformation

Далее проверяется, сконфигурирован ли сервер DNS:
dcpromoui t:0x42C 00241 Enter ConfigureDNSClientPage::OnSetActive
dcpromoui t:0x42C 00242 Enter DNS::IsClientConfigured
dcpromoui t:0x42C 00243 Calling DnsQuery
dcpromoui t:0x42C 00244 IpstrName : 1.0.0.127.in-addr.arpa
dcpromoui t:0x42C 00245 wType : DNS_TYPE_PTR
dcpromoui t:0x42C 00246 fOptions : DNS_QUERY_BYPASS_CACHE
dcpromoui t:0x42C 00247 aipServers : 0
dcpromoui t:0x42C 00248 ppQueryResultsSet : 0x6F384
dcpromoui t:0x42C 00249 pReserved : 0
dcpromoui t:0x42C 00250 Result 0x0
dcpromoui t:0x42C 00251 ERROR_SUCCESS
dcpromoui t:0x42C 00252 DNS client is configured
dcpromoui t:0x42C 00253 Exit DNS::IsClientConfigured
dcpromoui t:0x42C 00254 planning to Skip Configure DNS Client
                        page
dcpromoui t:0x42C 00255 Enter ConfigureDNSClientPage::Validate
dcpromoui t:0x42C 00256 Enter DNS::IsClientConfigured
dcpromoui t:0x42C 00257 Calling DnsQuery
dcpromoui t:0x42C 00258 IpstrName : 1.0.0.127.in-addr.arpa
dcpromoui t:0x42C 00259 wType : DNS_TYPE_PTR
dcpromoui t:0x42C 00260 fOptions : DNS_QUERY_BYPASS_CACHE
dcpromoui t:0x42C 00261 aipServers : 0

```

```

dcpromoui t:0x42C 00262
dcpromoui t:0x42C 00263
dcpromoui t:0x42C 00264
dcpromoui t:0x42C 00265
dcpromoui t:0x42C 00266
dcpromoui t:0x42C 00267

```

Теперь ищем корневой домен и:

Enter getForestName mycorp.ru

```

dcpromoui t:0x42C 00307
dcpromoui t:0x42C 00308
dcpromoui t:0x42C 00309
dcpromoui t:0x42C 00310
dcpromoui t:0x42C 00311
dcpromoui t:0x42C 00312
dcpromoui t:0x42C 00313
dcpromoui t:0x42C 00314

```

```
dcpromoui t:0x42C 00315
```

```
dcpromoui t:0x42C 00316
```

```
dcpromoui t:0x42C 00317
```

```
dcpromoui t:0x42C 00318
```

Проверяется, не используется ли уже имя **ДОМЕНА**, которое вы ввели в диалоговом окне:

```

dcpromoui t:0x42C 00483
dcpromoui t:0x42C 00484
dcpromoui t:0x42C 00485
dcpromoui t:0x42C 00486
dcpromoui t:0x42C 00487
dcpromoui t:0x42C 00488
dcpromoui t:0x42C 00489
dcpromoui t:0x42C 00490

```

```
dcpromoui t:0x42C 00491
```

```
dcpromoui t:0x42C 00492
```

```
dcpromoui t:0x42C 00493
```

```
dcpromoui t:0x42C 00494
```

```
dcpromoui t:0x42C 00495
```

А вот сообщение об успешном завершении:

```
dcpromoui t:0x42C 01269
```

```
dcpromoui t:0x42C 01270
```

```

ppQueryResultsSet : 0x6F30C
pReserved          : 0
Result 0x0
ERROR_SUCCESS
DNS client is configured
Exit DNS::IsClientConfigured

```

```

Enter myDsGetDcName
Calling DsGetDcName
ComputerName : (null)
DomainName   : mycorp.ru
DomainGuid   : (null)
SiteGuid     : (null)
Flags        : 0x40000000
DomainControllerName :
\\ROOT1.mycorp.ru
DomainControllerAddress :
\\10.1.2.1
DomainGuid :
{72B484AC-F61D-4E7B-8A1E-E8CA284DDAE5}
DomainName   : mycorp.ru
DnsForestName : mycorp.ru

```

Enter DS::IsDomainNameInUse

Enter myNetValidateName

Calling NetValidateName

lpServer ; (null)

lpName : msk.mycorp.ru

lpAccount : (null)

lpPassword : (null)

NameType :

NetSetupNonExistentDomain

Error 0x0 (!0 => error)

Exit myNetValidateName

The domain name msk.mycorp.ru is
NOT in use.

Exit DS::IsDomainNameInUse

Exit ValidateDomainDoesNotExist

Enter getCompletionMessage

Enter State::GetOperation CHILD

```

dcpromoui t:0x42C 01271      Exit  State::GetOperation CHILD
dcpromoui t:0x42C 01272      Enter State::GetOperationResultsCode
                              SUCCESS
dcpromoui t:0x42C 01273      Exit  State::GetOperationResultsCode
                              SUCCESS
dcpromoui t:0x42C 01274      Enter State::GetNewDomainDNSName
                              msk.mycorp.ru
dcpromoui t:0x42C 01275      Exit  State::GetNewDomainDNSName
                              msk.mycorp.ru
dcpromoui t:0x42C 01276      Enter State::GetInstalledSite
                              Default-First-Site-Name
dcpromoui t:0x42C 01277      Exit  State::GetInstalledSite
                              Default-First-Site-Name
dcpromoui t:0x42C 01278      Enter State::GetFinishMessages
dcpromoui t:0x42C 01279      Exit  State::GetFinishMessages
dcpromoui t:0x42C 01280      Exit  getCompletionMessage
dcpromoui t:0x42C 01281      Exit  FinishPage::OnSetActive
dcpromoui t:0x42C 01282      Enter  FinishPage::OnWizFinish
dcpromoui t:0x42C 01283      Exit  FinishPage::OnWizFinish
dcpromoui t:0x42C 01284      Exit  Wizard::ModalExecute
dcpromoui t:0x42C 01285      Enter  Dialog::ModalExecute
dcpromoui t:0x42C 01286      Exit  Dialog::ModalExecute
dcpromoui t:0x42C 01287      Enter  Reboot
dcpromoui t:0x42C 01288      OpenProcessToken
dcpromoui t:0x42C 01289      LookupPrivilegeValue
dcpromoui t:0x42C 01290      AdjustTokenPrivileges
dcpromoui t:0x42C 01291      ExitWindowsEx
dcpromoui t:0x42C 01292      Exit  Reboot
dcpromoui t:0x42C 01293      Exit  doWizard
dcpromoui t:0x42C 01294      Exit  doIt
dcpromoui t:0x42C 01295      closing log file

```

Просмотрев весь этот файл, вы выясните имя контроллера домена — источника репликации, разделы каталога, реплицированные на сервер, число элементов, реплицированных для каждого из разделов в каталоге, имена сконфигурированных служб, списки контроля доступа к ресурсам сервера, модифицированные в процессе исполнения программы, каталоги SYSVOL, сообщения об ошибках. Короче, изучение этого файла даст вам больше, чем чтение многих умных книг.

В начале файла вы увидите фразу `Loggin mask`. Эта маска устанавливает степень детализации файла. Она задается соответствующим параметром в реестре. Он находится в ветви `HKLM\Software\Microsoft\Windows\CurrentVersion\AdminDebug` и называется `DCPROMOUI`. Значение маски устанавливается побитово в соответствии со следующей таблицей:

**Управление степенью подробности регистрации
в журнале DCPromoUI.log**

Старший байт

0x0002	Отслеживание вызовов конструкторов и деструкторов
0x0004	Отслеживание вызовов AddRef и Release
0x0008	Отслеживание входа и выхода в функции
0x0010	Выводить сообщения трассировки
0x0020	Выводить заголовок со временем создания
0x0040	Перехватывать обращения к стеку при вызове оператора New

Младший байт

0x0001	Вывод в файл
0x0002	Вывод в отладчик

Netsetup.log

Файл **Netsetup.log** записывается во время работы программы **Netsetup**, вызываемой в данном случае для установки нужных сетевых компонентов. В следующем фрагменте файла зарегистрировано включение компьютера DC01 в домен **fyodor.home**. Контроллер домена, на котором выполняются проверки, называется **ETA**.

```
03/17 20:53:53 NetpDoDomainJoin
03/17 20:53:53 NetpMachineValidToJoin: 'DC01'
03/17 20:53:53 NetpGetLsaPrimaryDomain: status: 0x0
03/17 20:53:53 NetpMachineValidToJoin: status: 0x0
03/17 20:53:53 NetpJoinDomain
03/17 20:53:53 Machine: DC01
03/17 20:53:53 Domain: fyodor.home\ETA.fyodor.home
03/17 20:53:53 MachineAccountOU: (NULL)
03/17 20:53:53 Account: fyodor.home\administrator
03/17 20:53:53 Options: 0x27
03/17 20:53:53 OS Version: 5.0
03/17 20:53:53 Build number: 2195
03/17 20:53:53 ServicePack: Service Pack 2
03/17 20:53:53 NetpValidateName: checking to see if 'fyodor.home'
                        is valid as type 3 name
03/17 20:53:53 NetpCheckDomainNameIsValid [ Exists ] for
                        'fyodor.home' returned 0x0
03/17 20:53:53 NetpValidateName: name 'fyodor.home' is valid for type 3
03/17 20:53:53 NetpJoinDomain: status of connecting to dc
                        '\\ETA.fyodor.home': 0x0
03/17 20:53:53 NetpJoinDomain: Passed DC '\\ETA.fyodor.home' verified
                        as DNS name '\\ETA.fyodor.home'
03/17 20:53:53 NetpGetLsaPrimaryDomain: status: 0x0
03/17 20:53:53 NetpGetNt4RefusePasswordChangeStatus: trying to read
```



```

                                from '\\ETA.fyodor.home'
03/17 20:53:54 NetpGetNt4RefusePasswordChangeStatus: failed but
                                ignored the failure: 0x2
03/17 20:53:54 NetpLsaOpenSecret: status: 0xc0000034
03/17 20:53:54 NetpGetLsaPrimaryDomain: status: 0x0
03/17 20:53:54 NetpLsaOpenSecret: status: 0xc0000034
03/17 20:53:57 NetpJoinDomain: status of creating account: 0x0
03/17 20:53:57 NetpJoinDomain: status of setting netlogon cache: 0x0
03/17 20:53:57 NetpGetLsaPrimaryDomain: status: 0x0
03/17 20:53:57 NetpSetLsaPrimaryDomain: for 'FYODOR' status: 0x0
03/17 20:53:57 NetpJoinDomain: status of setting LSA pri. domain: 0x0
03/17 20:53:57 NetpJoinDomain: status of managing local groups: 0x0
03/17 20:53:57 NetpJoinDomain: status of setting
                                ComputerNamePhysicalDnsDomain to 'fyodor.home': 0x0
03/17 20:53:57 NetpJoinDomain: status of starting Netlogon: 0x0
03/17 20:53:57 NetpWaitForNetlogonSc: waiting for netlogon secure
                                channel setup...
03/17 20:53:58 NetpWaitForNetlogonSc: status: 0x0, sub-status: 0x0
03/17 20:53:58 NetpJoinDomain: status of disconnecting from
                                '\\ETA.fyodor.home': 0x0
03/17 20:53:58 NetpDoDomainJoin: status: 0x0

```

DCPromos.log

Файл DCPromos.log создается, только если выполняется обновление контроллера домена Windows NT до Windows 2000. Он содержит данные о работе графической части программы установки.

Как подобрать компьютер?

О выборе подходящей конфигурации спрашивают довольно часто. Никому уже не надо говорить, что выбирать технику надо, посоветовавшись со списком совместимого оборудования (<http://www.micro-soft.com/hcl/>). Это и так все знают. (Другое дело, что многие просто игнорируют этот список, так как используют не то, что нужно, а то, что у них есть, или то, что в состоянии купить). Большинство знакомо и с минимальными требованиями, предъявляемыми к серверной конфигурации Windows 2000.

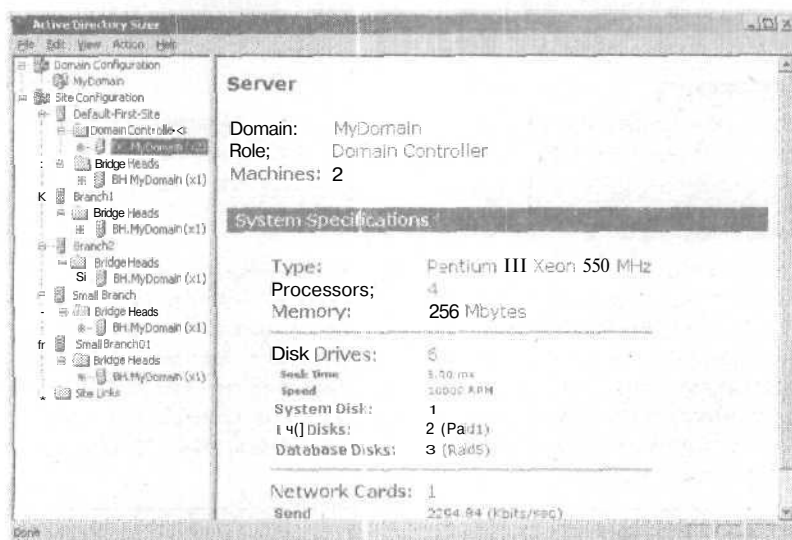
Контроллер домена на базе	Процессор:	Pentium 133 и выше
Windows 2000 Server	Оперативная память;	160 Мб
	Объем жесткого диска:	1 Гб

Думаю, никому, кто находится в здравом уме и ясной памяти, не придет в голову использовать минимальную конфигурацию в производственной системе. Но при всем том готового ответа на вопрос, какую конфигурацию использовать, дать нельзя. Все зависит от массы условий.

Если вы не готовы к самостоятельной оценке требуемых ресурсов, воспользуйтесь программой Active Directory Sizer, которая в первом приближении поможет оценить как количество компьютеров, так и их назначение и конфигурацию.

Совет Значения, полученные с помощью AD Sizer, довольно приближительны и могут как завышать, так и занижать конфигурацию. Поэтому используйте ее для первых прикидок, а точные расчеты делайте на основании рекомендаций, приведенных ниже.

Допустим, вы хотите рассчитать, сколько контроллеров домена и какой конфигурации вам понадобится для построения сети в организации, состоящей из головного офиса и 4 филиалов. Общее количество пользователей — 1 000, каждый работает на своем компьютере. В двух филиалах работает по 100 пользователей, а в оставшихся — по 10. На 50% компьютеров стоит Windows 2000, а на оставшихся — Windows 9x. В центральном офисе есть 20 серверов Windows 2000, на которых установлены приложения. В качестве почтовой системы используется Microsoft Exchange 5-5. Запустите программу и подсчитайте результат.



Окно Active Directory Sizer

Думаю, он вас удивит. И удивление будет как приятным, так и неприятным. Судите сами.

В центральном офисе надо установить 3 контроллера домена, один из которых будет выделенным сервером-форпостом и ГК. Если вы

хорошо знакомы с тем, как работает генератор топологии межсайтовой репликации (ISTG), то поймете, что либо надо добавить еще один сервер-форпост, либо держать работу КСС под постоянным контролем.

Конфигурация этих серверов видна на рисунке. Это, конечно, уже и не минимальные требования, но объем оперативной памяти у меня вызывает сомнения. Маловато будет! Попробуем поменять начальные значения и посмотрим, как на это отреагирует программа. Допустим, работа с Active Directory ведется весьма интенсивно, а именно в час пик до 100 пользователей в секунду регистрируется в домене интерактивно, по сети и как пакетные задания. Плюс к этому пусть каждый день администратор добавляет, удаляет и модифицирует по 5 учетных записей. Ну и, наконец, некоторые приложения, работающие с Active Directory, выполняют по 5 операций поиска, удаления, добавления и модификаций в секунду. Результат будет неожидан. Вам будет предложено дополнительно установить в центральном офисе еще 3 контроллера домена, 2 сервера ГК и 1 сервер-форпост (если вы догадаетесь добавить еще одну межсайтовую связь). И все эти серверы — в показанной конфигурации.

В двух малых офисах устанавливать контроллер домена нецелесообразно, так как там всего 10 пользователей, однако программа настойчиво советует это сделать. Исключая соответствующие компьютеры из списка, вы немного скрасите горечь предстоящих затрат.

Как видите, на результат расчетов влияет множество факторов. Попробуем их рассмотреть.

Требования к процессору

К процессору можно подойти с позиции «чем больше, тем лучше», однако следует всегда руководствоваться принципом разумной достаточности. Зачем гнаться за самым последним типом процессора с самой высокой тактовой частотой? Роль процессора зависит от степени загрузки контроллера домена, на которую в свою очередь влияют:

- ◆ наличие на контроллере мастеропераций, особенно имитатора PDC;
- наличие на контроллере дополнительных сетевых служб, таких как DNS, DHCP, WINS;
- ◆ выполнение контроллером функции выделенного сервера-форпоста;
- интенсивность внесения изменений в Active Directory;
- интенсивность регистрации в пиковые часы.

Служба Microsoft Consulting Services опубликовала интересный документ, в котором на основании тестов оцениваются аппаратные требования к контроллерам доменов. В таблице приведены результаты измерения количества пользователей, зарегистрировавшихся интерактив-

но за разные периоды времени. Измерения проводились на машинах с разным числом процессоров PIII Хеоп 500 МГц и объемом ОЗУ 512 Мб.

**Количество пользователей,
зарегистрировавшихся интерактивно**

Количество процессоров	1	2	4
1 минута	1 200-1 800	1 800-3 000	2 400-4 200
5 минут	6 000-9 000	9 000-15 000	12 000-21 000
10 минут	12 000-18 000	18 000-30 000	24 000-42 000

10 минут — это разумное время регистрации пользователей. (Трудно представить, что 15 000 пользователей захотят зарегистрироваться в сети в течение 1 минуты). Поэтому, если в организации всего 2-3 тысячи пользователей, их регистрацию вполне может обслужить один контроллер с одним процессором указанного типа.

Следующий тест учитывал членство пользователей в группах. В таблице показана зависимость скорости регистрации пользователей (регистрации в секунду) от числа процессоров и количества групп.

**Количество регистрации в секунду
при членстве пользователей в разном числе групп**

Количество процессоров	1	2	4
10 групп	19-28	28-47	39-68
20 групп	17-25	25-42	36-63
30 групп	16-24	23-40	34-60

Таким образом, представленные таблицы позволяют оценить требования к количеству процессоров с точки зрения скорости регистрации пользователей.

На количество процессоров влияет еще один фактор — выполнение компьютером функций сервера-форпоста. В нагруженных системах, когда на один форпост приходится несколько партнеров по репликации, большое значение имеет скорость выполнения репликаций. Дело в том, что, когда на всех партнерах произошли изменения в каталоге и они оповестили сервер-форпост об этом, он должен за отведенный период времени опросить по очереди каждый из контроллеров-партнеров и принять сведения о репликации. Если он не успеет это сделать в отведенное время, то захватит следующий период, препятствуя тем самым репликации новых изменений, накопившихся на контроллерах-партнерах за данное время. Это приводит к росту очереди репликации. Поэтому надо либо увеличивать количество серверов-форпостов, либо увеличивать производительность имеющегося. Справедливости ради замечу, что производительность в такой ситуации может ограничиваться уже не количеством процессоров, а пропускной способностью сетевой платы.

Требования к оперативной памяти

Объем оперативной памяти на контроллерах домена зависит от таких факторов.

- ◆ Объем базы Active Directory. В идеале при работе вся база должна размещаться в ОЗУ. Хотя начальный объем базы всего 10 Мб, после добавления пользователей и интенсивной работы он может составить 250 Мб, и это не предел. Если зоны DNS интегрированы с Active Directory, то это дополнительный вклад в объем базы.
- Является ли контроллер сервером ГК. Хотя ГК занимает и не такое пространство, как база домена, но при большом числе доменов и пользователей он может вносить в них существенный вклад.

В упоминавшемся тестировании была измерена зависимость скорости выполнения LDAP-запросов к серверу ГК от количества объектов в нем и от объема оперативной памяти:

Количество обработанных LDAP-запросов (компьютер с 2 процессорами PIII-Xeon)

Скорость посылаемых запросов (в секунду)	130	260	390	520	650	780
Количество запросов, обработанных ГК (запр./сек)						
200 000 объектов, ОЗУ 512 Мб	130	260	390	520	613	610
400 000 объектов, ОЗУ 512 Мб	130	260	380	375	377	377
400 000 объектов, ОЗУ 1 Гб	130	260	390	520	650	705

Хорошо видно, что при памяти 512 Мб и 400 000 объектов ГК достигает насыщения производительности всего при 390 поступающих запросах в секунду. Увеличение объема ОЗУ в два раза поднимает планку насыщения также вдвое.

- Выполняются ли на сервере такие службы, как WINS, DNS, DHCP. Эти службы имеют собственные базы, хранимые в кэше. Объем баз опять-таки зависит от количества компьютеров в сети.

Например, в уже упоминавшемся выше тесте исследовался компьютер, игравший только роли контроллера домена и сервера DNS. С этой целью был взят компьютер Compaq Proliant 6500 с 4 процессорами Pentium III Xeon — 500, ОЗУ — 1 Гб, подключенный к сети Fast Ethernet 100 Мб в полнодуплексном режиме. Результаты тестирования:

- максимальная скорость динамических регистраций (в секунду) — 199;
- максимальная скорость динамических удалений (в секунду) — 200;
- ◆ максимальное число обработанных запросов (в секунду) — 852.

При этом загруженность процессоров не превысила 25%.

Конфигурация жестких дисков

О конфигурировании дисковой подсистемы написано много: назову хотя бы [8] и справку к Windows 2000. Поэтому я просто приведу типовые конфигурации, прошедшие проверку в боевых условиях.

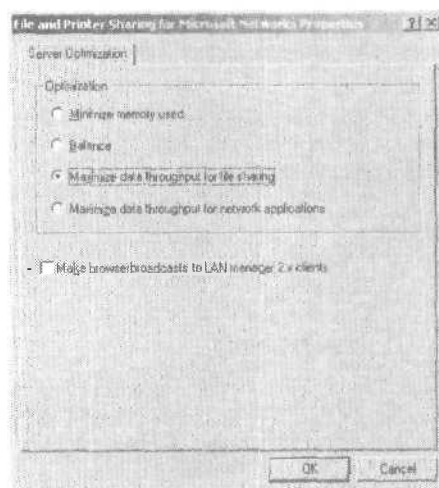
1. Тестовая конфигурация или небольшая организация (до 20 пользователей). Жестких дисков (как IDE, так и SCSI) в компьютере может быть не более двух. Если диск один, его желательно разбить на два раздела. Системный диск (раздел) имеет объем 3-4 Гб, второй диск (раздел) — от 3 Гб (в зависимости от того, какие дополнительные функции выполняет компьютер). Оба раздела — NTFS. На системном диске размещаются система и журналы транзакций, на втором диске — файлы базы Active Directory, каталог SYSVOL, базы сетевых служб и, если надо, профили пользователей и их домашние каталоги.
2. Оптимальная конфигурация для организации малого и среднего размера. Жестких дисков — 6 штук типа SCSI объемом 18 Гб каждый. Скорость вращения 10 000 об/мин. Все диски подключены к RAID-контроллеру. Конфигурация: диски попарно объединены в массивы RAID1. На первом массиве установлена система. Второй массив служит для размещения журналов транзакций. Третий массив служит для хранения базы Active Directory, каталога SYSVOL, базы сетевых служб и при необходимости профилей пользователей и их домашних каталогов.
3. Оптимальная конфигурация для крупных организаций и очень нагруженных контроллеров домена. Жестких дисков не менее 9. Тип UltraSCSI 160, от 10 000 до 15 000 об./мин. с возможностью замены в «горячем» режиме. Обязательное подключение к двухканальному RAID-контроллеру. К первому каналу подключено 6 дисков. Они попарно объединены в разделы RAID 1. Объем каждого раздела от 18 Гб. На первом — система, на втором — журналы транзакций, на третьем — база Active Directory. Раздел RAID 5 подключен ко второму каналу. Здесь размещаются каталог SYSVOL, базы сетевых служб, серверные приложения мониторинга и диагностики и при необходимости профили пользователей и их домашние каталоги.

Как проверить работоспособность контроллера домена

Ну что ж, спроектировали систему, сконфигурировали сетевые службы, запустили DCPROMO, перегрузили компьютер... А дальше? Можно приступить к работе? Конфигурировать остальные контроллеры? Не спешите. Сначала убедитесь, что все работает именно так, как вы и задумали. Не хочу пугать, но в жизни полно неожиданностей. Вы могли просто отвлечься во время ответов на вопросы DCPROMO и выбрать что-то не так, или на Солнце произошла мощная вспышка, но результат может быть любым. Поэтому выполните следующую проверку.

Совет Установив контроллер домена, не торопитесь увидеть все результаты установки сразу, особенно если вы устанавливаете не первый контроллер в лесу доменов. Подождите не менее 30 минут. За это время должна завершиться работа служб по конфигурированию DNS и Active Directory и выполниться внутрисайтовая репликация.

1. Просмотрите журналы событий в поисках предупреждений или сообщений об ошибках. Если они вам встретятся, выясните причину их появления и постарайтесь ее устранить. Многие из этих ошибок уже были описаны выше.
2. Убедитесь, что запущены все нужные для установленного типа запуска службы. Должны быть запущены все службы с автоматическим запуском.
3. Запретите запуск ненужных служб. Понимаю, что для многих это большой вопрос. А что называть лишними службами? Ну, для контроллеров домена это определенно Print Spooler, Messenger и Alerter. Если вы были столь неразумны, что по умолчанию установили IIS, запретите и его запуск. А вообще список нужных служб надо продумывать на этапе проектирования групповых правил для контроллеров доменов. Но об этом — в главе «Групповая политика».



Оптимизация серверной службы

4. Выберите правильную роль для службы Server. Подумайте, будете ли вы исполнять дополнительные приложения на этом сервере. Не забудьте про ресурс SYSVOL. Используются ли сценарии, как много пользователей и как часто имеет к ним доступ, где хранятся профили?

5. Проверьте параметры протокола TCP/IP. Все имена должны нормально разрешаться, а параметры, установленные для WINS и DNS, — верны. Используйте утилиты `ipconfig` и `nslookup`.
6. С помощью Netdiag проверьте сетевые подключения и регистрацию в WINS/DNS. Эта мощная утилита позволяет проверить все сетевые параметры компьютера. Вы можете выполнить как отдельные тесты, так и все сразу. Причем информацию о них можно выводить подробно или общо. Для примера разберем результат тестирования с выводом результатов без подробностей.

Для начала сообщаются общие сведения о компьютере.

```
Computer Name: DC01
DNS Host Name: dc01.fyodor.home
System info : Windows 2000 Server (Build 2195)
Processor : x86 Family 6 Model 8 Stepping 3, GenuineIntel
List of installed hotfixes :
Q147222
```

Далее тестируются сетевые платы. В данном случае вы видите предупреждение о том, что, возможно, плата не функционирует вследствие того, что это, например, единственный компьютер в сети:

```
Netcard queries test . . . . . : Passed
[WARNING] The net card 'Realtek RTL8139(A)-based PCI Fast
Ethernet Adapter' may not be working because it has not received
any packets.
```

Вот результаты тестирования каждого из интерфейсов. В нашем примере один является реальным интерфейсом, а другой — виртуальным, и именно с ним связаны все ошибки

Per interface results:

```
Adapter : Local Area Connection
Netcard queries test . . . , : Passed
Host Name . . . . . : dc01
IP Address. . . . . : 10.1.1.3
Subnet Mask . . . . . : 255.255.255.0
Default Gateway. . . . . :
Primary WINS Server. . . . : 10.1.1.3
Dns Servers. . . . . : 10.1.1.3
AutoConfiguration results. . . . . : Passed
Default gateway test . . . : Skipped
[WARNING] No gateways defined for this adapter.
NetBT name test. . . . . : Passed
WINS service test. . . . . : Passed
```

```
Adapter ; VMware Virtual Ethernet Adapter (basic host-only
support for VMnet1)
```



```
Netcard queries test . . . . . : Passed
Host Name . . . . . : dc01
IP Address . . . . . : 192.168.30.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway. . . . . :
Dns Servers . . . . . :
IpConfig results . . . . . : Failed
    Pinging DHCP server - not reachable
    WARNING: DHCP server may be down.
AutoConfiguration results. . . . . : Passed
Default gateway test . . . . . : Skipped
    [WARNING] No gateways defined for this adapter,
NetBT name test. . . . . : Passed
    No remote names have been found.
WINS service test. . . . . : Skipped
    There are no WINS servers configured for this interface.
```

Теперь следуют глобальные параметры, не требующие дополнительных разъяснений.

Global results:

```
Domain membership test . . . . . : Passed
NetBT transports test . . . . . : Passed
    List of NetBt transports currently configured:
        NetBT_Tcpip_{6C40DF85-48A3-4D93-941C-1D914F880907}
        NetBT_Tcpip_{B48C7C30-72DE-494C-BDB9-D9391C986AEF}
    2 NetBt transports currently configured.
Autonet address test. . . . . : Passed
IP loopback ping test . . . . . : Passed
Default gateway test . . . . . : Failed
    [FATAL] NO GATEWAYS ARE REACHABLE.
    You have no connectivity to other network segments.
    If you configured the IP protocol manually then
    you need to add at least one valid gateway,
NetBT name test . . . . . : Passed
Winsock test . . . . . : Passed
DNS test . . . . . : Failed
    [FATAL]: The DNS registration for 'dc01.fyodor.home'
    is incorrect on all DNS servers.
```

PASS - All the DNS entries for DC are registered on DNS server '10.1.1.3' and other DCs also have some of the names registered.

Увидев такое предупреждение, запустите `netdiag` с ключом `/v`. Чтобы сократить выводимую информацию, лучше всего указать конкретный тест. У нас это тест `DNS`. Проанализировав результат в конкретном примере, приходим к выводу, что виноват снова вирту-

альный сетевой интерфейс, который, несмотря на свою виртуальность, зарегистрирован в DNS как адрес сервера DNS в несуществующей сети 192.168.30.0.

Redir and Browser test: Passed

List of NetBt transports currently bound to the Redir

NetBT_Tcpip_{6C40DF85-48A3-4D93-941C-1D914F8B0907}

NetBT_Tcpip_{B48C7C30-72DE-494C-BDB9-D9391C986AEF}

The redir is bound to 2 NetBt transports.

List of NetBt transports currently bound to the browser

NetBT_Tcpip_{6C40DF85-48A3-4D93-941C-1D914F8B0907}

NetBT_Tcpip_{B48C7C30-72DE-494C-BDB9-D9391C986AEF}

The browser is bound to 2 NetBt transports.

Ну и, наконец, тесты самого контроллера домена. Для целей общей диагностики этого вполне достаточно. Путь к подробностям откроет вам ключик /v у команды:

DC discovery test.: Passed

DC list test.: Passed

Trust relationship test.: Skipped

Kerberos test.: Passed

LDAP test.: Passed

Bindings test.: Passed

WAN configuration test.: Skipped

No active remote access connections.

Modem diagnostics test.: Passed

IP Security test,: Passed

IPSec policy service is active, but no policy is assigned.

The command completed successfully

7. Утилита Dcdiag (о ее возможностях см. справку Support Tools Help) поможет выявить некорректности в работе контроллера: ее достаточно запустить без ключей. Выводимый результат предельно ясен и понятен. Если не все гладко, воспользуйтесь рекомендациями из главы «Поиск и устранение проблем».

Domain Controller Diagnosis

Performing initial setup:

Done gathering initial info.

Doing initial required tests

Testing server: Site-1\DC01

Starting test: Connectivity

.....DC01 passed test Connectivity

Doing primary tests

```
Testing server: Site-1\DC01
Starting test: Replications
.....DC01 passed test Replications
Starting test: NCSecDesc
.....DC01 passed test NCSecDesc
Starting test: NetLogons
.....DC01 passed test NetLogons
Starting test: Advertising
.....DC01 passed test Advertising
Starting test: KnowsOfRoleHolders
.....DC01 passed test KnowsOfRoleHolders
Starting test: RidManager
.....DC01 passed test RidManager
Starting test: MachineAccount
.....DC01 passed test MachineAccount
Starting test: Services
.....DC01 passed test Services
Starting test: ObjectsReplicated
.....DC01 passed test ObjectsReplicated
Starting test: frssysvol
.....DC01 passed test frssysvol
Starting test: kccevent
.....DC01 passed test kccevent
Starting test: systemlog
.....DC01 passed test systemlog

Running enterprise tests on : fyodor.home
Starting test: Intersite
.....fyodor.home passed test Intersite
Starting test: FsmoCheck
.....fyodor.home passed test FsmoCheck
```

Если приведенная последовательность тестов дает ясно понять, что все отлично и прекрасно работает, *смело* продолжаем *установку* других контроллеров.

Замечание На этом этапе перейти к установке других контроллеров можно в небольших тестовых сетях, когда все контроллеры можно сконфигурировать за несколько часов. Если же вы собираете рабочую систему, см. раздел «Все работает. Что делать?».

А теперь обратимся к не самому радостному варианту. У вас проблема. Что-то не работает. Как правильнее поступить в такой ситуации?

А если он все-таки не работает?

Если контроллер домена не работает после установки (а симптомами являются, например, многочисленные сообщения об ошибках в журналах, невозможность запуска средств контроля Active Directory и т. п.), то общий алгоритм действий такой.

- ◆ **Выясняется причина неработоспособности.** В 99% работоспособность можно восстановить. Если найдена причина, остальное уже дело техники.
- ◆ Если при выявлении причин трагедии выясняется, что вы попали в тот 1%, когда уже ничто не поможет, надо подумать о переустановке системы. Особо надо выделить ситуацию обновления контроллера домена Windows NT до Windows 2000.
- ◆ Наконец, когда вы занялись переустановкой системы на бывшем дефектном контроллере, нужно вычистить информацию о нем из Active Directory (конечно, только если вы не переустанавливаете первый и единственный контроллер в сети).

Попробуем выяснить причину

Я полностью посвятил одну главу книги поиску и устранению проблем в Active Directory. Но там речь идет о системе, которая работала, работала и... перестала. Здесь же я хочу очень кратко остановиться на самых первых шагах системы, которые она попыталась сделать, да не смогла. Все причины неработоспособности контроллера домена можно разбить на такие категории:

- некорректно заданные параметры TCP/IP или ошибки в сети;
- некорректная работа службы DNS;
- ◆ проблемы с **оборудованием**, в первую очередь с дисковой подсистемой;
- ◆ проблемы с репликацией Active Directory;
- ◆ проблемы с репликацией FRS.

Некорректные параметры TCP/IP или ошибки в сети

Если до запуска DCPROMO или в процессе ее работы с сетью все было нормально (хотя бы не было предупреждений или сообщений об ошибках), а сейчас возникают ошибки связанные с сетью, то возможно, что-то изменилось в параметрах протокола TCP/IP. Вы спросите: что могло измениться, когда никто ничего не изменял? Ну, например, если сервер — клиент DHCP и получает от него постоянный адрес, то после перезагрузки он этого адреса не получит или получит другой, не соответствующий своей подсети. И произойдет это потому, что кто-то очень «умный» в вашей сети запустит свой сервер DHCP «в тестовых целях».

Следовательно, первое ваше действие — выполнить команду `ipconfig /all`.

Если все правильно, проверяем, доступен ли с контроллера сервер DNS и другие контроллеры домена. Думаю, излишне напоминать, что этим занимается команда `ping`. Кстати, вероятность возникновения ошибки по вине сети наиболее вероятна, если:

- вы устанавливаете контроллер домена в удаленном офисе, связанном с центральным сайтом неустойчивым каналом;
- вы находитесь в отдельном сегменте сети, а маршрутизатор работает с перебоями;
- + часть сети, в которой установлен контроллер домена, расположена за межсетевым экраном, и за то время, пока шла установка контроллера, другой администратор изменил параметры экрана.

Кстати, `ping` позволит выявить и не вовремя «упавший» сервер DNS.

Некорректная работа службы DNS

Если же сервер DNS «жив», надо проверить его параметры. В первую очередь выполните `nslookup`. Устраните обнаруженные некорректности. Проверьте правильность делегирования зон, пересылки запросов, наличие необходимых зон, включая зону `_msdcs.<имя леса>`, а также ее доступность для контроллера. Короче, используйте все инструменты, о которых выше шла речь.

Здесь уместно описать фатальную ситуацию. Допустим, вы устанавливали второй контроллер домена в лесу. При перезагрузке после окончания работы DCPromo первый контроллер вышел из строя, и восстановить его невозможно (скажем, «умер» жесткий диск, а резервную копию вы еще не успели сделать). Сожалею, но в этом случае придется переустановить не только первый контроллер, но и второй.

Частным случаем, но с более тяжелыми последствиями, является установка контроллера домена в удаленном филиале. При перезагрузке происходит крупная авария у телекоммуникационного провайдера, на устранение которой потребуется несколько дней. Ждать вы не можете и бросаете все до «лучших времен». Ваша беспечность обойдется администратору предприятия хорошей чисткой Active Directory.

Проблемы с оборудованием, в первую очередь с дисковой подсистемой

Проблема настолько очевидна, что для ее диагностики не потребуется много времени. Журнал регистрации системных событий и Active Directory будет заполнен взаимодополняющими сообщениями об ошибках.

Проблемы с репликацией Active Directory

Проблемы с репликацией выявляются довольно быстро. Во-первых, надо подождать не менее 15 минут по окончании установки контроллера.

лера и перезагрузки компьютера. Если записи в DNS были внесены сразу, компьютер с этого момента станет доступным для репликации. Служба KCC перестроит топологию репликации так, что включит компьютер в общее кольцо,

О том, что компьютер готов к репликации, можно судить по появлению у него объектов связи с другими компьютерами. Эти объекты видны в оснастке Active Directory Sites and Services. Щелкнув объект связи правой кнопкой, выберите команду Replicate now. Если не будет выдано сообщений об ошибках, то скорее всего репликация работает нормально. Удостовериться в этом поможет команда `repadmin /showreps`. Если ошибок нет и показаны все партнеры по репликации, то этот этап проверки можно считать **завершенным**.

Если в ответ на команду вы получите сообщение об ошибке, не паникуйте. Возможно, начальная репликация еще не завершилась. Минут через 5-10 повторите команду.

Совет Не забывайте периодически обновлять состояние параметров NTDS Settings, выполняя команду Refresh. Ее надо **применять**, щелкая правой кнопкой имя сервера.

Если и теперь **наблюдаются** ошибки, см. главу «Репликация Active Directory». Здесь же отмечу, что если в сообщении об ошибке указано, что доступ запрещен (Access denied), то скорее всего у вас нет полномочий для административного доступа к тому контроллеру домена, на который вы хотите выполнить репликацию.

Проблемы с репликацией FRS

Проблемы с репликацией FRS встречаются гораздо реже, чем проблемы с репликацией Active Directory.

Чтобы убедиться, что репликация FRS завершилась, откройте каталог SYSVOL и сравните его содержимое с содержимым аналогичного каталога на других контроллерах того же домена. Если каталоги идентичны, можно считать, что репликация FRS работает. Для подстраховки положите в каталог Scripts какой-нибудь файл и, следуя топологии репликации, проверьте, как он будет последовательно появляться на всех контроллерах домена.

Если, однако, это не так и либо структуры каталогов SYSVOL на двух контроллерах домена не идентичны, либо файл в каталоге Scripts не тиражируется, откройте журнал регистрации FRS. В нем вы обнаружите сообщения, позволяющие выявить истоки проблемы. Это будет, например, сообщение о нехватке места в каталоге SYSVOL или об отказе в доступе к нему. Проверьте, не установлено ли у вас квотирование диска, не поменяли ли вы права доступа как к сетевым ресурсам Sysvol и Netlogon, так и списки контроля доступа NTFS к каталогам SYSVOL и Scripts.

Некорректная групповая политика

Проблемы, связанные с некорректной работой групповой политики на этом этапе вряд ли могут появиться. Дело в том, что для контроллеров домена определяется Default domain controllers group policy. Если вы устанавливаете первый контроллер в домене, то она еще просто не определена, и действуют значения по умолчанию, конфликтов с которыми нет.

Если же это не первый контроллер в домене, могут наблюдаться ошибки, определенные на уровне домена для общей политики безопасности. Характер таких ошибок может относиться скорее к казусам и невнимательности администратора.

А может, все переустановить?

Если поиск источника проблемы не дал желаемых результатов и все попытки заставить контроллер заработать не увенчались успехом, вы, может быть, и зададитесь этим вопросом.

Что ж, если это единственный контроллер в лесу, то, возможно, это наилучший выход. Главное, прежде чем все переустанавливать, постарайтесь все-таки докопаться до причины проблемы. Иначе никто не гарантирует, что вы не повторите той же ошибки.

Если это не первый контроллер домена, то идти на «мокруху» нужно крайне осмотрительно. Во-первых, попробуйте запустить DCPROMO и корректно понизьте статус контроллера до сервера в домене. Если это удалось, то на одном из оставшихся контроллеров откройте оснастку Active Directory Users and Computers и убедитесь, что данный объект переместился из контейнера Domain Controllers в контейнер Servers. После этого откройте оснастку Active Directory Sites and Services, найдите имя сервера, статус которого вы только что понизили, и удалите его. Если остались объекты-связи с этим компьютером у других контроллеров, удалите их.

Если понижение статуса завершилось неудачно, придется удалить контроллер домена из Active Directory вручную. Для этого запустите на одном из нормально работающих контроллеров домена утилиту ntdsutii. Войдите в ней в режим Connections и подключитесь к тому контроллеру домена, на котором запущена утилита. Затем в режиме Metadata Cleanup войдите в режим Select Operations Target и, поочередно просматривая списки сайтов, доменов в них и серверов в доменах, выберите сервер, который надо удалить из Active Directory. Вернувшись в Metadata Cleanup, удалите выбранный сервер. Далее откройте оснастку Active Directory Users and Computers и убедитесь, что объект исчез из контейнера Domain Controllers. Затем откройте оснастку Active Directory Sites and Services, найдите имя сервера, исключенного из Active Directory, и удалите его. Удалите также объекты-связи с ним у других контроллеров. Наконец, откройте оснастку

управления DNS и удалите все записи (если они, конечно, там появились), относящиеся к удаленному серверу.

Вот теперь повторно установите ОС и повысьте статус до сервера.

Внимание! Контроллера в существующие. Описанная процедура может использоваться только в случае установки новых контроллеров доменов Windows 2000. Если же обновляется контроллер домена Windows NT 4-0, см. ниже раздел «Обновление контроллера домена Windows NT 4.0 до Windows 2000».

Все работает. Что делать?

Убедившись, что все работает, не торопитесь устанавливать остальные контроллеры или подключать клиенты. Сначала надо подумать о резервном копировании контроллера домена. Вы можете сказать: «А что тут думать-то? Надо значит надо!» И все же представьте, что вы установили первый контроллер в лесу. Сделали резервную копию. Затем вы устанавливаете второй контроллер и делаете его резервную копию. Однако состояние Active Directory изменилось по сравнению с тем моментом, когда выполнялось резервное копирование первого контроллера домена. Следовательно, надо сделать для него повторную резервную копию? А надо ли?

Допустим, вскоре после установки второго контроллера домена произошел сбой первого. Переустановив его и восстановив содержимое резервной копии, вы добьетесь того, что состояние Active Directory будет соответствовать моменту времени, предшествовавшему тому, когда был установлен второй контроллер домена. Следовательно, USN восстановленных объектов будут меньше USN аналогичных объектов на втором контроллере. Это же справедливо и для вектора обновленности (updateness vector). (О репликации см. главу «Репликация Active Directory».) Поэтому начавшаяся репликация приведет к тому, что объекты с более высоким USN будут тиражированы на восстановленный контроллер и информация на нем станет актуальной. Вывод: вовсе не обязательно выполнять резервное копирование Active Directory на всех контроллерах доменов всякий раз после добавления нового контроллера. Достаточно сделать это сразу после установки контроллера и его синхронизации с остальными. В дальнейшем резервное копирование надо проводить на регулярной основе.

Совет Выполнив резервное копирование системного состояния, не успокаивайтесь. Попробуйте в тестовой зоне восстановить AD из резервной копии. Вы не только будете уверенно себя чувствовать в случае реального восстановления рабочей системы, но и будете хорошо представлять длительность этого процесса, что просто необходимо при планировании.

Обновление контроллера домена Windows NT 4.0 до Windows 2000

Рассмотренные выше вопросы установки контроллеров доменов в основном применимы при проектировании новых сетей. Однако часто встает вопрос о модернизации имеющейся сети, построенной на базе доменной структуры Windows NT, ее расширении или объединении нескольких сетей. Рассмотренные выше методики будут применимы и тогда, и все же тут есть ряд особенностей.

Тот, кто хорошо знаком с сетями на базе Windows NT, знает, что существует несколько моделей связи между доменами. Это может быть простая сеть, состоящая из одного домена, или несколько доменов, связанных между собой по схеме с одним или несколькими мастер-доменами и обеспечивающих полную централизацию управления, может быть и модель полностью доверительных отношений, предлагающая полную децентрализацию, а также — смесь нескольких различных моделей, соответствующая структуре организации (Подробнее см. [9]). Понятно, что для каждой из этих моделей существует оптимальный способ миграции на новую систему, обеспечивающий эффективный и безопасный перенос учетной информации и минимально воздействующий на конфигурацию клиентских рабочих мест. Подробное описание различных вариантов перехода со старой системы на новую, а также способы обеспечения нормального сосуществования в одной сети как старых систем, так и новых, см. в [1].

Здесь же мы рассмотрим процесс миграции одного домена, обращая внимание на вопросы, связанные с обновлением ОС на PDC.

Кое-что о Windows NT 4.0

Перед рассмотрением миграции вспомним некоторые основы работы сервера Windows NT 4.0 и доменов на его основе. Сервер может быть либо первичным контроллером домена (PDC), либо резервным контроллером (BDC), либо отдельно стоящим сервером. Роль, которую он будет играть в домене, определяется на этапе установки и не может быть изменена в дальнейшем. Так, в частности, контроллер домена нельзя сделать отдельно стоящим сервером, а сервер — контроллером домена, не переустановив их полностью. Можно лишь повысить роль резервного контроллера до статуса первичного, а первичный — понизить до резервного. На резервном контроллере можно остановить сервис регистрации, но это приведет только к тому, что он не будет использоваться для регистрации входящих в домен, однако своей роли он не изменит.

Так как в домене на базе Windows NT 4.0 широко применяются идентификаторы безопасности компьютеров, генерируемые при установке системы, и основанные на них доверительные отношения старого типа, то переместить контроллер из одного домена в другой, не при-

бегнув к полной переустановке системы, невозможно. Кроме того, вы не можете произвольно изменять имена контроллеров домена, не прибегая к полной их переустановке.

Вспомним также, что учетная информация в домене может изменяться только на первичном контроллере, а резервные контроллеры служат для регистрации пользователей. База учетных записей на BDC — точная копия базы PDC. Достигается это за счет тиражирования с одним мастером (single master replication).

Репликацию файловой системы (Сетевой ресурс Netlogon) выполняет служба Lmrep1, работа которой несовместима со службой репликации FRS в Windows 2000.

Контроллеры домена Windows NT 4.0 могут работать в домене Windows 2000. При этом домен должен обязательно работать в смешанном режиме (mixed mode) со всеми вытекающими из этого ограничениями, контроллеры Windows NT выполняют роль только резервных контроллеров и аутентифицируют клиентов по протоколу NTLM.

Обеспечение безопасной миграции

Вы уже поняли, сколько опасностей подстерегает на этапе установки контроллера домена. Но эффект от сбоя максимален при миграции сети, так как в этот процесс вовлечены сотни пользователей. Эффективность их работы во многом зависит от состояния сетевой инфраструктуры: бесперебойного доступа к файлам и принтерам, надежности электронной почты, работы приложений. Вторжение в отлаженную доменную структуру чревато тяжелыми последствиями. Именно поэтому требуется самое серьезное планирование и тестирование. Планирование включает в себя перечень организационных и административных мероприятий и тщательную проработку этапов миграции и отдельных ее операций.

Описание организационной стороны миграции выходит за рамки данной книги (см. об этом материалы Microsoft Solutions Framework: Infrastructure deployment planning), но затронуть технические аспекты безопасной миграции необходимо.

Две стратегии миграции

Существует два принципиально разных подхода к миграции. Выбор во многом зависит от того, в какой степени пользователи нуждаются в постоянной доступности, от того, как быстро вы можете сообщать пользователям об изменениях, и от ваших финансовых возможностей. Первый подход подразумевает, что вы обновляете систему. При этом тщательно прорабатываются этапы миграции, последовательность перехода на новую систему различных подразделений и территорий, процедура обновления и настройки клиентских рабочих мест. Для каждого шага предусматривается вариант отката в случае неудачи, для чего просчитывается длительность нормальной процедуры и разрабатываются сценарии «что, если».

Прежде чем начать миграцию, надо убедиться, что все обновляемые серверы соответствуют требованиям. Это относится как к типам устройств, используемых в компьютерах, так и к объему ресурсов: частоте процессора, объему памяти, объему жесткого диска. Последнее имеет особое значение. Если вы выполняете обновление не с компакт-диска, а по сети, то на локальный диск будет скопировано практически полное содержимое компакт-диска. Обратите внимание и на тип файловой системы. Если в обновляемом контроллере домена нет разделов с NTFS, обновление не состоится.

Если вы понимаете, что текущая конфигурация оборудования первичного контроллера домена не соответствует всем требованиям со стороны контроллера Windows 2000 и, более того, не может быть изменена, то существует два варианта развития событий. Первый: вы приобретаете более мощный сервер, спецификации которого соответствуют рассчитанным вами требованиям, устанавливаете на него Windows NT 4.0 Server в качестве резервного контроллера домена, а потом повышаете статус до PDC. Дальнейшая миграция этого сервера пройдет без проблем. Второй: если существующий сервер в принципе способен выполнять роль контроллера домена Windows 2000 без нагрузки, вы выполняете его обновление до Windows 2000, затем на новый сервер устанавливаете Windows 2000 в качестве контроллера домена и передаете все функции мастеров операций с прежнего PDC на вновь установленный сервер. Преимущество данного способа в том, что новый контроллер домена «не знал» старой версии Windows NT и не несет в себе ее наследия.

Следующий шаг — полное резервное копирование всех данных на мигрирующем сервере. Это может оказаться весьма полезным, если обновление системы почему-либо не будет выполнено.

Совет Вместо резервного копирования можно установить в домен дополнительный контроллер домена и после его полной синхронизации отключить от сети. Если при обновлении возникнут проблемы, то этот сервер можно будет использовать как источник информации. «не замутненный процессом миграции».

Может случиться, что не все серверные приложения, используемые в вашей организации, будут готовы к работе в Windows 2000. Тогда они могут продолжить работу на старой версии, но в рамках обновленного домена.

Преимущества и недостатки данного метода миграции таковы:

Преимущества	Недостатки
Последовательность действий	Необходимо выполнять работы в выходные дни
Можно создать пилотные зоны	Длительный процесс

см. след. стр.

Преимущества	Недостатки
Не требуется большое количество дополнительного оборудования	Необходимо проектировать большое количество процедур отката
Влияет на небольшой круг пользователей	Необходимо обеспечить существование «старой» и «новой» систем в переходный период
Можно использовать существующее оборудование	Необходимо проводить резервное копирование всех серверов

Другой метод обеспечивает максимальную безопасность миграции, однако он и самый дорогой.

В лабораторной сети вы создаете новый домен на базе Windows 2000 Server. Полностью конфигурируете все контроллеры домена и серверы приложений. Создаете структуру ОП.

Далее — подключение нового домена в существующую сеть. Пользователям вашего домена новый остается пока недоступным. Потом вы переносите учетные записи всех пользователей в новый домен. Перенос помогут выполнить либо сценарии cloneprincipal, либо Active Directory Migration Tool (ADMT).

После распределяете учетные записи по подразделениям из оснастки Active Directory Users and Computers. Здесь же вы формируете групповые и системные правила.

Следующий шаг — планомерное переключение пользователей на новую структуру. Переключение можно совместить с обновлением операционных систем на их компьютерах. С этого момента клиенты могут регистрироваться в новом домене. Если миграция прошла успешно, старый домен можно выключить.

Описанный способ пригоден, если у вас хватает компьютеров. Например, вы делаете обновление своего парка машин.

Преимущества	Недостатки
Полная независимость тестовой сети от рабочей	Необходимо выполнять ряд работ в выходные дни
Возможность тщательного тестирования	Требуется большое количество дополнительного оборудования
Система создается «с нуля»	Невозможно использовать существующее оборудование
Оказывает влияние на небольшой круг пользователей	Необходимо перенастраивать клиентские компьютеры
Миграция пользователей выполняется в предельно сжатые сроки	
Процедура отката предельно проста.	
Не требуется резервное копирование	

Второй метод миграции подразумевает, что установка контроллеров домена выполняется на новой системе, т. е. без обновления существующей.

Мигрируем домен Windows NT

Начиная миграцию домена Windows NT, вы должны четко представлять доменную структуру Active Directory. Как это описано в предыдущей главе, для небольшого предприятия наиболее вероятной доменной структурой может быть либо один домен, либо дерево из двух доменов. Корневой домен при этом пустой и играет роль носителя имени организации. Далее мы будем придерживаться этого предположения.

Замечание Миграция домена Windows NT в дерево, состоящее из двух доменов, является частным случаем включения одиночного домена Windows NT в лес Active Directory.

Обновление первичного контроллера домена

Начинается миграция домена с обновления ОС на PDC. Обновление первичного контроллера домена преследует две цели:

- ◆ сразу включить существующий домен в дерево, даже несмотря на смешанную структуру домена;
- ◆ использовать новые инструменты управления службой каталога и создания своих элементов в каталоге Active Directory.

Прежде чем начать обновление, убедитесь, что у вас есть сервер DNS, соответствующий требованиям Active Directory. Все, о чем написано в разделе, посвященном DNS, относится и к данному случаю.

Итак, если все предварительные условия выполнены, запускайте обновление ОС на первичном контроллере домена. Здесь предположим, что обновление самой системы прошло без осложнений. (В этом должна быть ваша заслуга, так как надо запастись драйверами оборудования, установленного в компьютере. Например, если это сервер Compaq, то нужен диск Smart Start с необходимыми драйверами. Именно с него нужно запускать обновление ОС.) Сразу по завершении работы программы установки ОС запустится DCPROMO.

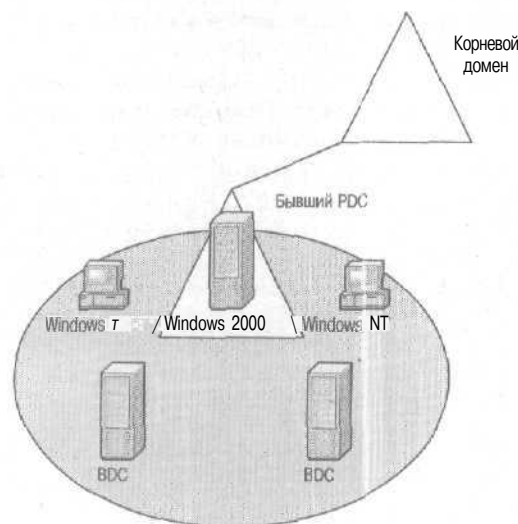
Внимание Если размер базы SAM велик (50–70 Мб), то на финальной стадии работы Winnt32 (это когда появляются сообщения «Performing final tasks» и «Save Settings») может показаться, что компьютер завис. Продолжительность паузы может достигать 2,5 часов. Настоятельно рекомендуется не прерывать работу компьютера и дать завершить все операции. Вы можете исключить возникновение такой ситуации, выполнив одно из следующих действий:

- ◆ установив максимальный размер реестра в 200 Мб;
- ◆ установив объем файла подкачки на 20% выше объема ОЗУ;
- ◆ повысив объем ОЗУ;

- ◆ уменьшив объем SAM, последовательно применив утилиты REGBACK и REGREST;
- ◆ добавив в систему новый BDC, повысив его статус до PDC, а потом обновив до Windows 2000.

Как и в процедуре установки, описанной для нового контроллера домена, вам будет предложено указать имя дерева, к которому будет присоединен данный домен, или создать новое дерево. В первом случае надо указать ссылку на будущий родительский домен. Если же мигрируемый домен единственный, то при установке надо указать, что это корневой домен нового дерева в новом лесу.

Может случиться, что вам понадобится изменить имя домена. Скажем, домен Windows NT имел NetBIOS имя CENTRAL, а новое имя домена Windows 2000 должно быть mycorp.ru. Если бы вы устанавливали домен с нуля, то его NetBIOS-имя по умолчанию было бы MYCORP. Так как вы выполняете обновление, NetBIOS-имя будет сохранено и останется CENTRAL. Такое сохранение важно с точки зрения пользователей домена: они по-прежнему будут регистрироваться в домене CENTRAL, и вам не придется оповещать их об изменениях.



Миграция домена Windows NT в дерево доменов Windows 2000

Это соответствие между NetBIOS-именем домена и DNS-именем домена поддерживается с помощью объектов класса CrossRef, расположенных в контейнере CN=Partitions,CN=Configuration,<имя леса>

По мере выполнения обновления системы DCPROMO перенесет в каталог Active Directory объекты из базы SAM: учетные записи пользователей, локальных и глобальных групп, а также машин. Каждый

объект безопасности переносится в контейнер со своим именем. Не будучи организационными единицами, эти контейнеры являются объектами с общим именем (сп). Ниже показано соответствие учетных записей и контейнеров, в которые они переносятся.

Учетные записи	Контейнер
Все пользователи	Users
Компьютеры	Computers
Встроенные локальные группы	Builtin
Встроенные глобальные группы	Users
Все остальные группы	Users

После установки протокола Kerberos будут запущены службы аутентификации и выдачи начального билета TGT, а вслед за этим установятся транзитивные двусторонние доверительные отношения с родительским доменом.

Контроллер родительского домена реплицирует данные в новый дочерний домен, который в свою очередь будет добавлен в структуру сайта. Все контроллеры домена получают уведомление о том, что к дереву подключен новый домен. Так как обновленный контроллер является первичным контроллером для остальных резервных контроллеров Windows NT, то все новые объекты будут тиражированы на них.

После обновления ОС на PDC до Windows 2000 компьютер становится **виден** как контроллер домена для всех серверов Windows 2000 и как первичный контроллер домена для серверов Windows NT 4.0. Windows 2000 обладает *обратной совместимостью* с предыдущей версией. При этом данный компьютер по-прежнему можно применять для создания новых объектов безопасности (учетных записей пользователей, групп и машин), сведения о которых будут тиражироваться на другие BDC в домене. Рабочие станции будут распознавать компьютер как PDC. Если выключить Windows 2000-компьютер, играющий роль PDC, то любой BDC может быть повышен до статуса PDC. Если же первичный контроллер домена с Windows 2000, выполняющий роль PDC, включен, то повышение статуса BDC невозможно.

Совет Обновив PDC, добавьте в домен новый контроллер Windows 2000, установленный на новую машину, и передайте ему все роли мастеров операций. Это не обязательное действие. Его цель — повысить устойчивость ОС, так как обновления не всегда работают стабильно.

Откат назад в случае сбоя

А если при обновлении ПОС произошел сбой? Во-первых, не паникуйте. В этой главе есть советы на все случаи вашей административной деятельности. Но так как эти советы касаются только на 100% «чистой» среды Windows 2000, то ниже я **расскажу**, как сделать, чтобы домен NT 4 продолжил нормально функционировать.

Итак, во время обновления контроллера домена в процессе работы DCPROMO произошел фатальный сбой, и вы поняли, что восстановлению система не подлежит. Дальнейшие ваши действия в домене Windows NT зависят от того, как именно вы подстраховались перед началом обновления.

1. Если вы выполнили резервную копию PDC, то восстановите ее на вновь установленный сервер Windows NT. В процессе репликации исходное состояние базы SAM будет тиражировано по всем BDC.
2. Если вы сохранили в отключенном состоянии BDC, то включите его в сеть, повысьте его статус до PDC, и предмиграционное состояние будет восстановлено во всем домене.

Завершив репликацию, убедитесь, что информация на всех контроллерах домена тождественна, а пользователи не испытывают проблем с регистрацией в сети и доступом к ресурсам.

Совместная работа контроллеров разных версий

На последней стадии миграции можно обновить ОС на других контроллерах домена и установить на них службу каталогов Active Directory. Также можно просто добавить в домен новые контроллеры с установленной Windows 2000 Server. Но прежде чем вы это сделаете, система будет эксплуатироваться в переходном состоянии, когда у вас будут работать контроллеры домена разных версий. Ниже описаны некоторые особенности этого периода.

Так как контроллеры домена с *старого* типа используют в своей работе последовательно возрастающие *относительные идентификаторы* (RID) из ряда всех идентификаторов безопасности (SID), то только первичный контроллер домена с Windows 2000 может служить для создания объектов системы безопасности. Объекты, не имеющие отношения к системе безопасности, например организационные единицы, могут быть созданы на любом контроллере с установленной службой каталогов Active Directory.

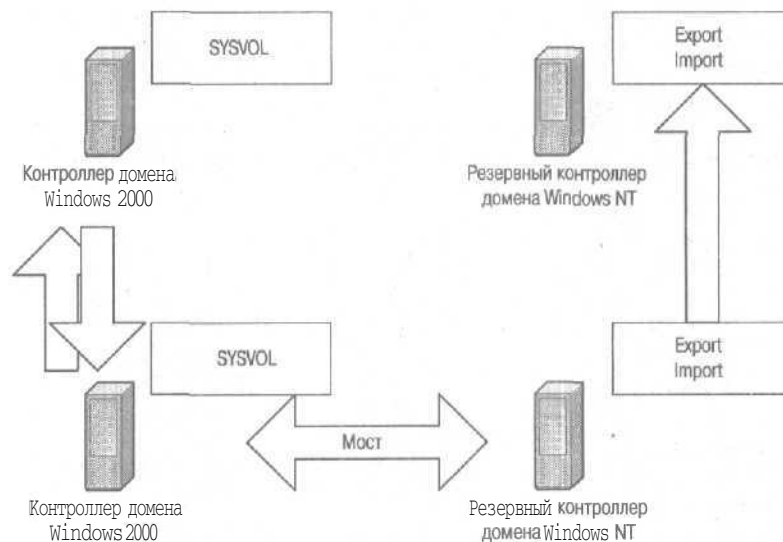
На первичном контроллере домена используется два протокола тиражирования: для систем на базе Windows NT 4.0 и ранних версий — с одним мастером и для партнеров на базе Windows 2000 — с несколькими,

Особо скажу о файловой репликации. Репликация FRS несовместима с механизмом репликации LMRepl. При работе в смешанной среде контроллеры Windows NT ничего не знают о файлах, реплицируемых контроллерами Windows 2000. Контроллер домена — имитатор PDC — не поддерживает работу LMRepl. В такой ситуации сценарии и файлы системной политики не тиражируются на контроллеры Windows NT. Для разрешения этой проблемы рекомендуется сделать следующее.

- Перед обновлением ОС на PDC нужно сконфигурировать любой BDC в качестве источника для службы LMRepl.

- Использовать файл Lbridge.cmd из состава Windows 2000 Server Resource Kit. Этот командный файл, запускаемый на одном из контроллеров Windows 2000, копирует файлы из каталога SYSVOL в каталог Export на том контроллере домена Windows NT, который вы сконфигурировали как источник для службы LMRepl.

Совет Файл Lbridge.cmd использует команду `xcopy` для копирования файлов. Лучше ее заменить на утилиту `robocopy` из Windows 2000 Server Resource Kit.



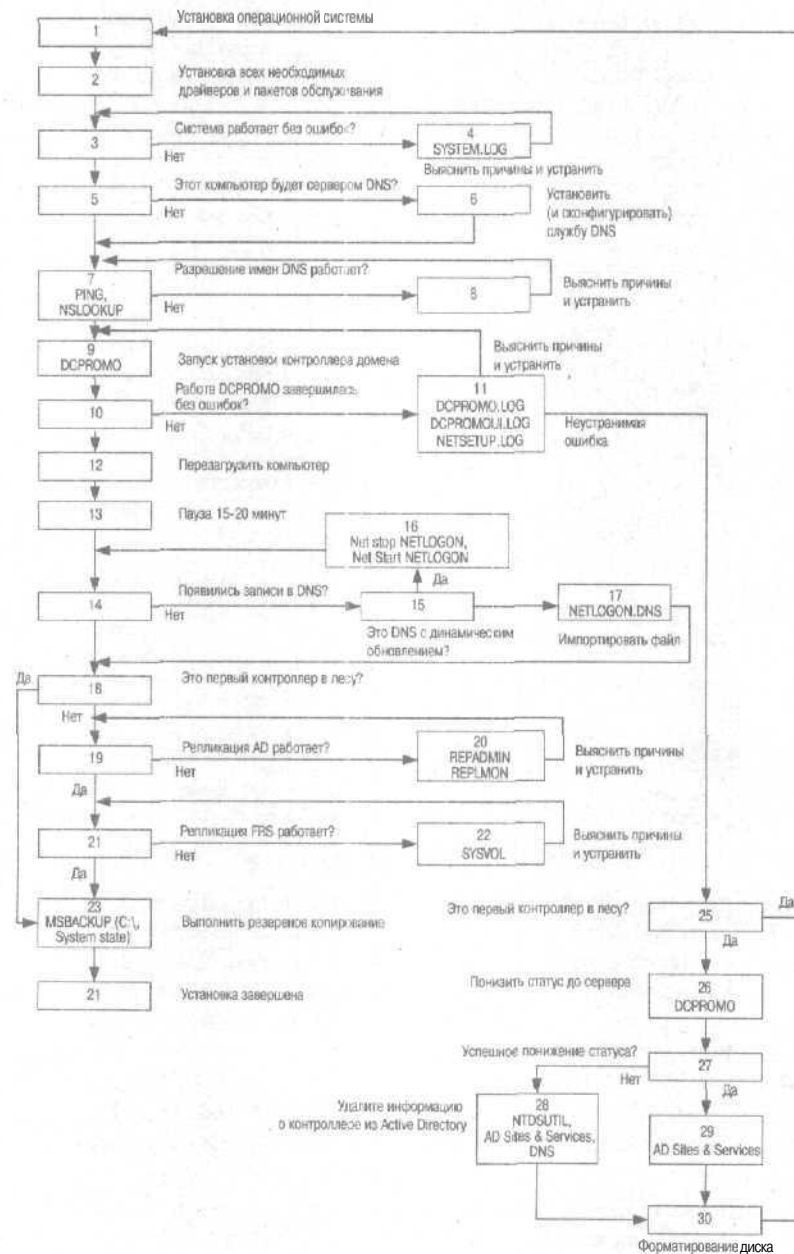
Организация моста для тиражирования файлов

Различия между моделями хранения и использования политики безопасности Windows 2000 и Windows NT слишком велики, поэтому перенос правил в процессе миграции невозможен. При подсоединении к существующему дереву доменов наследует объект политики только от сайта родительского домена. При обновлении отдельного домена в нем по умолчанию формируется новая политика и соответствующий объект в каталоге.

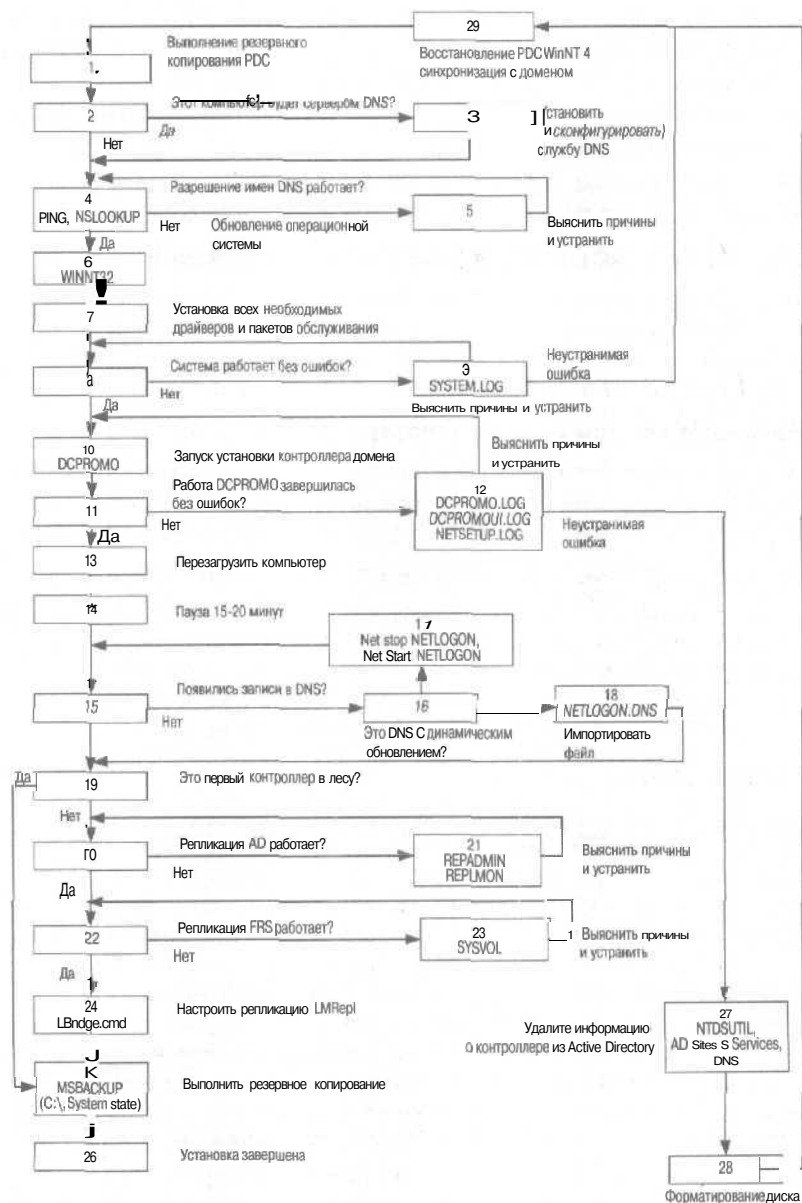
После перевода всех контроллеров в домене на Windows 2000 домен может быть переведен из смешанного режима работы в естественный.

При этом:

- в домене используется механизм тиражирования каталога Active Directory с несколькими мастерами; этот механизм применяется и для тиражирования объектов безопасности;



Алгоритм установки нового контроллера домена



Алгоритм обновления контроллера домена Windows NT

- 4 бывший первичный контроллер домена перестает поддерживать тиражирование с одним мастером; т. е. в домен более нельзя добавить контроллер под управлением Windows NT 4.0;
- все клиенты используют преимущества транзитивных доверительных отношений.

Решение о переводе домена в естественный режим принимает администратор — оно не может быть выполнено автоматически.

Алгоритмы установки контроллера домена

Это своего рода квинтэссенция содержания главы: здесь приводятся алгоритмы, отражающие последовательность действий при установке нового контроллера домена и обновлении существующего контроллера Windows NT 4.0.

Алгоритм установки нового контроллера

Алгоритм установки нового контроллера домена охватывает все этапы: подготовки, установки, проверки работоспособности, резервного копирования и действий при возникновении неустраняемых ошибок.

Алгоритм обновления контроллера Windows NT 4.0

Алгоритм обновления контроллера домена Windows NT также охватывает все этапы: предварительной подготовки, установки, проверки работоспособности, резервного копирования и действий в случае возникновения неустраняемых ошибок. Хотя последовательность основных операций сохранилась, есть и важные отличия.

Заключение

Рассмотренные в данной главе вопросы относятся к категории тех, что наиболее часто возникают на этапе установки контроллера домена. Конфигурирование DNS, DHCP, WINS, выполнение DCPRMO и поиск ошибок работы этой программы, обновление контроллера домена Windows NT 4.0 — все это перечень источников проблем, возникающих у корпоративных пользователей при миграции на платформу Windows 2000. Но не надо думать, что здесь описаны *все* проблемные ситуации и способы их разрешения. Есть ряд вопросов, которые я оставил за рамками книги. Если у вас возникнут проблемы, описание которых здесь не приведено, то первым источником должен стать Microsoft Technet. Это могут быть как диски, распространяемые по подписке, так и ресурс Интернета (support.microsoft.com).

В этой главе практически не рассматриваются вопросы поиска и устранения проблем с репликацией, ни слова не говорится о планировании доменной структуры и структуры подразделений, обойдены молчанием вопросы, связанные с групповой политикой. Их обсуждению посвящены отдельные главы этой книги.

Репликация Active Directory

Репликация — один из основных механизмов работы Active Directory. Как только речь заходит о том, что более двух компьютеров хранят одну и ту же информацию, встает вопрос о репликации, т. е. о тиражировании этих данных между серверами, обеспечивающем их идентичность.

Репликацию используют во многих системах. Так, база SAM в Windows NT реплицируется с главного контроллера домена на резервные. Говорят, что на главном контроллере домена имеется *мастер-реплика*, а на резервных — *резервные*. Изменения в БД можно вносить только в мастер-реплику — в Windows NT она единственная. Поэтому механизм репликации Windows NT называется репликацией с одним мастером.

Репликация Active Directory выполняется по топологии с *несколькими мастерами*. При этом также встает вопрос о *слабой связанности* между партнерами по репликации, что означает возможность наличия неодинаковых данных на партнерах в конкретный момент времени. А раз так, должен существовать процесс *конвергенции*, призванный уничтожить эти различия...

Как видите, **терминов**, характеризующих репликацию Active Directory, хватает, а сколько я еще не назвал! Словом, репликация — это сложный процесс, описанный во многих книгах и достаточно подробно. Увы, читать толстые книги и разбираться в премудростях процессов ОС любят не все. Возможно, они считают, что уж коль что-то там придумали, то оно будет работать бесперебойно. Многие прошедшие

школу Windows NT вообще не понимают, что может быть сложного в этом процессе, так как им он меньше всего доставлял неприятностей.

Однако в Windows 2000 репликация в корне изменилась. Главным источником всех потенциальных проблем стало то, что репликация выполняется по модели с несколькими мастерами. Если вы не понимаете, как именно она работает, как строится топология репликации и работают обеспечивающие ее компоненты, выявить проблему и, тем более, устранить ее вам будет не по зубам.

Вот почему я рискну повториться и рассказать о некоторых краеугольных камнях репликации — это нужно для того, чтобы мы с вами говорили на одном языке.

Немного о том, как работает репликация

Итак, вспомним основные компоненты и механизмы репликации Active Directory. В первую очередь — что тиражировать?

На каждом из контроллеров домена в лесу Active Directory имеется база, в которой хранится локальная реплика трех контекстов имен:

- схемы;
- конфигурации;
- ◆ домена.

Контексты схемы и конфигурации едины для всего леса, тогда как доменный контекст имен хранится только на контроллерах «своего» домена. Эта реплика является полной, т. е. содержит все атрибуты всех объектов в домене. Полные реплики доменного контекста имен тиражируются между контроллерами домена. Реплики схемы и конфигурации тиражируются между всеми контроллерами доменов в лесу.

Если контроллер является сервером Глобального каталога (ГК), то на нем, кроме контекста схемы и конфигурации, хранятся:

- полная реплика базы объектов того домена, контроллером которого он является;
- частичная реплика всех объектов из других доменов в лесу; частичная реплика содержит только те атрибуты, для которых в схеме определен атрибут `isMemberOfPartialAttributeSet`, значение которого равно `True`.

Частичные реплики тиражируются только между ГК.

Как уже упоминалось, репликация Active Directory выполняется по схеме с несколькими мастерами. Я бы уточнил, что не просто с «несколькими», а только со всеми мастерами.

Замечание Некоторые службы каталогов допускают наличие подчиненных партнеров по репликации наряду с мастерами. Однако в Active Directory такой подход не используется.

Все контроллеры домена выступают равноправными партнерами, т. е., изменение можно внести в каталог на любом из контроллеров домена и он обязан выполнить тиражирование на все остальные контроллеры в домене.

Замечание Тиражирование схемы выполняется с одним мастером. Тиражирование неотложных изменений также использует несколько отличную топологию.

Репликация выполняется не хаотично, а в соответствии с определенной топологией. Топология определяет последовательность передачи изменений в Active Directory между контроллерами. Причем правила обновления исключают появление рассогласования в информации на разных контроллерах. Наличие правил позволяет говорить о предсказуемости внесения изменений, что значительно упрощает поиск проблем репликации.

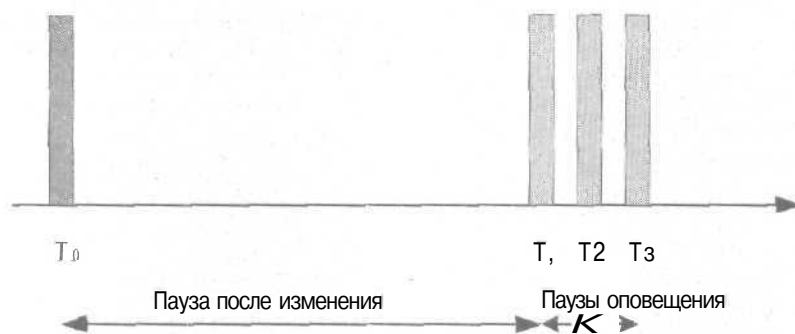
- **Первое правило** Режим «получил — сохранил — передал». Поясню его суть на примере: изменения, произошедшие на контроллере домена в Москве, не будут сразу переданы на все контроллеры домена в Санкт-Петербурге. В соответствии с топологией репликации они будут приняты тем контроллером в Москве, через который проводится репликация с Питером (сервер-форпост). На нем они будут храниться до открытия окна репликации, а потом переданы на питерский сервер-форпост и уж только с него тиражируются по питерским контроллерам. Такое поведение существенно освобождает каналы связи.
- **Второе правило** Механизм «вытягивания» информации: узнав, что на каком-то из партнеров по репликации произошли изменения, контроллер домена обращается к нему и скачивает измененную информацию к себе. Мы еще рассмотрим этот процесс подробно, а пока ограничимся тем, что сравним его с «проталкиванием» информации. Это прямо противоположный механизм тиражирования данных и подразумевает, что при изменении информации на одном из партнеров по репликации он рассылает изменения по остальным партнерам. При этом его не интересует, готов ли партнер к приему и нужны ли ему эти данные. Механизм «проталкивания» в репликации Active Directory не применяется.

- **Третье правило** Репликация Active Directory использует статус объектов для определения необходимости их обновления. Когда контроллер домена получает оповещение об изменении реплики у партнера, он сравнивает полученную информацию о статусе измененных объектов с хранящейся у него. Если, с точки зрения данного контроллера, статус объекта не изменился, то надобности в репликации нет. Если же это не так, контроллер запросит у партнера измененные объекты. Статус служит также и средством разрешения конфликтов, так как позволяет решить, какое из изменений является более «свежим», и запросить именно его.

Обновления в Active Directory

Представим, что на одном из контроллеров домена произошло изменение атрибутов объекта Active Directory. Обозначим этот момент T_0 (см. рисунок). Контроллер выдерживает после этого «паузу после изменения» и в момент T_1 сообщает об изменении своему первому партнеру по репликации внутри сайта, затем, выдержав «паузу оповещения», в момент T_2 оповещает второго партнера. Спустя очередную «паузу оповещения» информируется третий партнер и т. д., пока все партнеры по репликации не будут оповещены. Получив оповещение, партнеры запрашивают изменения. Пауза в оповещении позволяет предотвратить одновременное обращение всех контроллеров к своему партнеру.

Длительность «паузы после изменения» по умолчанию — 5 минут, «паузы оповещения» — 30 секунд. Еще раз подчеркну, что описанный процесс относится только к внутрисайтовой репликации. Межсайтовая репликация выполняется по расписанию.



Временная диаграмма оповещения партнеров по внутрисайтовой репликации

Паузы можно изменить: откройте ветвь `HKLM\System\CurrentControlSet\Services\NTDS\Parameters`. Параметр `ReplicatorNotify pause after`

modify (sec) устанавливает длительность паузы после изменения и по умолчанию равен 300. Параметр Replicator notify pause between DSAs (sec) устанавливает длительность паузы оповещения и равен 30.

Замечание Уменьшение этих параметров вряд ли приведет к сколь-
нибудь заметным результатам. Дело в том, что все срочные измене-
ния (типа паролей) тиражируются по иной *схеме*, а 5-минутного
интервала вполне хватает для распространения изменений внутри
сайта в течение 15 минут (почему это так, см. ниже). Если же вам
нужно срочно реплицировать изменения на какой-то контроллер, то
это можно сделать через оснастку Active Directory Sites and Services.

Посмотрим теперь, что происходит после *того*, как партнеры по ре-
пликации оповещены. Для этого надо напомнить о таких понятиях, как
исходные обновления и последовательные номера обновлений, ис-
пользуемые для разрешения конфликтов.

Изменения атрибутов объекта Active Directory являются атомарными
транзакциями. Если один LDAP-запрос к каталогу должен выполнить
модификацию нескольких атрибутов объекта, то этот запрос рассмат-
ривается как транзакция. Невозможность *изменения* хотя бы одного
из запрошенных атрибутов приводит к откату транзакции. Если тран-
закция была завершена, то говорят, что произошло *исходное обнов-*
ление (originating update) объекта. Если в дальнейшем это обновление
тиражируется на другой контроллер, оно становится *реплицирован-*
ным обновлением и отличается от исходного.

USN

Контроллер домена, уведомленный партнером по репликации в том,
что у него произошло обновление базы, должен как-то решить, знает
ли он об этом *обновлении*. Зачем лишний раз тиражировать обнов-
ления, если они уже известны? Отследить обновления позволяют *по-*
следовательные номера обновлений (USN — update sequence number).
USN отсчитывается на каждом контроллере домена независимо от
других контроллеров. Произошло обновление атрибута какого-то
объекта — номер *USN* увеличивается на 1. Но для каждого контролле-
ра *USN* начинает отсчитываться в разные моменты. Скажем, самый
большой *USN* будет у первого контроллера в лесу — он ведь установ-
лен раньше *всех*, а *значит*, на нем произошло больше всего измене-
ний объектов. Поэтому и бесполезно сравнивать абсолютные значе-
ния *USN* на разных контроллерах: для целей отладки важнее отсле-
живать изменение *USN* в динамике.

Измененный *USN* сохраняется вместе с реплицируемым объектом.
При этом способ сохранения зависит от типа *обновления*. Для исход-

ного обновления существует три способа записи **USN**, а для реплицированного обновления — два. Вот они.

- Для каждого измененного атрибута объекта сохраняется его *локальный* номер **USN** независимо от типа обновления. Узнать этот номер позволяет команда `repadmin /showmeta <DN` объектов. В выводимой на экран таблице значение локального **USN** будет в столбце **Loc USN**.
- Среди измененных атрибутов есть такой, чей локальный **USN** будет самым большим. Например, если у пользователя поменяли пароль и имя, локальный **USN** для этих двух атрибутов увеличится на 1. Если вслед за этим снова поменять пароль, то *увеличится* только локальный **USN** для этого атрибута. Вот это максимальное число заносится в специальный *атрибут объекта* `usnChanged`. Посмотреть значение этого атрибута можно, например, в программе **ADSI Edit**.
- Если выполняется исходное обновление объекта, то для каждого измененного атрибута записывается значение *исходного* **USN** этого атрибута. Узнать этот номер позволяет команда `repadmin /showmeta <DN` объектов. В выводимой на экран таблице значение исходного **USN** будет в столбце **Org. USN**.

USN является 64-разрядным числом, что на практике означает его уникальность в течение всей жизни контроллера домена. Если предположить, что атрибуты изменяются в **Active Directory** непрерывно со скоростью 1 атрибут в секунду, то на исчерпание запаса номеров **USN** уйдет почти 585 миллиардов лет. Наша Вселенная гораздо моложе.

Штамп

Предположим теперь, что изменения одного и того же атрибута у объекта были выполнены на двух разных контроллерах домена примерно одновременно, т. е. еще до того, как репликация раннего изменения завершилась. Нужен механизм, который бы гарантировал разрешение конфликтных ситуаций.

Таким механизмом является добавление *штампа* к любому реплицируемому атрибуту. Штамп путешествует с ним от одного партнера по репликации к другому. Если значение *штампа*, пришедшего с реплицируемым атрибутом, больше имеющегося у атрибута на контроллере, то значения локального атрибута и его штампа переписываются на новые. Если нет, изменение игнорируется.

Что содержит штамп? Информацию, аналогичную той, что иногда проставляют секретари на исходящих письмах.

- **Версия** Всякий раз, как при исходном обновлении изменяется значение атрибута, номер его версии изменяется на 1. Если атрибут никогда не изменялся, его версия равна 1.
- **Исходное время** Это тот момент времени на часах контроллера домена, когда выполнилось исходное обновление атрибута.
- ◆ **Исходный DSA** Это GUID того контроллера домена, на котором было выполнено исходное обновление атрибута.

Штамп позволяет просмотреть команда `repadmin /showmeta <DN объекта>`. Столбец Ver. содержит номера версий. Org. Time/Date — исходное время, а Originating DSA — исходный DSA. Вот пример вывода данных для пользовательского объекта:

```
repadmin /showmeta "cn=Федор Зубанов,cn=users,dc=fyodor,dc=home"
Loc. USN      Originating DSA  Org. USN      Org. Time/
                Date Ver Attribute
=====
3903 8e36de48-93cd-4b5e-9bc4-d697acea7470 2763 2001-02-06
                22:34.42 1 objectClass
3903 Site-1\DC01 3903 2002-03-17
                20:56.05 1 cn
3903 8e36de48-93cd-4b5e-9bc4-d697acea7470 2763 2001-02-06
                22:34.42 1 sn
3903 8e36de48-93cd-4b5e-9bc4-d697acea7470 2764 2001-02-06
                22:34.42 1 description
3903 8e36de48-93cd-4b5e-9bc4-d697acea7470 2763 2001-02-06
                22:34.42 1 givenName
3903 8e36de48-93cd-4b5e-9bc4-d697acea7470 2763 2001-02-06
                22:34.42 1 instanceType
3903 8e36de48-93cd-4b5e-9bc4-d697acea7470 2763 2001-02-06
                22:34.42 1 whenCreated
3903 8e36de48-93cd-4b5e-9bc4-d697acea7470 3805 2001-02-10
                14:20.35 5 homeDrive
3903 8e36de48-93cd-4b5e-9bc4-d697acea7470 2765 2001-02-06
                22:34.43 2 dBCSPwd
```

При сравнении двух штампов сначала сравниваются версии. Тот атрибут, чья версия больше, имеет преимущество, и его значение будет записано как реплицированное обновление. Если версии одинаковы, сравнивается исходное время. Атрибут, исходное время которого позже, победит. Наконец, если совершится столь маловероятное событие, что в обоих штампах исходное время также одинаково, победит тот, чей GUID больше. В последнем условии, конечно, нет никакого смысла, но ведь кто-то должен победить!

Удаление объекта

Выше рассмотрены процессы создания и модификации объектов. А как быть в случае удаления объекта? Ведь если просто удалить объект на одном из контроллеров, надо как-то оповестить другие об этом событии. В Active Directory удаление объекта равноценно его изменению. Дело в том, что объекты не удаляются физически, а просто помечаются как удаленные. Вот как это делается:

- ◆ значение атрибута `Deleted` устанавливается равным `true`;
- объект помечается как памятник, что означает, что объект удален, но не изъят из Active Directory;
- относительное отличительное имя объекта изменяется так, что его нельзя изменить с помощью LDAP-приложения;
- ◆ из всех атрибутов остаются только `objectGuid`, `objectSid`, `distinguishedName`, `nTSecurityDescriptor` и `usnChanged`;
- памятник перемещается в специальный скрытый контейнер.

После этого партнеры по репликации оповещаются о том, что произошло изменение, и репликация выполняется так, как это описано выше. Но не думайте, что все эти памятники так и остаются в Active Directory. В Active Directory каждые 12 часов выполняется сбор мусора. Этот процесс проверяет, нет ли памятников, срок существования которых завершился. Если есть, они физически удаляются из Active Directory. Мусор собирается независимо на каждом контроллере домена. Срок существования памятников по умолчанию — 60 дней. Этого хватает, чтобы выполнялась репликация на все контроллеры в домене.

Замечание Срок существования памятников (`tombstonelifetime`) и интервал сбора мусора (`garbagecolperiod`) можно изменить, определив соответствующие атрибуты объекта `CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,<имя леса>`.

Процесс репликации от А до Я

Теперь рассмотрим репликацию в подробностях. Без понимания этого процесса бесполезно заниматься поиском проблем с репликацией (ну, за исключением самых простых).

Создание объекта

Представим себе, что установлен новый контроллер домена DCA и на нем создается новый пользователь. Для простоты вместо GUID будем использовать имя контроллера, а вместо полного набора его атрибутов — только несколько.

Пусть в момент создания пользователя USN контроллера домена был равен 2763. Добавление пользователя увеличит его на 1.

Замечание В реальности при добавлении пользователя **USN** увеличивается больше, чем на 1, но для нас это не существенно: главное, что он увеличивается.

В соответствии с этим будут присвоены значения и остальным атрибутам и номерам. Для простоты все значения сведены в таблицу.

UsnCreated: 2764				UsnChanged: 2764		
Атрибут	Значение	USN	Версия	Исходное время	Исходный DSA	Исходный USN
cn	Иван Петров	2764	1	22:34.42	DCA	2764
givenname	Иван	2764	1	22:34.42	DCA	2764
userPassword	*****	2764	1	22:34.42	DCA	2764

Таким образом, выполнено *исходное добавление*.

Через 5 минут контроллер DCA оповестит своего партнера по репликации, контроллер DCB, о том, что у него произошло изменение. Текущий **USN** контроллера DCB равен 1533- После записи информации о пользователе его **USN** увеличится на 1. Соответственно изменятся значения номеров **usnChanged** и **usnCreated**. Остальные параметры штампа останутся прежними.

UsnCreated: 1534				UsnChanged: 1534		
Атрибут	Значение	USN	Версия	Исходное время	Исходный DSA	Исходный USN
cn	Иван Петров	1534	1	22:34.42	DCA	2764
givenname	Иван	1534	1	22:34.42	DCA	2764
userPassword	*****	1534	1	22:34.42	DCA	2764

Так выполнилось *реплицированное добавление*.

Модификация объекта

Допустим теперь, что немного погодя пользователь изменил пароль и изменение произошло на контроллере DCB. К этому моменту **USN** этого контроллера был равен 2211 (мало ли какие объекты модифицировались за это время). Значит, после изменения пароля **USN** контроллера увеличится на 1, а метаданные объекта будут выглядеть таю

UsnCreated: 1534				UsnChanged: 2212		
Атрибут	Значение	USN	Версия	Исходное время	Исходный DSA	Исходный USN
cn	Иван Петров	1534	1	22:34.42	DCA	2764
givenname	Иван	1534	1	22:34.42	DCA	2764
userPassword	*****	2212	2	09:30.00	DCB	2212

Заметьте, как изменились USN и штамп атрибута userPassword, а также атрибут usnChanged объекта. Теперь они указывают на то, что *исходное обновление* этого атрибута выполнено на контроллере DCB.

Обновленный атрибут тиражируется на контроллер DCA, номер USN которого к этому моменту равен 3517. Метаданные объекта записываются на этом контроллере так:

UsnCreated: 1534				UsnChanged: 3518		
Атрибут	Значение	USN	Версия	Исходное время	Исходный DSA	Исходный USN
cn	Иван Петров	1534	1	22:34.42	DCA	2764
givenname	Иван	1534	1	22:34.42	DCA	2764
userPassword	*****	3518	2	09:30.00	DCB	2212

Как видите, меняется атрибут объекта usnChanged и USN. Так выполняется *реплицированное обновление*.

Демпфирование распространения изменений

В реальной сети между контроллерами доменов может быть несколько путей, по которым выполняется репликация. Это в свою очередь может привести к тому, что одни и те же изменения придут на контроллер домена дважды, а то и трижды. Кроме того, из нашего примера можно сделать вывод о том, что, получив реплику от партнера по репликации, контроллер домена оповестит его о том, что у него произошло изменение, и предложит те данные, которые только что он от него же и получил. Словом, может возникнуть положительная обратная связь, которая породит бесконечный цикл репликаций. Ну, уж коли мы использовали термин из радиотехники (я имею в виду положительную обратную связь — ПОС), то очевидно, что оттуда же можно позаимствовать название термина борьбы с ПОС — демпфирование. Демпфирование затрудняет развитие обратной связи. Значит, и в процессе репликации нужны механизмы, которые бы не просто затрудняли развитие паразитных репликаций, но препятствовали их возникновению. К таким механизмам относятся «верхняя ватерлиния» (high watermark) и «вектор обновленности» (up-to-dateness vector).

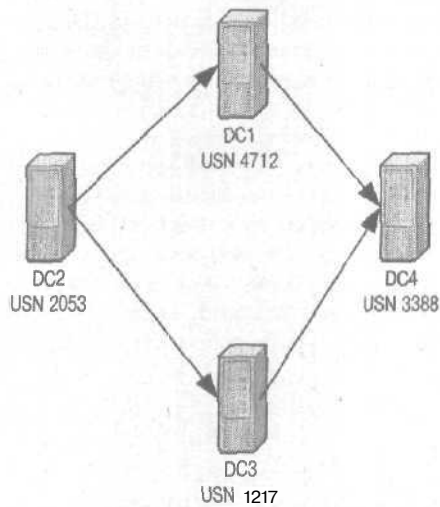
Термин «ватерлиния» пришел из мореплавания. Верхняя ватерлиния обозначает предел осадки корабля. В репликации же это число, которое на контроллере-приемнике соответствует изменениям объекта, полученным последними с контроллера-источника. С другой стороны, это число используется контроллером-источником для фильтрации объектов, предлагаемых партнерам по репликации.

Как я уже говорил, у каждого контроллера домена есть свой **USN**, отслеживающий число изменений на контроллере. Также каждый контроллер хранит таблицу с записями известных ему максимальных значений **USN** партнеров по репликации. Эта таблица называется вектором ватерлинии. Когда партнер запрашивает изменения, он посылает на контроллер-источник известное ему значение верхней ватерлинии для этого контроллера. Контроллер-источник анализирует полученное значение и реплицирует только те объекты, у которых значение атрибута **usnChanged** больше полученного значения верхней ватерлинии, так как только они еще не были им посланы партнеру. Партнер, получив обновления, изменяет значение верхней ватерлинии для данного партнера. Тем самым сокращается объем репликации.

Дополнительно к верхней ватерлинии на контроллерах домена хранится и постоянно обновляется еще одна таблица. Она содержит **GUID** контроллеров домена, выполняющих оригинальное обновление, и их номера **USN**. Эта таблица называется вектором обновленности и зависит от контекста имен. В Active Directory она записана как атрибут **replUpToDateVector** контекста имен. Когда контроллер домена запрашивает изменения для раздела каталога, он передает свой вектор обновленности на запрашиваемый контроллер. Тот, основываясь на этом значении, определяет, актуальны ли значения атрибута на запросившем контроллере, и, если нет, отправляет новое значение. Если же значение актуально, то для этого атрибута не выполняется пересылка данных.

Верхняя ватерлиния и вектор обновленности являются взаимодополняющими. В то время как верхняя ватерлиния не позволяет контроллеру-источнику рассматривать неподходящие объекты применительно к одному партнеру, вектор обновленности помогает источнику отфильтровывать неподходящие атрибуты на основе взаимоотношений между всеми источниками исходных обновлений и одним партнером. Для одного раздела Active Directory контроллер домена отслеживает верхнюю ватерлинию только тех контроллеров, с которых он запрашивает изменения, а вектор обновленности — для всех контроллеров, на которых хоть раз выполнялось исходное обновление, т. е. практически всех контроллеров, хранящих полную реплику данного раздела.

Рассмотрим пример. Пусть в домене четыре контроллера **DC1-DC4**. Будем считать, что исходные обновления к данному моменту выполнялись только на контроллерах **DC1** и **DC2** и, может быть, на контроллере **DC4**.



Пример выполнения репликации

Пусть USN для каждого из контроллеров равны DC1 — 4711, DC2 — 2052. DC3 — 1217. DC4 — 3388. Тогда вектор обновленности и верхнюю ватерлинию на контроллере DC4 можно записать как:

Вектор обновленности DC4		Верхняя ватерлиния DC4	
GUID контроллера	Максимальный номер исходного USN	GUID контроллера	Максимальный известный USN
DC1	4711	DC1	4711
DC2	2050	DC3	1217

Пусть на контроллере домена DC2 добавили нового пользователя. Его USN увеличится на 1 и станет равным 2053.

После этого контроллер DC2 оповестит своего партнера по репликации DC1 об изменении. Тот, сравнив последний известный ему USN для контроллера DC1, поймет, что нужно получить изменения, получит их и увеличит свой USN на 1, т. е. станет равным 4712. При этом, как мы уже знаем, на контроллере DC1 для этого объекта будет записано, что его исходное обновление было выполнено на контроллере DC2. Далее DC1 оповестит DC4 о происшедшем изменении. В ответ на это DC4 пошлет запрос GetChange, который будет включать следующую информацию.

- ◆ Контекст имен, для которого запрашиваются изменения (NC).
- ◆ Если на DC4 хранится неполная реплика этого контекста имен (т. е. это ГК и контроллер другого домена), то список тех атрибутов,

которые на нем хранятся для данного контекста. Будем считать, что DC4 хранит полную реплику.

- ◆ Максимальный известный номер **USN**, связанный с контроллером DC1 и с этим контекстом имен. (В рассматриваемом случае — 4711.)
- ◆ Максимальное число **измененных** объектов, которое может запросить контроллер,
- ◆ Максимальное число атрибутов, которое может запросить контроллер,
- ◆ Вектор обновленности.
 - Логическую переменную, указывающую на необходимость пересылки объекта родительского по отношению к запрошенному.

В ответ на запрос **DC1** пошлет на DC4 запрашиваемые данные, измененный номер **USN** для последнего объекта, а также флаг, указывающий, все ли данные были переданы или есть еще. Если есть другие данные, посылается дополнительный вектор обновленности. В итоге репликации вектор обновленности и верхнюю ватерлинию на контроллере DC4 можно записать так:

Вектор обновленности DC4		Верхняя ватерлиния DC4	
GUID контроллера	Максимальный номер исходного USN	GUID контроллера	Максимальный известный USN
DC1	4711	DC1	4712
DC2	2053	DC3	1217

Когда **пользователь** был добавлен на контроллере DC2, то, помимо DC1, был также оповещен и второй партнер по репликации — контроллер DC3. Аналогично тому, как это было для DC1, его **USN** после репликации изменится на **1218**.

Контроллер DC3 оповестит DC4 об изменении, и последний запросит его, пошлав свой вектор обновленности. Так как в векторе обновленности для источника изменений (т. е. DC2) уже записано актуальное значение (2053), то DC3 не станет посылать данные, а ограничится лишь номером **USN** последнего измененного объекта и **вектором** обновленности. После завершения репликации вектор обновленности и верхняя ватерлиния на контроллере DC4 будут выглядеть так:

Вектор обновленности DC4		Верхняя ватерлиния DC4	
GUID контроллера	Максимальный номер исходного USN	GUID контроллера	Максимальный известный USN
DC1	4711	DC1	4712
DC2	2053	DC3	1218

Поскольку изменений на контроллере DC4 не произошло, он не будет оповещать партнеров (DC1 и DC3), а значит, репликация завершится. Если бы не использовались механизмы демпфирования, процесс репликации пошел бы на второй круг, но в обратном направлении.

Разрешение конфликтов

Я уже показывал, как разрешать конфликты, сравнивая версии атрибутов. Однако в каталоге LDAP с несколькими мастерами могут возникать у другие конфликты. Вот они.

Возможные конфликты в Active Directory и способы их разрешения

Конфликт	Описание	Способ разрешения
Значение атрибута	На одном контроллере домена операция Modify изменяет значение атрибута. Одновременно на другом контроллере атрибуту присваивается иное значение	Атрибут с наибольшим значением штампа побеждает
Выполнение операций Add или Move под удаленным родителем, удаление непустого контейнера	Операциями Add или Move объект С делается дочерним по отношению к объекту Р. Одновременно на другом контроллере объект Р удаляется	Объект Р удаляется. Объект С переносится в контейнер <i>LostAndFound</i>
Конфликт равноправных имен	Операции Add или Move служат для создания у объекта Р дочернего объекта С1 с относительным отличительным именем R. Одновременно на другом контроллере у объекта Р создается дочерний объект С2 с таким же именем	Для объекта, чье относительное отличительное имя имеет меньшую величину штампа, создается новое уникальное имя по такому правилу: если до разрешения конфликта rdn объекта было ABC, то после разрешения оно станет ABC*CNF:<GUID>, где CNF — константа, обозначающая разрешение конфликта, а GUID — значение GUID объекта

Таким образом, все потенциальные конфликты имеют свой механизм разрешения.

Топология репликации

В Active Directory под топологией репликации понимается набор соединений, используемых контроллерами доменов для синхронизации

общих разделов каталога в масштабах леса. Заправляет процессом создания топологии репликации процесс Knowledge Consistency Checker (KCC). В дословном переводе это значит нечто вроде «проверяющий однородность знаний». О каких знаниях идет речь? Этот процесс выполняется каждые 15 минут и, проверяя доступность контроллеров доменов, создает связи между ними для тиражирования данных. Таким образом, речь идет о знаниях, известных каждому контроллеру. И именно KCC заботится о том, чтобы на каждом контроллере домена хранилась идентичная информация, т. е. он обеспечивает однородность знаний контроллеров.

Репликация призвана синхронизировать информацию в Active Directory в масштабах всего леса. Однако, как мы только что видели, фактически в каждый конкретный момент времени она выполняется только между двумя контроллерами. Решение о том, с каким контроллером установить связь для выполнения тиражирования данных, принимается на основе целого ряда факторов, таких как разделы каталога, хранимые на разных контроллерах, полнота этих разделов, принадлежность к сайту и др. Так, все контроллеры одного домена должны быть способны синхронизировать полную реплику своего раздела каталога. С другой стороны, все контроллеры в лесу обязаны синхронизировать контексты имен схемы и конфигурации. Топология репликации схемы и конфигурации отличается от топологии доменной репликации, однако в простых случаях они совпадают.

Если рассмотреть все возможные топологии репликации Active Directory, то получим:

- ◆ репликация конфигурации и схемы внутри сайта;
- репликация каждого из разделов каталога внутри сайта;
- ◆ репликация разделов ГК внутри сайта;
- ◆ репликация конфигурации и схемы между сайтами;
- репликация каждого из разделов каталога между сайтами;
- ◆ репликация разделов ГК между сайтами.

Ряд объектов Active Directory составляет основу топологии репликации. Здесь я их только перечислю — подробности см. в главе «Проектируем Active Directory».

Во-первых, это сайты и контроллеры доменов в них. Сайты — это участки сети с высокой пропускной способностью. Каждый сайт определяется минимум одной подсетью. Сведения о подсетях в сайте используются для поиска контроллеров домена. Контроллеры домена — партнеры по репликации представляются контейнерными объектами, содержащими специальный объект NTDS Settings, который хранит информацию о входящих соединениях.

Входящие соединения определяют направление репликации и представляют собой следующую категорию объектов репликации. Соединения являются однонаправленными от одного контроллера к другому. КСС пытается, там где это возможно, использовать одни и те же соединения повторно, удаляет ненужные соединения или создает новые.

Чтобы соединения между сайтами стали возможны, нужны связи, иначе КСС не сможет создать соединения, а значит, не будет и репликации. По умолчанию создается только первая связь, которую и использует КСС, но ее может быть недостаточно. Для каждой связи существует расписание, определяющее сроки выполнения репликации.

Связи не должны быть беспорядочными. Если внутри сайта практически не важно, между какими партнерами выполняется репликация, то связи между сайтами должны иметь четкий характер. С этой целью КСС выбирает контроллер, через который будут осуществляться взаимоотношения с другими сайтами. Этот контроллер называется *сервером-форпостом*. Форпосты следят за тем, чтобы репликация между партнерами шла в основном внутри сайта, а внешние связи выполнялись по графику.

Можно довериться выбору КСС и не вмешиваться в процесс назначения форпоста. Но КСС может ошибаться и назначать далеко не лучшего кандидата на роль форпоста. Дабы предупредить такие ошибки, можно вручную назначать выделенные серверы-форпосты (см. главу «Проектируем Active Directory»).

Ну и, наконец, остается *сетевой протокол*, по которому тиражируются данные при репликации. Протокол выбирается на основании того, сколь надежна связь между сайтами и что надо реплицировать. Если это качественный канал, доступность которого не вызывает сомнений, оптимальным протоколом является IP. Если же канал ненадежен, большую часть времени бывает недоступен или перегружен, то используется SMTP. Но об этом мы поговорим ниже.

Какой транспорт предпочесть?

Как вы уже знаете, в Windows 2000 два транспорта репликации. Это RPC поверх IP и SMTP. Первый служит для внутрисайтовой репликации и для синхронной межсайтовой, второй — для асинхронной межсайтовой. При этом надо придерживаться следующих правил.

- Репликация внутри сайта осуществляется всегда только посредством RPC поверх IP. Топология репликации — кольцо. Сжатие данных не используется.
- ◆ Репликаций между сайтами может использовать как RPC поверх IP, так и SMTP. Топология репликации — дерево. При передаче используется сжатие данных.

- + Репликация по SMTP поддерживается только между контроллерами из разных доменов. Контроллеры одного домена должны использовать RPC поверх IP независимо от качества канала. Следовательно, SMTP может применяться только для репликации раздела схемы, конфигурации и ГК.

Свойства внутрисайтовой и межсайтовой репликации таковы:

Сравнение свойств внутри- и межсайтовой репликаций

	Внутрисайтовая репликация	Межсайтовая репликация
Транспорт	RPC поверх IP	RPC поверх IP или SMTP
Топология	кольцо	дерево
Расписание	зависит от частоты оповещений	зависит от доступности канала
Модель репликации	Уведомление и запрос	Запрос по расписанию или хранение и передача
Сжатие	нет	да

Синхронная и асинхронная передача

Синхронная репликация Active Directory предполагает, что контроллер домена, запрашивая изменения у партнера по репликации, ожидает, пока запрашиваемый контроллер обработает запрос, составит и перешлет ответ. В период ожидания новые запросы не выполняются, т. е. в любой момент времени контроллер домена занят только одним запросом. Если у него 10 партнеров по репликации, он будет опрашивать их по очереди.

Если репликация асинхронная, то контроллер, послав запрос, не ждет ответа. Он может послать запрос следующему партнеру. Главное отличие асинхронной репликации в том, что время ответа на запрос неизвестно, в то время как при синхронной репликации гарантирован максимальный интервал ожидания.

Внутрисайтовый транспорт

Как я уже говорил, внутрисайтовый транспорт — это RPC поверх IP. Это быстрый механизм, способный с небольшими интервалами пересылать обновления внутри сайта. Так как из определения сайта следует, что все связи между контроллерами имеют большую полосу пропускания, нет смысла выполнять сжатие передаваемых данных. При обычной частоте тиражирования внутри сайта это приведет к дополнительному расходу ресурсов процессора.

Удаленный вызов процедур RPC использует динамическое назначение портов TCP. Обращаясь к Active Directory, клиент подключается по RPC к хорошо известному порту — 135. Сервер запрашивает у локатора

RPC порт, назначенный в данный момент для репликации Active Directory. По умолчанию этот порт назначается динамически при старте Active Directory и может быть любым среди портов с высокими номерами. (Поэтому в главе, посвященной планированию Active Directory, я сказал, что для обеспечения репликации через межсетевой экран надо открывать много портов.)

Номер порта можно зафиксировать. Для этого надо в ветви реестра HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters изменить параметр TCP/IP Port. Значение может быть любым, кроме зарезервированных за другими службами.

Особенности транспорта SMTP

Говоря о межсайтовом транспорте, обычно подразумевают RPC, а SMTP предпочитают не применять. Во-первых, это часто связано с тем, что в сайтах располагаются контроллеры из одного домена, что автоматически исключает использование SMTP. Во-вторых, асинхронная природа SMTP не позволяет гарантированно тиражировать изменения в течение заданного интервала. Если в удаленном сайте есть ГК, изменения до него могут доходить с большим опозданием, что при неудачном стечении обстоятельств может воспрепятствовать доступу пользователей к ресурсам или, наоборот, предоставить его в тот момент, когда он уже отобран.

Асинхронность SMTP приводит к тому, что расписание доступности канала, устанавливаемое для связи, полностью игнорируется. Что бы вы ни указали, это не будет иметь никакого значения. Можно указать лишь частоту обращения к партнеру удаленного сервера.

В то же время и RPC, и SMTP имеют некоторые общие характеристики, используемые при репликации:

- ◆ для передачи данных между сайтами посредством обоих транспортных используется сжатие данных;
- у Active Directory существует максимальное число изменений, которые можно переслать в ответ на один запрос; оно зависит от размера конфигурируемого пакета репликации;
- каждому партнеру по репликации для каждого раздела каталога может быть передан только один запрос изменений;
- ◆ изменения, пересылаемые в ответ на запрос, передаются в одном или нескольких фреймах в зависимости от общего числа изменений;
- если передача части данных сорвалась, требуется повторно передать все данные;
- ◆ если полоса пропускания мала, то для настройки используются одни и те же параметры TCP.

Помимо недостатков, SMTP имеет ряд преимуществ, делающих его порой незаменимым.

- **Асинхронность.** Помните, мы это свойство записали в недостатки? Но представьте себе жуткий канал, по которому тиражируются данные. При синхронной репликации процесс может затянуться, так как из-за постоянных тайм-аутов транзакции *будут* незавершенными, и, следовательно, потребуются выполнять многократные откаты. И пока не будет *завершена* одна транзакция, не начнется другая. При асинхронной репликации транзакции растянуты, и не нужно ждать завершения одной, прежде чем инициировать следующую. Поэтому на плохих линиях SMTP как транспорт репликации имеет преимущество.
- Трафиком SMTP можно управлять, выполнять мониторинг и защиту.
- Там, где нет трафика по протоколу IP, репликация может выполняться по SMTP. Это могут *быть, например*, участки, базирующиеся на X.400.

Управление пакетом репликации

Если на контроллере *установлено* от 100 до 1 000 Мб ОЗУ, размер пакетов репликации равен 0,01 от объема ОЗУ. С другой стороны, размер пакетов в объектах равен 1/1 000 000 от объема ОЗУ (т. е. от 100 до 1 000 объектов). Одно исключение: размер пакета для асинхронной *межсайтовой* репликации не превышает 1 Мб. Это связано с тем, что на многих почтовых системах стоит ограничение на максимальный размер передаваемых сообщений.

Эти значения по умолчанию можно изменить, определив параметры в ветви реестра `HKLM\System\CurrentControlSet\Services\NTDS\Parameters`. По умолчанию этих параметров в реестре нет.

Параметры реестра, ответственные за размер пакетов при репликации

Параметр	Назначение	Допустимая величина
Replicator intra site packet size (objects)	Для репликации RPC внутри сайта	от 1
Replicator into site packet size (bytes)	Для репликации RPC внутри сайта	от 10 ко
Replicator inter site packet size (objects)	Для репликации RPC между сайтами	от 1
Replicator inter site packet size (bytes)	Для репликации RPC между сайтами	от 10 кб
Replicator async inter site packet size (objects)	Для репликации SMTP между сайтами	от 1
Replicator async inter site packet size (bytes)	Для репликации SMTP между сайтами	от 10 кб

Автоматическая генерация топологии

Рассмотрим генерацию внутрисайтовой топологии, выполняемую КСС. Мы пойдём от простого к сложному.

Простейший случай — один контроллер домена: репликация при этом не нужна, а значит, нет и топологии репликации.

Добавим второй контроллер. Естественно, между контроллерами устанавливаются две связи: для репликации от А к Б и наоборот. Причем обе будут использоваться для репликации как доменного контекста имен, так и схемы и конфигурации.

При добавлении третьего контроллера домена образуется простейшее кольцо. Каждый из контроллеров связан с двумя другими четырьмя связями — по две связи на соединение.

Простая топология для одного контекста имен

Как только добавляется четвертый контроллер домена, между ним и двумя ближайшими контроллерами устанавливается **соединение**, как показано на рисунке. Налицо очевидная избыточность связей для контроллеров DC2 и DC3. Они, конечно могут продолжать репликацию напрямую, но есть и еще два пути: через контроллеры DC1 и DC2. Поскольку КСС стремится создать кольцо, то избыточные связи между DC2 и DC3 будут удалены.

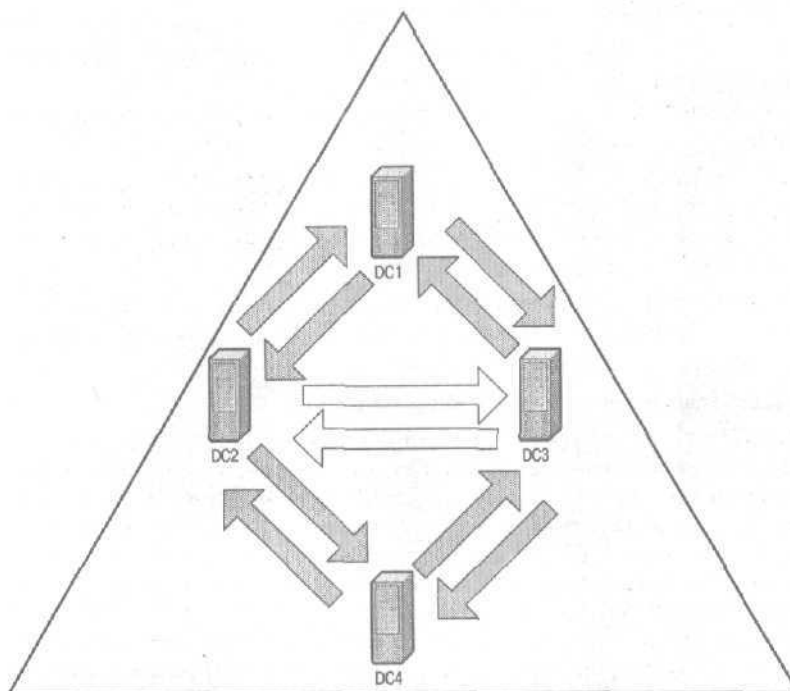
Замечание В ряде случаев КСС не удаляет избыточные связи. Их можно удалить вручную.

Как же определить, какой из контроллеров домена является ближайшим соседом? Ведь внутри сайта все соединения имеют одинаково высокую пропускную способность, а других факторов будто нет. КСС считает, что, коль естественной разницы между контроллерами нет, надо ввести искусственную и использует номера **GUID** контроллеров. Определив число доступных в момент проверки контроллеров определенного домена, он ранжирует их по возрастанию номера **GUID**. КСС, исполняемый на каждом контроллере домена, выбирает два контроллера с ближайшими номерами и создает для них односторонние связи.

Сложная топология для одного контекста имен

Если продолжить наращивание числа контроллеров, то кольцо репликации будет расти в диаметре. Сколь бесконечен этот рост? Критерий, влияющий на размер кольца и определяющий наличие дополнительных связей, есть.

Примечание Критерий внутрисайтовой репликации определяется так: между любыми двумя контроллерами одного домена в сайте должно быть не более 3 «прыжков» (hops) репликации.



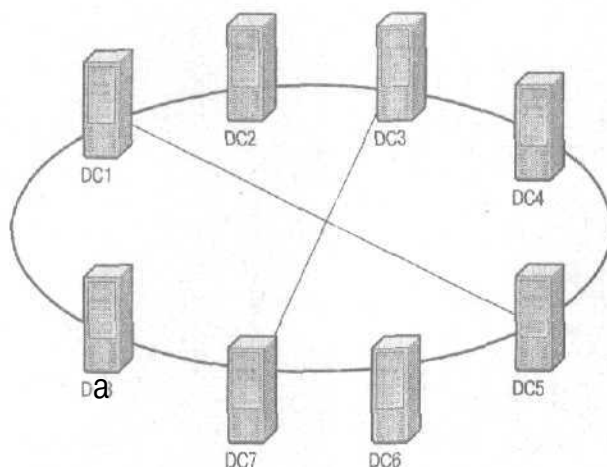
Топология репликации: если контроллеров домена всего три, то каждый связан с двумя другими. При добавлении четвертого контроллера он устанавливает связи с двумя контроллерами, непосредственные связи между которыми становятся лишними

Длительность прыжка — 5 минут (по истечении этого времени контроллер уведомляет партнера об изменении) — гарантирует, что время полной репликации внутри сайта не превышает 15 минут.

Если продолжить наращивание числа контроллеров в домене, то топология в виде кольца удовлетворяет критерию только при числе контроллеров не более 7. Стоит добавить восьмой контроллер, как мы сразу переходим к усложненной схеме генерации топологии. Каждый КСС создает произвольное дополнительное число связей с другими контроллерами. Изначально это число может быть любым, но не меньше такого, чтобы удовлетворялся критерий репликации. Например, на рисунке изображен случай 8 контроллеров. Рассмотрим процесс генерации топологии во времени.

Допустим, первым начал работать КСС на контроллере DC1. Проанализировав число контроллеров, он вычислил, что для репликации изменений с DC1 на самый дальний от него контроллер DC5 по кольцевой схеме понадобится 4 прыжка. Поэтому, кроме соединений

с ближайшими соседями, он создаст прямое соединение с DC5. Этот контроллер в свою очередь также создаст три соединения: два с ближайшими соседями и одно с DC1.



Основное правило при генерации топологии репликации — не более 3 «прыжков» между любым из контроллеров домена

Далее предположим, что КСС запущен на DC3. Он также вычислит, что нужно создать **соединение** с самым далеким от него DC7. Тот ответит на это созданием встречного соединения и пары соединений с соседями.

КСС на остальных контроллерах уже будут знать о новых соединениях и обнаружат, что им не требуется создавать дополнительные связи, кроме связей с ближайшими партнерами. Таким образом, формирование топологии репликации для данного контекста имен завершится.

В реальности совершенно не обязательно, что будет сформирована именно такая топология. Выше мы предположили, что КСС запускается на контроллерах домена в такой последовательности: DC1 — DC5 — DC3 — DC7 — DC2 — DC4 — DC6 — DC8. Если же предположить, что КСС на контроллере DC2 запущен сразу после DC5, а потом запущен КСС на DC7, то топология будет совершенно иной, и главное, связи «туда» и «обратно» не будут созданы между одними и теми же парами контроллеров. Но результат все равно будет тот же, т. е. полное соответствие критерию репликации.

Топология для нескольких контекстов имен

Что ж, усложним задачу. Пусть внутри сайта расположен не один, а два домена, т. е. кроме репликации общих контекстов схемы и кон-

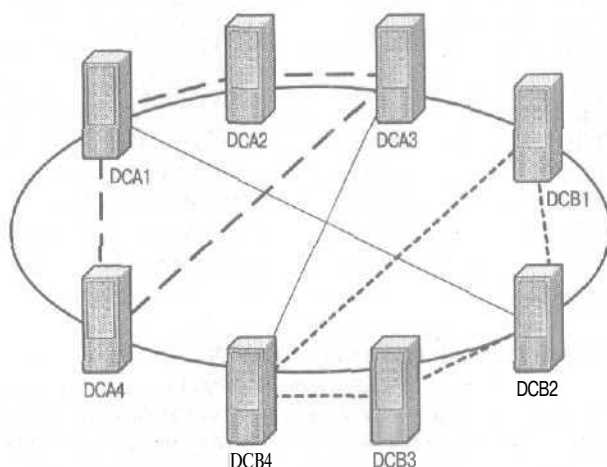
фигурации, должна выполняться раздельная репликация каждого из доменных контекстов имен.

Сначала разберемся в топологии репликации схемы и конфигурации. Не трудно догадаться, что поскольку это один контекст имен, то формирование топологии для него будет выполняться по тем же правилам, что и для одного домена в сайте. В частном случае с 8 контроллерами получим ту же топологию, что и на предыдущем рисунке.

Замечание Дальше будем считать, что в сайте нет серверов ГК.

Пусть в сайт с одним доменом добавили еще один домен, установив первый контроллер. Так как база Active Directory на этом контроллере хранит раздел того домена, для которого в сайте нет других контроллеров, то это будет равносильно единственному контроллеру в сайте, а значит, отсутствие репликации. Но не следует забывать, что раздел схемы и конфигурации должен тиражироваться на новый контроллер, а значит, он будет включен в общее кольцо для этого контекста.

После добавления еще одного контроллера для этого контекста мы добьемся того, что между двумя контроллерами установятся встречные связи. Добавление третьего контроллера приведет к образованию простейшего кольца и т. д. в точном соответствии с тем описанием, которое приведено для случая с одним контекстом имен.



Репликация каждого контекста имен выполняется по своему кольцу

Пока общее число контроллеров в двух доменах в сайте не превысит 7, топология репликации будет состоять из 3 колец: по одному для каждого доменного контекста и одного для схемы и конфигурации.

С ростом числа доменов топология будет усложняться. Но в любом случае будет соблюдаться соответствие критерию репликации.

КСС и его возможности

Вся эта интеллектуальная работа по генерации **внутрисайтовой** топологии выполняется КСС. Как мы уже знаем, КСС — это процесс, выполняемый на каждом контроллере домена. КСС не стартует сразу после запуска компьютера. Сначала он ждет некоторое время, называемое задержкой запуска топологии. По умолчанию — 5 минут.

После первого выполнения повторный запуск КСС состоится только через 15 минут. Итак, каждые 15 минут КСС выполняет свою работу.

Замечание Указанные **интервалы** устанавливаются по умолчанию. Их можно изменить в ветви реестра `HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters`. На время начальной задержки влияет параметр `Repl topology update delay (secs)`. По умолчанию он равен 300 секундам. Если у вас не очень быстрый компьютер, а служба DNS установлена на нем же, это значение стоит увеличить до 500 секунд. Интервал времени между последовательными запусками КСС определяет параметр `Repl topology update period (secs)`, по умолчанию — 900 секунд.

Что же конкретно выполняет КСС? У него две задачи.

1. Основываясь на сетевой топологии, описываемой объектами Active Directory, **создает** объекты связи, используемые для репликации:
 - для источников **внутри сайта** — входящей по отношению к контроллеру домена, на котором выполняется КСС;
 - для источников в других сайтах — входящей по отношению к тому сайту, в котором **выполняется** КСС; при этом контроллер, **на** котором он работает, должен быть выбран генератором **межсайтовой** топологии.
2. Преобразует объекты **связи** Active Directory, созданные как КСС, так и администратором, в **конфигурацию**, понятную для механизма репликации.

Этот процесс не имеет интерфейса с пользователем в привычном понимании. Нет ни утилиты командной строки, ни графической консоли, позволяющих задавать параметры работы или управлять запуском/остановкой процесса. Все сведения о работе КСС можно почерпнуть из **журнала** регистрации. Степень подробности зависит от параметра «Knowledge Consistency **Checker**» в ветви реестра `HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics`. Если он равен 3 и выше, в журнал будет заноситься максимум **информации**, однако к такому радикальному методу стоит прибегать только в крайних **слу-**

чаях и на непродолжительное время, так как производительность контроллера домена очень сильно **снижается**.

Работой КСС можно управлять следующими инструментами.

- **Редактор реестра** служит для определения параметров КСС на одном отдельно взятом контроллере домена.
- Оснастка **Active Directory Sites and Services** позволяет контролировать и корректировать топологию репликации.
- ◆ **ADSIEdit** или **Ldp** служат для изменения атрибутов объекта CN=NTDS Site Settings,CN=<имя сайта>,CN=Sites,CN=Configuration,<имя леса>. Позволяют изменять работу всех КСС в сайте.
- ◆ **Сценарии** удобнее всего использовать для выполнения комплексных операций над всеми КСС в сайте.

Вот простейшие примеры использования этих инструментов. Пусть, редактируя топологию репликации, вы случайно **лишили** один из **сайтов** всех объектов связи. Это, естественно, приведет к прекращению тиражирования данных между этим сайтом и другими. Установив через реестр **уровень** диагностики работы КСС равным 3- вы обнаружите в журнале регистрации **сообщение** об ошибке 1311. В соответствии с этим сообщением об ошибке вы откроете Active Directory Sites and Services и выполните корректировку

Второй пример. Вам может понадобиться остановить КСС на всех контроллерах домена, например, при оптимизации **внутрисайтовой** топологии в больших сетях. Для этого вы открываете, скажем, ADSIEdit, находите объект CN=NTDS Site Settings,CN=<имя сайта>,CN=Sites,CN=Configuration,<имя леса> и измените значение атрибута options. Если ему задать 1. автоматическая генерация **внутрисайтовой** топологии остановится.

Генератор межсайтовой топологии

Среди задач, выполняемых КСС, особенно интересна генерация объектов связи для межсайтовой репликации. Рассмотрим ее подробнее,

Внутри сайта есть один контроллер домена на котором КСС выполняет, помимо обычных, и дополнительные обязанности. Он анализирует доступность партнеров по репликации из других сайтов для серверов-форпостов. При этом сам он может и не быть форпостом (скорее всего так и будет). Такой сервер принято называть генератором межсайтовой топологии ISTG. Обнаружив необходимость создания нового объекта связи, ISTG изменяет Active Directory на своем локальном контроллере домена. Это изменение тиражируется с помощью обычного механизма внутрисайтовой репликации на все контроллеры домена в том числе и на серверы-форпосты. Процессы КСС, которые работают на форпостах, анализируют пришедшее изменение и

преобразуют объекты связи в соединения, используемые для репликации из удаленных сайтов.

ISTG также периодически записывает в Active Directory атрибут, указывающий на то, что именно он является генератором межсайтовой топологии для данного сайта.

Замечание Генератор межсайтовой топологии всегда только один внутри сайта независимо от числа контекстов имен, которые должны быть реплицированы.

По умолчанию такая запись выполняется каждые 30 минут. Вы можете задать иную величину интервала в параметре KCC site generator renewal interval (minutes) в ветви реестра HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters. Эта информация тиражируется на все остальные контроллеры домена в сайте. KCC, исполняемые на них, проверяют, когда была выполнена последняя запись указанного атрибута. Если в течение последнего часа такая запись не была выполнена, выбирается новый сервер ISTG. Срок, в течение которого должно произойти обновление атрибута принадлежности к ISTG, задается параметром KCC site generator fail-over (minutes) в той же ветви реестра.

Генератором межсайтовой топологии по умолчанию является самый первый контроллер домена в сайте. Если он вовремя не изменит атрибут в Active Directory, на его место будет выбран тот контроллер, чей номер GUID будет следующим в порядке возрастания. При возникновении этого события повторно произойдет выбор контроллера по тому же принципу. При этом самый первый контроллер будет находиться в конце очереди.

Узнать, какой контроллер домена в сайте является генератором межсайтовой топологии, позволяет значение атрибута interSiteTopologyGenerator у объекта CN=NTDS Site Settings,CN=<имя сайта>,CN=Sites,CN=Configuration,<имя леса>. Оно содержит отличительное имя контроллера, выполняющего эту роль.

Что произойдет, если выборы нового ISTG состоялись, а прежний еще жив? В этом случае временно могут существовать соединения, созданные этими двумя компьютерами. Но стоит репликации в сайте завершиться, «старый» генератор прекратит свою деятельность, а созданные им соединения будут удалены.

Теперь вернемся к рассмотренной выше ситуации, при которой требуется остановить работу ISTG. Как об этом написано в главе «Проектирование Active Directory», KCC имеет ограничение, выражаемое формулой:

$$(1+D)*S^2 \leq 100000$$

где **D** — число доменов, а **S** — число сайтов.

При большом числе сайтов КСС должен быть **остановлен**. Для этого надо изменить у объекта CN=NTDS Site Settings, CN=<имя сайта>, CN=Sites, CN=Configuration, <имя леса> значение атрибута options. Допустимые значения;

- 0 — по умолчанию; КСС и ISTG работают в нормальном режиме;
- 1 — генерация топологии **внутрисайтовой** репликации остановлена;
- 16 — генерация **топологии** межсайтовой репликации остановлена;
- 17 - КСС и ISTG остановлены.

На практике оказывается неразумно останавливать КСС и генератор топологии межсайтовой репликации. При этом бремя отслеживания соединений и объектов связи ляжет на администратора. Он должен просчитывать оптимальную топологию и заботиться о ее поддержании. Альтернативой является временное включение/отключение КСС в периоды незначительной загрузки сети. При включении КСС проверит топологию внутри сайта и между сайтами и, если надо, обновит их. Затем его можно выключить до следующего раза. Нагрузка, которая при этом ляжет на контроллеры доменов, не скажется на пользователях, так как эту работу лучше выполнять во вне рабочее время.

Управление работой КСС одновременно в нескольких сайтах облегчают **сценарии**. Следующий сценарий на VBScript позволяет останавливать/возобновлять автоматическую генерацию топологии репликации сразу во всех сайтах. Не составит никакого труда упростить его и использовать для тех же целей, но внутри одного сайта.

Сценарий остановки и запуска КСС

```
On Error Resume Next
'прием параметров командной строки
Set Args = WScript.Arguments
if Args.Count=0 then Wscript.Quit
If lcase(Args(0))="/enable" or lcase(Args(0))="/disable" then
Call ConfigureKCC()
end if

Public Sub ReportError ()
'сообщить об ошибке
wscript.Echo "Произошла ошибка: (" + cstr(hex(err.number)) + _
" ) " + cstr(err.description)
End Sub

Public Sub ConfigureKCC ()
```

см. след. стр.

On Error Resume Next

```

'узнать имя локального компьютера
wscript.echo "Подключение к компьютеру..."
set localMachine=GetObject("LDAP://localhost/rootdse")
if err.number <> 0 then ReportError:Wscript.Quit
ServerName=localMachine.get("dnsHostName")
if err.number <> 0 then ReportError:WScript.Quit
wscript.echo "Обнаружен локальный компьютер " + ucase(ServerName)

'получить конфигурацию контекста имен
configNC=localMachine.get("configurationNamingContext")
if err.number < 0 then ReportErrorWscript.Quit
wscript.echo "Контекст имен конфигурации: " + configNC

'подключиться к контейнеру Sites
Set ObjSites = GetObject("LDAP://" & ServerName & "/CN=Sites,"
    & configNC)
objSites.filter = array("Site")
For each obj in ObjSites
wscript.echo "Имя сайта: " + obj.CN
Set SiteSettings = Obj.GetObject("nTDSiteSettings", "CN=NTDS Site
    Settings")

'извлечь значение атрибута options
origOptions=SiteSettings.Get("options")
if hex(err.number) = "8000500D" then origOptions=0

elseif err.number=0 then
'ничего не надо
else
ReportError:Wscript.Quit
end if
modOptions=origOptions

'выяснить, что делать с KCC
if lcase(Args(0))="/disable" then
'запретить KCC, если он разрешен, или оставить как есть
if modOptions And 16 then
wscript.echo " Автоматическая генерация топологии запрещена.
    Изменений не вносится."
else
modOptions=modOptions Or 16
wscript.echo " Автоматическая генерация топологии разрешена. Запрещаем."

```

см. след. стр.


```
SiteSettings.Put "options", mod2Options
SiteSettings.SetInfo
if err.number <> 0 then
'если значения еще нет, то все нормально
if hex(err.number) = "8000500D" then
'записываем значение
else
ReportError
wscript.echo "Ошибка изменения значения атрибута options."
wscript.echo "Проверьте правильность текущего значения."
wscript.echo "Выполнение прервано."
Wscript.Quit
end if
end if
end if
else
'если автоматическая генерация запрещена, то разрешить.
Иначе оставить неизменным.
if modOptions And 16 then
wscript.echo " Автоматическая генерация топологии запрещена.
Разрешаем."
mod2Options=modOptions XOr 16
SiteSettings.Put "options", mod2Options
SiteSettings.SetInfo
if err.number <> 0 then
'если значения еще нет, то все нормально
if hex(err.number) = "8000500D" then
'записываем значение в любом случае
else
ReportError
wscript.echo " Ошибка изменения значения атрибута options."
wscript.echo " Проверьте правильность текущего значения."
wscript.echo " Выполнение прервано."
Wscript.Quit
end if
end if
else
wscript.echo " Автоматическая генерация топологии разрешена.
Изменений не вносится."
end if
end if
Next

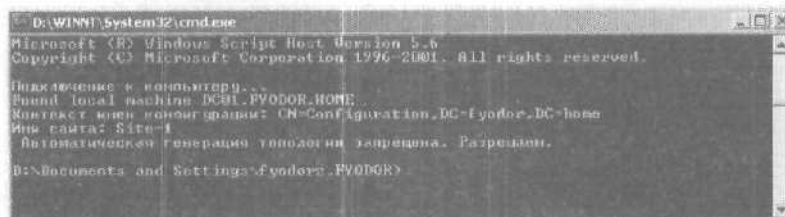
End Sub
```

Для запуска сценария скопируйте текст в файл с расширением VBS и в командной строке введите:

```
cscript <имя файла>.VBS /аргумент
```

где аргумент — enable для разрешения автоматической генерации топологии, а disable — для ее запрещения.

Вот результат работы сценария (не забудьте, что вы должны обладать достаточными административными полномочиями в рамках леса):



```
D:\WINNT\System32\cmd.exe
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

Подключение к компьютеру...
Found local machine DC01.FYODOR.HOME
Контекст имен конфигурации: CN=Configuration,DC=fyodor,DC=home
Имя сайта: Site-1
Автоматическая генерация топологии запрещена. Разрешаю.

B:\Documents and Settings\fyodor\FYODOR>
```

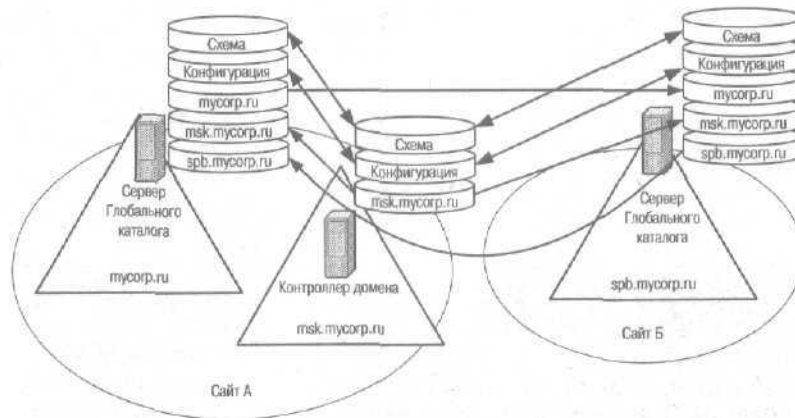
Пример работы сценария: разрешение автоматической генерации топологии

Репликация глобальных каталогов

Серверы ГК, как известно, отличаются от остальных контроллеров домена тем, что, помимо полной реплики того пространства имен, которому принадлежит контроллер, а также реплик конфигурации и схемы, они хранят усеченные версии реплик остальных разделов Active Directory. Необходимость хранения того или иного атрибута в ГК определяет атрибут `isMemberOfPartialAttributeSet`. Если его значение изменяется (с true на false или наоборот), то в течение следующего цикла репликации он или включается в частичную реплику, или изымается из нее.

Замечание Данный процесс порождает значительный трафик репликации, так как обновляется не только данный атрибут, но и все объекты, обладающие данным атрибутом.

Партнером по репликации ГК могут выступать как обычные контроллеры доменов, так и другие серверы ГК. Допустим, в сайте А находятся два домена `mysocp.ru` и `msk.mysocp.ru`, а в сайте Б — домен `spb.mysocp.ru`. Сначала будем считать, что в каждом сайте — по одному серверу ГК. Для ясности расположим ГК в сайте А на контроллере домена `mysocp.ru`. Тогда полную реплику контекста `mysocp.ru` он будет получать от партнеров по репликации в домене `mysocp.ru`, частичную реплику `msk.mysocp.ru` — от одного из контроллеров домена `msk.mysocp.ru`, с которым будет установлена связь репликации, а частичную реплику `spb.mysocp.ru` — с сервера форпоста в сайте Б.



Репликация Глобальных каталогов

Специально для этого будет установлена новая связь репликации, либо будет использована имеющаяся связь репликации схемы и конфигурации. Многое в этом процессе зависит от того, является ли сервер-форпост в сайте А выделенным. Если да, то скорее всего для репликации ГК будут задействованы связи репликации схемы и конфигурации; нет — сервер ГК в сайте А будет назначен форпостом, и будет использована новая прямая связь.

Теперь добавим в сайт А еще один сервер ГК. Столь незначительное изменение приведет к тому, что одному из этих серверов ГК не понадобится создавать связь репликации с форпостом в сайте Б. Он может получить всю нужную информацию от своего партнера, А вот тому уже придется действовать так, как описано выше.

А что, если все контроллеры домена в лесу являются также и серверами ГК? Очевидно, для репликации будут задействованы связи, созданные для репликации схемы и конфигурации. Таким образом, нагрузка на КСС при этом снижается, но трафик репликации растет.

Репликация критических событий

Все изменения тиражируются между контроллерами доменов не сразу, а на основе оповещений или по расписанию. По умолчанию полное время репликации внутри сайта — около 15 минут, а между сайтами определяется расписанием и числом сайтов, связанных с сайтом-источником, и также составляет не менее 15 минут. В то же время существуют события в Active Directory, информация о которых должна тиражироваться сразу на все контроллеры домена. Перечень этих событий зависит от типа взаимодействующих контроллеров. Это может быть взаимодействие между контроллерами Windows 2000 и между контроллером Windows NT 4.0 и контроллером Windows 2000.

Критические события репликации**Windows 2000 <—> Windows 2000****Windows 2000 <—> Windows NT 4.0**

Репликация вновь заблокированных учетных записей

Изменение секрета LSA (особенно доверительной составляющей учетных записей компьютеров)

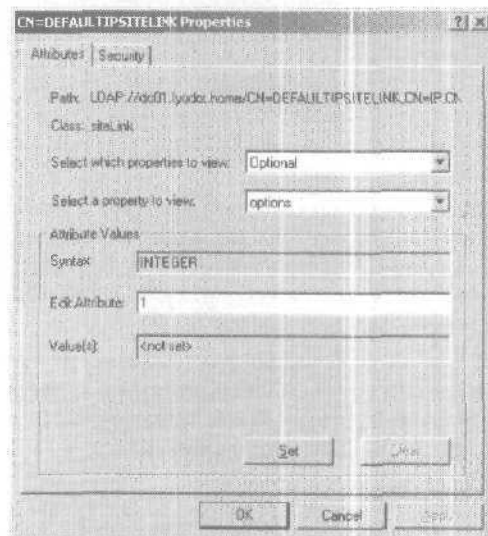
Изменение состояния RID-мастера

Репликация вновь заблокированных учетных записей

Изменение секрета LSA (особенно доверительной составляющей учетных записей компьютеров)

Изменение пароля доверительных отношений между доменами

Внутри одного сайта оповещения о таких изменениях тиражируются между контроллерами, а вот что касается нескольких **сайтов**, то тут все гораздо хуже. По умолчанию оповещения не тиражируются по **межсайтовым** связям. А это значит, что в худшем случае информация, например о новом пуле относительных адресов, дойдет до удаленного контроллера домена не **ранее**, чем через **15 минут**, что может привести к **появлению** объектов с одинаковыми **ID**.

**Настройка трансляции оповещений между сайтами**

Если такие задержки в распространении критических изменений между сайтами недопустимы, можно разрешить распространение оповещений между сайтами. Для этого нужно изменить значение атрибута **options** для того объекта связи между сайтами, тиражирование изменений по которому наиболее критично. Выполнить это позволяют утилиты **ADSIEdit** или **Ldp**. Скажем, если между двумя сайтами су-

существует объект связи DEFAULTIPSITELINK, то отличительное имя этого объекта в Active Directory запишется как CN=DEFAULTIPSITELINK, CN=IP, CN=Inter-Site Transports, CN=Sites, CN=Configuration, <имя домена>. Значение атрибута options устанавливается либо в 1 (если до этого оно не было установлено), либо определяется, исходя из побитовой операции ИЛИ.

В результате данной модификации между сайтами будут передаваться все оповещения о срочных и не очень изменениях в Active Directory так, как это было бы внутри сайта. Замечу, что трансляция изменений возможна только для связей по протоколу IP, но не по SMTP.

Замечание Не рекомендуется активизировать трансляцию изменений по коммутируемым каналам, так как это приведет к неоправданно завышенному времени связи.

Тиражирование паролей

Не менее критичной информацией являются пароли учетных записей пользователей. В Windows NT изменить пароль можно было только на главном контроллере домена, в Windows 2000 — на любом. Это в свою очередь порождает следующую проблему. Допустим, в сети два сайта — А и Б, и в каждом по контроллеру домена. Пусть администратор изменил пароль на контроллере в сайте А. Некоторое время спустя пользователь пытается зарегистрироваться в сети в сайте Б. Пароль передается на локальный контроллер домена, который к этому моменту времени еще ничего не знает о выполненном изменении. Если бы не было специального механизма, доступ пользователя в сеть был бы отвергнут.

В Windows NT в такой ситуации пользователь переадресовывался на главный контроллер домена, где и проходил авторизацию. Аналогичный механизм есть и в Windows 2000. Когда администратор изменяет пароль на любом из контроллеров, пароль «проталкивается» на имитатор PDC, который оповещает своих партнеров по репликации об изменении, и начинается обычный цикл репликации. Пользователь, пытающийся зарегистрироваться на контроллере, до которого еще не дошла репликация, будет переадресован на имитатор PDC, где ему будет предоставлено право регистрации.

Этот механизм работает по умолчанию. Однако в случае медленных связей между сайтами он может быть другим. Для этого в ветви реестра HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters надо изменить значение параметра AvoidPDConWan. По умолчанию оно равно 0. Если задать 1, новый пароль не будет передаваться на имитатор PDC с удаленного контроллера домена в ускоренном режи-

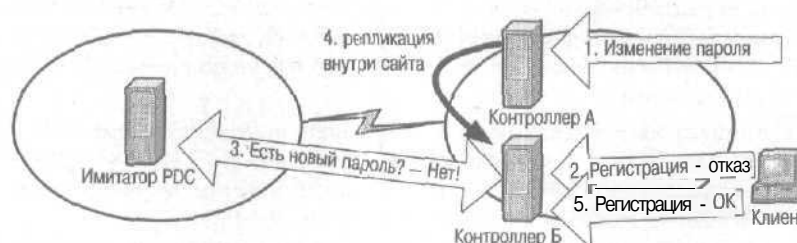
ме. Вместо этого будет задействован обычный механизм репликации. Данный режим целесообразно применять на коммутируемых линиях.



Репликация изменения пароля по умолчанию

Если в нашем примере предположить, что в сайте Б два контроллера домена, на одном из которых администратор изменяет пароль, на другом регистрируется пользователь, а имитатор PDC расположен в сайте А, то значение 1 параметра `AvoidPDConWan` в 1 приведет к тому, что:

- новый пароль не передается в ускоренном режиме на имитатор PDC;
- ◆ пользователь не обращается к имитатору PDC, если контроллер, к которому он подключился, не может его авторизовать;
- ◆ изменение пароля будет тиражировано внутри сайта Б обычным образом.



Репликация изменения пароля при значении 1 параметра AvoidPDConWan

Замечание Хотя параметр `AvoidPDConWan` на контроллере домена равен 1, контроллер обратится к имитатору PDC, если пользователь введет неверный пароль. Эта ошибка исправлена только в SP2.

Диагностика репликации

Работа репликации Active Directory зависит от:

- работоспособности контроллеров доменов;

- пропускной способности и доступности каналов связи;
- ◆ настройки серверов DNS;
- конфигурации топологии репликации;
- конфигурации параметров системы безопасности (пароли, доверительные отношения, IPSec);
- знаний и умений администраторов.

Для диагностики репликации могут применяться разные инструменты как с интерфейсом командной строки, так и снабженные графическим интерфейсом. Выбор зависит от того, какой способ администрирования вы предпочитаете: удаленный в командной строке или удаленный в терминальном режиме.

Большая часть этих инструментов входит в состав вспомогательных средств Support tools, поставляемых на том же компакт-диске, что и система. Эти инструменты наряду со средствами Windows 2000 Resource Kit должны быть установлены на всех контроллерах домена, а также на рабочих станциях, предназначенных для администрирования.

Если вы делали все правильно и следовали моим советам, проблем с репликацией не должно быть вообще. Легче всего убедиться в этом, если;

- ◆ поискать в журналах регистрации записи об ошибках и предупреждения, относящиеся к системе репликации Active Directory;
- ◆ запустить оснастку Active Directory Sites and Services, выбрать любые соединения и выполнить команду Replicate now; сообщение об успешном завершении репликации будет свидетельством того, что выбранный сервер выполнил загрузку информации по указанному соединению.

Данный способ пригоден, если у вас один сайт и небольшое число контроллеров домена. В крупной сети такая методика может оказаться неэффективной. Ее можно рассматривать только как средство для локальной диагностики и решения небольших проблем.

Как известно, репликация выполняется между партнерами на основании их GUID. Номера GUID записаны в зоне DNS `_msdcs.<имя леса>` (подробнее см. главу «Установка Active Directory»). Для контроля доступности этой зоны и ее содержимого служит утилита Nslookup.

Основными инструментами, позволяющими контролировать топологию репликации и состояние партнеров по репликации являются `gpadmin` (интерфейс командной строки) и `repmon` (графический интерфейс).

Комплексную информацию о состоянии контроллеров доменов и базе Active Directory предоставляет DsaStat. Он позволяет сравнить содержимое разделов Active Directory на двух разных контроллерах или в

двух ГК. Удобно использовать сценарии диагностики, которые будут вызывать данные утилиты в процессе своей работы.

В диагностике репликации надо придерживаться определенной последовательности. Во-первых, надо решить, для какого контроллера домена выполнить диагностику. Я уже говорил, что обычно репликация работает сразу и без проблем. Поэтому в качестве контроллера выберем тот, где возникли проблемы: сообщения об ошибках в журнале регистрации, невозможность регистрации пользователей или что-то в этом роде.

Второе — выясните партнеров по репликации. По возможности надо оценить топологию репликации для разных контекстов имен, наличие связи с ними, наличие межсайтовых связей (если партнеры находятся в других сайтах), доступность информации о партнерах в DNS. Затем надо попытаться выполнить репликацию вручную. Для этого можно выполнить самый широкий спектр утилит и программ, начиная со стандартной оснастки Active Directory Sites and Services.

Если репликацию выполнить не удастся, то переходим к этапу поиска и устранения проблем. Понимая, как работает репликация, и зная доступные инструменты, вы справитесь с этой задачей без особых усилий. В противном случае поиск проблем может затянуться.

Вот почему после того, как мы подробно рассмотрели механизмы репликации, надо остановиться на инструментах диагностики. Мы обсудим их в связи с поставленными задачами. Для каждого типа задач мы рассмотрим применение всех доступных инструментов.

Выяснение списка партнеров по репликации

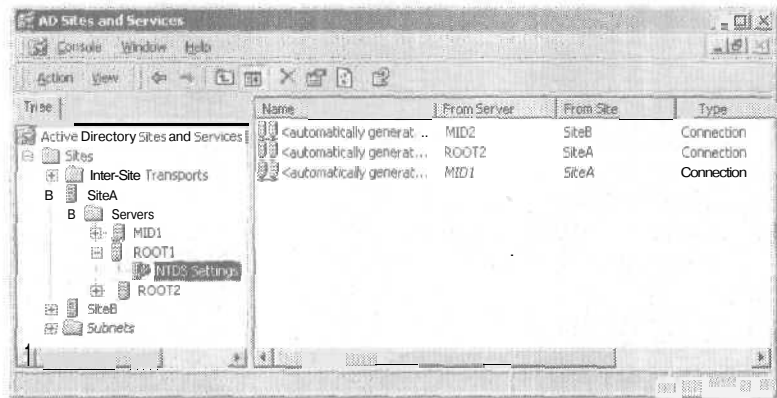
Для выяснения списка партнеров по репликации для данного контроллера домена удобно использовать:

- стандартную оснастку Active Directory Sites and Services;
- утилиту repadmin с ключом /showreps;
- графическую программу Replication Monitor.

Active Directory Sites and Services

Оснастка является стандартной, и вы обязаны уметь ее применять. Поэтому я лишь напомню, как с ее помощью определить партнеров по репликации данного контроллера. Сразу скажу, что из предлагаемых инструментов она обладает минимальными возможностями.

Итак, как только вы ее запустите на любом из контроллеров домена, появится такое окно:



Окно оснастки Active Directory Sites and Services

Открыв в левой части ветвь, соответствующую выбранному серверу, и щелкнув объект NTDS Settings в правой части, вы увидите перечень соединений с другими контроллерами. Информация, которой вы при этом обладаете, — имя сервера-партнера и сайта, в котором он находится. Информация о реплицируемых контекстах имен доступна только в окне свойств, а о том, когда была последняя удачная или неудачная репликация, — недоступна вообще.

Repadmin /showreps

Гораздо более подробную информацию позволяет получить `repadmin`. Ниже приведен образец выводимой информации с комментариями. Начинается вывод с сообщения о контроллере домена, на котором запущена утилита. Из этой секции видно, к какому сайту принадлежит контроллер и является ли он сервером ГК. Поля `objectGuid` и `invocationID` — это одноименные атрибуты объекта NTDS Settings для данного контроллера домена. В нашем примере они равны, хотя это не всегда так. Для целей диагностики представляет интерес значение `objectGuid`. Именно это значение должно быть представлено в качестве записи CNAME в DNS-зоне `_msdcs.<имя леса>`. Любой из партнеров по репликации будет искать данный контроллер в DNS не по имени, а по значению `objectGuid`.

```
Default-First-Site-Name\ROOT1
```

```
DSA Options : IS_GC
```

```
objectGuid : a4818f4f-bd9a-4dd9-b8f9-f4e26a84eb7a
```

```
invocationID: a4818f4f-bd9a-4dd9-b8f9-f4e26a84eb7a
```

Далее следует перечень партнеров по репликации, информация с которых тиражируется на данный контроллер. Партнеры рассортиро-

ваны по контекстам имен. В рассматриваемом примере специально были созданы условия для возникновения ошибок. Разбор этих ошибок проведем чуть ниже, а пока ограничимся только лишь констатацией факта их наличия.

```
==== INBOUND NEIGHBORS =====
CN=Schema,CN=Configuration,DC=mycorp,DC=ru
Default-First-Site-Name\MID1 via RPC
objectGuid: 19c9dbc3-d5d2-47cc-94e3-5135adfc4bcb
Last attempt @ 2002-05-07 13:00.52 failed, result 8524:
    Can't retrieve message string 8524 (0x214c), error 1815.
Last success @ 2002-05-06 19:52.36.
4 consecutive failure(s).
Default-First-Site-Name\ROOT2 via RPC
objectGuid: a6563e8f-9a97-40a9-9c28-23ba4f348593
Last attempt @ 2002-05-07 13:39.47 was successful.
```

Из предыдущего раздела видно, что для контекста схемы у рассматриваемого контроллера домена есть два партнера по репликации: ROOT2 и MID1. Оба этих партнера принадлежат к тому же сайту, и репликация выполняется по протоколу IP (RPC через IP). Тиражирование данных с компьютера ROOT2 было успешным, тогда как с компьютера MID1 его уже четырежды постигала неудача, а последняя удачная попытка была почти сутки назад. Практически та же ситуация наблюдается и для контекста конфигурации.

```
CN=Configuration,DC=mycorp,DC=ru
Default-First-Site-Name\MID1 via RPC
objectGuid: 19c9dbc3-d5d2-47cc-94e3-5135adfc4bcb
Last attempt @ 2002-05-07 13:01.13 failed, result 1722:
    Can't retrieve message string 1722 (0x6ba), error 1815.
Last success @ 2002-05-06 21:48.10.
2 consecutive failure(s).
Default-First-Site-Name\ROOT2 via RPC
objectGuid: a6563e8f-9a97-40a9-9c28-23ba4f348593
Last attempt @ 2002-05-07 13:39.47 was successful.
```

Далее идет информация о партнерах по репликации доменного контекста mycorp.ru. Для рассматриваемого контроллера есть только один партнер по репликации этого контекста — ROOT2, и проблем с тиражированием не наблюдается,

```
DC=mycorp,DC=ru
Default-First-Site-Name\ROOT2 via RPC
ObjectGuid: a6563e8f-9a97-40a9-9c28-23ba4f348593
Last attempt @ 2002-05-07 13:39.47 was successful.
```

Так как рассматриваемый сервер является ГК, у него должны быть установлены связи репликации с другими ГК или контроллерами дру-

гих доменов. Ниже видно, что для контекста имен msk.mycorp.ru существует один партнер — сервер MID1, связи с которым уже не было в течение двух последовательных попыток.

```
DC=msk,DC=mycorp,DC=ru
Default-First-Site-Name\MID1 via RPC
objectGuid: 19c9dbc3-d5d2-47cc-94e3-5135adfc4bcb
Last attempt o 2002-05-07 13:02.16 failed, result 1722:
    Can't retrieve message string 1722 (0x6ba), error 1815.
Last success @ 2002-05-06 21:47.40.
2 consecutive failure(s).
```

Следующий блок информации — сообщение о партнерах по репликации, которым будут рассылаться оповещения в случае изменений на контроллере ROOT1.

==== OUTBOUND NEIGHBORS FOR CHANGE NOTIFICATIONS =====

Все партнеры тут тоже разбиты по контекстам имен. Для контекстов схемы и конфигурации существуют те же два партнера: ROOT2 и MID1. Только теперь в отличие от предыдущего случая нам неизвестно, получили ли партнеры уведомления об изменениях и забрали ли они новую информацию. Для этого нужно запустить `repadmin` на этих компьютерах либо указать в командной строке их имена.

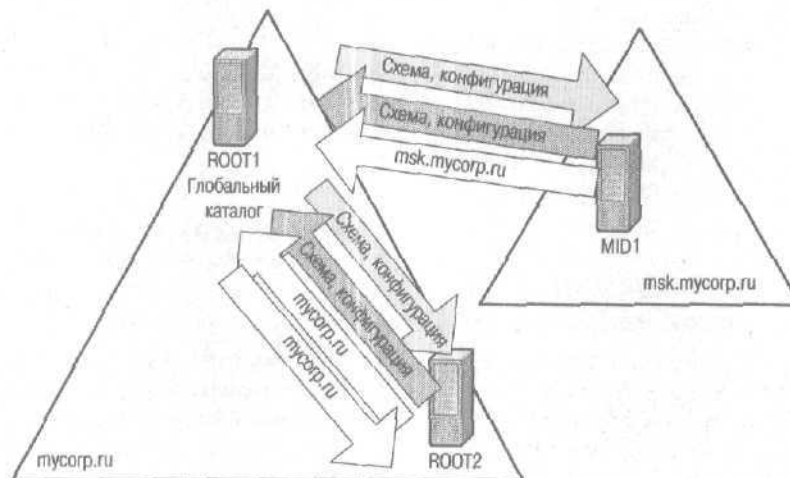
```
CN=Schema,CN=Configuration,DC=mycorp,DC=ru
Default-First-Site-Name\MID1 via RPC
ObjectGuid: 19c9dbc3-d5d2-47cc-94e3-5135adfc4bcb
Default-First-Site-Name\ROOT2 via RPC
objectGuid: a6563e8f-9a97-40a9-9c28-23ba4f348593
CN=Configuration,DC=mycorp,DC=ru
Default-First-Site-Name\MID1 via RPC
objectGuid: 19c9dbc3-d5d2-47cc-94e3-5135adfc4bcb
Default-First-Site-Name\ROOT2 via RPC
objectGuid: a6563e8f-9a97-40a9-9c28-23ba4f348593
```

Партнер по репликации контекста mycorp.ru тоже только один. А вот оповещаемых партнеров по репликации контекста msk.mycorp.ru нет. И это правильно, так как данный контроллер домена не входит в домен msk.mycorp.ru, а является всего лишь сервером ГК. Значит, он не может быть инициатором изменений в данном контексте имен и не может оповещать партнеров.

```
DC=mycorp,DC=ru
Default-First-Site-Name\ROOT2 via RPC
objectGuid: a6563e8f-9a97-40a9-9c28-23ba4f348593
```

Анализ данной информации позволяет построить топологию репликации для данного примера. Она изображена на рисунке ниже. Понятно, что это не полная топология, а только та ее часть, которая

«видна» с одного отдельно взятого сервера на основании приведенной информации. Для построения полной топологии нужно запустить утилиту `repadmin` на каждом контроллере домена.



Топология репликации, построенная на основании результатов, предоставленных `repadmin /showreps`

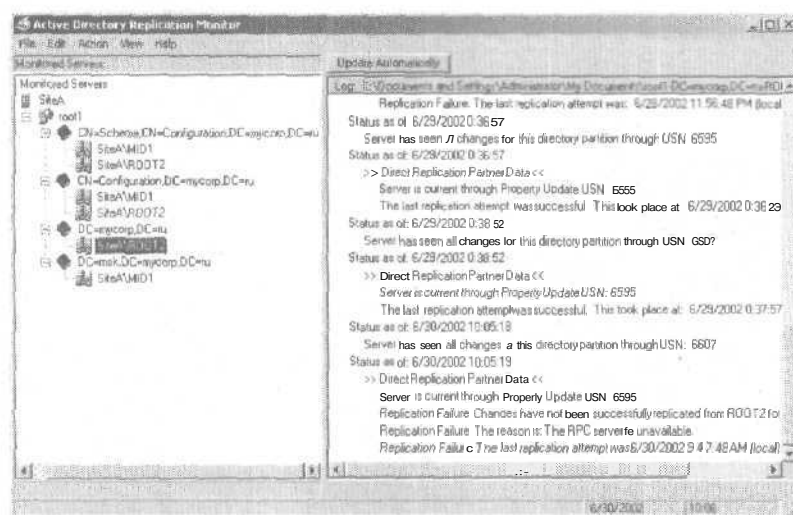
Замечание Узнать о соединениях между контроллерами, используемых для репликации, позволяет команда `repadmin /showconn`.

Replication Monitor

Второй инструмент обладает графическим интерфейсом и не меньшими возможностями, чем описанный выше. Тому, кто предпочитает работать с графическими программами, лучше всего использовать Replication Monitor. К нему можно быстро привыкнуть и обнаружить такие функции, каких нет в `repadmin`.

Чтобы увидеть партнеров по репликации у выбранного сервера, надо добавить этот сервер в меню File. Сразу после этого на экране появится изображение вроде показанного ниже.

Достоинство этой программы не только в том, что вы сразу же видите всех партнеров по репликации, рассортированных по контекстам имен и с сообщениями об успешности репликации, но и в том, что появляется возможность просмотра журнала, в котором собирается информация о корректности тиражирования данных с заданными вами интервалами времени.

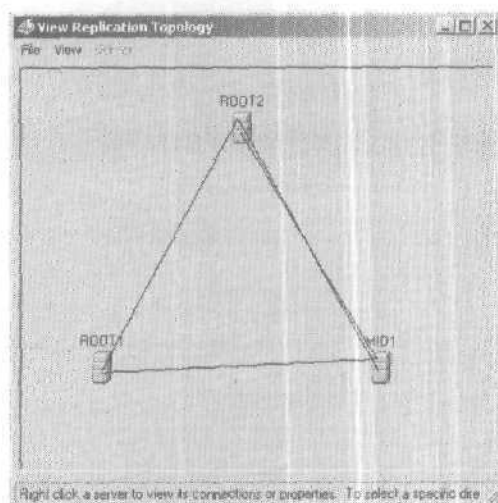


Главное окно программы *Replication Monitor*

Вы можете использовать предоставленную информацию и построить репликацию аналогично тому, как это было сделано в случае с *her-admin*. Можно поступить и проще. В контекстном меню рассматриваемой программы есть команда показа топологии репликации. К сожалению, ее работа не вполне очевидна. Чтобы отобразить топологию, сделайте так.

- Щелкните правой кнопкой в левой части окна имя сервера и выберите в контекстном меню команду *Show replication topologies*.
- В появившемся окне *View Replication Topology* отобразятся все контроллеры доменов в сайте. Связей между ними не будет.
- Выберите в меню *View* команду *Connection Objects only*. На экране ничего не изменится.
- Щелкните правой кнопкой изображение выбранного сервера и в контекстном меню выберите команду *Show Intra-site connections*. Будут показаны связи данного сервера с партнерами по репликации. Эти связи направлены к выбранному серверу, т. е. по ним тиражируются изменения с других контроллеров.

Выполняя последнюю операцию для каждого из изображенных серверов, можно построить полную топологию. К сожалению, на рисунке не видно, какие именно контексты имен используют каждое из соединений. Однако в сложных системах данная функция позволяет быстро оценить топологию и вычислить компьютеры, для которых репликация не выполняется.



Построение топологии репликации в программе Replication Monitor

Контроль состояния партнеров по репликации

Обнаружить проблемный контроллер домена — только половина дела. Главное — выяснить корни проблемы. Обычно для этого надо исследовать состояние локальных баз Active Directory на каждом из партнеров по репликации и найти различия, которые могли вызвать проблему.

DsaStat

Утилита `DsaStat` позволяет выявить различия в контекстах имен, хранящихся на разных контроллерах доменов. Например, после интенсивных операций добавления пользователей и компьютеров в домен можно сравнить содержимое контекста имен на всех контроллерах домена. Вот пример сравнения для двух контроллеров `ROOT1` (где выполнялось добавление) и контроллере `ROOT2`. Команда выглядит так:

```
dsastat -s: root1;root2 -b:dc=mycorp,dc=ru -gcattr:objectclass -p:16 -
filter:(objectclass=user)
```

Я не раскрываю всех ключей команды (они подробно описаны в справочном файле программы `dsastat`), но хочу обратить ваше внимание на ключ `-s`. Он задает количество контроллеров, на которых будет выполняться сравнение, а также номера портов, по которым будет посылаться LDAP-запрос. Если бы надо было сравнить содержимое базы на контроллере с содержимым ГК, то за именем сервера ГК следовало бы поставить номер порта 3268.

Вот результат работы программы:

```
Stat-Only mode.
Unsorted mode.
Opening connections...
  root1...success.

Сначала выводится сообщение о поочередном подключении к контроллерам доменов и выполнении указанного запроса:
Connecting to root1...
reading...
  **> ntMixedDomain = 0
reading...
  **> Options = 1
Setting server as [root1] as server to read Config Info...
  root2...success.
Connecting to root2...
reading...
  **> ntMixedDomain = 0
reading...
LocalException <0>: Cannot get Options <2>.
Generation Domain List on server root1...
> Searching server for GC attributes OID list
Retrieving statistics...
Paged result search...
Paged result search...
... (Terminated query to root1, <No result present in message>)
... (Terminated query to root2, <No result present in message>)
```

По окончании запроса и форматирования результаты выдаются на экран (или в файл).

-->>|***DSA Diagnostics ***|<<--

Objects per server;

Obj/Svr	root1	root2	Total
computer	2	2	4
user	7	6	13
--	9	8	17

FAIL Server total object count mismatch

Как видно из приведенной таблицы, число объектов типа user на двух контроллерах домена различно. Это явно говорит о том, что репликация не была выполнена или не завершилась. Точнее можно сказать, проанализировав начальные условия. Скажем, если вы добавляли 500 пользователей и компьютеров, а программа показывает, что разница

между контроллерами составляет 1-2 объекта, то скорее всего репликация не завершилась и надо подождать окончания следующего цикла. Если разница составляет именно то число объектов, которые вы добавили, то репликация еще и не началась. Это может свидетельствовать о том, что:

- внутри сайта не завершился цикл репликации — надо подождать 15–20 минут;
- между сайтами не выполнялась репликация, так как окно репликации еще не открывалось согласно расписанию; надо подождать, пока откроется окно репликации, выполнится межсайтовая репликация и потом повторно запустить `dsastat`;
- имеются проблемы с репликацией.

Далее следует статистическая информация, не играющая принципиальной роли при диагностике репликации.

Bytes per object:

```

computer          164
user              429

```

Bytes per server:

```

root1             313
root2             280

```

Checking for missing replies...

```

No missing replies! INFO: Server sizes are not equal (min=313,
max=280).

```

Заключительная фраза выглядит, как приговор. Здесь подводится итоговое число рассогласований в базах.

```

*** Different Directory Information Trees. 1 errors (see above). ***

```

```

FAIL             ==>> FAIL <<==

```

```

closing connections...

```

```

root1; root2;

```

Dcdiag

Эта утилита также имеет интерфейс командной строки и в плане диагностики репликации ее возможности сходны с возможностями утилиты `repadmin`. Правда, она позволяет выполнять диагностику сразу всех контроллеров домена, проверять межсайтовую репликацию и

дает более подробную информацию. Рассмотрим три контроллера домена из нашего примера. Команда выполняет лишь один из тестов, позволяющий понять причину неудачной репликации.

```
dcdiag /test:replications /a
```

Результат работы с комментариями таков:

```
DCDiagnosis
performing initial setup:
    Done gathering initial info.
Doing initial non skippeable tests
    Testing server: Default-First-Site-Name\ROOT1
        Starting test: Connectivity
            ..... ROOT1 passed test Connectivity
```

Первым выполнялся тест на подключение. Суть теста в том, что сначала имя компьютера разрешается в адрес IP, а потом выполняется ping по указанному адресу. Контроллер ROOT1 выдержал его, а вот MID1, как это видно из следующего фрагмента, нет, что позволяет предположить недоступность этого компьютера в сети. Возможно, он просто выключен.

```
Testing server; Default-First-Site-Name\MID1
Starting test: Connectivity
    Server MID1 resolved to this IP address 10.1.2.2,
    but the address couldn't be reached(pinged), so check the network.
    The error returned was: Win32 Error 11010
    This error more often means that the targeted server is
    shutdown or disconnected from the network
    ..... MID1 failed test Connectivity
```

Контроллер ROOT2 также прошел тест на подключение.

```
Testing server: Default-First-Site-Name\ROOT2
Starting test: Connectivity
    ..... ROOT2 passed test Connectivity
```

Далее запускается основной тест, указанный в командной строке. Проверяется репликация всех возможных контекстов с сервера MID1.

```
Doing primary tests
    Testing server: Default-First-Site-Name\ROOT1
        Starting test; Replications
        [Replications Check,ROOT1] A recent replication attempt failed:
            From MID1 to ROOT1
            Naming Context: CN=Schema,CN=Configuration,DC=mycorp,DC=ru
            The replication generated an error (1722):
            Win32 Error 1722
            The failure occurred at 2002-05-07 19:10.02.
            The last success occurred at 2002-05-06 19:52.36.
```

```

11 failures have occurred since the last success.
The source remains down. Please check the machine.
[Replications Check,ROOT1] A recent replication attempt failed:
From MID1 to ROOT1
Naming Context: CN=Configuration,DC=mycorp,DC=ru
The replication generated an error (1722):
Win32 Error 1722
The failure occurred at 2002-05-07 19:10.44.
The last success occurred at 2002-05-06 21:48.10.
9 failures have occurred since the last success,
The source remains down. Please check the machine.
[Replications Check,ROOT1] A recent replication attempt failed:
From MID1 to ROOT1
Naming Context: DC=msk,DC=mycorp,DC=ru
The replication generated an error (1722):
Win32 Error 1722
The failure occurred at 2002-05-07 19:11.26.
The last success occurred at 2002-05-06 21:47.40.
9 failures have occurred since the last success.
The source remains down, Please check the machine.
.....ROOT1 passed test Replications

```

Как и следовало ожидать, все тесты завершились неудачно. Более того, программа констатирует, что источник по-прежнему недоступен и надо проверить указанный компьютер.

Следующим в списке проверяемых идет сервер MID1. Но он не может быть проверен, так как не отвечает на запросы. Поэтому соответствующий тест пропускается:

```

Testing server: Default-First-Site-Name\MID1
Skipping all tests, because server MID1 is
not responding to directory service requests

```

Аналогичные проблемы наблюдаются и при тиражировании изменений с сервера MID1 на ROOT2. Но на этот раз рассматриваются только два контекста имен — схемы и конфигурации, так как эти контроллеры принадлежат разным доменам и ни один не является сервером ГК.

```

Testing server: Default-First-Site-Name\ROOT2
Starting test: Replications
[Replications Check,ROOT2] A recent replication attempt failed:
From MID1 to ROOT2
Naming Context: CN=Schema,CN=Configuration,DC=mycorp,DC=ru
The replication generated an error (1722):
Win32 Error 1722
The failure occurred at 2002-05-07 18:50.46.

```

```

The last success occurred at 2002-05-06 19:53.29,
10 failures have occurred since the last success,
The source remains down. Please check the machine.
[Replications Check, ROOT2] A recent replication attempt failed:
From MID1 to ROOT2
Naming Context: CN=Configuration,DC=mycorp,DC=ru
The replication generated an error (1722):
Win32 Error 1722
The failure occurred at 2002-05-07 18:50.25,
The last success occurred at 2002-05-06 21:48.38.
8 failures have occurred since the last success.
The source remains down. Please check the machine.
.....ROOT2 passed test Replications

```

Running enterprise tests on : mycorp.ru

Repadmin

Вернемся к утилите repadmin. Ее возможности диагностики не ограничиваются описанными выше. Допустим, мы выяснили, что репликация не завершилась. Как узнать, что именно осталось незавершенным? Нам поможет команда repadmin с аргументом getchanges:

```
repadmin /getchanges dc=mycorp,dc=ru root2.mycorp.ru a4818f4f-bd9a-4dd9-b8f9-f4e26a84eb7a
```

Она позволяет узнать, какие изменения в контексте имен mycorp.ru должны быть переданы на контроллер root2 с контроллера, чей номер GUID указан в конце командной строки.

Сначала проверяется текущий статус указанного партнера по репликации. Обратите внимание на номера USN (для наглядности они выделены):

```
Building starting position from destination server root2.mycorp.ru
```

```
Source Neighbor:
```

```
dc=mycorp,dc=ru
```

```
Default-First-Site-Name\ROOT1 via RPC
```

```
objectGuid: a4818f4f-bd9a-4dd9-b8f9-f4e26a84eb7a
```

```
Address: a4818f4f-bd9a-4dd9-b8f9-f4e26a84eb7a.msdc.mycorp.ru
```

```
ntdsDsa invocationId: a4818f4f-bd9a-4dd9-b8f9-f4e26a84eb7a
```

```
WRITEABLE SYNC_ON_STARTUP DO_SCHEDULED_SYNC
```

```
USNs: 4798/OU, 4798/PU
```

```
Last attempt a 2002-05-07 20:05.51 was successful.
```

Далее выясняется вектор обновленности для двух партнеров:

Destination's Up To Dateness Vector:

2ff7fbba-6607-472c-b3a5-ccf8445de5bf 9 USN 4973

a4818f4f-bd9a-4dd9-b8f9-f4e26a84eb7a @ USN 4847

Наконец, сообщается о том, что надо передать **изменение** фамилии

(атрибута sn) для **объекта** CN=u2,OU=test,DC=mycorp,DC=ru:

== SOURCE DSA: a4818f4f-bd9a-4dd9-b8f9-f4e26a84eb7a._msdcs.mycorp.ru ==

Objects returned: 1

(0) modify CN=u2,OU=test,DC=mycorp,DC=ru

1> objectGUID: db92fe3d-d14a-49b9-98ae-ec905ec39bf1

1> sn: Petrov

1> instanceType: 4

По завершении репликации можно повторно выполнить указанную выше команду. Результат показан ниже. Снова взгляните на номера USN. Как и следовало ожидать, они увеличились:

Source Neighbor:

dc=mycorp,dc=ru

Default-First-Site-Name\ROOT1 via RPC

objectGuid:a4818f4f-bd9a-4dd9-b8f9-f4e26a84eb7a

Address: a4818f4f-bd9a-4dd9-b8f9-f4e26a84eb7a._msdcs.mycorp.ru

ntdsDsa invocationId: a4818f4f-bd9a-4dd9-b8f9-f4e26a84eb7a

WRITEABLE SYNC_ON_STARTUP DO_SCHEDULED_SYNC

USNs: 4850/OU, 4850/PU

Last attempt @ 2002-05-07 20:12:37 was successful.

Destination's Up To Dateness Vector:

2ff7fbba-6607-472c-b3a5-ccf8445de5bf @ USN 4989

a4818f4f-bd9a-4dd9-b8f9-f4e26a84eb7a 9 USN 4860

== SOURCE DSA: a4818f4f-bd9a-4dd9-b8f9-f4e26a84eb7a._msdcs.mycorp.ru ==

No changes.

На этот раз никакие **изменения** не **ожидают** очереди на тиражирование. Но вернемся к номерам USN. Выполните команду:

repadmin /showmeta CN=u2,OU=test,DC=mycorp,DC=ru

т. е. посмотрите метаданные для того объекта, который был реплицирован на контроллер root2. В частности, интерес представляет USN атрибута sn. Он равен 4850, т. е. как раз тому значению, что указано в качестве максимального USN для контроллера домена.

Loc.USN	Originating DSA Org.USN	Org.Time/Date	Ver	Attribute
=====	=====	=====	===	=====
4678	Default-First-Site-Name\ROOT1	4678 2002-05-07	18:03.21	1 objectClass
4678	Default-First-Site-Name\ROOT1	4678 2002-05-07	18:03.21	1 cn
4850	Default-First-Site-Name\ROOT1	4850 2002-05-07	20:09.15	4 sn
4679	Default-First-Site-Name\ROOT1	4679 2002-05-07	18:03.22	1 description
4678	Default-First-Site-Name\ROOT1	4678 2002-05-07	18:03.21	1 givenName
4678	Default-First-Site-Name\ROOT1	4678 2002-05-07	18:03.21	1 instanceType
4678	Default-First-Site-Name\ROOT1	4678 2002-05-07	18:03.21	1 whenCreated
4679	Default-First-Site-Name\ROOT1	4679 2002-05-07	18:03.22	1 displayName

Общая информация о параметрах репликации

Если нужно получить всеобъемлющую информацию о состоянии репликации, объектах **связи**, форпостах, номерах USN и т. п., лучшего инструмента, чем Replication Monitor, не найти. Для этого надо использовать его способность создавать отчеты. При этом можете указать, какие сведения вы хотели бы в нем видеть.

В полном объеме размер отчета велик, и я не буду его приводить здесь. Однако ряд элементов отчета может вызвать интерес при анализе.

Первое, что бросается в **глаза**, — хорошая структурированность отчета,

Active Directory Replication Monitor

Printed on 07.05.2002 20:45:06

This report was generated on data from the server: ROOT1

Приводимый образец был создан на сервере **ROOT1**, у которого два партнера по репликации. **Вначале** приводятся сведения о самом сервере. Помните, мы получили их с помощью **repadmin**? Но если раньше эту информацию приходилось извлекать, анализируя сообщения программы, то теперь она предоставлена на блюдечке.

```
*****
                        ROOT1 Data
*****
```

This server currently has writable copies of the following directory

partitions:

```
-----
CN=Schema,CN=Configuration,DC=mycorp,DC=ru
CN=Configuration,DC=mycorp,DC=ru
DC=mycorp,DC=ru
```

Как видите, перечислены все контексты имен, содержащиеся на данном контроллере. Также указано, что этот сервер является ГК, и перечислены дополнительные контексты имен.

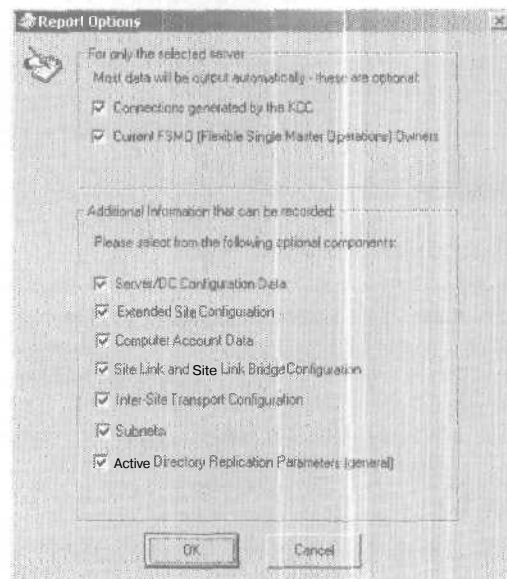
Because this server is a Global Catalog (GC) server, it also has copies of the following directory partitions:

```
-----
DC=msk,DC=mycorp,DC=ru
```

Следующий шаг — перечисление объектов связи с партнерами по репликации. Дополнительно к информации, которую позволяет получить `repadmin`, приводятся сведения о том, кто и зачем создал эти объекты. Это удобно при отслеживании репликации. Вот информация только для одного из объектов связи:

Current NTDS Connection Objects

```
-----
Default-First-Site-Name\MID1
Connection Name : 828a2adb-a24b-45d8-bf0c-b65aa4cbfb95
Administrator Generated?: AUTO
```



Выбор информации, включаемой в отчет

Обратите внимание на название связи: это номер GUID. В окне оснастки Active Directory Sites and Services имя этого объекта будет обозначено <Automatically generated>. Стоит только внести изменения в свойства объекта, как его имя изменится на указанный номер GUID. Об этом свидетельствует фраза AUTO в поле Automatically generated. Если бы использовался объект связи, созданный администратором, данная запись выглядела бы так:

```
Default-First-Site-Name\MID1
Connection Name : From MID1
Administrator Generated?: YES
```

т. е. имя связи показано в том виде, как его создал администратор.

Далее приведены причины, по которым была создана данная связь. Обратите внимание на новый термин — Ring neighbor. Дословно его можно перевести как «сосед по звонку». На практике это относится к связям, создаваемым для оповещения ближайших партнеров по репликации:

```
Reasons for this connection:
Directory Partition (DC=msk,DC=mycorp,DC=ru)
Replicated because the replication partner is a ring neighbor,

Directory Partition (CN=Schema,CN=Configuration,DC=mycorp,DC=ru)
Replicated because the replication partner is a ring neighbor.

Directory Partition (CN=Configuration,DC=mycorp,DC=ru)
Replicated because the replication partner is a ring neighbor.
```

В противоположность такой причине может быть указано «surpassed the allowed failure limit». Это значит, что между контроллером и его партнерами неоднократно наблюдались проблемы с репликацией. Дабы их искоренить, были созданы новые связи. Как правило, они создаются КСС. Если в сети есть альтернативные маршруты между указанными серверами, будут использованы они.

```
Directory Partition (CN=Schema,CN=Configuration,DC=mycorp,DC=ru)
This replication connection is created because another
replication partner has surpassed the allowed failure limit.
```

Замечание Сообщение о данном событии появляется в журнале регистрации событий Active Directory под номером 1308 от имени КСС. Описание этого события выглядит примерно так: «The Directory Service consistency checker has noticed that 2 successive replication attempts with CN=NTDS Settings,CN=ROOT2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=mycorp,DC=ru have failed over a period of 787 minutes. The connection object for this server will

be kept in place, and new temporary connections will be established to ensure that replication continues. The Directory Service will continue to retry replication with CN=NTDS Settings,CN=ROOT2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=mycorp,DC=ru; once successful the temporary connection will be removed».

Далее следует описание состояния всех партнеров по репликации для каждого из контекста имен. Эта информация во многом повторяет ту, что позволяет получить `gpadmin /showreps`, но содержит и дополнительные сведения. Например, если проблем с репликацией нет, то информация записывается таю

Current Direct Replication Partner Status

Directory Partition: CN=Schema,CN=Configuration,DC=mycorp,DC=ru

Partner Name: Default-First-Site-Name\ROOT2

Partner GUID: 2FF7FBAA-6607-472C-B3A5-CCF8445DE5BF

Last Attempted Replication: 5/7/2002 7:59:14 PH (local)

Last Successful Replication: 5/7/2002 7:59:14 PH (local)

Number of Failures: 0

Failure Reason Error Code: 0

Failure Description: The operation completed successfully.

Synchronization Flags: DRS_WRIT_REP, DRS_INIT_SYNC, DRS_PER_SYNC

USN of Last Property Updated: 4928

USN of Last Object Updated: 4928

Transport: Intra-SiteRPC

А если были проблемы, узнать их источник совсем легко:

Directory Partition: CN=Schema,CN=Configuration,DC=mycorp,DC=ru

Partner Name: Default-First-Site-Name\MID1

Partner GUID: 531BD902-1AEF-4F29-A8DC-D27A0CFC3003

Last Attempted Replication: 5/8/2002 9:52:06 AM (local)

Last Successful Replication: 5/7/2002 7:59:14 PH (local)

Number of Failures: 2

Failure Reason Error Code: 1722

Failure Description: The RPC server is unavailable.

Synchronization Flags: DRS_WRIT_REP, DRS_INIT_SYNC, DRS_PER_SYNC

USN of Last Property Updated: 6117

USN of Last Object Updated: 6117

Transport: Intra-SiteRPC

Обратите внимание на выделенные строки. Видно, что было 2 ошибки репликации, вызванные недоступностью сервера RPC. О том, как

бороться с такой ошибкой и ее вероятных причинах, я расскажу в конце главы.

Следующая часть отчета содержит информацию о партнерах, уведомляемых об изменениях.

Внимание Данная часть отчета может обескуражить,

В том, что показано ниже, ничего необычного. Приведены имя партнера по репликации, номер его GUID, дата создания, транспорт репликации... Все хорошо и не вызывает подозрений. К сожалению, такая запись — скорее исключение, чем правило:

Change Notifications for this Directory Partition

```
-----
Server Name: Default-First-Site-Name\RO0T2
Object GUID: A6563E8F-9A97-40A9-9C28-23BA4F348593
Time Added: 23.03.2002 13:14:31
Flags:      DRS_WRIT_REP
Transport:  RPC
```

Чаще всего картина несколько иная:

```
Server Name: Site-1\VM20002
Object GUID: 5E29E488-863B-46B1-B7EB-6C54A63D6A44
Time Added: 23.06.2016 14:27:53
Flags:      DRS_WRIT_REP
Transport:  RPC
```

Для наглядности я выделил дату создания. Она больше реальной примерно на 15 лет. Мне не удалось заметить какой-либо точной зависимости между этим превышением и реальной датой создания. Иногда разница чуть меньше 15 лет, иногда — чуть больше. Все мои попытки отыскать причину закончились неудачей. Могу только с определенностью сказать, что на работу репликации это не влияет.

Далее в отчете приводятся сведения, влияющие на работу репликации и КСС. С параметрами, ответственными за это, мы познакомились выше. Если значение какого-либо параметра не указано, используются умолчания:

Performance Statistics at Time of Report

REPLICATION

```
-----
Replicator notify pause after modify (secs): 300
Replicator notify pause between OSAs (secs): 30
```

```

Replicator intra site packet size (objects):
Replicator intra site packet size (bytes):
Replicator inter site packet size (objects):
Replicator inter site packet size (bytes):
Replicator maximum concurrent read threads:
Replicator operation backlog limit:
Replicator thread op priority threshold:
Replicator intra site RPC handle lifetime (secs):
Replicator inter site RPC handle lifetime (secs):
Replicator RPC handle expiry check interval (secs):

```

KCC

```

Repl topology update delay (secs):
Repl topology update period (secs):
KCC site generator fail-over (minutes):
KCC site generator renewal interval (minutes):
KCC site generator renewal interval (minutes):
CriticalLinkFailuresAllowed:
MaxFailureTimeForCriticalLink (sec):
NonCriticalLinkFailuresAllowed:
MaxFailureTimeForNonCriticalLink (sec):
IntersiteFailuresAllowed:
MaxFailureTimeForIntersiteLink (sec):
KCC connection failures:
IntersiteFailuresAllowed:
IntersiteFailuresAllowed:

```

Как видите, предоставляемый отчет позволяет разом получить исчерпывающую информацию о работе репликации Active Directory и ее параметрах. К недостаткам стоит отнести значительный объем отчета при большом числе контроллеров. При этом приходится долго продирааться сквозь дебри избыточной информации, чтобы докопаться до нужной.

Поиск и устранение проблем репликации

Сообщения об ошибках репликации можно получать по-разному. Но знать об ошибке еще не значит устранить ее причины. Ниже приводятся наиболее характерные ошибки репликации и способы их устранения. В любом случае виноваты вы, т. е. администратор. Это могут быть и «кривые руки», и невнимательность, и непонимание механизмов репликации. Надеюсь, данная глава устраняет последнюю причину. Ну, а с остальными — читайте дальше и боритесь самостоятельно.

Запрет доступа (Access Denied)

Сообщение о запрете доступа при выполнении репликации может появиться в двух случаях:

- ◆ когда вы выполняете принудительную репликацию, находясь, например, в оснастке Active Directory Sites and Services;
- ◆ когда выполняется обычный цикл репликации.

В первом случае выводится сообщение «The following error occurred during the attempt to synchronize the domain controllers: Replication access was denied*». Это, пожалуй, самое безобидное сообщение, причина которого в несоответствии полномочий учетной записи, под которой вы зарегистрированы в системе. Например, вы зарегистрированы как обычный пользователь домена. Репликацию нельзя инициировать от имени такой учетной записи. Другой пример — вы администратор дочернего домена и пытаетесь инициировать репликацию с партнером в родительском домене. Если вы не член группы Enterprise Admins, такая попытка также будет отвергнута. Дабы убедиться в том, что причин для беспокойства нет, запустите оснастку Active Directory Sites and Services от имени той учетной записи, которая может инициировать репликацию (например, включенной в группу Enterprise Admins для междоменной репликации). Если теперь репликация выполняется успешно, покорите себя за забывчивость и постарайтесь так больше не ошибаться.

Все гораздо серьезнее, если в журнале регистрации появилось сообщение 1265: «The attempt to establish a replication link with parameters failed with the following status: Access is denied». При этом в результате выполнения `repadmin /showreps` информация не выводится.

Не менее серьезна ситуация, когда в журнале регистрации не появляются настораживающих записей, а вот выполнение команды `repadmin /showreps` выводит сообщение для одного или нескольких контекстов имен о том, что последняя попытка выполнить репликацию была неудачной, с ошибкой «Access denied error».

Вероятная причина

Самое вероятное — рассинхронизировались контроллеры. Это случается, если контроллер домена был отключен от сети долгое время, что приводит к тому, что пароль учетной записи компьютера отличается от того, что хранится в Active Directory.

Замечание Еще одной причиной может быть отсутствие права доступа к контроллерам доменов по сети. Это особенно актуально при обновлении контроллера Windows NT до Windows 2000.

Решение

Есть два способа решения данной проблемы.

1. Остановите службу KDC (Key Distribution Center), удалите все билеты Kerberos, сбросьте пароль учетной записи компьютера, синхронизируйте доменный контекст имен и все остальные контексты имен. Используйте этот способ в первую очередь.

Рассмотрим данные процедуры подробнее.

- а) На локальном контроллере домена выполняется команда:

```
net stop kdc
```

Если служба не останавливается, то в ее свойствах указывается запрет запуска (disabled), и контроллер перегружается.

- б) Если служба kdc была остановлена, запустите утилиту klist с ключом /purge (утилита входит в Windows 2000 Resource Kit).
- в) Выполните команду:

```
netdom resetpwd /server:<имитатор PDC>  
/userd:<домен>\administrator /passwordd:*
```

В результате пароль учетной записи компьютера будет сброшен. Если же появится сообщение о невозможности сброса пароля, проверьте, находится ли данный компьютер в подразделении Domain Controllers.

- г) Убедитесь, что рассматриваемый контроллер домена является непосредственным партнером по репликации для имитатора PDC в домене. Если это не так, создайте репликационное соединение между ними. Для этого выполните команду:

```
repadmin /add <доменный контекст><полное имя контроллера><полное  
имя имитатора PDC> /u:<домен>\administrator /pw:*
```

и пропустите **пункт д.**

- д) Выполните команду:

```
repadmin /sync <доменный контекст><имя контроллера домена><GUID  
имитатора PDC>
```

- е) Проверьте, что репликация работает, выполнив команду:

```
repadmin /showreps
```

Если в результате не будет партнеров по репликации, выполните:

```
repadmin /kcc
```

- ж) Синхронизируйте все оставшиеся контексты аналогично тому, как это сделано в пункте д. Вместо GUID имитатора PDC укажите GUID обычных партнеров по репликации.

- з) Запустите kdc:
- ```
net start kdc
```
2. Если `repadmin /kcc` или `repadmin /sync` выводят новое сообщение об ошибке 1265 с причиной отказа в доступе, нужно создать временную связь между локальным контроллером домена и его партнером по репликации контекстов имен.
- а) Для контекста имен конфигурации выполните команду:
- ```
repadmin /add <контекст конфигурации><полное имя контроллера><полное имя партнера по репликацию /u:<домен>\administrator /pw: *
```
- б) Повторите предыдущую команду для контекста схемы.
- в) Повторите предыдущую команду для контекста доменных имен.

В результате работа репликации должна нормализоваться.

Замечание Эти команды инициируют репликацию, и в крупной сети они могут выполняться довольно долго.

Чтобы убедиться в том, что все работает нормально, выполните `repadmin /showreps`.

Неизвестная служба аутентификации (Authentication service is Unknown)

Данная ошибка может возникнуть в одном из двух случаев.

- Контроллер домена не может установить связь репликации. При этом в журнале регистрации событий появляется сообщение от «NTDS KCC» Event ID 1265 «Intersite Transport (if any) ... failed with the following status: The authentication service is unknown».
- ◆ Связь существует, но выполнить репликацию не удастся. При этом в журнал регистрации ничего не заносится, но команда `repadmin /showreps` сообщает, что «Last attempt at <дата-время> failed with the error Authentication service is unknown».

Способ разрешения этой проблемы схож с описанным выше.

Контроллер домена не может установить связь репликации

Для устранения проблемы придерживайтесь следующего алгоритма.

- а) Остановите службу KDC и удалите все билеты Kerberos.
- б) На контроллере домена запустите `repadmin /kcc`. При этом контроллер свяжется со своими партнерами и аутентифицирует себя с целью создания связей репликации,
- в) Проверьте в журнале регистрации появление события 1264 о создании связей. Если такое сообщение есть, репликация начнет

работать при наступлении следующего цикла. Если нет, вы увидите сообщение об ошибке (Event ID 1265) с описанием причины.

- г) Если все работает нормально, запустите службу kdc.

Связь репликации существует

Сделайте так.

- а) Остановите службу KDC и удалите все билеты Kerberos.
- б) Синхронизируйте контекст схемы (схема выбрана из тех сообщений, что ее контекст самый маленький). Для этого выполните:
`gpadmin /sync cn=schema,cn=configuration,<имя леса> <имя контроллера домена> <GUID партнера по репликации>`
- в) Если предыдущий шаг не вызвал ошибок, синхронизируйте остальные контексты имен.
- г) Если появились ошибки репликации, выясните их причину и найдите соответствующее описание в этом разделе.
- д) Если ошибок нет, запустите службу kdc.

Неверное имя учетной записи цели (Target account name is incorrect)

Такая ошибка возможна при попытке установить связь между контроллерами разных доменов или выполнении репликации. Например, при попытке выполнить репликацию из окна оснастки Active Directory Sites and Services или в окне Replication monitor появляется сообщение «Logon Failure: The target account name is incorrect». Также можно обнаружить в журнале регистрации сообщение от «NTDS Replication», Event ID 1645:

The Directory Service received a failure while trying to perform an authenticated RPC call to another Domain Controller. The failure is that the desired Service Principal Name (SPN) is not registered on the target server. The server being contacted is afb720fd-38c7-4505-aa9f-b658ca124773._msdcs.mycorp.ru. The SPN being used is

E3514235-4B06-11D1-AB04-00C04FC2DCD2/afb720fd-38c7-4505-aa9f-b658ca124773/mycorp.ru@mycorp.ru.

Please verify that the names of the target server and domain are correct.

Please also verify that the SPN is registered on the computer account object for the target server on the KDC servicing the request. If the target server has been recently promoted, it will be necessary for knowledge of this computer's identity to replicate to the KDC before this computer can be authenticated.

Еще одним свидетельством этой ошибки может стать сообщение в журнале регистрации от «NTDS KCC», Event 1265:

The attempt to establish a replication link with parameters

Partition:

CN=Configuration,DC=MyDomain,DC=net Source DSA DN: CN=NTDS
Settings,CN=MyServer,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=MyDomain,DC=com
Source DSA Address: 5e5abf03-e902-48e2-a326-
41977dee176d. _msdcs.mycorp.ru

Inter-site Transport (if any): failed with the following status:
Logon

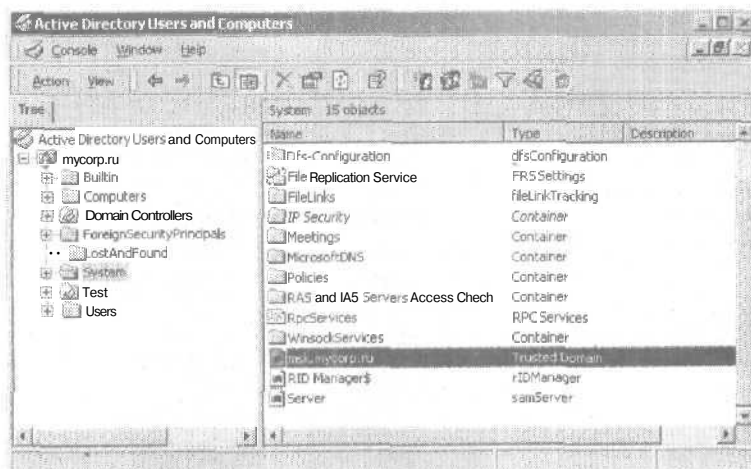
Failure; The target account name is incorrect. The record data is the
status code. This operation will be retried.

Причин возникновения этой ошибки две:

- ◆ требуемый набор главных имен службы (Services Principle Name — SPN) не совпадает на обоих контроллерах;
- ◆ на контроллерах разных доменов отсутствует объект `crustedDomain` (TDO), который должен находиться в контейнере `System`.

Отсутствие объекта `trustedDomain`

Чтобы понять, имеется ли TDO в контейнере `System`, откройте его в оснастке `Active Directory Users and Computers` и найдите в контейнере объект с именем того домена, в котором находится партнер по репликации, например `msk.mycorp.ru`. Тип объекта будет указан как «Trusted Domain».



Здесь должен находиться объект TDO

Если этот объект есть, переходите к следующему разделу, если нет — его надо создать.

- а) В том домене, где находится проблемный контроллер, откройте оснастку Active Directory Domains and Trusts, подключитесь к контроллеру — имитатору PDC и откройте окно свойств домена.
- б) Открыв в этом окне вкладку Trusts, создайте двусторонние доверительные отношения с доменом, в котором расположен партнер по репликации. При этом вы получите сообщение о невозможности проверки доверия. Не смущайтесь. Скажите **ОК**, и будет создано транзитивное доверие- помеченное как «сокращение* (shortcut).
- в) Далее будет предложено проверить доверие. Введите имя учетной записи, которая обладает административными правами в двух доменах и проверьте доверие. Вновь **появится** сообщение о невозможности проверки доверия, И опять не смущайтесь.
- г) Выполните команду:

```
NETDOM TRUST локальный.домен /Domain:удаленный.домен  
/UserD:administrator /PasswordD:* /UserO:administrator /PasswordO:*  
/Reset /TwoWay
```

где UserD и UserO — имена учетных записей администраторов локального и удаленного домена.
- д) Перегрузите контроллер домена, на котором выполнялись изменения.
- е) После перезагрузки подождите, пока KCC не восстановит соединение. Отсутствие ошибок контролируйте по журналу регистрации.

Не совпадает набор SPN

Для разрешения этой проблемы сделайте так

- а) Определите адрес IP контроллера, с которым должно установиться соединение. Для этого выполните команду ping того номера GUID, который фигурирует в сообщении об ошибке. В нашем примере это `afb720fd-38c7-4505-aa9f-b658ca124773._msdcs.<имялеса>`. В результате вы узнаете имя партнера по репликации.
- б) На обоих партнерах по репликации запустите ADSIEdit, выделите объекты, соответствующие локальному контроллеру домена, и откройте окно их свойств.

Совет В данном случае ADSIEdit лучше запустить дважды на одном контроллере: для локального контроллера домена и для удаленного.

- в) В списке атрибутов найдите `servicePrincipalName`. Этот атрибут имеет много значений, одно из которых состоит как бы из двух

номеров GUID. Например, в нашем примере это будет E3514235-4B06-11D1-AB04-00C04FC2DCD2/afb720fd-38c7-4505-aa9f-b658ca124773/mycorp.ru.

- г) Выделите это значение, нажмите кнопку Remove. Поле Edit Attribute заполнится приведенным выше значением. Скопируйте его в буфер обмена и нажмите кнопку Add.
- д) Скопируйте содержимое буфера обмена в поле Edit Attribute и в самый конец этой записи добавьте «@<имя.домена>». Скопируйте все содержимое поля в буфер обмена и нажмите кнопку Add.
- е) В окне свойств второго контроллера домена добавьте то же значение к атрибуту servicePrincipalName.

После этого можно вновь попробовать выполнить репликацию.

Замечание Выполняя указанные действия, можно столкнуться с двумя проблемами:

- партнеры по репликации имеют разные пары GUID;
- ◆ один из списков значений атрибута servicePrincipalName пуст.

Для избавления от этих проблем скопируйте значения атрибута с другого контроллера домена.

Недоступен сервер RPC (RPC Server Not Available)

Это одна из самых распространенных ошибок. Причиной для ее возникновения могут быть:

- ◆ невозможность создания связи репликации;
- ◆ отсутствие соединения с компьютером.

При невозможности создания связи репликации в журнале регистрации появится сообщение 1265: «The attempt to *establish* a replication link with parameters failed with the following status: The RPC Server is *unavailable*».

Если связь есть, но компьютер недоступен, сообщений в журнале регистрации не будет, а вот герадмин /showreps сообщит об ошибке.

Для выяснения причины в первую очередь надо проверить доступность указанного партнера по сети командой ping. Проверку лучше делать по номеру GUID. Если результат будет аналогичен изображенному ниже, то скорее всего сервер выключен или отключен от сети.

```
ping 19c9dbc3-d5d2-47cc-94e3-5135adfc4bcb._msdcs.mycorp.ru
```

```
Pinging mid1.msk.mycorp.ru [10.1.2.2] with 32 bytes of data:
```

```
Request timed out.
```

Request timed out.
Request timed out.
Request timed out.

Ошибка поиска в DNS (ONS Lookup failure)

Эта ошибка тоже часто встречается. Обычно — на этапах **создания** **дерева** **Active Directory** и при подключении новых контроллеров доменов. И все же появление этой ошибки возможно и потом из-за проблем с сетью. В любом случае при отсутствии соединения репликации в журнале регистрации появляется сообщение об ошибке 1265: «The attempt to establish a replication link with parameters failed with the following status: DNS lookup failure».

Если соединение есть, в журнале ошибки не появляются, зато команда `repadmin /showreps` сообщает о такой же ошибке.

Проблема скорее всего в неверной конфигурации клиента **DNS** — иного просто **быть** не **может**, поэтому советую обратиться к разделу «Что делать с **DNS**?» главы «Установка **Active Directory**». Здесь же я дам общие рекомендации по поиску источника проблем.

На сбойном контроллере домена выполните `ping` по номеру **GUID** партнера по репликации. Если имя не разрешается, проверьте доступность зоны `_msdcs.<имялеса>` с этого компьютера. С помощью `nslookup` выясните, какой сервер **DNS** первичный. Посмотрите, возможно ли разрешение имени через рекурсию или через настроенные переадресации запросов. Особое внимание обратите на то, нет ли отрицательного ответа по указанному адресу в кэше **DNS**.

Если причина отсутствия ответа не в этом, выполните команды:

```
net stop dns client
net start dns client
```

Если это сработает, значит, в какой-то момент клиент **DNS** переключился на альтернативный сервер.

Если имя разрешается, но ответ от партнера не приходит, возможно, дело в аппаратном сбое **сетевое** оборудования. Если нет, посмотрите, не изменялся ли адрес **IP** партнера. Не исключено, что в локальном кэше хранится старый адрес. Выполните `ipconfig /flushdns`. Также проверьте, отражена ли **новая** информация в записи **CNAME** на том сервере **DNS**, который указан первичным для рассматриваемого контроллера. Если нет, то выясните причину этого. Возможно, наблюдается проблема «островов».

Служба каталогов перегружена (Directory service too busy)

В случае **возникновения** такой ошибки в журнале регистрации появляется сообщение от «NTDS Replication» с Event ID=1083:

"Replication warning: The directory is busy. It couldn't update object CN=ROOT2,CN=Servers,CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=mycorp, DC=ru with changes made by directory afb720fd-38c7-4505-aa9f-b658ca124773._msdcs.mycorp.ru. Will try again later."

Сообщение содержит отличительное имя объекта, вызвавшего проблему, и номер GUID партнера по репликации.

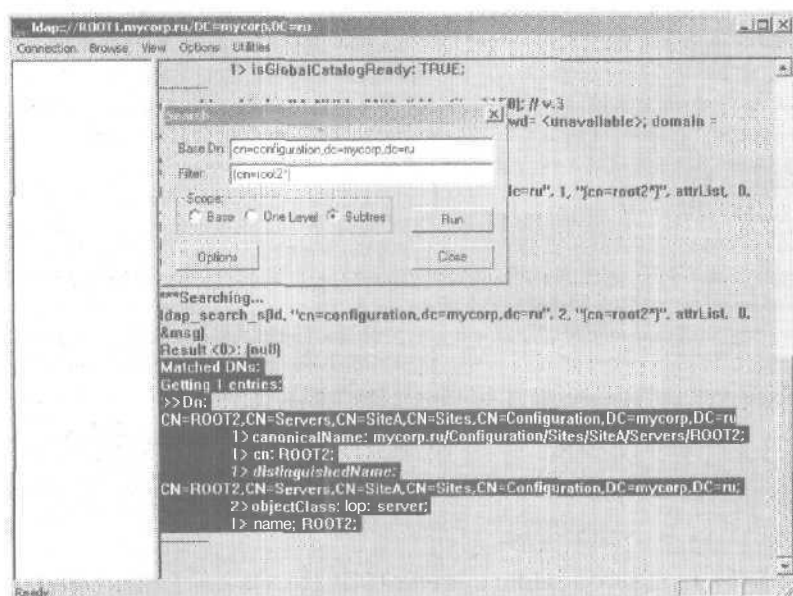
Причина

Причиной данной ошибки является появление в Active Directory дубля объекта **связи** для партнера по репликации.

Разрешение

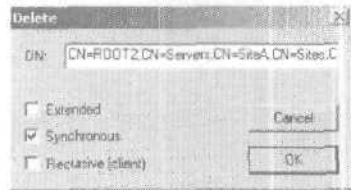
Эту проблему можно разрешить так.

- Выполните ping по номеру GUID для выяснения имени и адреса IP партнера по репликации. В рассматриваемом примере это:
ping afb720fd-38c7-4505-aa9f-b658ca124773._msdcs.mycorp.ru
- Запустите программу Ldp, подключитесь к найденному адресу партнера и выполните bind с правами администратора.
- Выполните поиск проблемного объекта. Поиск надо вести по под-дереву того домена, в котором находится объект.



Поиск дубля объекта **связи**

Если обнаружен дубль (на рисунке он не показан), то выделите в правой части окна Ldp его имя и скопируйте в буфер обмена. Затем выберите команду Delete и вставьте в поле DN содержимое буфера обмена. Нажмите OK.



Удаление дубля объекта из каталога

Удалив объект, убедитесь, что дублей больше нет.

Если вы не обнаружили дублированных записей, перенесите проблемный объект в другой сайт или подразделение. Это изменит отличительное имя объекта. Обязательно зафиксируйте данное изменение для последующего восстановления.

Выполните синхронизацию контекста конфигурации и домена.

```
repadmin /sync cn=configuration,<имя леса> <имя контроллера домена>
<GUID партнера по репликации>
repadmin /sync <имя леса> <имя контроллера домена> <GUID партнера по
репликации>
```

Если репликация возобновит нормальную работу, то в журнал будет записано сообщение 1083. После этого перенесенный объект можно вернуть на прежнее место.

Замечание Если вы не установили на контроллер SP2 или выше, то может наблюдаться периодическая остановка входной репликации с записью в журнале регистрации «Event ID 8438 The directory service is too busy to complete the replication operation at this time». Установите последний пакет обновления для решения этой проблемы.

Разница во времени (Ошибка LDAP 82)

Как я говорил в главе «Установка Active Directory», синхронизация во времени между контроллерами доменов играет очень важную роль. Рассинхронизация приводит к ряду печальных результатов, один из которых — невозможность репликации. В таком случае в журнале регистрации появляется сообщение от NTUS KCC с ID=1265: «The attempt to establish a replication link with parameters ... failed with the following status: There is a time difference between the client and server».

Причина

Причина рассогласования во времени может быть только одна – невозможность доступа к родительскому серверу времени. Отбросим случай недоступности имитатора PDC как маловероятный. Остается отказ в доступе.

Устранение

Чтобы убедиться в том, что причиной является именно отказ в доступе, выполните команду:

```
net time \\\имя_имитатора_PDC /set
```

Если в результате получите сообщение Access denied, перейдите к разделу, описывающему борьбу с этой ошибкой.

Если команда выполнена успешно, репликация возобновит свою работу. Вам же надо будет выяснить причину, по которой возникла рассинхронизация времени.

Внутренняя ошибка системы репликации

О возникновении внутренней ошибки в системе репликации свидетельствует сообщение в журнале регистрации с ID=1084 «Replication failed with an internal error» либо сообщение с тем же самым ID, но более информативным:

```
Replication error: The directory replication agent (DRA) couldn't
update object CN="8f03823f-410c-4483-86cc-8820b4f2103f
DEL:66aab46a-2693-4825-928f-05f6cd12c4e6",CN=Deleted
Objects,CN=Configuration,DC=mycorp,DC=ru (GUID
66aab46a-2693-4825-928f-05f6cd12c4e6) on this system with changes
which have been received from source server 62d85225-76bf-4b46-b929-
25a1bb295f51._msdcs.mycorp.ru. An error occurred during the
application of the changes to the directory database on this system.
```

Причины

В локальной базе, вероятно, есть объект, чей родительский объект в Active Directory был удален так давно, что стал фантомом, а значит, репликация его дочерних объектов невозможна. С другой стороны, сборщик мусора не может удалить фантом если у него есть дочерние объекты. Подобная ситуация невозможна после применения SP2, но если уж такие объекты появились, SP2 их не уничтожит.

Еще одной причиной может быть некорректно выполненное авторитетное восстановление объектов, выполненное устаревшей версией ntdsutil (см. главу «Поиск и устранение проблем»).

Устранение

Эту ошибку можно устранить так.

- 1) Найдите в сообщении об ошибке номер GUID проблемного объекта. В приведенном примере это 66aab46a-2693-4825-928f-05f6cd12c4e6. Скопируйте его в буфер обмена.
- 2) Запустите `Ldp` и подключитесь к локальному контроллеру домена. Выполните `bind` с привилегиями администратора.
- 3) Выберите команду `Delete`, вставьте в поле DN содержимое буфера обмена и нажмите ОК.
- 4) Проверьте, как работает репликация. Если вновь появляется сообщение 1084 с другим именем объекта, повторите пп. 1–3.

Отсутствие конечной точки (No more end-point)

Эта ошибка может возникнуть при выполнении команды `gpadmin /showreps`. Причины ее появления скорее всего следующие.

- Отсутствуют конечные точки для установления TCP сеанса с партнером по репликации. Выяснить это позволяет команда `netstat`. Единственный способ избавиться от ошибки — закрыть текущие сеансы TCP.
- Партнер по репликации доступен, но интерфейс `RPC Directory Replication Service` не зарегистрирован. Обычно это указывает на то, что имя DNS контроллера домена зарегистрировано с неверным адресом IP.

Ошибка ЮАР 49

Эта ошибка связана с локальной службой `KDC`. Чтобы ее устранить, остановите службу `KDC`. Затем синхронизируйте контексты имен командой `gpadmin /sync`. Если все пройдет успешно, команда `gpadmin /showreps` ошибок не покажет. После этого можно вновь запустить службу КОС. Если возникнут другие ошибки, устраните их, как я показал в этой главе.

Сообщения, не являющиеся ошибками

Иногда при выполнении `gpadmin /showreps` появляются сообщения, очень похожие на сообщения об ошибках, хотя таковыми не являются.

Active Directory replication has been pre-empted

Означает, что при тиражировании данных от партнера был выполнен запрос на выполнение более приоритетной репликации. Тиражирование продолжится в следующий цикл репликации.

Replication posted, waiting

Появляется, когда контроллер домена послал запрос на тиражирование данных и ожидает ответа. Это означает, что репликация выполняется в данный момент.

Last attempt @ ... was not successful

Может быть вызвано тем, что КСС создал связи репликации, но репликация еще не прошла, например потому, что не открылось окно по расписанию. Проверить, так ли это, можно, инициировав репликацию вручную.

Другая причина в том, что очередь на репликацию от других партнеров столь велика, что она не дошла пока до рассматриваемого партнера. Чтобы проверить это предположение, запустите монитор производительности и посмотрите значение счетчика DRA Pending Replication Synchronizations.

Заключение

В этой главе мы обсудили одну из важнейших функций Active Directory — репликацию. Установить единственный контроллер домена и начать работу с ним может практически каждый — правильное конфигурирование крупной системы доступно немногим. Вы должны досконально разобраться в механизме, иначе вы рискуете оказаться в затруднительном положении. Увы, люди обычно обращаются за помощью, лишь когда рассинхронизированная система перестает адекватно работать, что лишний раз подтверждает народную мудрость: «гром не грянет, мужик не перекрестится».

В этой главе я опустил описания ошибок, возникавших в системе до появления пакета обновления SP2, потому что установка SP2 является обязательным условием адекватной работы системы.

Описание наиболее распространенных ошибок и способов их разрешения — изюминка этой главы. Вряд ли вы найдете другой источник информации, в котором было бы приведено столько подробностей. Тем не менее настоятельно рекомендую прочитать раздел Advanced Troubleshooting в [3], [6], особенно часть, посвященную репликации.

Групповая политика

Сегодня вряд ли стоит доказывать необходимость применения политики для управления рабочими станциями и серверами. То, что это заметно повышает управляемость системы и снижает совокупную стоимость владения, вполне очевидно. Для тех, кто представляет, что, как и зачем делать.

Групповая политика в Windows 2000 неразрывно связана с Active Directory — ее архитектурой, топологией репликации и системой безопасности. Связь эта двусторонняя: любой сбой в работе Active Directory непременно отразится на работе групповых правил; неправильно примененные групповые правила могут воспрепятствовать нормальной работе Active Directory. Порочный круг!

Но не все так страшно, если вы разберетесь в устройстве механизма групповой политики. Эта глава содержит теоретические сведения о работе и применении групповых правил ровно в том объеме, который достаточен для понимания тонкостей планирования правил и их внедрения, а также поиска проблем.

Общие сведения

Тот, кто работал с Windows NT, помнит, что в той ОС существовала системная политика — набор правил, позволявший управлять параметрами клиентских компьютеров. Если вы считаете, что о системной политике надо забыть и переключиться на групповую политику Windows 2000, то должен вас огорчить: это не так. В то время как системная политика распространялась на клиенты Windows 9x/NT, групповая политика поддерживается только клиентами под управлением Windows 2000/XP. И виноваты в этом не разработчики Windows

2000. Как вы увидите дальше, мало создать хорошие правила — надо научить клиенты их понимать и обрабатывать. Увы, все клиенты, выпущенные до Windows 2000, обрабатывать групповую политику не умеют. Microsoft, конечно, не мирится с этим и, там где это возможно, выпускает дополнения к устаревшим клиентам Windows, призванные обеспечить обработку **самых** важных правил. Но далеко не все технически осуществимо.

Клиент, **сервер** или **кто** важнее

В процессе регистрации в домене Windows NT 4.0 клиент обращался к файлу config.pol или **ntconfig.pol**, лежащему по умолчанию на контроллере домена в совместно используемом ресурсе **NETLOGON**. Такой файл был единственным для всего домена и содержал набор правил, определенных отдельно для пользователей и для компьютеров. Эти правила позволяли модифицировать две ветви реестра; **HKEY_CURRENT_USER** (HKCU) для параметров пользователя и **HKEY_LOCAL_MACHINE** (HKLM) для параметров компьютеров,

Групповая же политика может быть применена не однократно в пределах домена, а многократно к разным элементам в иерархии Active Directory. Достигается это за счет объектов групповой политики (ОГП). Групповая политика хранится на сервере в разных местах: в папках совместно используемого ресурса **SYSVOL** и контейнерах в Active Directory. Соответственно и сами групповые правила состоят из двух частей: *шаблоны* и *контейнеры* групповых правил. Для каждого ОГП имеется свой контейнер в Active Directory.

Еще одно важное отличие системных правил от групповых в том, когда они применяются к клиенту. Если первые действовали только при регистрации пользователя на компьютере, то вторые применяются несколько раз: **сначала** на этапе старта клиентской машины и ее обращения к сети в поисках «своего» домена, затем при регистрации пользователя в домене, а потом периодически с устанавливаемым интервалом. Так что от клиента не зависит, получит ли он групповую политику. Коль это Windows 2000 или Windows XP Pro, то политика обязательно будет **применена**.

Но у каждого клиента своя локальная **политика**, хранящаяся в каталоге **%systemroot%\system32\grouppolicy**. Будет ли она переписана примененной политикой полностью или частично либо будет главенствовать? Думаю, что, читая книги по **групповой** политике на английском языке, вы сталкивались с аббревиатурой **LSDOU**. Это сокращение служит для запоминания последовательности применения **групповых** правил:

- ◆ локальные (L);
- ◆ для сайта(S);

- + для домена (D);
- ◆ для организационных подразделений (OU).

Таким образом, первыми применяются локальные правила. Вторыми — те, что определены на уровне сайта, и если они противоречат первым, то первые игнорируются. Далее идут правила, применяемые на уровне домена. Они имеют преимущество перед сайтовыми и локальными правилами. И, наконец, — правила уровня ОП. Они важнее всех предыдущих. Если вспомнить о том, что ОП в домене могут выстраиваться в иерархию, то ряд можно продолжить и дальше: правила, примененные к ОП второго уровня имеют преимущества перед правилами ОП первого, правила третьего «перебивают» правила предыдущих и т. д.

Но мало определить групповые правила на сервере, мало задать последовательность их применения. Надо, чтобы и клиенты понимали, как обрабатывать эти правила. Для этого на всех клиентах Windows 2000/XP устанавливается по умолчанию набор динамических библиотек — клиентские расширения групповой политики. Именно в этих динамических библиотеках реализована нужная функциональность. Узнать, какие расширения установлены на вашем компьютере, можно в ветви реестра `HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\Gpextensions`. Кроме стандартных, различные приложения могут устанавливать собственные расширения для обработки специфических групповых правил.



Перечень клиентских расширений групповой политики в реестре

Как видите, однозначно сказать, кто главнее в процессе применения групповой политики: сервер или клиент, — нельзя. Эти компоненты дополняют друг друга. И если на клиентской машине не будет файла `sseccli.dll`, то групповая политика вообще не будет действовать.

Типы групповых правил

Групповые правила делятся на две основные категории: относящиеся к компьютерам и относящиеся к пользователям. Первые действуют на этапе загрузки компьютера, вторые — при регистрации пользователя в домене. Поэтому, даже если компьютер просто подключен к сети и является членом домена, то независимо от того, зарегистрировался ли на нем пользователь, групповые правила к нему уже применены.

Для каждой из этих двух категорий существует определенный набор правил, применение которых возможно по умолчанию:

Наборы правил для компьютеров и пользователей

Правила	Описание
<i>Правила для компьютеров</i>	
Software settings — Software Installation	Позволяет назначать установку на компьютеры приложений, использующих технологию Windows Installer
Windows Settings — Security settings	Обеспечивает конфигурирование системы безопасности компьютеров по шаблонам безопасности
Windows Settings — Scripts	Позволяет исполнять сценарии при загрузке или выключении компьютера. Сценарии могут быть обычными командными файлами или сценариями Windows Scripting Host (WSH)
Administrative Templates	Шаблоны для конфигурирования HKLM ветви реестра
<i>Правила для пользователей</i>	
-Software settings — Software Installation	Позволяет назначать установку приложений, использующих технологию Windows Installer, на те компьютеры, где зарегистрировались пользователи
Windows Settings — Internet Explorer Maintenance	Позволяет настраивать Internet Explorer для каждого пользователя в отдельности
Windows Settings — Folder Redirection	Перенаправление таких папок, как Desktop, My Documents и Startup, в каталоги, отличные от используемых по умолчанию
Windows Settings — Security settings	Позволяют управлять параметрами инфраструктуры открытых ключей для пользователей
Windows Settings — Remote Installation Services	Определяют, конфигурацию средств удаленной установки ОС для каждого пользователя
Windows Settings — Scripts	Позволяют исполнять сценарии при регистрации пользователя в домене или выходе из него. Сценарии могут быть обычными командными файлами или сценариями Windows Scripting Host (WSH)
Administrative Templates	Шаблоны для конфигурирования HKCU ветви реестра

Мы еще обсудим эти типы правил, а пока подробно рассмотрим механизм групповой политики.

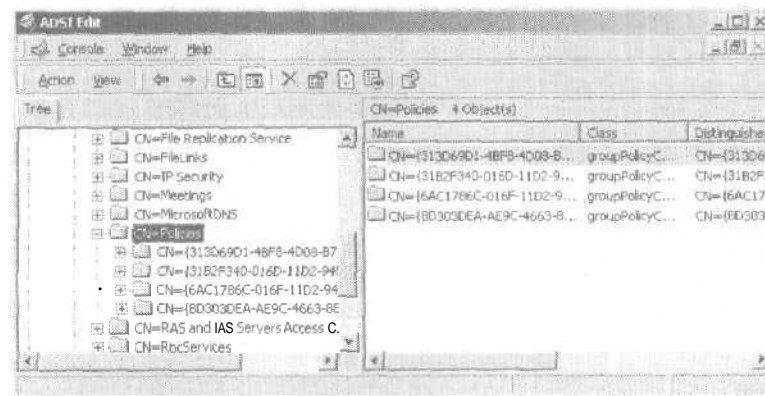
Структура и обработка групповой политики

А начнем мы с внутреннего устройства объектов групповой политики — это окажет неоценимую услугу в поиске проблем.

Устройство объекта групповой политики

Как я уже говорил, объект групповой политики на самом деле не является одним объектом. Это набор параметров, хранящихся в Active Directory и связанных с набором файлов в каталоге SYSVOL. Та часть информации, что хранится в Active Directory, обычно называется контейнером групповой политики (Group Policy Container — GPC). Вторая часть называется шаблоном групповой политики (Group Policy Template — GPT).

Отличительное имя контейнера групповой политики CN=Policies, CN=System, <имя домена>. Его можно увидеть в окне оснастки Active Directory Users and Computers, но с точки зрения понимания объекта это мало что даст. Гораздо информативнее утилита ADSI Edit. Первое, что бросится в глаза. — это содержимое данного контейнера. В нем будет минимум два объекта с длинным названием, подозрительно напоминающим GUID. Это и есть GUID групповых политик. По умолчанию в любом домене две групповые политики: Default domain policy (Доменная политика, применяемая по умолчанию) и Default domain controllers policy (Политика для контроллеров доменов, применяемая по умолчанию). Вот именно их GUID и будут храниться в контейнере. Если же вы определите дополнительные правила, то для них будут существовать отдельные объекты с уникальными номерами GUID.



Контейнер групповой политики в Active Directory

Почему я рекомендовал ADSI Edit? В отличие от оснастки Active Directory Users and Computers она позволяет просмотреть атрибуты любого объекта и их значения.

Может, и найдутся любители ориентироваться в групповых правилах по их GUID, но только не я. Поэтому, чтобы узнать полное имя политики, соответствующей конкретному GUID, надо посмотреть значение его атрибута `displayName`. Из чего мы узнаем, например, что объект с GUID `{6AC1786C-016F-11D2-945F-00C04FB984F9}` соответствует групповой политике `Default domain controllers policy`. Среди прочих атрибутов интерес представляет еще один — `gPCFileSysPath`: он содержит строку с полным путем к шаблону групповой политики. Отношение между каждым контейнером групповой политики и шаблоном — 1:1, т. е. нельзя сделать так, чтобы на один шаблон ссылалось несколько контейнеров.

Так вот, значение атрибута `gPCFileSysPath` для рассмотренного выше контейнера будет равно `\\имя.домена\sysvol\имя.домена\Policies\{6AC1786C-016F-11D2-945F-00C04FB984F9}`. Это и есть место хранения шаблона. То, что GUID объекта и имя папки совпадают, значительно облегчает процесс поиска и устранения проблем.

Очевидно, что связь между контейнером и шаблоном должна существовать всегда. Ее нарушение может привести к серьезным проблемам применения групповых правил. Если же вспомнить, как создаются групповые правила, можно выделить два ключевых момента.

- Контейнер создаваемой групповой политики помещается в локальную базу на том контроллере, где политика создается. Затем контейнер тиражируется на остальные контроллеры в домене.
- Каталог шаблона групповой политики создается и редактируется в каталоге `SYSVOL` на том контроллере, где политика создается. Затем каталог тиражируется на все остальные контроллеры в домене.

Вроде никакого подвоха, но... Если подумать, становится понятно, что в то время, как объект в Active Directory тиражируется, используя механизм репликации Active Directory, содержимое `SYSVOL` тиражируется, применяя механизм репликации NTFRS. Хотя оба этих механизма используют единую топологию репликации, расписание тиражирования может быть разным, а значит, может случиться, что контейнер политики уже будет на контроллере домена, а шаблон — еще нет.

Хранение параметров групповой политики

Кроме упомянутых атрибутов контейнера групповых правил `displayName` и `gPCFileSysPath`, стоит рассмотреть и такие:

Атрибут	Описание
<code>gPCFunctionalityVersion</code>	Определяет версию расширения оснастки Group Policy, в которой был создан ОГП

см. след. стр.

Атрибут	Описание
gPCMachineExtensionsName	Указывает номер GUID для динамической библиотеки, реализующей функциональность данной групповой политики применительно к компьютерам
gPCUserExtensionsName	Указывает номер GUID динамической библиотеки, реализующей функциональность данной групповой политики применительно к пользователям
versionNumber	Версия политики в каталоге. Эта версия сравнивается со значением, записанным в файле gpt.ini в папке шаблона данной групповой политики, чтобы понять, нуждается ли политика в синхронизации или нет

Эти атрибуты нам понадобятся в дальнейшем.

Как вы помните, ОГП хранятся в двух местах: в Active Directory и в каталоге SYSVOL. Для каждого контейнера существуют два вложенных контейнера Machine и User, что, как легко догадаться, имеет отношение к правилам для компьютеров и пользователей. Если раскрыть любой из этих контейнеров для политики, определяющей установку ПО, то внутри будет контейнер Class Store. Примечательный контейнер. Во-первых, в нем находится еще один контейнер — Packages, где хранятся объекты класса packageRegistration — назначенные или опубликованные приложения. Во-вторых, Class Store можно рассматривать как ветвь реестра HKEY_CLASSES_ROOT, но хранимую в Active Directory. Как известно, эта ветвь содержит ассоциации расширений файлов с разными программами и зарегистрированные в системе COM-объекты. Если поместить в Class Store сведения о COM-объекте, то этот объект будет доступен на всех компьютерах или для всех пользователей, на которых распространяется действие данного ОГП.

Теперь вернемся к хранилищу шаблонов групповой политики. Если открыть папку любого из шаблонов (т. е. название которой совпадает с номером GUID объекта групповой политики), то внутри обнаружатся еще три папки и один файл:

Объект	Что хранится
Папка Adm	Все административные шаблоны, используемые политикой. Находятся в файлах с расширением .adm
Папка Machine	Все правила, применимые к компьютерам, включая правила реестра
Папка User	Все правила, применимые к пользователям, включая правила реестра
Файл Gpt.ini	Информация о версии шаблонов

Содержимое папок Machine и User примерно одинаково и зависит в общем случае от того, какие именно правила были применены. Ниже

перечислены папки, которые там могут находиться, условия их появления и описание содержимого:

Папка	Когда создается	Содержимое
Applications	При назначении или публикации приложений	Файлы сценариев установки приложений. Имя файла имеет формат <GUID>.aas. Сценарий ссылается на пакет, описанный в контейнере групповой политики
Documents & Settings	При перенаправлении папок	<p>Файл INI, в котором перечисляются условия перенаправления. В разделе FolderStatus перечислены параметры перенаправления. А далее для каждой папки указывается условие в виде SID объекта=путь к папке. Например:</p> <pre> [FolderStatus] Application Data=11 Desktop=11 My Documents=11 My Pictures=2 Start Menu=0 Programs=2 Startup=2 [Application Data] s-1-1-0=\\fzhub\personal\%username%\ Application data [Desktop] s-1-1-0=\\fzhub\personal\%username%\ Desktop [My Documents] s-1-1-0=\\fzhub\personal\%username%\My Documents [My Pictures] [Start Menu] s-1-1-0=\\fzhub\personal\%username%\ Start Menu [Programs] [Startup] </pre>
Microsoft	При конфигурировании параметров Security Configuration Editor, IE Admin, RIS	<p>Папки, соответствующие каждому из приложений. Так, для Security Editor создаются вложенные папки \Windows NT\Secedit, куда помещается gpntmpl.inf — файл, содержащий по сути правила доменной безопасности. Например:</p> <pre> [Unicode] Unicode=yes [System Access] </pre>

см. след. стр.

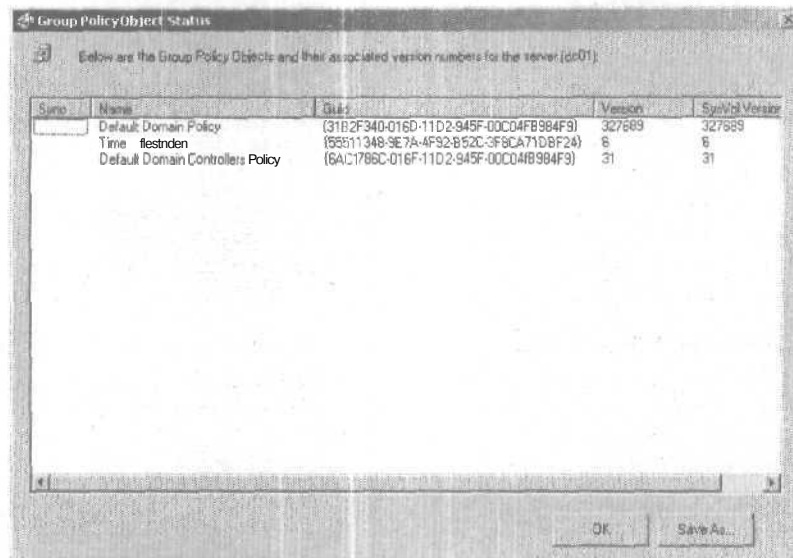
Папка	Когда создается	Содержимое
		<pre> MinimumPasswordAge = 0 MaximumPasswordAge = 42 MinimumPasswordLength = 0 PasswordComplexity = 0 PasswordHistorySize = 1 LockoutBadCount = 0 RequireLogonToChangePassword = 0 ForceLogoffWhenHourExpire = 0 ClearTextPassword = 0 [Kerberos Policy] MaxTicketAge = 10 MaxRenewAge = 7 MaxServiceAge = 600 MaxClockSkew = 5 TicketValidateClient = 1 [Version] signature="\$CHICAGO\$" Revision=1 </pre>
Scripts	При конфигурировании сценариев загрузки/выключения системы и входа/выхода пользователей	Файл <code>scripts.ini</code> . В нем записаны ссылки на файлы сценариев, параметры, которые можно им передать, а также условия вызова сценария
Название компании-производителя программ	При конфигурировании параметров приложений третьих фирм, если разработчиками это предусмотрено	Папки, соответствующие каждому из приложений

Помимо указанных, в папках `User` и `Machine` находится файл `Registry.pol`. Он содержит параметры, активизированные в разделе `Administrative Templates` объекта групповой политики. Содержимое этого файла тесно связано с файлами, лежащими в каталоге `Adm`. Именно в нем записано, какие шаблоны из тех, что лежат в `Adm`, и как должны быть применены для конфигурирования системы.

Версии и ревизии

Версия ОГП хранится как в контейнере групповой политики в `Active Directory` (атрибут `versionNumber`), так и в виде числа — в файле `gpt.ini`. Но не все так просто с версионностью групповой политики.

Чтобы разобраться в этом механизме, предлагаю запустить `AD Replication Monitor`, щелкнуть любой из контроллеров в домене правой кнопкой и выбрать команду `Show Group policy object status`. Появится диалоговое окно, аналогичное этому:



Версии групповых политик

Здесь перечислены все групповые политики, определенные в домене, и номера их версий, хранящиеся как в Active Directory, так и в папке SYSVOL. Если вы изменяли политики хоть несколько раз, то величины версий *будут* иметь тот же порядок, что и на рисунке. Не думайте, что у вас ослабла память до такой *степени*, что вы изменяли политику 327 689 раз и забыли об этом. Не стоит подозревать и врагов, тайно завладевших паролем администратора и меняющих политику ежеминутно. Это все следствие того неочевидного правила изменения версий. Но прежде чем его объяснить, я напущу еще больше тумана. Открыв окно свойств *групповой* политики, вы увидите поле Revisions с иными цифрами, например. 3 (User) 2 (Computer). Попытка обнаружить корреляцию между этими ревизиями и номером версии кончится неудачей.

Причина такой запутанности в следующем. Когда вы редактируете правила для компьютера, это не отражается на правилах для пользователя, и наоборот. Значит, надо отдельно считать версии пользовательских и компьютерных правил. Для этого и существуют ревизии. Всякий раз, когда вы меняете правило для *пользователей* (не всю политику, а только одно правило!) номер ревизии увеличивается на 1. При этом на 1 увеличивается и номер версии. Скажем, если я изменю 10 параметров для *пользователей*, ревизия запишется как 0 (Computer), 10 (User), а версия станет равной 10.

Совсем иная картина при изменении компьютерных правил. При изменении одного компьютерного правила ревизия увеличивается на 1, а номер версии — на 65 536! Значит, в нашем примере ревизия запишется как 1 (Computer), 10 (User), а номер версии — как 65 546. Всякий раз при изменении правила для компьютера к версии будет прибавляться 65 536.

Для тех, кто еще не понял фокуса, объясняю, что тип атрибута version-Number — INTEGER. Младшие 16 разрядов отвечают за номер пользовательской ревизии, а старшие — за номер ревизии политики для компьютеров. Вместе получается полная версия.

Клиентские расширения

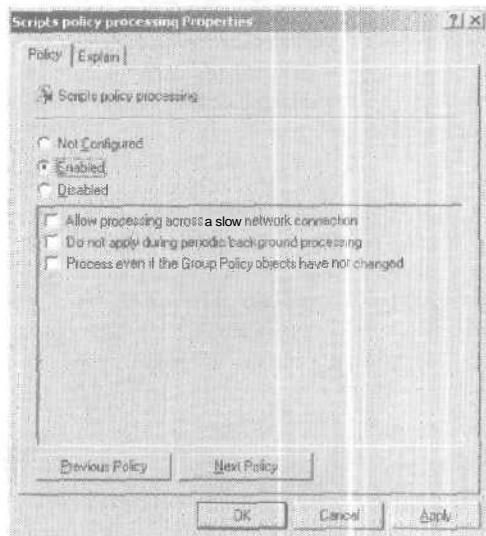
Как вы помните, на каждом клиентском компьютере есть набор DLL, ответственных за обработку правил и называемых клиентскими расширениями групповых правил. Эти расширения загружаются по мере надобности. Когда на компьютере рассматривается перечень групповых правил, которые должны быть к нему применены, то проверяется, нет ли среди них таких, что требуют расширений. Если такое правило находится, подгружается соответствующее расширение.

Каждое расширение хранится в реестре в виде номера GUID:

Соответствия номеров GUID расширениям и DLL.

Расширение	Номер GUID	Название DLL
Квотирование дисков	{3610eda5-77ef-11d2-8dc5-00c04fa31a66}	dskquota.dll
Установка параметров в реестре	{35378EAC-683F-11D2-A89A-00C04FBBCFA2}	userenv.dll
Перенаправление папок	{25537BA6-77A8-11D2-9B6C-0000F8080861}	fdeploy.dll
Обработка сценариев	{42B5FAAE-6536-11d2-AE5A-0000F87571E3}	gptext.dll
Обработка политики по таймеру в Windows XP	{426031c0-0b47-4852-b0ca-ac3d37bfc39}	gptext.dll
Управление параметрами безопасности	{827D319E-6EAC-11D2-A4EA-00C04F79F83A}	scecli.dll
Настройка Internet Explorer	{A2E30F80-D7DE-11d2-BBDE-00C04F86AE3B}	iedkcs.dll
Управление политикой восстановления EFS	{B1BE8D72-6EAC-11D2-A4EA-00C04F79F83A}	scecli.dll
Установка программ	{c6dc5466-785a-11d2-84d0-00c04fb169f7}	appmgmts.dll
Управление политикой безопасности IP	{e437bc1c-aa7d-11d2-a382-00c04f991e27}	gptext.dll

Вы можете управлять тем, как именно **клиентские расширения** включаются в процесс обработки **правил**. Делается это опять-таки через специальную групповую политику. Существует не более трех вариантов управления, Я говорю *не более*, потому что к некоторым **расширениям** некоторые варианты неприменимы.



Варианты управления клиентскими расширениями групповой политики

Обработка по медленным каналам связи

Разрешать обработку по медленным каналам связи (Allow processing across a slow network connection). Для каждого клиентского расширения существуют значения по умолчанию, согласно которым они используются или нет. Так, если канал медленный, а применение правил приводит к передаче по нему большого количества **данных**, то это может вызвать **перегрузку** канала, что **нежелательно**. Я считаю умолчания достаточно разумными, но если в конкретных условиях надо применять и другие **правила**, то это нетрудно **сделать**.

По умолчанию применяются такие расширения независимо от полосы пропускания канала:

- обработка реестра (административные шаблоны);
- ◆ изменение параметров безопасности.

Такой выбор вполне оправдан. Судите сами: разве можно запретить задавать параметры безопасности? Чем **пользователи**, расположенные в удаленном сайте, связанном **медленным каналом**, хуже (или лучше)

остальных? Если в домене заданы определенные правила паролей, то они должны относиться ко всем независимо от того, в каком сегменте сети пользователи находятся. Главный критерий то, что они принадлежат данному домену.

Редактирование параметров реестра также зачастую связано с безопасностью. Обычно эти параметры влияют на доступность на клиентских компьютерах критичных элементов интерфейса. К примеру, вы не хотите, чтобы пользователь мог запускать неразрешенные приложения. А ведь их запуск можно ограничить только через реестр.

Именно поэтому оба эти расширения не только применяются на любых каналах по умолчанию, но и *нельзя запретить* их использование вообще! А вот *остальные* расширения вы *можете* разрешить на медленных каналах. Скажем, если установка какого-то приложения обязательна для всех пользователей и ради этого вы готовы пожертвовать пропусканием канала, разрешите соответствующее клиентское расширение.

А какой канал считать медленным? И как система должна понять, что этот канал медленный, а другой нет? Алгоритм вычисления скорости канала следующий:

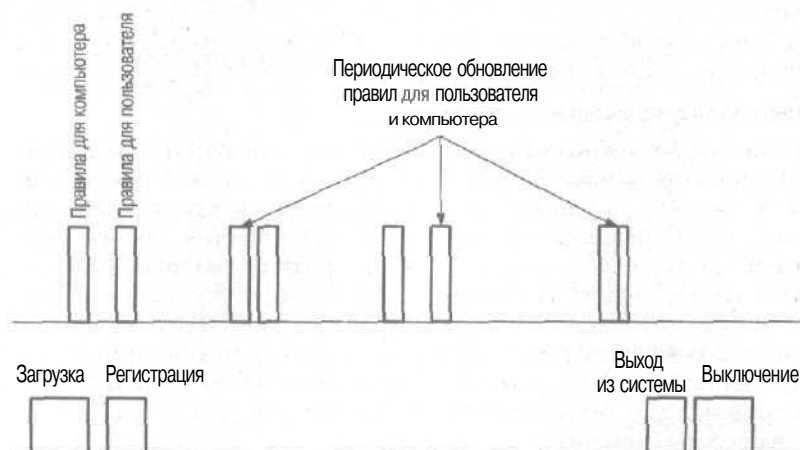
1. на сервер посылается пакет, содержащий 0 байт данных, и измеряется время отклика (t_1);
2. на сервер посылается пакет, содержащий 4 кб данных, и измеряется время отклика (t_2);
3. измеряется разница $D=t_2-t_1$;
4. данная процедура выполняется трижды, и каждый раз к величине D добавляется *новое* значение D ;
5. выполняется усреднение D : $D=D/3$;
6. $B=(4K * 1000/D * 8)/1024$ (кб/с).

Специальное правило в групповой политике — Group policy slow link detection — отвечает за установление порога скорости. Если оно не определено, то медленным каналом считается любой, чья пропускная способность ниже 500 кбит/с. Устанавливая данное правило, вы можете указать граничную полосу пропускания канала в диапазоне от 0 до 4,294,967,200 кбит/с. Любой канал, пропускная способность которого меньше указанной вами, будет считаться медленным. Если указать 0, все каналы будут считаться быстрыми.

Периодическое фоновое применение

Групповая политика применяется к компьютерам неоднократно. Первый раз это происходит на этапе загрузки компьютера; при этом действуют правила, относящиеся к компьютеру. Второй раз — при регистрации пользователя в системе; на этот раз применяются только

пользовательские правила. Наконец, правила применяются регулярно в фоновом режиме. Интервал между последовательными применениями зависит от типа политики и от параметров, определенных в соответствующих правилах. Некоторые правила никогда не применяются в фоновом режиме: это правила установки ПО и перенаправления папок. В самом деле, представьте, что у вас сконфигурировано перенаправление папки My Documents в каталог на сервере А. В какой-то момент данное правило администратор изменил так, что папка перенаправляется в каталог на сервере Б. Если в момент периодического обновления политики клиентское расширение, ответственное за перенаправление папок (fdeploy.dll), обнаружит изменение и начнет перемещать файлы в новое место, это может оказаться весьма критично как для пользователя, который уже открыл несколько документов в этой папке, так и для клиентского расширения, которое не сможет переместить открытые файлы.



Применение групповой политики к компьютеру

Ниже приведены величины интервалов для разных типов клиентов.

Интервалы применения политик в фоновом режиме

Политика	Интервал по умолчанию	Диапазон
Для компьютеров (обычный клиент)	90 минут + (0–30) минут	(7 секунд–45 дней) + (0–24) часа
Для пользователей (обычный клиент)	90 минут + (0–30) минут	(7 секунд–45 дней) + (0–24) часа
Для контроллеров домена	5 минут	(7 секунд–45 дней) + (0–24) часа

Как видите, по умолчанию только на контроллерах домена правила применяются через фиксированные промежутки времени. Для остальных клиентов существует разброс в пределах 30 минут. Этот разброс введен для того, чтобы не все клиенты получали политику одновременно и не загружали каналы. Значения по умолчанию являются оптимальными, и вряд ли стоит их менять.

Иногда фоновое изменение любых правил не требуется совсем. Например, вы знаете, что политика в корпоративной сети может изменяться только в соответствии с жестко прописанной процедурой после многократных согласований. Изменения выполняются во вне-рабочее время, когда нет включенных компьютеров. Фоновое применение правил в такой системе лишь напрасно расходует ресурсы сети и компьютеров. Дабы уменьшить негативное влияние, можно запретить фоновое применение каких-либо правил вообще. Для этого надо установить правило *Запрета фонового обновления групповой политики* (Disable background refresh of Group Policy). После этого правила будут действовать только при загрузке компьютера и регистрации пользователей в системе.

Применение неизменной политики

Периодическое обновление правил кажется излишним и тогда, когда сами правила не меняются. По умолчанию это так и есть: пока правила не изменились, клиентские расширения их не обрабатывают. Однако все мы знаем наших пользователей. В то время как основная масса занята исключительно работой, находятся пытливые «юзеры», которые, обнаружив административные полномочия на локальном компьютере, начинают перекраивать систему под себя. В итоге устанавливаются непонятные программы, удаляются нужные файлы, поверхность экрана захламляется разными картинками и т. п. И бедные сотрудники службы ИТ вынуждены сверхурочно работать, переустанавливая приложения, а то и всю систему.

Бывают и горе-администраторы, способные ставить эксперименты на работающей системе, в частности, на контроллерах домена. Они изыскивают всевозможные способы включения себя в группы с более высокими полномочиями, чтобы проверять свои «теории».

Есть, наконец, мерзкие программы-трояны, пытающиеся включить себя в административные группы. Понятно, что такие попытки можно предотвратить, определив, например, правила ограниченного членства в группах. Но если сами правила не меняются, клиентское расширение не сможет проконтролировать неизменность состава группы.

Потому и существует правило *Обрабатывать даже неизменные объекты групповой политики* (Process even if the Group Policy Objects have not changed). Установите его, и правила будут применяться к пользователю и компьютеру независимо от того, менялись они или нет.

Параметры клиентских расширений

Для каждого из клиентских расширений в реестре прописано несколько параметров.

Параметры клиентских расширений

Параметр	Назначение	Значения
DllName		Имя динамической библиотеки
ProcessGroup-Policy		Имя функции, вызываемой при обработке групповой политики данным расширением
ProcessGroup-PolicyEx		Имя функции, вызываемой при обработке групповой политики данным расширением в Windows XP
NoMachinePolicy	Определяет, обрабатывает ли клиентское расширение групповую политику для компьютеров	0 (или отсутствие) — обрабатывает, 1 — не обрабатывает
NoUserPolicy	Определяет, обрабатывает ли клиентское расширение групповую политику для пользователей	0 (или отсутствие) — обрабатывает, 1 — не обрабатывает
NoSlowLink	Определяет, обрабатывает ли клиентское расширение групповую политику на медленных каналах	0 (или отсутствие) — обрабатывает, 1 — не обрабатывает
NoBackground-Policy	Определяет, обрабатывает ли клиентское расширение групповую политику в фоновом режиме	0 (или отсутствие) — обрабатывает, 1 — не обрабатывает
NoGPOList-Changes	Определяет, обрабатывает ли клиентское расширение групповую политику, если она не изменилась по сравнению с предыдущим значением	0 (или отсутствие) — обрабатывает, 1 — не обрабатывает
PerUserLocal-Settings	Если установлено, пользовательские правила кэшируются для каждой машины и каждого пользователя	0 (или отсутствие) — не установлено, 1 — установлено
RequiresSuccessfulRegistry	Если установлено, то требуется успешная регистрация клиентского расширения, прежде чем будет обрабатываться политика	0 (или отсутствие) — не установлено, 1 — установлено
EnableAsynchronousProcessing	Определяет, продолжать ли обработку групповой политики, пока клиентское расширение не завершило обработку предыдущего правила	0 (или отсутствие) — синхронно (одно за другим), 1 — асинхронно

Применение групповых правил

А теперь я постараюсь объяснить, как работать с групповой политикой. О том, какое диалоговое окно открыть и какую кнопку **нажать**, я рассказывать не стану: это вы и так должны знать. Речь пойдет о том:

- ◆ как изменить порядок применения групповых правил;
- ◆ как выполнять фильтрацию;
- ◆ где создавать правила;
 - как делегировать полномочия по созданию правил.

Предварительно замечу, что для того, чтобы создавать, редактировать или удалять объекты групповой политики и чтобы изменять последовательность их применения, нужно быть членом одной из групп:

- ◆ Domain Admins;
- ◆ Administrators;
 - Enterprise Admins;
- ◆ Group Policy Creators.

Изменение последовательности

Акроним **LSDOU**, как я уже говорил, показывает последовательность применения групповых правил: **правила**, определенные на более глубоком уровне, имеют преимущество перед определенными на верхних уровнях. С одной **стороны**, это весьма удобно, так как позволяет централизованно назначить политику на весь домен и в то же время, изменять отдельные правила для ОП. С другой — иногда такое наследование политик нежелательно, либо его нужно **существенно** изменить. В Windows 2000 несколько механизмов изменения последовательности применения правил:

- ◆ блокировка наследования;
- ◆ принудительный приоритет;
- ◆ перемычки;
- ◆ деактивизация правил.

Блокировка наследования

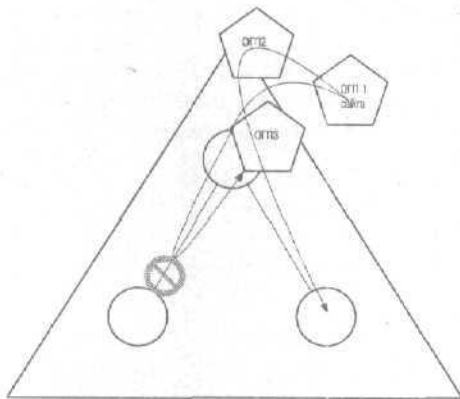
Представьте ситуацию, когда администратор домена делегировал администрирование некоторого ОП другому пользователю. Для всего домена назначена политика настройки интерфейса запрещающая работать с приложениями, не соответствующими корпоративному стандарту. Пользователи упомянутого ОП занимаются тем, что тестируют разнообразные приложения с целью выдачи рекомендаций об их пригодности и включении в корпоративный стандарт. Очевидно,

что групповая политика, ограничивающая их возможности по запуску приложений им совершенно не подходит.

Эту проблему можно решить несколькими способами.

1. Попросить администратора домена создать группу тестеров и включить в нее упомянутых пользователей. Указать эту группу в качестве фильтра для объекта групповой политики, чтобы политика не применялась к членам этой группы
2. Попросить администратора или пользователя, которому делегированы полномочия администрирования ОП, создать отдельную групповую политику, которая бы разрешала работать с любыми приложениями, и применить эту политику к ОП.
3. Попросить пользователя, которому делегированы административные полномочия, заблокировать действие общей групповой политики.

Хотя все три подхода приведут к желаемому результату, именно третий выглядит предпочтительней, так как не требует создания новой политики. Но такое решение подойдет, только когда надо отменить действие всех правил, которые могут быть унаследованы. Если из большого списка правил надо отменить лишь несколько, блокировка наследования не является оптимальной, так как будет сопряжена с созданием правил, фактически повторяющих большинство из унаследованных,



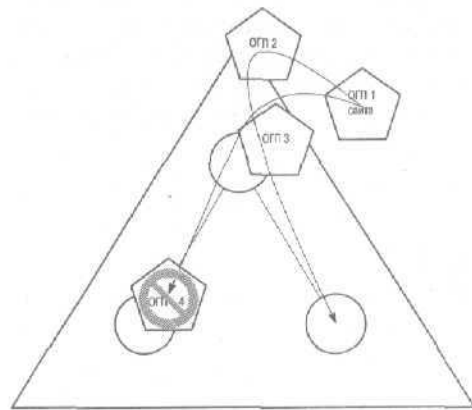
Блокировка наследования

Блокировка наследования правил может выполняться на уровне домена и на уровне любого ОП. Если она действует на уровне домена, то отменяется наследование любых правил, заданных для сайта. Если на уровне ОП, то отменяется действие всех правил, заданных на уровне сайта, домена и вышестоящих ОП.

Замечание Блокировка наследования не отменяет действия тех правил, для которых выставлено принудительное наследование.

Принудительное наследование

Рассмотрим наш пример несколько с иной стороны. Допустим, в нашем ОП пользователи должны *вкусить все* прелести политики, назначенной на уровне домена. Администратор домена не может на 100% быть *уверенным*, что пользователь, которому даны права по управлению ОП, не заблокирует наследование. Постоянно контролировать пользователя *невозможно*. Раз так, надо применить метод, препятствующий блокированию, — принудительное наследование (No override). Помните, что этот метод *устанавливается* не для объекта групповой политики, а для его связи с определенным контейнером. Иначе говоря, объект групповой политики может быть применен к одному контейнеру с принудительным наследованием и к другому контейнеру — без него.



Принудительное наследование позволяет игнорировать локальные правила

Принудительное наследование распространяется только на правила, определенные в групповой политике. Если какое-то правило задано в политике, примененной к дочернему контейнеру, но не задано в политике родительского, в итоге будет действовать заданное.

Перемычки

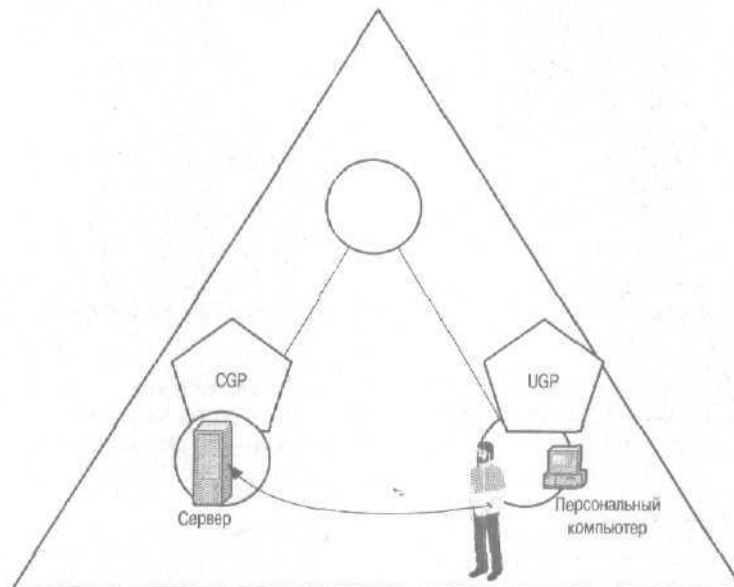
Теперь представим организацию, в которой, кроме обычных компьютеров пользователей, есть и специальные, например терминал-серверы. Требования к параметрам пользователей, открывающим терминальные сеансы, могут отличаться от их обычных параметров.

Скажем, в терминальной сессии может быть запрещено видеть все локальные диски и работать с Windows Explorer. Понятно, что это страшно неудобно при работе на своем персональном компьютере.

Как вы, должно быть, знаете, упомянутые правила являются пользовательскими, но не распространяются на компьютеры. Учитывая, что учетную запись пользователя нельзя одновременно поместить в два контейнера, можно прийти к выводу, что реализовать нужную функциональность средствами групповой политики нельзя. Но это не так.

В групповых правилах существуют так называемые *перемычки* (loop-back processing). Смысл перемычек заключается в следующем. Пусть для некоторого ОП определена групповая политика UGP. Пользователь U имеет все параметры в соответствии с этой политикой при работе на своем компьютере. Для другого ОП, в котором расположен сервер S, определена групповая политика CGP, которая описывает как правила для пользователей, так и для компьютеров. Если бы в этом ОП находились учетные записи пользователей, они бы применяли правила политики CGP. Пусть пользователь U регистрируется на компьютере S. В общем случае результат будет таков:

- ◆ параметры компьютера будут взяты из политики CGP;
- параметры пользователя — из политики UGP.



Перемычка правил

В случае перемишек правил действуют два механизма создания результирующей для пользователя политики: *слияние* и *замещение*.

При слиянии правила из политики CGP будут объединены с правилами из политики UGP. Если, например, в UGP стоит *перенаправление* папки My Documents на совместно используемый ресурс на сервере, а в политике CGP это правило не определено, то результат — перенаправление папки на сервер. Если же правила в политиках CGP и UGP конфликтуют, то преимущество будет иметь правило в политике CGP, т. е. в той, где расположен компьютер.

При замещении все правила из *пользовательской* политики UGP будут заменены пользовательскими правилами политики CGP независимо от *того*, заданы они в ней или *нет*.

Деактивизация правил

Теперь обратимся к ситуации, когда вы отлаживаете результирующую *групповую* политику на клиентских компьютерах. При этом полезно отключить временно действие каких-либо правил. С этой целью можно задействовать механизм *деактивизации* ОПП.

При деактивизации все правила, заданные этой групповой политикой, перестают *действовать* сразу после следующего цикла применения. Это значит, что если правилами предписывалось выполнить *перееддресацию* папки My Documents на сервер, то после их деактивизации папка должна вернуться в исходное состояние или в *то*, что указывает вышестоящая политика.

Все это так и работает, но за одним исключением. Есть правила, в которых надо дополнительно описать изменение правил после удаления или деактивизации политики. К таковым относятся, в частности, правила *перееддресации* папок. По умолчанию предполагается, что *деактивизация* соответствующей политики не приведет к переносу содержимого папок в другое место. Во-первых, это может быть нежелательно. Политика может охватывать десятки и сотни пользователей, и не у каждого на компьютере может хватить места, чтобы принять все документы только из-за того, что вы отлаживаете политику *для* кого-то одного. Во-вторых, *из-за* объема перемещаемых данных сервер и сеть окажутся просто перегружены. Чтобы деактивизация правил *перемещения* папок приводила к их *возврату* в исходное положение, надо отметить соответствующий флажок в параметрах.

Фильтрация

Итак, групповая политика может быть применена на уровне сайта, домена и ОП. Но такая прямолинейность не всегда удобна. Например, администраторов домена не надо ограничивать в доступе к приложениям, сетевым дискам и иным *ресурсам*. Если же в домене *осущест-*

ляется политика, запрещающая пользователям некоторые действия, она будет распространена и на администраторов. Если администраторов вынести в отдельное ОП, придется создавать специальную политику, отменяющую действие доменной.

Повысить гибкость работы с политиками позволяет фильтрация. Суть этого механизма проста: у каждой политики, как у любого объекта Active Directory, есть список контроля доступа. Помимо таких строк, как Read, Write, Full Control, в нем есть и Apply Group Policy. Отдельно от Read разрешение Apply не имеет смысла. Но если для группы пользователей в списке контроля доступа политики указаны оба этих разрешения, политика будет применена к этой группе.

Разрешение Read означает, что член группы может только посмотреть параметры правил, но они не будут применены к нему. Всякий раз при создании нового объекта групповой политики к нему применяются разрешения, заложенные в схеме. Вот список таких разрешений:

Разрешения, применяемые к объекту групповой политики по умолчанию

	Full Control	Read	Write	Create All child objects	Delete All child objects	Apply Group Policy
Authenticated Users		/				/
Creator owners						
Domain Admins		/	✓	/	/	
Enterprise Admins		/	/	/	✓	
SYSTEM		/	✓	/	✓	

Как видите, по умолчанию политика применяется ко всем членам группы Authenticated Users, в которую по умолчанию входят все зарегистрированные в лесу пользователи, кроме анонимов и гостей. Следуя этой логике, можно предположить, что и для администраторов, как для членов группы Authenticated Users, также будет применяться политика, хотя ниже указано, что к ним она не применяется.

Это не так. Дело в том, что, рассматривая список контроля доступа, надо обращать внимание не на алфавитный порядок групп, а на их расположение. Достаточно открыть редактор списка контроля доступа, чтобы увидеть, что на первой строчке — разрешения для группы Domain Admins. Так как для них разрешение Apply Group Policy не указано, то правила к ним применяться не будут.

Замечание По умолчанию группа Enterprise Admins стоит в списке контроля доступа на последнем месте. Если ее члены не входят в группу Domain Admins, то с точки зрения политики, они такие же пользователи, как и все другие, и правила будут применены к ним.

Обратим внимание на группу Creator Owners. То, что для нее по умолчанию не определено стандартных прав, ничего не значит. Дело в том, что в списке контроля доступа для них заданы дополнительные разрешения, применяемые ко всем дочерним для данного объектам, в результате чего по отношению к создателям политика ведет себя так:

- ◆ создатель политики (не администратор) может просматривать и модифицировать только те правила, которые создал сам;
- он же может только просматривать, но не редактировать правила, разработанные другими создателями;
- ◆ правила по умолчанию не применяются к создателям.

Умолчания не всегда подходят, поэтому естественно, что для тщательной фильтрации применяются измененные списки контроля доступа. Правила работы со списками похожи на те, что действуют при работе со списками контроля доступа к каталогам файловой системы или объектам Active Directory, но есть и отличия.

Замечание Разрешения, о которых идет речь, применяются к ОПП, а не к связям между объектами и контейнерами, к которым применяется политика.

Во-первых, наличие группы **Authenticated Users** не всегда желательно. Например, вы применяете политику к ОП, но хотите, чтобы она распространялась только на сотрудников группы маркетинга внутри этого ОП. Поэтому можно либо лишить группу **Authenticated Users** разрешения **Apply Group Policy**, либо вовсе удалить ее из списка контроля доступа. Плюс к тому надо включить в список локальную группу **домена**, в которую входят сотрудники маркетинга.

Во-вторых, никогда не **включайте** отдельных пользователей в список контроля доступа. Это правило является универсальным и применимо для всех типов списков контроля доступа.

В-третьих, вам дано **право** применить явное запрещение доступа **Deny**. Скажем, вы хотите, чтобы политика применялась ко всем пользователям в домене, кроме небольшой группы технических специалистов. Вариантов достижения цели несколько:

- из списка контроля доступа к объекту групповой политики удалить **Authenticated Users** и включить все группы пользователей, кроме группы технических специалистов;
- ◆ создать отдельное подразделение, включить в него технических специалистов и заблокировать распространение правил на это ОП;
- ◆ в список контроля доступа ввести новую строку — запрет на применение политики (**Deny Apply Group Policy**) для группы технических специалистов.

Последний вариант кажется самым предпочтительным, так как требует совершить минимум действий. Не спешите! Применение явных запрещений со временем *может* превратиться в большую головную боль. Поэтому вместо безоглядного использования Deny проанализируйте конкретную ситуацию.

Если в домене и так существует структура ОП и технические специалисты могут быть помещены в свое собственное, то выберите этот путь. Он не окажется трудоемким.

Если вы используете рекомендации по применению групп безопасности (см. главу «Проектируем Active Directory»), то первый из предложенных вариантов выглядит достаточно разумным.

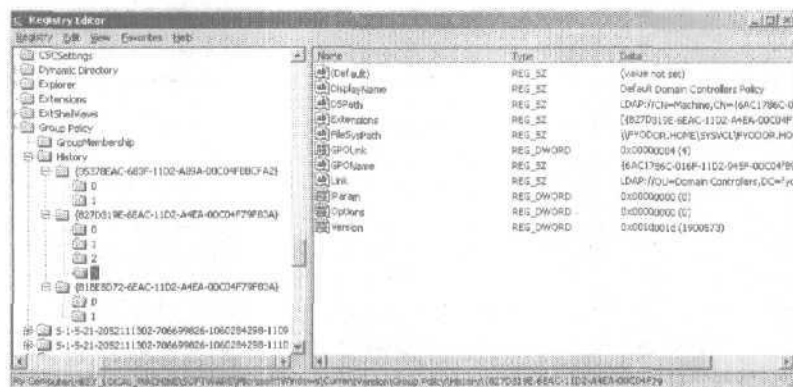
Наконец, если у вас ни групп безопасности, ни ОП, можно использовать явное запрещение Deny.

Совет Если вы пошли по последнему пути, то очень рекомендую программу **FAZAM 2000** компании **FullArmor**. Этот инструмент позволит значительно упростить процесс отладки групповых правил и анализа результата применения в самых сложных случаях.

История применения правил

Узнать, какие правила применены к компьютеру или пользователю в данный момент, можно из истории применения правил (это можно сделать и иначе, но об этом позже). История применения правил — это хранящийся в реестре список клиентских расширений и политик, которые каждое из расширений обрабатывало. Причем политики перечисляются в той последовательности, в какой были применены. История политик компьютеров хранится в ветви реестра `HKLM\Software\Microsoft\Windows\CurrentVersion\Group Policy\History`, а пользовательских правил — в ветви `HKCU\Software\Microsoft\Windows\CurrentVersion\Group Policy\History`.

Каждый элемент в списке представляет собой номер GUID клиентского расширения. Для каждого расширения приведены численные элементы 0, 1, ..., соответствующие порядковому номеру использования расширения. Например, 0 соответствует расширению для обработки локальных правил, 1 — правил сайта, 2 — правил домена и т. д. Всякий раз, как расширение обрабатывает правило, в историю записывается новый параметр, номер которого на 1 больше предыдущего. Для каждого параметра записывается ряд поясняющих значений.



История применения компьютерных правил в реестре

Параметры истории применения правил

Параметр	Назначение
DisplayName	Имя огп
DSPATH	Отличительное имя контейнера групповой политики в Active Directory. Для локальных правил этого параметра нет, так как локальные правила не хранятся в Active Directory
FileSysPath	Путь к шаблону групповой политики. Путь записывается в виде UNC-пути к каталогу SYSVOL. Для локальной политики он всегда начинается с %SystemRoot%\System32\GroupPolicy
GPOLink	Указывает область применения ОГП: 0 — нет информации; 1 — ОГП связан с машиной (локальный); 2 — ОГП связан с сайтом; 3 — ОГП связан с доменом; 4 — ОГП связан с подразделением
GPOName	Имя объекта групповой политики. Для локальной политики это «Local Group Policy». Для остальных ОГП — это номер GUID данного объекта
Iparam	Используется для выполнения различных функций над ОГП. Клиентские расширения применяют его по своему усмотрению (точнее, по усмотрению программиста)
Options	Отражает параметры, которые администратор установил при конфигурировании групповой политики. К ним относятся, например, деактивизация или принудительное наследование
Version	Номер версии ОГП на тот момент, когда данные правила были применены в последний раз

Взглянув на историю правил, можно примерно оценить, сколь сложно будет выяснить результирующий набор параметров. Но замечу, эти

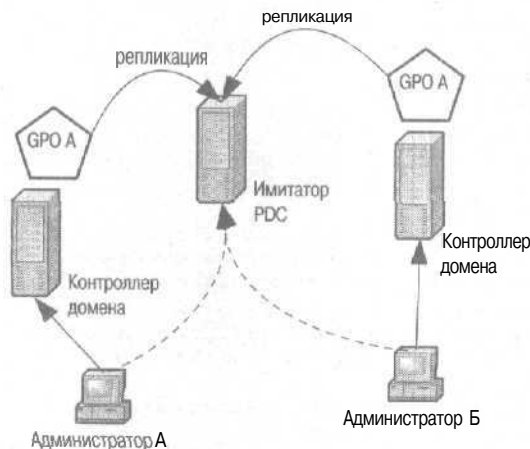
параметры реестра нужны не столько администратору, сколько клиентским расширениям. Они определяют, например, изменилась ли политика по сравнению с предыдущей, обращаясь к этой ветви реестра.

Где создавать и редактировать правила?

Странный вопрос — конечно, только на контроллере домена, скажете вы, и будете почти правы.

Напомню, что объект групповой политики хранится как в Active Directory, так и в каталоге `SYSVOL`, а репликация этих источников выполняется несинхронно. А значит, вы рискуете, что в какой-то момент для некоторых контроллеров домена будет наблюдаться рассинхронизация. Кроме того, можно представить ситуацию, в которой два администратора домена одновременно занимаются редактированием групповых правил на разных контроллерах домена. Пока не завершится полная репликация, сведения о правилах на многих контроллерах также будут асинхронны.

По умолчанию редактирование выполняется на том контроллере, к которому подключена оснастка Group Policy. Обычно ее вызывает другая оснастка — Active Directory Users and Computers. Открывая ее, вы, как правило, не задумываетесь, к какому контроллеру она подключилась, так как это не принципиально. Это значит, что и оснастка Group Policy открывается на любом произвольном контроллере, и для двух одновременно работающих администраторов это скорее всего будут разные контроллеры.



Одновременное редактирование правил на разных контроллерах приведет к конфликту при репликации

Дабы исключить такую рассинхронизацию, можно заниматься редактированием только на контроллере, исполняющем функцию имитатора PDC. Это единственный контроллер, который можно указать для использования оснасткой в принудительном порядке.

Увы, этот выбор не всегда удачен. Пусть в какой-то момент контроллер оказался недоступен. Тогда вы не сможете создать или отредактировать политику. Предоставить постоянный доступ можно, выбрав функцию использования любого контроллера в домене, но это повысит риск рассинхронизации.

Словом, палка о двух концах. Что же выбрать? Ответ, как всегда, зависит от условий работы. Если редактированием политики может заниматься только один человек, то открывать консоль оснастки лучше всего на любом из контроллеров домена. Если нельзя исключить возможность одновременной работы двух администраторов, но вы знаете, что каналы связи надежны, то лучше редактировать все правила только на имитаторе PDC. А если этот компьютер все-таки может быть временно недоступен? Ну, во-первых, такую ситуацию нужно исключать на стадии проектирования Active Directory (см. главу «Проектируем Active Directory»). Во-вторых, если все спроектировано правильно, то не беда, что имитатор PDC недоступен из какого-либо одного сайта — он обязательно доступен из другого. Раз так, то минимум один администратор сможет работать с правилами.

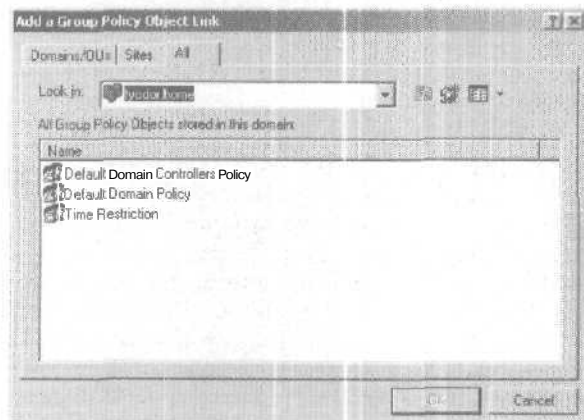
Есть еще одно мнение о месте создания и редактирования правил. Оно основано на том, что сами по себе ОГП не влияют на назначаемые правила, пока они не связаны с каким-либо контейнером или сайтом в Active Directory. Каждый ОГП может быть связан с несколькими контейнерами. А раз так, то где лучше хранить ОГП?

Обычно, создавая ОГП, вы его сразу же привязываете к некоторому объекту Active Directory. Причем выходит это автоматически: вы выбираете объект, открываете окно его свойств, выбираете вкладку Group Policy, нажимаете кнопку New и... и готово! Создается новая политика, связанная с выбранным объектом. Эта неочевидность шутит порой очень зло, когда вы указываете фильтрацию правил. Вы наивно полагаете, что указываемые права доступа относятся к политике применяемой к данному объекту, а реально это относится к ОГП в целом и, значит, влияет на все объекты, с которыми ОГП связан.

Потом вы можете связать ОГП с любым количеством объектов. А вот можно ли создать ОГП, который не был бы связан ни с одним контейнером в Active Directory? Да, и минимум — двумя способами.

Первый я бы назвал интуитивным. Вы создаете ОГП, связанный с некоторым объектом, а потом разрываете связь, Куда при этом денется

ОГП? Попадет в корневой контейнер всех ОГП. Вы можете просмотреть его содержимое, если вместо того, чтобы нажать кнопку New при создании новой политики, нажмете кнопку Add и в появившемся диалоговом окне щелкните вкладку All.



Перечень всех объектов групповых правил

Второй способ: вы сразу создаете ОГП в этом контейнере. Новый ОГП не будет связан ни с одним из объектов Active Directory. Корневой контейнер удобен в том плане, что вы всегда знаете, какие ОГП вы создали. Если же они разбросаны по доменам и ОП, вы потратите массу времени на поиски.

Делегирование полномочий

В крупной организации создание групповых правил централизовано. Это предполагает понимание каждым администратором того, что происходит в удаленном ОП. Так как на практике это неосуществимо, приходится прибегать к делегированию этих полномочий лицам, понимающим:

- зачем создавать групповые правила;
- ◆ как их создавать.

Работа с групповыми правилами включает три этапа: создание, связывание с объектами Active Directory и редактирование. Значит, лицо, ответственное за создание и поддержание групповых политик, должно иметь право выполнять эти три функции.

Простейший способ делегировать полномочия — включить учетную запись пользователя в группу, наделенную требуемыми полномочиями. Я уже говорил, что создавать групповые правила могут по умол-

чанию члены групп Administrators, Enterprise Admins, Domain Admins, Group Policy Creator Owners. Вот только возможности членов этих групп различны:

Сфера ответственности и разрешенные действия при работе с групповой политикой

Группа	Сфера ответственности	Разрешения
Enterprise Admins	Все сайты, домены, ОП в лесу	Создание, редактирование, удаление ОПГ и их привязка к объектам AD
Domain Admins	Домен и все ОП в нем	Создание, редактирование, удаление ОПГ и их привязка к домену и ОП; в корневом домене — привязка к сайтам
Administrators	Домен	Создание ОПГ Редактирование и удаление ОПГ, созданных членами этой группы; привязка к домену и ОП
Group Policy Creator Owners	Домен	Создание ОПГ Редактирование правил, созданных им самим (но не другими членами группы)

Все члены этих групп могут создавать ОПГ. Поэтому, включив пользователя в одну из них, вы достигнете желаемого результата. И не только, к сожалению: ведь эти группы имеют еще массу полномочий и разрешений, которых нельзя давать обычным пользователям!

Пожалуй, единственное исключение — группа Group Policy Creator Owners (GPCO). Она обладает только перечисленными полномочиями. Но их явно мало. Судите сами. Пусть пользователь А является членом группы GPCO. Он создал политику для своего ОП и хочет ее связать с ним. А этого права он-то и лишен! Это прерогатива членов групп Administrators или Domain Admins (членов Enterprise Admins мы вообще трогать не будем; их мало, и у них есть другие задачи). Следовательно, эти лица должны хотя бы посмотреть, что там сотворил пользователь А, и лишь затем привязать политику к ОП.

Допустим, в созданной политике они нашли кучу недочетов и решили, что ее должен исправить пользователь Б. тоже член GPCO. Увы! Члены GPCO могут редактировать только ОПГ, созданные ими самими. В этом легко убедиться, взглянув на список контроля доступа к ОПГ. В нем нет группы GPCO — лишь имя ее создателя.

Значит, делегирование полномочий по созданию и редактированию групповых правил через включение в группу GPCO не вполне удобно, и этому способу надо придумать замену.

Замечание Вообще-то такой регламент делегирования полномочий оправдан. Администратор домена не должен пускать процесс создания групповых правил на самотек. Но если вы уверены, что делегированные вами полномочия не будут использованы во вред, прислушайтесь к приведенным далее рекомендациям.

Делегирование прав на создание и модификацию ОГП

Давайте вспомним, что ОГП состоит из двух частей: контейнера групповой политики в Active Directory и каталога с номером GUID в каталоге SYSVOL. Как у контейнера, так и у каталога имеется свой список контроля доступа. Хотя полномочия доступа к объектам Active Directory и к каталогам файловой системы различны, суммарный эффект приводит к эквивалентным разрешениям. Ниже перечислены разрешения, применимые в этих списках контроля доступа, и эквивалентные им разрешения, относящиеся к групповой политике.

Разрешения, применяемые к контейнеру групповой политики и соответствующий им результат

Разрешение	Позволяет
Full Control	Просмотр, создание, редактирование и удаление ОГП
Read	Просмотр ОГП и его свойств в оснастке Group Policy
Write	Редактирование ОГП
Create all child objects	Создание и редактирование ОГП
Delete all child objects	Удаление ОГП

Разрешения, применяемые к каталогу шаблона групповой политики и соответствующий им результат

Разрешение	Позволяет
Full Control	Просмотр, создание, редактирование и удаление ОГП
Modify	Просмотр, создание, редактирование и удаление ОГП
Read & Execute	Просмотр ОГП
List folder contents	
Read	
Write	Просмотр, создание, редактирование и удаление ОГП

Как видите, можно создать группу и включить ее в списки контроля доступа как контейнера групповой политики, так и папки с шаблоном. При этом можно подобрать искомую комбинацию разрешений. Но делегирование прав на создание и модификацию ОГП — это только полдела. Надо уметь делегировать полномочия привязки ОГП к контейнерам в Active Directory.

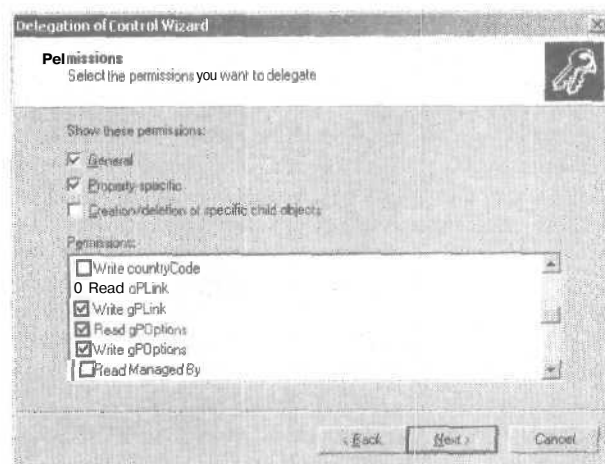
Делегирование полномочий на привязку ОГП к объектам Active Directory

Лицо, обладающее возможностью привязать ОГП к конкретному контейнеру в Active Directory, должно иметь права доступа к атрибутам этого контейнера. Какие же это атрибуты?

Во-первых, *gpLink*. Именно он содержит информацию обо всех ОГП, связанных с данным объектом. Чтобы выполнять связывание, пользователь должен обладать правами *Read* и *Write* на этот атрибут.

Во-вторых, как мы уже знаем, привязка ОГП к ОП может сопровождаться блокированием наследования правил от вышестоящих контейнеров. За это отвечает атрибут *gpOptions*. Как и в предыдущем случае пользователь должен иметь разрешения *Read* и *Write* для этого атрибута.

Изменить разрешения можно разными инструментами. Самый простой — мастер делегирования полномочий. Еще один — редактор списка контроля доступа в оснастке Active Directory Users and Computers. Ну и, наконец, это ADSIEdit и Ldp.



Делегирование возможности привязки ОГП к контейнеру в мастере делегирования

Типы правил

В начале этой главы я перечислял основные типы правил:

- * Software settings (Установки программного обеспечения);
- Windows Settings (Установки Windows);
- ◆ Administrative Templates (Административные шаблоны).

Каждый тип включает в себя несколько категорий правил, которые теперь мы и рассмотрим. Мы начнем с наборов правил для компьютеров и рассмотрим их в том порядке, в каком они представлены в оснастке Group Policy.

Правила установки ПО для компьютеров

Правила установки ПО описывают, как программы должны устанавливаться на компьютер. При этом предполагается, что любое приложение использует для установки Microsoft Installer. Этот компонент ОС берет в качестве исходных MSI-файлы — их называют пакетами установки. Пакет содержит список файлов и каталогов приложения, а также другую контрольную информацию. Обычно пакет поставляется вместе с приложением. Скажем, для Microsoft Office, кроме файла установки setup.exe, поставляются два MSI-файла: data1 и msowc. Первый является пакетом для установки офисного пакета целиком, второй — только для установки его компонентов для Web.

В групповых правилах установки описано, как именно должен быть установлен выбранный пакет.

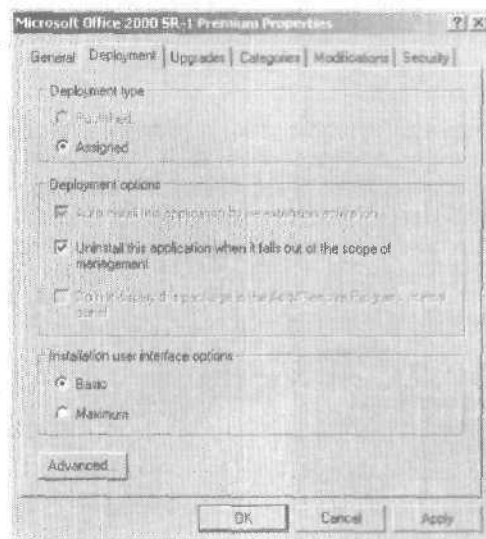
В первую очередь указывается местоположение пакета. Это можно сделать только раз — при создании правила. Путь к пакету указывается в виде пути UNC. При этом нужно позаботиться о том, чтобы файлы были доступны. Часто администратор считает, что раз он имеет доступ к исходным файлам, то и во время установки доступ к ним также будет возможен. Обычно это справедливо, поскольку дистрибутивные файлы располагаются на серверах — членах домена. Однако если они хранятся на отдельно стоящем сервере или на сервере — члене того домена, с которым нет доверительных отношений, данный вариант не пройдет. Дело в том, что доступ к файлам будет выполняться от имени учетной записи компьютера, а не администратора.

Далее нужно решить, как будет установлено приложение. В правилах для компьютеров выбор не богат: приложение может быть либо назначено, либо вы можете описать дополнительные параметры назначения. Эти правила не позволяют публиковать приложения. Описывать дополнительные параметры не обязательно. Можно использовать значения по умолчанию, но тогда пакет будет установлен также по умолчанию, например, со всеми дополнительными функциями, которые, вероятно, нужны не всем.

Выбрав редактирование, вы можете указать следующее.

- ◆ Как поступить с приложением, когда компьютер выйдет из зоны действия политики. Например, политика определена для ОП *Маркетинг*, в котором находится компьютер W2KIVANOV. Компьютер

перемещается в ОП *Продажи*. Что делать с приложением? Удалить или оставить?

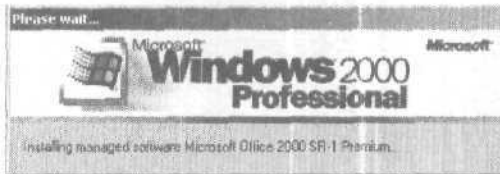


Правила установочного пакета

- Сколь велико участие пользователя в процессе установки? Должен ли он отвечать на вопросы программы установки или его участие минимально?
- ◆ Что делать, если приложение уже установлено на компьютере самим пользователем или **иными** средствами? Его можно удалить или выполнить повторную установку.
- Если приложение поддерживает несколько языковых интерфейсов, то надо ли выбирать интерфейс в зависимости от региональных параметров компьютера или можно их проигнорировать?
- Если этот пакет является обновлением для установленного ранее, можно указать, для какого именно. Это важно в компаниях, использующих приложения собственной разработки. Новые версии программ будут централизованно заменять старые.
- Для пакетов Microsoft Installer допускается применение файлов-модификаторов, или трансформеров. **Трансформеры** имеют расширение **MST** и описывают изменения в параметрах пакета, которые должны быть применены. Например, устанавливая офисные приложения на терминальный сервер, без трансформера не обойтись.

- Наконец, можно указать права доступа к данному пакету. Обратите внимание на разницу между правами доступа к ОГП и к установочному пакету. Внутри одной политики может быть задано сразу несколько установочных правил, Разграничение доступа к ним позволяет назначать разные приложения разным группам пользователей в рамках одной политики.

После того как политика установки приложения определена и связана с контейнером Active Directory, любому компьютеру, чья учетная запись хранится в этом контейнере, будет назначена установка приложения. При следующей загрузке компьютера появится сообщение, аналогичное показанному на рисунке. Если приложение крупное, возникнет довольно длительная пауза.



Установка приложения, определенного в групповой политике во время загрузки компьютера

Вот основные характеристики приложений, заданных в правилах установки для компьютера:

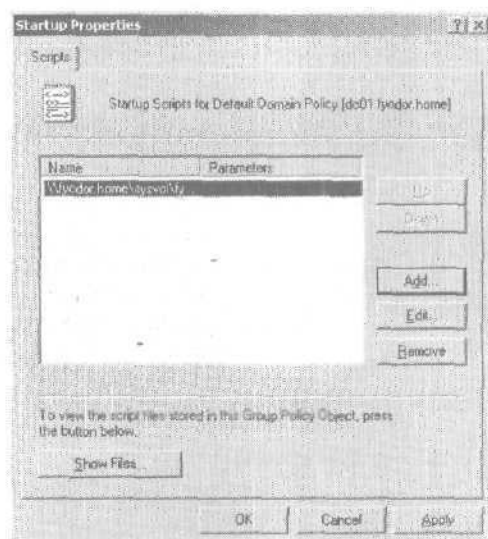
- приложение устанавливается во время загрузки компьютера;
- ◆ приложение доступно любому пользователю компьютера;
- + приложение может удалить пользователь, имеющий нужные полномочия, но оно будет восстановлено при следующей загрузке.

Удалить правило установки пакета можно с удалением приложений с компьютеров, входящих в область действия политики, и без удаления. Какой способ выбрать, решает администратор.

Установки Windows для компьютеров — сценарии

Сценарии, указываемые в групповой политике для компьютеров, — это командные файлы или файлы Windows Scripting Host, исполняемые на этапе загрузки или выключения компьютера. Как я уже говорил, они хранятся в каталоге `Sysvol\имя_домена\Policies\{GUID политики}\Machine\Scripts` в подкаталогах Startup и Shutdown.

То, что они исполняются на столь ранней стадии работы компьютера (или на столь поздней), подразумевает, что эти сценарии не должны взаимодействовать с пользователем. Любые команды, требующие реакции пользователя (вплоть до простого нажатия клавиши) недопустимы, так как вызовут «зависание» компьютера,



Определение списка сценариев, исполняемых при загрузке компьютера

Если же взаимодействие на данном этапе необходимо, разрешить его можно через правила в административных шаблонах:

Правила выполнения сценариев

Наименование правила	Описание
Run logon scripts synchronously	Синхронное исполнение сценариев регистрации
Run startup scripts asynchronously	Асинхронное исполнение сценариев загрузки
Run startup scripts visible	Видимое для пользователя исполнение сценариев загрузки
Run shutdown scripts visible	Видимое для пользователя исполнение сценариев выключения системы
Maximum wait time for Group Policy scripts	Максимальное время ожидания исполнения сценариев групповой политики

Возможно, вы привыкли к тому, что файлы сценариев должны храниться в каталоге `Sysvol\имя.домена\Scripts`. Вы можете поместить файлы туда, но никакой выгоды от этого не получите. В любом случае вы включаете файлы сценариев в ОГП.

Параметры Windows для компьютеров: правила безопасности

Безопасность — один из важнейших аспектов правил. Политики безопасности распространяются как на отдельные компьютеры и пра-

вила доступа к ним, так и на взаимодействие компьютеров в системе. Правила безопасности для компьютеров делятся на следующие группы:

- ◆ правила учетных записей;
 - локальные правила;
- ◆ правила журнала регистрации;
- ◆ правила групп с ограниченным членством;
- ◆ правила системных служб;
 - правила реестра;
 - правила файловой системы;
- ◆ правила открытых ключей;
 - правила IPSecurity.

Правила учетных записей

Правила учетных записей состоят из трех групп:

- правил паролей;
- правил блокировок учетных записей;
- правил Kerberos.

Действие правил учетных записей распространяется на весь домен. Нельзя создать отдельные правила для сайта или ОП. Вот правила паролей и их краткое описание (подробнее о правилах, устанавливаемых в системах разной степени защищенности см. [1]).

Правила паролей

Наименование правила	Описание
Store passwords under reversible encryption for all users in domain	Равносильно разрешению хранения паролей в открытом (не зашифрованном) виде. Представляет серьезную угрозу для безопасности системы. Требуется для обеспечения сквозной аутентификации в гетерогенных системах
Enforce password history	Позволяет хранить историю паролей. Пока не будет использовано указанное число паролей, невозможно задействовать ни один из них. Эффективно при обязательной смене паролей через определенный интервал и запрете смены пароля в течение другого интервала
Maximum password age.	Максимальный срок, по истечении которого пароль должен быть изменен. Правила паролей позволяют установить срок действия пароля в пределах от 1 до 999 дней или сделать его постоянным
Minimum password age	Параметр, ограничивающий минимальное время, через которое пользователь может изменять свой пароль: от 1 до 999 дней

см. след. стр.

Наименование правила	Описание
Minimum password length	Минимальная разрешенная длина пароля
Passwords must meet complexity requirements	Если определено данное правило, пароли должны отвечать критерию сложности. Система следит за тем, чтобы пароль содержал минимум три из перечисленных ниже типа символов: прописные буквы латинского алфавита; строчные буквы латинского алфавита; цифры; специальные символы
User must logon to change password,	Подразумевает обязательность для пользователя регистрироваться в системе, с тем чтобы сменить пароль

Правил блокировки учетных записей всего три. Они позволяют обезопасить систему от «словарных атак» — программ взлома системы защиты, выполняющих подбор пароля путем перебора наиболее часто используемых слов и фраз из своего словаря.

Правила блокировки учетных записей

Наименование правила	Описание
Account lockout threshold	Устанавливает количество неудачных попыток зарегистрироваться в системе после достижения которого учетная запись будет заблокирована
Account locout duration	Устанавливает срок блокировки в минутах
Reset lockout count after	Сбрасывает отсчет неверных попыток входа в систему по истечении определенного времени

Правила Kerberos устанавливают основные параметры протокола Kerberos (о Kerberos см. [1], [3]).

Правила Kerberos

Наименование правила	Описание
Maximum lifetime for user ticket	Максимальное время жизни билета TGT. Устанавливается в часах. По умолчанию — 10 часов
Maximum lifetime for service ticket	Максимальное время жизни сеансового билета. Устанавливается в минутах. Это время должно быть больше 10 минут, но меньше, чем максимальное время жизни билета TGT
Maximum lifetime for user ticket renewal	Максимальный срок, в течение которого билет может обновляться. Устанавливается в днях. По умолчанию — 7 дней
Maximum tolerance for computer clock synchronization	Максимально допустимый разброс в показаниях часов компьютеров. Устанавливается в минутах, По умолчанию — 5 минут

см. след. стр.

Наименование правила	Описание
Enforce user logon restrictions	Когда установлен этот параметр (Enabled), KDC, выдавая сеансовый билет, проверяет, имеет ли право клиент, запросивший билет, регистрироваться локально или по сети на том компьютере, доступ к которому запрашивается. Этот параметр установлен по умолчанию, хотя и замедляет работу, так как требует выполнения нескольких дополнительных шагов

Локальные правила

Локальные правила также состоят из трех групп правил:

- правила аудита;
- назначения прав пользователей;
- параметры безопасности

Правилами аудита предписывается заносить в журнал события, относящиеся к категории безопасности. Поэтому записи о них будут появляться в журнале Security. Возможна регистрация как удачных, так и неудачных событий.

Правила аудита

Наименование правила	Описание
Audit Account Logon events	Аудит событий регистрации учетной записи. События происходят при обращении одного компьютера к другому
Audit Account Management	Аудит управления учетными записями. Всякий раз при изменении атрибутов учетных записей в журнал заносится запись
Audit Directory Service Access	Аудит доступа к службе каталогов
Audit Logon Events	Аудит событий регистрации пользователей.
Audit Object Access	Аудит доступа к объектам файловой системы или реестра
Audit Policy Change	Аудит изменения групповых правил
Audit Privilege Use	Аудит использования привилегий
Audit Process Tracking	Аудит отслеживания процессов. Не рекомендуется применять в рабочих системах, так как заметно снижает производительность. Требуется только при отладке приложений
Audit System Events	Аудит системных событий

Права пользователей в системе имеют большое значение для ее безопасности. Ряд прав нужно применять только на контроллерах доменов, ряд — на серверах. Некоторые права действуют при делегировании полномочий. Поскольку детальное описание каждого права выходит за рамки книги, я их просто перечислю.

Права пользователей

Наименование правила	Описание
Access this computer from the network	Доступ к компьютеру по сети. По умолчанию определен для всех компьютеров
Act as part of the operating system	Позволяет действовать как части ОС. Требуется для учетных записей, от имени которых работают разные службы
Add workstations to domain	Позволяет добавлять рабочие станции в домен. По умолчанию любой пользователь может добавить до 10 рабочих станций в домен
Back up files and directories	Позволяет выполнять резервное копирование файлов и каталогов на данном компьютере
Bypass traverse checking	Позволяет при наличии разрешений иметь доступ к тем дочерним каталогам, у которых доступ к родительским закрыт
Change the system time	Позволяет изменять системное время. На контроллерах доменов можно только изменить временную зону, так как время все равно будет установлено по серверу точного времени
Create a pagefile	Позволяет создавать файл подкачки
Create a token object	Позволяет создавать объект-жетон. По умолчанию не дано никому
Create permanent shared objects	Позволяет создавать объекты, предоставленные в постоянное совместное использование
Debug programs	Позволяет отлаживать программы
Deny access to this computer from the network	Запрещает доступ к компьютеру по сети
Deny logon as a batch job	Запрещает регистрацию в качестве пакетного задания
Deny logon as a service	Запрещает регистрироваться в качестве службы. Целесообразно назначать для учетных записей администраторов, дабы предотвратить использование их учетных записей в побочных целях
Deny logon locally	Запрещает регистрироваться локально
Enable computer and user accounts to be trusted for delegation	Разрешает применять учетные записи пользователей и компьютеров для делегирования. Позволяет осуществлять доступ других учетных записей к иным системам от имени указанных учетных записей
Force shutdown from a remote system	Разрешает выключать компьютер удаленно
Generate security audits	Позволяет генерировать аудит безопасности
Increase quotas	Позволяет увеличивать квоты
Increase scheduling priority	Позволяет повышать приоритет процессов
Load and unload device drivers	Позволяет устанавливать и изымать драйверы устройств

см. след. стр.

Наименование правила	Описание
Lock pages in memory	Позволяет записывать страницы в памяти
Log on as a batch job	Позволяет регистрироваться в качестве пакетного задания
Log on as a service	Позволяет регистрироваться в виде службы. Обязательно для учетных записей всех служб.
Log on locally	Позволяет регистрироваться локально
Manage auditing and security log	Позволяет управлять журналом аудита и безопасности
Modify firmware environment values	Позволяет изменять параметры окружения firmware. Для платформы Intel не актуально
Profile single process	Позволяет профилировать процесс
Profile system performance	Позволяет профилировать производительность системы
Remove computer from docking station	Позволяет извлекать компьютер из «дока». Странное разрешение: выключенный компьютер все равно можно извлечь
Replace a process level token	Позволяет заменять жетон уровня процесса
Restore files and directories	Позволяет восстанавливать файлы и каталоги
Shut down the system	Позволяет выключать систему
Synchronize directory service data	Позволяет выполнять синхронизацию данных службы каталогов
Take ownership of files or other objects	Позволяет вступать во владение объектами

Параметры безопасности определяют дополнительные характеристики, определяющие поведение системы. Можно сказать, что умолчания, определенные в системе, соответствуют необходимому уровню безопасности. Изменять данные правила требуется только при повышении уровня защиты.

Параметры безопасности

Наименование правила	Описание
Additional restrictions for anonymous connections	Дополнительные ограничения для анонимных подключений
Allow server operators to schedule tasks (domain controllers only)	Разрешение членам группы Server Operators планировать задания на контроллерах доменов
Allow system to be shut down without having to log on	Разрешение выключать систему без предварительной регистрации в пей. По умолчанию запрещено
Allowed to eject removable NTFS media	Разрешение извлекать носители данных, отформатированные в NTFS
Amount of idle time required before disconnecting session	Время простоя системы, после которого сеанс отключается

см. след. стр.

Наименование правила	Описание
Audit the access of global system objects	Аудит доступа к глобальным системным объектам
Audit use of Backup and Restore privilege	Аудит использования привилегий резервного копирования и восстановления
Automatically log off users when logon time expires	Автоматическое отключение пользователей от домена по истечении времени работы
Automatically log off users when logon time expires (local)	Автоматическое отключение пользователей от локальной станции при истечении времени работы. По умолчанию запрещено. Для клиентов Windows XP в домене Windows 2000 это правило не работает. Требуется установка SP1 для Windows XP
Clear virtual memory pagefile when system shuts down	Предписание очищать содержимое файла подкачки при выключении системы
Digitally sign client communication (always)	Обязательная цифровая подпись обмена с клиентом
Digitally sign client communication (when possible)	Необязательная цифровая подпись обмена с клиентом
Digitally sign server communication (always)	Обязательная цифровая подпись обмена с сервером
Digitally sign server communication (when possible)	Необязательная цифровая подпись обмена с сервером
Disable CTRL+ALT+DEL requirement for logon	Запрещение ввода CTRL+ALT+DEL для входа в систему. Рекомендуется применять на общедоступных системах типа киосков
Do not display last user name in logon screen	Запрещение отображения имени последнего пользователя, зарегистрировавшегося в системе
LAN Manager Authentication Level	Устанавливает уровень аутентификации LAN Manager. Не рекомендуется применять уровни ниже NTLM в системах с клиентами Windows 9x и ниже NTLM v.2 в системах с Windows NT-клиентами
Message text for users attempting to log on	Текст сообщения для пользователей, регистрирующихся в системе
Message title for users attempting to log on	Заголовок для окна сообщения, описанного выше
Number of previous logons to cache (in case domain controller is not available)	Количество успешных регистраций на клиенте в отсутствие контроллера домена. Максимальное значение — 50
Prevent system maintenance of computer account password	Запрещает изменение пароля компьютера каждые 7 дней. В противном случае пароль компьютера меняется еженедельно
Prevent users from installing printer drivers	Запрещает членам группы Users устанавливать драйверы принтеров
Prompt user to change password before expiration	Определяет, за сколько дней до истечения пароля пользователи будут предупреждаться о необходимости сменить пароль

см. след. стр.

Наименование правила	Описание
Recovery Console: Allow automatic administrative logon	Разрешает автоматический вход администратора в консоль восстановления
Recovery Console: Allow floppy copy and access to all drives and all folders	Разрешает применять в параметрах окружения консоли восстановления команды: <code>AllowWildCards</code> — использование символов подстановки в командах; <code>AllowAllPaths</code> — использование всех файлов и каталогов; <code>AllowRemovableMedia</code> — копировать файлы на съемные носители такие, как дискеты; <code>NoCopyPrompt</code> — не предупреждать при переписывании файла
Rename administrator account	По умолчанию эти возможности запрещены
Rename guest account	Новое имя учетной записи Administrator
Restrict CD-ROM access to locally logged-on user only	Новое имя учетной записи Guest
	Определяет доступ к накопителю на CD. Если установлено, доступ к CD имеют только локально зарегистрировавшиеся пользователи. Если локальных пользователей нет, доступ к CD возможен по сети. Если не установлено, доступ к CD могут иметь как локальные, так и сетевые пользователи
Restrict floppy access to locally logged-on user only	Определяет доступ к дисководу. Если установлено, доступ к дисководу имеют только локально зарегистрировавшиеся пользователи. Если локальных пользователей нет, доступ к дисководу возможен по сети. Если не установлено, доступ к дисководу могут иметь как локальные, так и сетевые пользователи
Secure channel: Digitally encrypt or sign secure channel data (always)	Если определено это правило, то взаимодействие с контроллерами доменов использует шифрование и цифровую подпись для всех передаваемых данных. При этом автоматически активизируется следующее правило
Secure channel: Digitally encrypt secure channel data (when possible)	Если установлено, взаимодействие с контроллерами доменов может использовать шифрование для всех передаваемых данных
Secure channel: Digitally sign secure channel data (when possible)	Если установлено, взаимодействие с контроллерами доменов может использовать цифровую подпись для всех передаваемых данных
Secure channel: Require strong (Windows 2000 or later) session key	Если установлено, используются криптоустойчивые ключи (Windows 2000 или позже). В противном случае длина ключа определяется в ходе переговоров с контроллером домена

см. след. стр.

Наименование правила	Описание
Secure system partition (for RISC platforms only)	Защита системного раздела для RISC-платформ
Send unencrypted password to connect to third-party SMB servers	Это правило используется для взаимодействия с SMB-серверами сторонних фирм, например SAMBA
Shut down system immediately if unable to log security audits	Если установлено, система останавливается при переполнении журнала безопасности
Smart card removal behavior	Устанавливает последовательность действий при вынимании смарт-карты или электронного брелока. Доступно три варианта: No Action — ничего не предпринимать; Lock Workstation — запретить рабочую станцию; Force Logoff — инициировать выход из системы
Strengthen default permissions of global system objects (e.g. Symbolic Links)	Если установлено, обычные пользователи могут иметь доступ к системным объектам (устройствам DOS, мьютексам и семафорам) только на чтение. В противном случае они могут их создавать и модифицировать
Unsigned driver installation behavior	Предписывает, как реагировать на установку драйвера устройств, не имеющего цифровой подписи. Возможны три варианта: Silently succeed — установить без предупреждения; Warn but allow installation — предупредить, но разрешить установку; Do not allow installation — не разрешать установку
Unsigned non-driver installation behavior	То же самое, что и выше, но для установки не-драйверов, например для COM-объектов

Правила журнала регистрации

Правила журнала регистрации определяют максимальные объемы журналов и способы отслеживания их переполнения. По умолчанию для рабочих станций и серверов задаются одинаковые правила. Для контроллеров доменов существует одно отличие — на них запрещается выключать систему при переполнении журнала.

Объемы журналов безопасности и приложений во многом определяются правилами аудита и установленными приложениями. Если информация в журнале вам интересна, позаботьтесь о том, чтобы она была доступна. С одной стороны, этого можно добиться увеличением размера журнала, с другой — определением правил обновления ин-

формации в журнале. Максимальный объем журнала — 4 Гб. Обновление информации может выполняться тремя способами:

- при заполнении журнала новая информация будет заноситься в его начало и переписывать существующую;
- ◆ информация будет заноситься в начало журнала по истечении определенного срока; максимально можно задать 365 дней;
- старую информацию администратор должен удалять вручную.

Правила журналов регистрации

Наименование правила	Описание
Maximum Log size for Application Log	Максимальный объем журнала приложений, по умолчанию — 512 кб
Maximum Log Size for Security Log	Максимальный объем журнала безопасности, по умолчанию — 512 кб
Maximum Log Size for System Log	Максимальный объем системного журнала, по умолчанию — 512 кб
Restrict Guest access to Application Log	Ограничить доступ гостей к журналу приложений
Restrict Guest access to Security Log	Ограничить доступ гостей к журналу безопасности
Restrict Guest access to System Log	Ограничить доступ гостей к системному журналу
Retain Application Log for	Срок, по истечении которого журнал приложений будет обновлен
Retain Security Log for	Срок, по истечении которого журнал безопасности будет обновлен
Retain System Log for	Срок, по истечении которого системный журнал будет обновлен
Retention method for Application Log	Метод обновления журнала приложений
Retention method for Security Log	Метод обновления журнала безопасности
Retention method for System Log	Метод обновления системного журнала
Shutdown system when security audit log is full	Выключать систему при переполнении журнала безопасности

Параметры Windows для компьютеров: правила групп с ограниченным членством

Правила для групп с ограниченным членством устанавливают:

- имена таких групп;
- имена учетных записей, включенных в эти группы;
- имена групп, в которые можно включать группы с ограниченным членством; это правило относится к именам локальных групп на рабочих станциях и серверах.

Эти правила особенно важны для корневого домена в лесу. Если для группы Enterprise Admins указать, кто именно может входить в эту группу, то остальные администраторы не смогут себя включить в эту «супергруппу».

Замечание Включить-то учетную запись в группу с ограниченным членством можно, но она будет выброшена оттуда при следующем применении правил.

Довольно часто администратор задает *перечень* групп с ограниченным членством, забывая указать членов этих групп. Как только политика применяется, содержимое указанных групп обнуляется. Особенно забавно видеть учетную запись, еще недавно бывшую в группе Enterprise Admins, ставшую теперь рядовым пользователем.

Параметры Windows для компьютеров: правила системных служб

Правилами системных служб устанавливаются тип запуска службы и права доступа к ней. Обычно тип запуска каждой службы задается в оснастке Computer Management Services. Однако в целях безопасности системы для некоторых служб устанавливаются правила, которые нельзя обойти. Существует три вида запуска служб:

- ◆ Automatic (Автоматический);
- Manual (Ручной);
- Disabled (Деактивизирована)

Помимо этого правила, указывают, кто конкретно может осуществлять доступ к службам и к какой именно. Основные виды доступа;

- Full control (Полный контроль);
- ◆ Read (Чтение информации о конфигурации);
- ◆ Start, Stop and Pause (Запуск, остановка и приостановка);
- Write (Запись информации о конфигурации);
- Delete (Удаление)

Параметры Windows для компьютеров: правила реестра

Правила реестра регламентируют разрешения доступа к ветвям реестра. Можно указать один из вариантов применения правил:

- Inherit (Наследовать) — применяются как к указанной ветви, так и ко всем дочерним при условии, что для них не установлена блокировка наследования;

- ◆ **Overwrite (Переписать)** — применяются как к указанной ветви, так и ко всем дочерним **независимо** от того, установлена для них блокировка наследования или нет;
- ◆ **Ignore (Игнорировать)** — данная ветвь и все дочерние в правилах игнорируются.

Правила, устанавливаемые по умолчанию, существенно различны для рабочих станций, серверов и контроллеров домена.

Параметры Windows для компьютеров: правила файловой системы

Правилами файловой системы регламентируются разрешения доступа к отдельным файлам и каталогам, установки аудита доступа к ним, а также владельцы файлов. Как и в правилах **реестра**, можно указать один из вариантов:

- ◆ **Inherit (Наследовать)** — применяются как к указанному объекту, так и ко всем дочерним, если для них не установлена **блокировка наследования**.
- **Overwrite (Переписать)** — применяются как к указанному объекту, так и ко всем дочерним **независимо от того**, установлена для них блокировка наследования или нет.
- **Ignore (Игнорировать)** — данный объект и все дочерние в правилах игнорируются.

Параметры Windows для компьютеров: правила открытых ключей

Правила открытых ключей охватывают такую область, как работу с сертификатами (подробнее об этом см. [3]):

Правила открытых ключей для компьютеров

Правило	Описание
Automatic Certificate Request Settings	Позволяет автоматически выдавать и обновлять сертификаты всем компьютерам, которые входят в область действия данной политики, а также указывает , какой удостоверяющий центр и какой шаблон сертификатов использовать. Работает при наличии минимум одного удостоверяющего центра предприятия
Trusted Root Certification Authorities	Позволяет указать, какой удостоверяющий центр является доверенным для всех компьютеров, на которые распространяется действие данной политики. Это может быть как удостоверяющий центр предприятия, так и любой сторонний удостоверяющий центр. Для создания правила нужно лишь импортировать сертификат удостоверяющего центра

см. след. стр.

Правило	Описание
Enterprise Trust	Позволяет создать списки доверенных сертификатов для того, чтобы определить, какие сертификаты и для таких целей могут использоваться
Encrypted Data Recovery Agents	Позволяет назначать агентов восстановления EFS. По умолчанию агентом восстановления является локальный администратор первого контроллера домена. Так как это чаще всего недопустимо, требуется выбрать агента из пользователей, имеющих соответствующий сертификат

Параметры Windows для компьютеров: правила IPSecurity

Правила IPSecurity конфигурируют, если требуется защищенное взаимодействие с или между серверами или контроллерами доменов. В главе «Планирование Active Directory», например, разбирается случай использования IPSecurity для организации репликации через межсетевой экран. При этом два контроллера, расположенные по разные стороны экрана, общаются только с применением шифрования. С другой стороны, они должны взаимодействовать с другими контроллерами в своем сайте, а те — должны обслуживать запросы на авторизацию, поступающие от обычных клиентов.

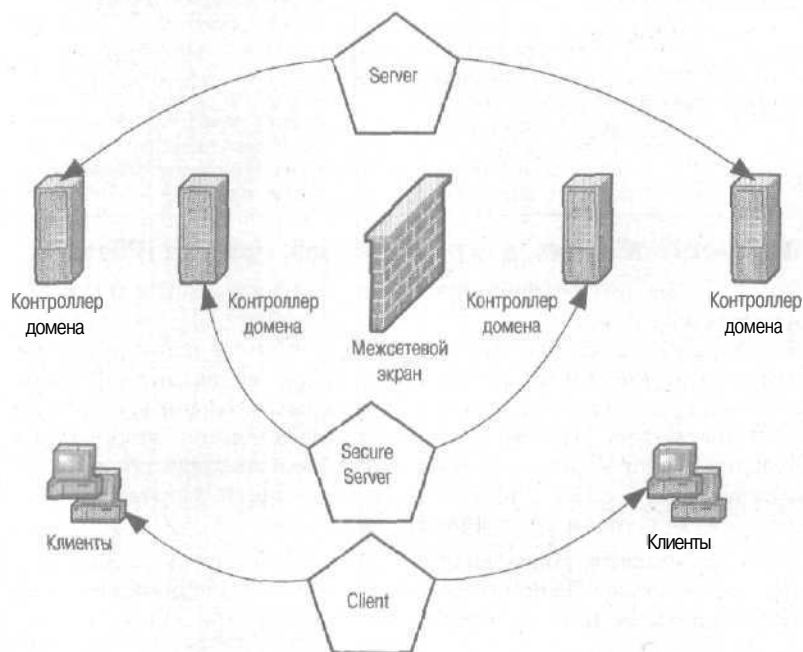
Способов конфигурирования правил IPsec множество, но для простоты можно применить те правила, что уже сконфигурированы, но не активизированы. Вот эти правила:

Правила IPSecurity

Наименование правила	Описание
Secure server (require security)	Подразумевает, что взаимодействие с данным сервером осуществляется только с использованием IPsec
Server (Request security)	Настраивает протокол взаимодействия так, что сервер сначала пытается установить взаимодействие по IPsec, но если клиент не может ответить, то устанавливается открытое взаимодействие
Client (Respond only)	Подразумевает отсутствие шифрования по умолчанию. Если сервер запрашивает защищенное соединение по какому-либо порту или протоколу, шифруется только требуемое

Думаю, вполне очевидно, что в нашем примере к контроллерам домена, взаимодействующим через межсетевой экран, должно быть применено правило Secure Server. К остальным же контроллерам — Server, так как они могут выступать и клиентами и серверами при репликации. Правило, применяемое к клиентам, — Client, что позво-

лит им авторизоваться на всех контроллерах домена в своем сайте, включая защищенные.



Использование стандартных правил IPSec для организации репликации через межсетевой экран

Административные шаблоны для компьютеров

Это файлы с расширением .ADM, в которых в текстовом виде записаны установки, модифицирующие реестр компьютера, к которому применяется групповая политика. Новые параметры для компьютеров заносятся в ветвь реестра `HKEY_LOCAL_MACHINE`.

Перечислять все параметры бесполезно — лучше показать, как их применяют, на конкретных примерах, что я и сделаю чуть позже. Здесь же я приведу лишь базовые параметры, доступные для конфигурирования по умолчанию.

Внимание Перечисленные административные шаблоны появляются в Windows 2000, только если:

- установлен пакет обновления SP2 или выше;
 - ◆ установлены все последние заплатки для системы безопасности;
 - в домене есть клиенты Windows XP.
-

Административные шаблоны для компьютеров

Наименование правила	Описание
<i>Компоненты Windows</i>	
Net Meeting	Позволяет запрещать предоставление удаленного рабочего стола в совместное использование
Internet Explorer	Позволяет определять зоны безопасности, указывать параметры прокси-сервера для компьютера в целом, управлять обновлением Internet Explorer
Task Scheduler	Позволяет управлять утилитой запуска приложений по расписанию
Terminal Services	Полностью управляет настройкой терминальных серверов. Настраиваются практически все параметры реестра, ответственные за конфигурацию терминальных служб. (Подробнее см. [1])
Windows Installer	Устанавливает такие параметры Windows Installer, как учетная запись, от имени которой он работает, параметры интерфейса, разрешение использования из административного терминального сеанса и пр.
Windows Messenger	Запрещает/разрешает использование Windows Messenger
<i>Системные компоненты</i>	
User profiles	Определяет работу с блуждающими профилями пользователей: кэширование, работа на медленных каналах, распространение на серверы и т. п.
Scripts	Управляет исполнением сценариев загрузки, регистрации и выключения системы. Позволяет исполнять сценарии включения системы в режиме, видимом для пользователя. Устанавливает синхронный или асинхронный режим исполнения сценариев
Logon	Управляет поведением системы при регистрации пользователей. Позволяет выбрать вид программы регистрации для клиентов Windows XF, запретить выводить предупреждения и выполнение программ из списка однократного исполнения, исполнять специфические приложения
Disk Quotas	Конфигурирует параметры квотирования дискового пространства, управляет регистрацией событий квотирования
Net Logon	Управляет параметрами службы NetLogon. Применимо, в основном, только для серверов Windows .Net Server
Group Policy	Правила обработки групповой политики (см. ранее)
Remote Assistance	Управляет режимом удаленной помощи на компьютерах с Windows XP
System Restore	Запрещает использовать функцию восстановления системы в случае сбоя на компьютерах с Windows XP

см. след. стр.

Наименование правила	Описание
Error Reporting	Управляет функцией сообщения об ошибках в Windows XP
Windows File Protection	Управляет подсистемой защиты системных файлов. Указывает расположение кэша файлов, ограничивает его размер, управляет сканированием
Remote Procedure Call	Управляет параметрами поиска проблем в механизме RPC. Применяется для клиентов Windows XP
Windows Time Service	Управляет параметрами службы времени в Windows .Net Server
<i>Сетевые компоненты</i>	
DNS client	Управляет параметрами клиента DNS. Делает то, что не может сделать сервер DHCP: определяет имена серверов DNS, первичный суффикс, перечень и последовательность вторичных суффиксов, времена жизни, параметры безопасности. Применяется для клиентов Windows XP. Первичный суффикс можно определять и для клиентов Windows 2000
Offline files	Управление параметрами автономных папок; разрешение использования, размер кэша, предупреждения на экране, назначение. Для клиентов Windows XP дополнительно определяет параметры безопасности
Network connections	Для клиентов Windows 2000 запрещает предоставление соединения с Интернетом в совместное использование. Для клиентов Windows XP добавляются запреты использовать межсетевой экран на таких соединениях и конфигурировать мосты в сети DNS, а также устанавливает имя удостоверяющего центра для беспроводных сетей
QoS Packet Scheduler	Управляет параметрами качества обслуживания. Только для клиентов Windows XP
SNMP	Определяет сообщества, ловушки для сообщества Public, менеджеров. Недоступен в чистой сети Windows 2000
Принтеры	Управляет публикацией принтеров в Active Directory, установкой принтерных драйверов, просмотром списка принтеров, печатью через Web и другими параметрами, часть которых доступна только для клиентов Windows XP

Так как файлы административных шаблонов являются обычными текстовыми файлами, то их можно модифицировать для управления дополнительными элементами (см. об этом [1]).

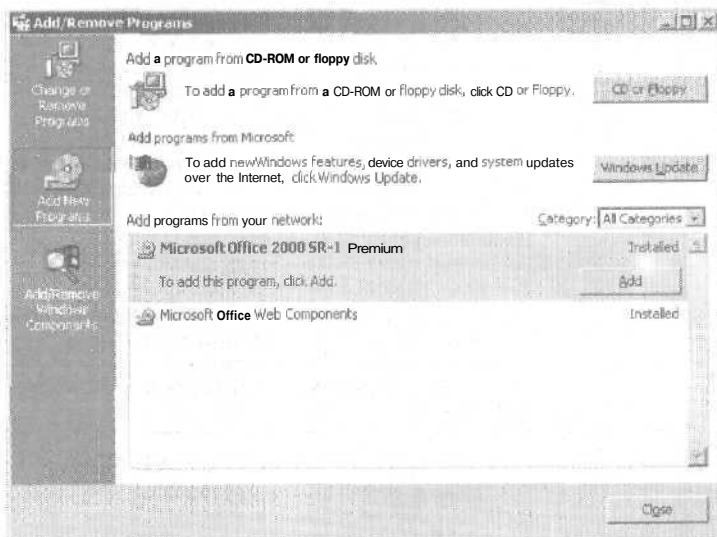
Правила установки ПО для пользователей

Эти правила описывают, как ПО должно устанавливаться на компьютер при регистрации пользователя.

В групповых правилах установки описывается, как именно должен быть установлен выбранный пакет. Они во многом схожи с правилами для компьютеров, но есть и отличия.

- ◆ Указывая местоположение пакета, помните, что доступ к файлам будет выполняться от имени учетной записи пользователя.
- Приложение может быть не только назначено, но и опубликовано в Active Directory. Это значит, что такое приложение не будет сразу установлено, а объявление о нем будет размещено в панели управления в разделе Установка приложений. Это право пользователя установить такое приложение, или отвергнуть его.
- Даже назначенное приложение не устанавливается полностью. Вместо этого в системе будут зарегистрированы COM-объекты, ассоциации с расширениями файлов и созданы необходимые пункты меню. Реальная установка будет выполнена, только когда пользователь выберет соответствующий пункт в меню или щелкнет документ, ассоциированный с данным приложением.

После того как политика установки приложения определена и связана с контейнером Active Directory, для любых пользователей, чьи учетные записи располагаются в этом контейнере, приложение будет опубликовано или будет назначена установка приложения.



Опубликованные приложения доступны для установки пользователем

Таким образом, основными характеристиками приложений, определенных в правилах установки для пользователей, являются:

- ◆ приложение устанавливается при регистрации пользователя;
- ◆ приложение доступно только для тех пользователей, на которых распространяется действие политики;
- приложение может быть удалено пользователем, имеющим на то полномочия, но оно будет восстановлено при следующей попытке запуска его пользователем или при следующей регистрации.

Администратор может удалить правило установки пакета двумя способами: с удалением приложений с компьютеров, входящих в область действия политики, и без их удаления.

Параметры Windows для пользователей: настройка Internet Explorer

Эта категория правил представляет собой значительную часть Internet Explorer Authorization Kit (IEAK) и предназначена для настройки параметров Internet Explorer и изменения его внешнего вида и поведения. Правила разбиты на несколько групп.

Параметры настройки Internet Explorer

Наименование правила	Описание
<i>Интерфейс с пользователем</i>	
Browser title	Заголовок обозревателя. Позволяет изменять заголовок Internet Explorer и Outlook Express. Введенный текст будет добавлен после фраз «Microsoft Internet Explorer provided by» и «Outlook Express provided by*». Можно указать и графический файл, который будет наложен в виде фона на панель инструментов Internet Explorer
Animated Bitmaps	Позволяет заменить шарик, вращающийся в правом углу Internet Explorer
Custom Logo	Позволяет заменить стилизованную букву «e» на все, что вам заблагорассудится
Browser Toolbar buttons	Позволяет добавить на панель инструментов новые кнопки и связать их с программами или сценариями
<i>Соединения</i>	
Connection settings	Позволяет импортировать установки соединений, выставленные на том компьютере, где запущена консоль оснастки групповой политики
Automatic Browser Configuration	Позволяет указать путь к файлу конфигурации .INS или имя автопрокси-сервера
Proxi settings	Позволяет указать, какой прокси-сервер и для каких протоколов используется

см. след. стр.

Наименование правила	Описание
User Agent String	Это строка, которая посылается обозревателем в ответ на вопрос о его типе и версии. Например, Mozilla 4.0 (compatible; MSIE 5.0; Windows NT; ваша строка)
URL Favourites and Links	Позволяет указать перечень страниц, которые помещаются в разделы Избранное и Соединения по умолчанию
Important URLs	Пути к домашней странице, странице поиска и справки
Channels	Список Интернет-каналов
Безопасность	
Security zones and content ratings	Определяют зоны безопасности и рейтинг содержимого страниц (насилие, секс и т. п.)
Authenticode settings	Здесь вы определяете, каким производителям ПО для Интернета вы доверяете и соответственно разрешаете загрузку на компьютеры пользователей программных модулей
Программы	
Programms	Вы можете импортировать параметры исполняемых программ, выставленные на том компьютере, где запущена консоль оснастки групповой политики

Параметры Windows для пользователей: сценарии

Сценарии, указываемые в групповой политике для пользователей, — это командные файлы или файлы Windows Scripting Host, исполняемые на этапе регистрации пользователя в домене или выхода из него. Как я уже говорил, они находятся в каталоге Sysvol\имя_домена\Policies\{GUID политики}\USER\Scripts в подкаталогах Logon и Logoff.

Сценарии регистрации выполняются асинхронно. Если вас это не устраивает, то в административных шаблонах для компьютера надо установить правило Run logon scripts synchronously, позволяющее исполнять их один за другим. Это, естественно, увеличивает время входа в систему.

Возможно, вы привыкли к тому, что файлы сценариев должны размещаться в каталоге Sysvol\имя_домена\Scripts. Вы можете поместить файлы туда, однако никаких дополнительных удобств от этого не получите. В любом случае вы включаете файлы сценариев в ОПП.

Замечание Не путайте эти сценарии с теми, что определяются в профилях учетных записей. Если они определены, то будут выполняться по-прежнему.

Параметры Windows для пользователей: правила безопасности

Для пользователей можно установить только одно правило безопасности — Enterprise Trust. Оно позволяет вам создать списки доверенных сертификатов, с тем чтобы определить, зачем и какие сертификаты может применять пользователь. Остальные правила безопасности определяются только на уровне компьютеров.

Параметры Windows для пользователей: служба удаленной установки

Это правило определяет возможности пользователя во время автоматической удаленной установки ОС с использованием службы RIS. Существуют три варианта применения правил:

- ◆ Allow — правила применяются;
- ◆ Don't care — применяются правила, стоящие в иерархии выше, например, для правил, определенных на уровне ОП, будут применены правила домена;
- ◆ Deny — правила не применяются.

Можно задать четыре правила:

- **автоматическая установка** — система устанавливается в автоматическом режиме без учета, какой пользователь регистрируется в сети;
- ◆ **настраиваемая установка** — данный тип установки может учитывать имя пользователя и компьютера и в соответствии с этим устанавливать специфические параметры;
- **перезагрузка** — позволяет выполнить перезагрузку компьютера и повторный запуск установки системы в случае неудачной попытки установки;
- ◆ **инструменты** — предоставляет доступ пользователя к диагностическим и отладочным программам.

Параметры Windows для пользователей: перенаправление папок

Четыре папки на локальном компьютере используются чаще всего и хранят самые важные для пользователя сведения:

- My Documents (и вложенная в нее папка My Pictures);
- Application Data;
- ◆ Start Menu;
- Desktop.

В папке My Documents хранятся файлы, с которыми работает пользователь (а как ему не хранить их там, если по умолчанию в диалоговом окне сохранения или открытия файла всегда показывается ее содержимое!), в остальных — информация о персональных параметрах.

Скрытая папка Application Data расположена по умолчанию на системном диске в каталоге Documents and settings\имя пользователя. В нее приложения пишут информацию о своих персональных параметрах. Так, созданный нами шаблон документа Microsoft Word сохранен не в общем каталоге Templates, а в подкаталоге \Word\Templates в папке Application Data. Когда в вы захотите создать документ на основе этого шаблона, то в списке доступных шаблонов вы увидите как общие шаблоны, так и те, что хранятся в вашем личном каталоге.

Папка Start Menu расположена по умолчанию на системном диске в каталоге Documents and settings\имя пользователя и содержит те элементы меню Start, которые имеют отношение только к вам. Все элементы меню Start делятся на общие и личные. Первые присутствуют в меню всех пользователей, вторые же подгружаются только в зависимости от того, какой пользователь зарегистрировался.

Папка Desktop расположена по умолчанию на системном диске в каталоге Documents and settings\имя пользователя и содержит элементы рабочего стола, принадлежащие вам. Как и пункты меню Start, они отображаются на рабочем столе в соответствии с тем, какой пользователь вошел в систему.

Содержимое этих папок поддерживает ту атмосферу работы, которую каждый пользователь создает на своем компьютере. Стоит ему сменить компьютер — и где комфорт? Все надо создавать сначала. А ведь нередко пользователь работает более чем на одном компьютере и везде хочет видеть привычное окружение. Вот тут-то на помощь и приходят правила перенаправления папок.

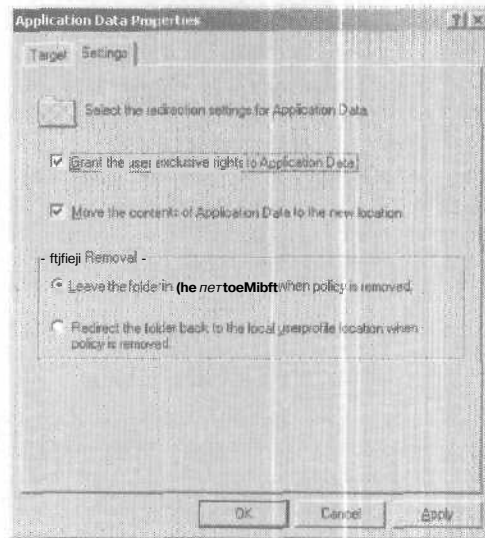
Если папки расположить на общедоступном сервере в личных каталогах пользователей, то независимо от того, на каком компьютере пользователь зарегистрировался, он будет иметь доступ и к своим документам и к своему окружению. Другой плюс перенаправления папок — возможность выполнения централизованного резервного копирования и проверки на вирусы. Вряд ли пользователи занимаются этим на локальных компьютерах. Наконец, если на сервере задать автономное использование перенаправленных папок, то мобильные пользователи, отключенные от сети, все равно смогут работать с документами и иметь привычное окружение.

Замечание По умолчанию все перенаправленные папки доступны автономно. Это свойство можно отменить с помощью пользовательского административного шаблона, описанного далее.

Но у перенаправления есть и недостаток — увеличенный сетевой трафик. Все документы приходится открывать уже не локально, а по сети, что несколько **снижает** производительность.

Существует две возможности перенаправления папок.

- Для всех пользователей указывается общий путь. При этом можно в пути задействовать переменную %username%, например \\root 1\users\%username%\My Documents. При этом для каждого пользователя будет создан персональный каталог с названием, соответствующим имени его учетной записи.
- ◆ Для отдельных групп пользователей можно указать свои пути. Такой способ перенаправления удобен при создании временных групп, работающих над общим проектом.



Условия перенаправления папок

Правила перенаправления папок содержат несколько условий.

- Можно указать на необходимость предоставления эксклюзивных прав доступа к перенаправленной папке. При этом права полного доступа будут предоставлены тому **пользователю/группе**, для которого создается папка. Администраторам будут предоставлены права на чтение,
- 4 Текущее содержимое папки полностью перемещается в новое место.
- ◆ Если к указанному пользователю политика перестает применяться, то папка может быть либо оставлена в том месте, куда она была

перенесена, либо будет перенаправлена на старое место в профиле пользователя.

- Папку My Pictures, вложенную в My Documents, можно либо перенести вместе с родительской, либо не применять к ней политику и перенести в иное место.

Административные шаблоны для пользователей

Это файлы с расширением .ADM, в которых в текстовом виде записаны параметры, модифицирующие реестр компьютера, на котором регистрируется пользователь входящий в область действия групповой политики. Новые параметры для компьютеров заносятся в ветвь реестра HKEY_CURRENT_USER.

Перечислять все параметры бесполезно. Я лучше покажу их применение на конкретных примерах, что и сделаю немного позже. Здесь же я лишь приведу базовые параметры, доступные для конфигурирования по умолчанию.

Внимание Перечисленные административные шаблоны появляются в Windows 2000, только если:

- установлен пакет обновления SP2 или выше;
- установлены все последние заплатки для системы безопасности;
- ◆ в домене есть клиенты Windows XP.

Административные шаблоны для пользователей

Наименование правила	Описание
Компоненты Windows Net Meeting	Шаблоны для пользователей в отличие от шаблонов для компьютеров позволяют управлять предоставлением в совместное использование компонентов Net Meeting, управлять параметрами звука, внешним видом страницы параметров и другими параметрами
Internet Explorer	Позволяет определять доступность различных функций Internet Explorer для пользователя.
Windows Explorer	Очень важный шаблон. Управляет доступностью элементов интерфейса Windows 2000/Windows XP. Вот правила, общие для Windows 2000 и Windows XP: <ul style="list-style-type: none"> ◆ удаление команды Folder Options в меню Tools; ф удаление меню File в Windows Explorer; • удаление функций «Map Network Drive» и «Disconnect Network Drive»; ф удаление кнопки Search в Windows Explorer; ◆ удаление контекстно-зависимого меню;

см. след. стр.

Наименование правила	Описание
	<ul style="list-style-type: none"> ◆ удаление команды Manage в контекстно-зависимом меню; ◆ использование только разрешенных расширений оболочки; ф запрет отслеживания ярлыков при перемещении; ◆ запрет отображения указываемых дисков компьютера; ◆ запрет доступа к дискам; ◆ удаление вкладки Hardware; ◆ удаление вкладки DFS; ◆ удаление средств изменения эффектов анимированного меню; ◆ удаление средств изменения параметров индикатора клавиатуры; ◆ удаление «Computers Near Me» в папке My Network Places; ◆ удаление «Entire Network» в папке My Network Places; ◆ ограничение числа показываемых документов в списке недавно открытых; ◆ запрещение запроса альтернативных полномочий; ◆ выполнение запроса полномочий для сетевых установок. <p>Следующие правила применимы только к клиентам Windows XP:</p> <ul style="list-style-type: none"> ◆ удаление вкладки Security; ◆ удаление функций записи компакт-дисков; ◆ запрет переноса удаленных файлов в корзину; ф требование подтверждения при удалении файлов; ◆ максимальный размер корзины; ◆ удаление Shared Documents из My Computer; ф отключение кэширования слайдов рисунков; ф использование классического вида оболочки. <p>Кроме перечисленных, существуют правила управления видом диалогового окна File Open. Доступность элементов окна влияет на защищенность системы</p>
Microsoft Management Console	Позволяют ограничить доступ пользователей к оснасткам MMC. Особо отмечу возможность ограничения доступа к редактированию правил групповой политики. Эти правила удобно применять при делегировании полномочий
Task Scheduler	Позволяет управлять доступностью функций утилиты запуска приложений по расписанию

см. след. стр.

Наименование правила	Описание
Terminal Services	Позволяет управлять настройкой пользовательских сеансов для терминальных серверов. Только для Windows XP/Windows .Net Server
Windows Installer	Устанавливает некоторые пользовательские параметры Windows Installer
Windows Messenger	Запрещает/разрешает работу с Windows Messenger данному пользователю. Только для систем Windows XP
Windows Update	Запрещает пользователю доступ к функции обновления системы Windows XP
Windows Media Player	Управляет внешним видом и параметрами медиапроигрывателя
Меню Start и панель задач	Управляет содержимым меню Start и поведением панели задач. В частности, элементы меню, соответствующие программам, назначенным для установки групповыми правилами, но еще не установленным, можно показывать бледно
Рабочий стол	Позволяет управлять доступностью элементов рабочего стола
Active Desktop	Разрешает использование Active Desktop и ограничивает возможности по его модификации
Active Directory	Управляет средствами доступа к Active Directory: поиском в каталоге, возможностью использования фильтров или просто ее просмотра в окне Network Neighborhood
Панель управления	Управляет доступом к отдельным компонентам панели управления или ко всей панели в целом. Для Windows XP позволяет включать классическое представление окна панели
Add/Remove Programs	Управляет доступностью элементов окна добавления/удаления приложений
Display	Управляет доступностью настройки отдельных компонентов экрана и устанавливает некоторые параметры
Printers	Разрешает/запрещает поиск принтеров в локальной сети и на Web, а также их добавление
Regional and Language Options	Запрещает выбор языка меню и диалоговых окон в приложениях
Папки совместного доступа	Разрешает/запрещает публикацию в Active Directory совместно используемых папок или корней распределенной файловой системы DFS
Сеть	
Offline Files	Определяет доступ к функциям управления доступом и использования автономных папок. Так, можно отменить свойство перенаправленных папок быть доступными автономно
Network Connections	Ограничивает доступ к элементам папки Network Connections: управлению параметрами протоколов, созданию новых соединений, просмотра статуса соединений и т. п.

см. след. стр.

Наименование правила	Описание
Системные компоненты	<p>Позволяет установить правила работы с системой, специфичные для каждого пользователя. Так как эти правила используют очень часто, я приведу их все. Сначала следуют правила, общие для Windows 2000 и Windows XP:</p> <ul style="list-style-type: none"> ◆ не показывать приветственный экран при регистрации пользователя; + интерпретация века для дат позже 2000 года; ◆ цифровая подпись драйверов устройств; ◆ приложение, используемое в качестве оболочки; + запрет доступа к командной строке; ◆ запрет доступа к средствам редактирования реестра; • перечень разрешенных к запуску приложений; • перечень запрещенных к запуску приложений; ◆ отключение автопроигрывания компакт-дисков. <p>Следующие правила применимы только в системах на базе Windows XP:</p> <ul style="list-style-type: none"> ◆ загрузка пропущенных компонентов COM; ◆ разрешение автоматического поиска и установки обновлений Windows; • перечень мест где могут быть драйверы устройств; • перечень программ, запрещенных к запуску из справочной системы
User profiles	Ограничение размера профиля, исключение каталогов из блуждающих профилей
Scripts	Управление видимостью и синхронностью выполнения сценариев входа в систему
Ctrl+Alt+Del Options	Управление доступностью функций в окне, вызываемом на экран по нажатию Ctrl+Alt+Del во время сеанса
Logon	Управление списком программ, исполняемых при регистрации пользователя в системе
Group Policy	Правила применения групповых правил для пользователей (см. ранее)
Power Management	Предписание вводить пароль при выходе системы из состояния гибернации или приостановки

Планирование групповой политики

В главе «Планирование Active Directory» много говорится о критериях построения доменной структуры, планирования структуры ОП и сайтов. Там же я вкратце затрону вопросы применения групповой политики. Пришла пора поговорить об этом подробно.

Начальство хочет, вы — желаете

Итак, я говорил о противоречиях с руководством. Боссам нужно, чтобы «палочки были поперек», т. е. чтобы структура Active Directory отражала структуру предприятия. Ваше желание — сделать так, чтобы система была защищенной, управляемой и не требующей постоянного внимания. Групповая политика — это рубеж, отделяющий ваши желания от желания руководства. Так как же и волков накормить, и овец сохранить?

Вы уже знаете, что групповая политика позволяет сделать следующее.

- Установить в организации централизованную политику безопасности. Иначе говоря (это для начальства), создает такие условия, при которых каждый пользователь и каждый компьютер в системе находятся под постоянным контролем, так что все несанкционированные действия пресекаются автоматически, сведения о них регистрируются, а сам пользователь подвергается наказанию.
- Централизованно управлять приложениями, с которыми работают пользователи. Или же (сами понимаете, кому это говорится), создаются условия, при которых обеспечивается соблюдение корпоративной политики работы с приложениями, так что пользователи:
 - работают только с теми приложениями, что одобрены к применению;
 - не могут сами устанавливать игры и прочие «вредоносные» программы;
 - переходят на новые версии или обновляют существующие централизованно;
 - не могут случайно или преднамеренно уничтожить установленные программы.
- ◆ Управлять пользовательскими профилями. Проще говоря; все параметры интерфейса на компьютерах пользователей задаются централизованно, так что при смене компьютера они сохраняются и не позволяют пользователю сделать такое действие, которое может нанести вред его персональной или любой иной системе.
- Управлять автоматической установкой ОС на компьютеры. Чтобы поставить систему на новый компьютер, не надо приглашать технического специалиста на рутинные процедуры: все будет сделано автоматически в соответствии с ролью владельца компьютера, которую он играет в организации.

А главное то, что достигается это не путем найма огромного штата технических специалистов, работающих в две смены без выходных и требующих за это надбавки к жалованию и премий, а минимальным

количеством квалифицированных инженеров со стабильной достойной зарплатой. Экономия!

Изложите это руководству так, чтобы оно прочувствовало смысл затеи с Active Directory, и **особенно** последний аргумент, — тогда оно если не станет вашим союзником, то хоть не будет **настаивать** на своем видении этой задачи и ставить палки в колеса.

От простого к сложному

Подумаем, с какого конца лучше подойти к групповой политике.

Полагаю, вам хорошо знакомы Windows NT и политика безопасности в этой ОС, т. е. ограничения паролей, правила блокировки и т. д. А раз так, вот вам **первый совет**: начните применение групповой политики с того, что вы хорошо **знаете**, например, с политики безопасности. Тем **более**, что применение этой политики облегчается готовыми шаблонами безопасности [1]. Если вы работали с системной политикой Windows 9x или Windows NT, то применение административных шаблонов не представит проблем.

Однако не торопитесь. Садясь за руль новой незнакомой машины, никто не выжимает сразу полный газ — надо привыкнуть к ее характеру. Так и с политикой. Примените ее сначала к тестовому контейнеру, посмотрите, как это скажется на компьютерах и на пользователях, поиграйте с параметрами, поймите, что можно, а что нельзя. Это **второй совет**.

Попробовали и хотите расширить плацдарм? Спокойнее! Примените политику на верхних уровнях иерархии Active Directory и не стремитесь привязать ОГП к куче подразделений. Посмотрите: может, этого и не стоит делать. Это **третий совет**.

Наконец, вы задумываетесь о делегировании полномочий. Правильное решение — только реализовывать его надо с умом. Если есть у вас единомышленники, которые, как и вы, знакомы с групповой политикой, делегируйте полномочия им. Посмотрите, **потренируйтесь**, выявите все узкие места. И, только набравшись достаточно опыта в делегировании и написав соответствующие **инструкции**, можете передавать управление другим **пользователям** на местах. **Четвертый совет** в том и заключается, чтобы не передавать полномочий незнакомым людям, пока вы не будете уверены, что это не приведет к нежелательным результатам.

Я настоятельно прошу вас следовать этим советам. Путь от простого к сложному позволит вам не наломать дров и получить солидный опыт применения правил.

Советы по применению

Как же внедрить политики в организации? Прежде всего ответьте на пять вопросов.

Вопрос 1. Принималось ли в расчет желание использовать групповую политику при проектировании структуры Active Directory?

Вопрос 2. Какую функциональность групповой политики вы хотели бы использовать?

Вопрос 3. Как вы хотите управлять политикой: централизованно или децентрализованно?

Вопрос 4. Хотите ли вы применять правила к ОП или, применив политику к домену, использовать фильтрацию?

Вопрос 5. Как вы собираетесь управлять политикой, вычислять результирующий набор правил и вносить изменения?

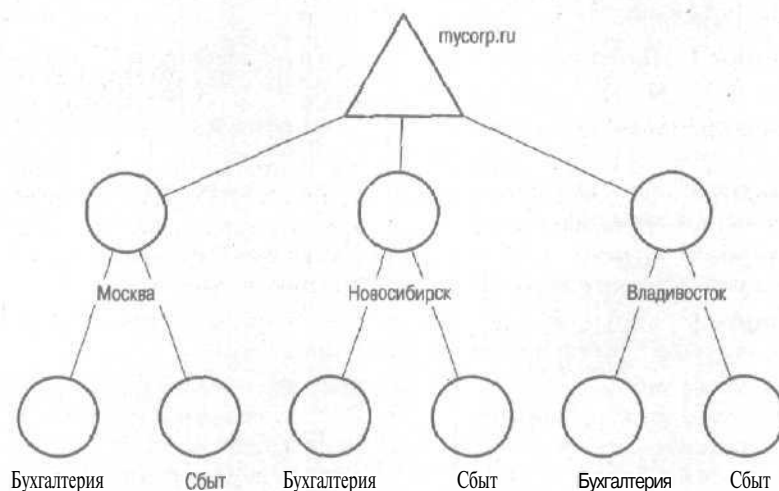
Ответы на них позволят понять, сколько ОП надо создать, где их хранить, с какими объектами Active Directory связать, кого из администраторов сделать ответственным за применение правил и т. п. Разберем несколько примеров, в которых используем наш вопросник.

Один домен

Допустим, нужно применить групповую политику в организации, только что мигрировавшей с Windows NT 4.0 и структура Active Directory которой представляет собой единственный домен. Вы задали эти вопросы руководителю службы ИТ и получили такие ответы.

Вопрос	Ответ
Принималось ли в расчет желание применять групповую политику при проектировании структуры Active Directory?	Нет, структура Active Directory полностью отражает потребности бизнеса, и это для нас очень важно
Какую функциональность групповой политики вы хотели бы использовать?	Мы бы хотели использовать политику блокировок учетных записей и настройку интерфейса, применявшиеся в домене Windows NT, интерес также представляет перенаправление папок. О других правилах мы пока не думали
Как вы хотите управлять политикой: централизованно или децентрализованно?	Это дело нашей централизованной службы ИТ
Хотите ли вы применять правила к ОП или, применив политику к домену, использовать фильтрацию?	Мы бы хотели избежать сложностей. Но мы хотим держать правила под полным контролем
Как вы собираетесь управлять политикой, вычислять результирующий набор правил и вносить изменения?	Мы об этом не думали и не хотели бы задумываться в дальнейшем

Ответ на первый вопрос был подкреплён такой структурой Active Directory:



Структура Active Directory компании

Как видите, структура ОП построена по классической организационной модели, которая менее всего подходит для применения политики. Но что ж делать, отступить поздно, поэтому подумаем, как оптимальнее реализовать политику,

После миграции в домене остались такие локальные группы:

- Msk-Acct;
- ◆ Msk-Sales;
- + Nsk-Acct;
- ◆ Nsk-Sales;
- East-Acct;
- ◆ East-Sales;

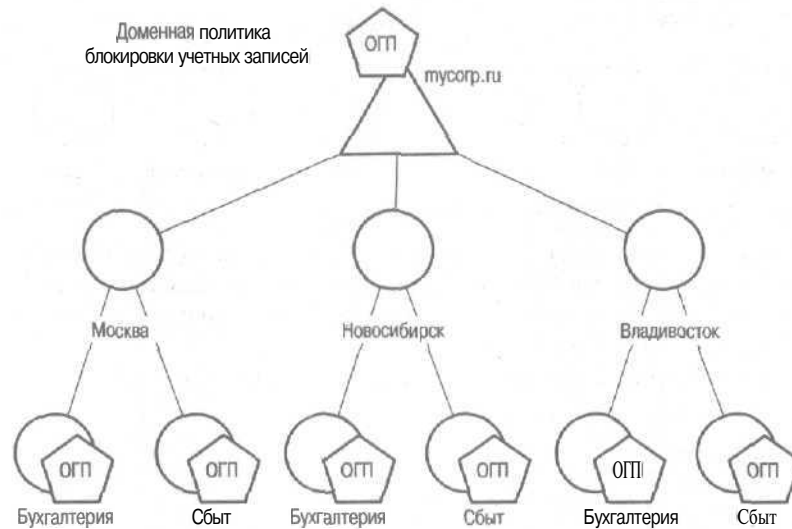
Системная политика в домене Windows NT применялась к этим шести группам пользователей. Причем параметры интерфейса были свои для каждой из групп.

Зная эти исходные данные, подумаем, какие ОГП и где разместить. Решений может быть несколько, но пойдём по порядку: от лобового к оптимальному.

Начнём с доменной политики блокировок учетных записей. Это правило относится к политике безопасности и, следовательно, применяется только ко всему домену в целом. Раз так, то соответствующий ОГП определим на уровне домена. Он будет единственным.

Далее рассмотрим правило перенаправления папок, которое, как вы помните, может быть простым и сложным. В первом случае папки для всех пользователей перенаправляются в одно место, во втором – перенаправление можно поставить в зависимость от принадлежности к группе. Выберем первый вариант. Тогда для каждого ОП второго уровня надо создать свой ОГП, отвечающий за перенаправление папок сотрудников этого ОП.

Наконец, правила настройки интерфейса. Учитывая, что они должны быть различны для каждого ОП, создаем шесть ОГП. Для простоты объединим эти правила с правилами перенаправления папок. В итоге получим структуру ОГП, показанную на рисунке. Каждый ОГП имеет свое имя, расположен и связан со своим уникальным ОП.



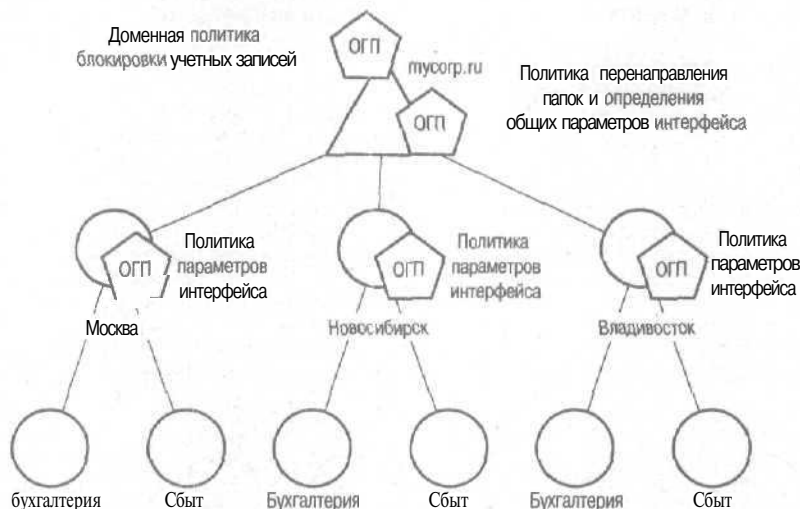
Все указанные ОГП определяют политику перенаправления папок и настройки интерфейса для каждого ОП.

Вариант размещения и привязки ОГП

Это решение отвечает требованиям, но, кажется, сложновато. Упростим?

В первую очередь применим сложное перенаправление папок — тогда можно создать один ОГП, а в нем указать путь перенаправления для каждой группы. Тогда этот ОГП можно создать на уровне домена и связать с доменом, а не с ОП. На уровне домена у нас уже есть ОГП, определяющий политику безопасности. Можно правила перенаправления включить в него, но лучше этого не делать, чтобы легче было использовать ОГП.

Второй путь упрощения не так очевиден. Он связан с анализом правил настройки интерфейса. Скажите, что особенного можно придумать для трех бухгалтерий, чтобы их параметры кардинально отличались от параметров отдела сбыта? Опыт показывает (да и дополнительный анализ правил в этом примере), что обычно 90% правил настройки интерфейса **совпадают**. Существуют лишь незначительные различия, которыми в принципе можно пренебречь. В нашем примере выяснилось, что различаются правила только по регионам. Поэтому оптимально оделать таю к домену применить ОГП, который определяет 90% общих параметров интерфейса, а к ОП первого уровня — ОГП, определяющие оставшиеся 10%. Вот вариант такого размещения ОГП,



Второй вариант размещения и привязки ОГП

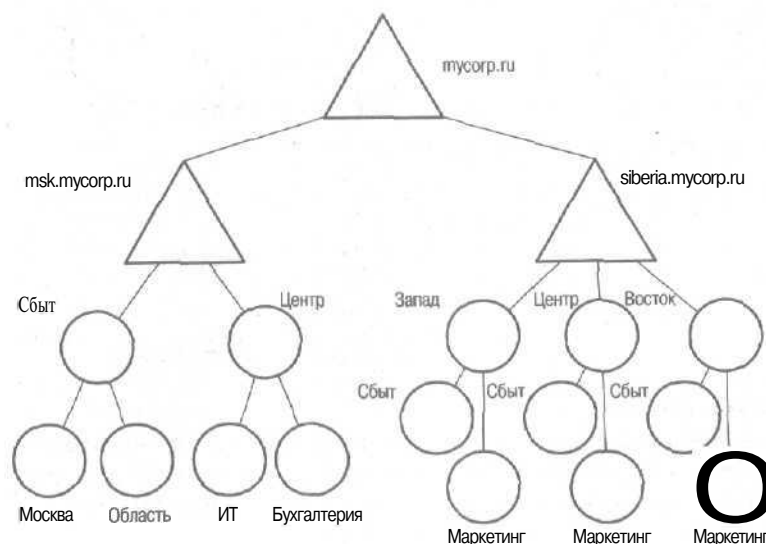
Этот вариант стал возможен во многом благодаря тому, что параметры интерфейса совпадают. Если бы это было не так, пришлось бы остановиться на первом варианте. Понятно, что, кроме предложенных вариантов, могут быть и несколько отличные от них, но это не суть важно. Главный урок, который нужно вынести из этого примера, звучит так: *упрощайте решение и уменьшайте количество ОГП, используйте анализ требуемых правил и стремитесь их обобщать.*

Несколько доменов

Теперь рассмотрим случай посложнее. Допустим, надо спроектировать групповую политику для крупной компании, образовавшейся из двух различных организаций. Ответы на пять вопросов выглядят так.

Вопрос	Ответ
Принималось ли в расчет желание использовать групповую политику при проектировании структуры Active Directory?	Да, структура Active Directory проектировалась именно с таким расчетом
Какую функциональность групповой политики вы хотели бы применять?	Мы хотели бы применить максимальное количество правил, включая политику безопасности, правила установки ПО и административные шаблоны
Как вы хотите управлять политикой: централизованно или децентрализованно?	Создание ОГП и их привязка к доменам и сайтам должна выполняться централизованно, но привязку локальных политик к ОП мы хотели бы делегировать региональным администраторам
Хотите ли вы применять правила к ОП или, применив политику к домену, использовать фильтрацию?	Мы хотим по мере возможности воздержаться от фильтрации и применять правила к контейнерам, максимально близким для пользователей. Если же это будет иногда невозможно, то согласны на использование фильтров
Как вы собираетесь управлять политикой, вычислять результирующий набор правил и вносить изменения?	Мы хотим контролировать номера версий правил и анализировать результирующий набор правил. Кроме того, нам бы не хотелось, чтобы к одному пользователю применялось более 10 ОГП

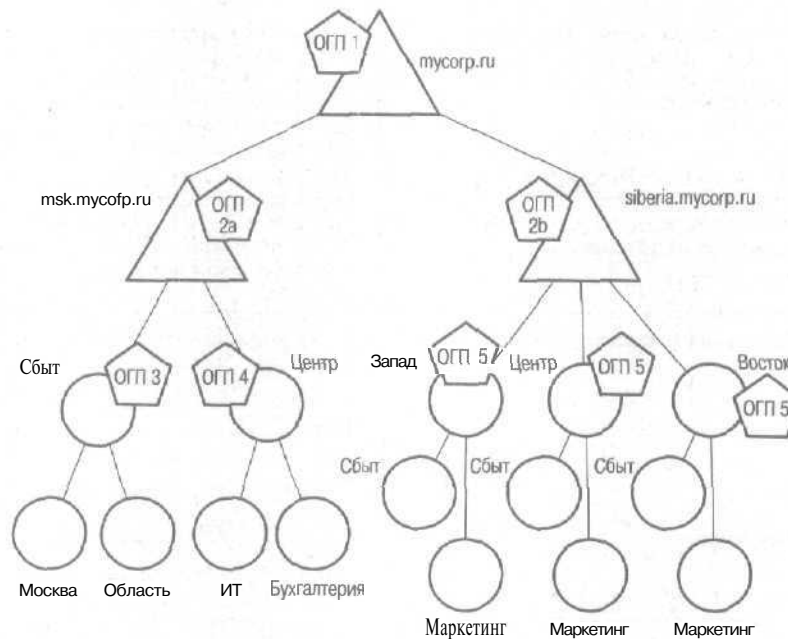
Доменная структура компании показана на рисунке.



Доменная структура компании

Если вы внимательно читали главу «Планирование Active Directory», то, взглянув на структуру, возмутитесь до глубины души. Разве эта структура разрабатывалась с учетом применения групповой политики? Да она вообще вся кривая! ОП первого уровня в доменах msk и Siberia организованы по разным принципам. В первом — по организационному, во втором — по территориальному. Все так, но напомним, что компания образовалась при слиянии двух других, каждая из которых имела свою структуру ИТ. В Москве две группы администраторов управляют ОП Сбыт и Центр, а в Сибирском отделении имеется три региональных центра ИТ. Раз так, то показанная структура как раз отражает административную модель.

Предлагаемый вариант применения политики показан на рисунке.



Вариант применения групповой политики

Администраторы предприятия размещаются в домене mscorp.ru. Больше никаких учетных записей пользователей здесь нет. К этому домену должна быть применена специальная «жесткая» политика безопасности. Именно она реализуется с помощью ОПП. Этот ОПП создан в домене mscorp.ru и привязан к нему.

С точки зрения безопасности, домены msk и Siberia равноправны. Можно было бы создать один ОПП на уровне домена mscorp.ru, а за-

тем связать его с каждым из дочерних доменов. Но это неверное решение, И вот почему: всякий раз при применении правил безопасности в дочернем домене будет выполняться доступ к родительскому домену для каждого из объектов, к которому применяется политика. Это вдвое увеличит загрузку. Кроме того, при отладке правил могут возникнуть затруднения из-за удаленности ОП. В связи с этим запомните: *доменные политики надо создавать в том домене, к которому они привязаны*. Именно поэтому администраторы создают два совершенно одинаковых ОП (ОП2а и ОП2б) в каждом из дочерних доменов и связывают их с ними.

Теперь рассмотрим остальные политики в домене *msk.mycorp.ru*. В соответствии с пожеланиями руководителя службы ИТ ОП создаются администраторами предприятия на уровне домена. Далее права по привязке ОП делегируются службам ИТ, обслуживающим ОП Сбыт и Центр. Здесь предполагаем, что правила одинаковы для всей службы сбыта независимо от того, где она находится — в Москве или в области. Иные правила распространяются на ОП Центр, но они также одинаковы для всех дочерних подразделений.

Сходную картину наблюдаем для домена *siberia.mycorp.ru*. Вся разница в том, что независимо от региона должна применяться единая политика. Можно было бы соответствующий ОП создать на уровне домена и связать с *доменом*. Но *вспомните*: руководитель ИТ службы хочет делегировать право привязки ОП к ОП локальным администраторам. Да будет так! ОП5 создается на уровне домена, а региональные администраторы связывают его со своими ОП.

Чтобы не загромождать рисунок, я указал минимум ОП. Но главное здесь не количество, а принцип создания и связи. Если в каком-то ОП возникает потребность в отдельных *правилах*, то администраторы *предприятия* создают нужный ОП на уровне того домена, в котором расположен ОП. и сообщают о его создании региональным администраторам. Администраторы, нуждавшиеся в этом ОП, применяют его сразу. Остальные могут выяснить необходимость применения этих правил в их зоне *ответственности*, выполнить анализ результирующего набора правил и, если *понадобится*, связать ОП со своими ОП.

Как видите, удовлетворены все запросы. Предложенное решение хорошо, но может быть и иным. Думаю, вы уже поняли, сколько «мелочей» могут изменить дизайн групповой политики.

Поиск и устранение проблем

А теперь обратим взгляд на такую животрепещущую тему, как поиск и устранение проблем, связанных с групповой политикой. Правила настолько эффективны, что сложно говорить о проблемах с правилами, возникшими по вине системы. Как всегда, виноваты мы — админи-

страторы. Первопричина всех проблем — «горе от ума»: либо придумываются взаимоисключающие правила, либо их набор столь велик и применяются они столь сложно, что результат оказывается совершенно не тот, которого ждали, либо в процессе создания правил допущены досадные ошибки — вами или вашим коллегой.

Справедливости ради отмечу, что случаются проблемы, причиной которых являются сбои в Active Directory или файловой системе. Но это скорее исключения, чем правило.

Средства поиска проблем

Начнем со знакомства со средствами анализа и управления групповой политикой. Из тех, с которыми работал я и которые считаются наиболее полезными:

- ◆ GPRESULT — утилита командной строки для анализа результирующего набора правил на компьютере;
- ◆ GPOTool — средство проверки ГП на контроллерах доменов;
- ◆ ADDIAG — инструмент, позволяющий отслеживать статус ПО, устанавливаемого с помощью групповых правил;
- ◆ SECEDIT — средство конфигурации и анализа политики безопасности;
- ◆ FAZAM2000 — графическая программа, позволяющая анализировать результирующий набор правил и выполнять анализ «что — если».

GPRESULT

Собирает информацию о правилах, назначаемых для пользователя и компьютера, и о политиках, ставших источником этих правил. У этой утилиты четыре параметра:

- + /v — информация выводится с подробностями;
- /s — информация выводится с «супер»-подробностями; выводится даже двоичное представление данных;
- /c — выводится информация только о правилах для компьютера;
- ◆ /u — выводится информация о правилах только для пользователя.

Использовать утилиту несложно, однако замечу, что, запустив ее без указанных параметров, вы получите урезанный результат — только имена групповых правил без объяснения того, что было ими сделано на компьютере.

Чаще всего утилиту сначала запускают без параметров. Анализируя выведенную информацию, оценивают, какие из правил заслуживают более подробного рассмотрения. Например, может быть непонятно,

к каким последствиям приводит правило или последовательность сходных правил. Поэтому далее запускают программу с параметром /v. Если некоторые значения в реестре являются двоичными величинами, то Gpresult запускают с ключом /s.

Разберем пример результата, выводимого утилитой, запущенной с параметром /v.

Начинается вывод информации с сообщения сведений об ОС:

```
Microsoft (R) Windows (R) 2000 Operating System Group Policy Result tool
Copyright (C) Microsoft Corp. 1981-1999
Created on 13
```

Operating System Information:

```
Operating System Type:      Professional
Operating System Version:    5.0.2195
Terminal Server Mode:       Not supported
```

Обратите внимание на строку Created on (Создан ...) — Заметили загадочное число 13? Это следствие ошибки в Windows 2000. Если установить американские региональные установки, то будет выведена полная дата. Эта ошибка исправлена в Windows XP.

Теперь посмотрите на строку Terminal Server Mode. На клиентах Windows XP этот режим поддерживается по умолчанию.

Следующий раздел — предоставление исчерпывающей информации о пользователе, зарегистрированном в данный момент в системе. О полноте судите сами:

User Group Policy results for:

CN=u2,OU=test,DC=mycorp,DC=ru

```
Domain Name:      MYCORP
Domain Type:      Windows 2000
Site Name:        Default-First-Site-Name
Roaming profile:   (None)
Local profile:     C:\Documents and Settings\u2
```

The user is a member of the following security groups:

```
MYCORP\Domain Users
\Everyone
BUILTIN\Users
\LOCAL
NT AUTHORITY\INTERACTIVE
NT AUTHORITY\Authenticated Users
```

The user has the following security privileges;

```
Bypass traverse checking
Shut down the system
Remove computer from docking station
```

Как видите, профили, членство в группах и привилегии приведены полностью. Список привилегий должен привлечь ваше внимание. Ведь если вы хотели в правилах безопасности указать привилегии для пользователя, они должны быть тут отражены. Если их нет, проверьте:

- не ошиблись ли вы в определении правил;
- когда была применена доменная политика в последний раз (именно доменная, так как политика безопасности определяется на уровне домена);
- была ли применена компьютерная часть.

Следующий раздел посвящен правилам групповой политики, примененным к указанному пользователю. Начинается он с сообщения о времени, когда политика была применена в последний раз, и имени контроллера домена, с которого она была применена.

Last time Group Policy was applied: 13 Group Policy was applied from: R00T1.mycorp.ru

Заметьте, что и здесь ошибка с выводом даты. Для целей диагностики это весьма неудобно, поэтому рекомендую временно установить на этом компьютере регион US.

Далее идет перечисление всех правил, примененных для модификации параметров реестра, т. е. административных шаблонов. Политики перечисленные в порядке их применения. Сначала указывается имя политики, в которой определены эти шаблоны;

The user received "Registry" settings from these GPOs:

```
Restrict Environment
Revision Number: 72
Unique Name: {0DBEB430-79EB-4C3A-8118-A427B95E02BC}
Domain Name: mycorp.ru
Linked to: Organizational Unit (OU=test,DC=mycorp,DC=ru)
```

Для каждого ОГП указываются:

- ◆ дружественное имя (Restrict Environment);
- номер версии (72), из которого можно сделать примерный вывод о том, сколько параметров будет изменено (во всяком случае не больше, чем номер версии);
- 4 номер GUID политики (или Local Policy для локальной политики);
- имя домена, в котором она определена;
- информация о связи ОГП с объектов в Active Directory; в нашем примере видно, что это подразделение OU=test,DC=mycorp,DC=ru.

Если утилиту запустить без параметра /v, на этом информация о данном ОГП кончится. Но так как мы задали отображение подробностей,

далее следует перечисление изменений в реестре, выполненных при применении политики:

```

KeyName:    Software\Microsoft\Windows\CurrentVersion\Policies\Comdlg32
ValueName:  NoPlacesBar
ValueType:  REG_DWORD
Value:      0x00000001
KeyName:    Software\Microsoft\Windows\CurrentVersion\Policies\Comdlg32
ValueName:  NoFileMru
ValueType:  REG_DWORD
Value:      0x00000001
KeyName:    Software\Microsoft\Windows\CurrentVersion\Policies\Comdlg32
ValueName:  NoBackButton
ValueType:  REG_DWORD
Value:      0x00000001

```

Формат выводимой информации таков:

- ◆ Key Name — имя ветви в реестре;
- ◆ Value Name — имя параметра;
- ◆ Value Type — тип параметра;
- ◆ Value — значение.

Значение показывается, только если тип параметра не BINARY. Для вывода значений этого типа надо использовать параметр /s в командной строке запуска Gpresult.

Замечание Групповая политика модифицирует только две ветви в реестре: \Software\Policies и \Software\Microsoft\Windows\CurrentVersion\Policies. Если модифицируются другие ветви реестра, то перед сообщением об этом правиле будет предупреждение Warning! The next registry setting is not a true policy setting and will be left in the registry when the GPO that created it is no longer applied (Внимание! Следующее значение реестра не является правильным параметром политики и останется в реестре после завершения применения политики).

Далее следует информация о правилах перенаправления папок.

The user received "Folder Redirection" settings from these GPOs:

```

Restrict Environment
Revision Number: 72
Unique Name: {0DBEB430-79EB-4C3A-8118-A427B95E02BC}
Domain Name: mycorp.ru
Linked to: Organizational Unit (OU=test,DC=mycorp,DC=ru)
Desktop is redirected to \\root1\personal\%username%\Desktop.
My Documents is redirected to \\root1\personal\%username%
\My Documents.

```

My Pictures is redirected to \\root1\personal\%username%\My Documents\My Pictures.
 Start Menu is redirected to \\root1\personal\%username%\Start Menu.
 Programs is redirected to \\root1\personal\%username%\Start Menu\Programs.
 Startup is redirected to \\root1\personal\%username%\Start Menu\Programs\Startup.
 Application Data is redirected to \\root1\personal\%username%\Application Data.

Как видите, формат данных о политике аналогичен описанному ранее. Добавляется указание точного пути к перенаправленным папкам. Далее могут идти сведения о других правилах в аналогичном формате. Для некоторых правил дополнительной информации не приводится. Так, если вы **модифицировали** внешний вид Internet Explorer, сообщение об этом правиле будет весьма лаконичным:

The user received "Internet Explorer Branding" settings from these GPOs:

Default: Domain Policy

Revision Number: 2

Unique Name: {31B2F340-016D-11D2-945F-00C04FB984F9}

Domain Name: mycorp.ru

Linked to: Domain (DC=mycorp,DC=ru)

Additional information is not available for this type of policy setting.

К счастью, таких правил не так много. В основном приводится столько информации, что ее хватит для анализа результата на компьютере. Бот, например, сведения о политике установки приложений:

The user received "Application Management" settings from these GPOs:

Install Office

Revision Number: 5

Unique Name: {BB0B08E9-3E4F-4EAE-AA84-188CB97B3E8F}

Domain Name: mycorp.ru

Linked to: Organizational Unit (OU=test,DC=mycorp,DC=ru)

The user has been assigned the following applications:

MicrosoftOfficeWeb Components

GPO Name: Install Office

Removal Option: Application is orphaned when policy is removed

Microsoft Office 2000 SR-1 Premium

GPO Name: Install Office

Removal Option: Application is uninstalled when policy is removed

The user has installed the following published applications:

(None)

Как видите, здесь перечислены установленные приложения, а также сказано, что с ними произойдет при удалении групповой политики. Если же утилиту `Gpresult` запустить с параметром `/s`, то дополнительно к показанной выше информации будет также сообщено о приложениях, доступных для установки (опубликованных), и об их статусе.

The user has the following applications available

in Add/Remove Programs:

Microsoft Office 2000 SR-1 Premium

GPO Name: Install Office

Installed: Yes

Microsoft Office Web Components

GPO Name: Install Office

Installed: Yes

В следующем разделе описаны правила, примененные к компьютеру. Как и для пользовательских правил, в начале идет сообщение об объекте применения, т. е. о компьютере:

Computer Group Policy results for:

CN=W2KPRO,OU=test,DC=mycorp,DC=ru

Domain Name: MYCORP

Domain Type: Windows 2000

Site Name: Default-First-Site-Name

The computer is a member of the following security groups:

BUILTIN\Administrators

\Everyone

BUILTIN\Users

MYCORP\W2KPRO\$

MYCORP\Domain Computers

NT AUTHORITY\NETWORK

NT AUTHORITY\Authenticated Users

Следующее затем сообщение о времени применения политики также неинформативно при установленном российском регионе.

Формат вывода информации о правилах для компьютеров полностью идентичен описанному выше формату правил для пользователей. Если значение параметра реестра имеет тип `BINARY`, выводимая информация имеет такой вид:

The following settings were applied from: Default Domain Policy

KeyName: Software\Policies\Microsoft\SystemCertificates\EFS

ValueName: EFSBlob

ValueType: REG_BINARY

Value:

30 50 31 16 30 14 06 03 55 04 03 13 0d 41 64 6d 0P1.0...U...Adm
696e6973747261746f72310c300a0603inistrator1.0...

```

55 04 07 13 03 45 46 53 31 28 30 26 06 03 55 04 U....EFS1(0&...U.
0b 13 1f 45 46 53 20 46 69 6c 65 20 45 6e 63 72 ...EFS.File.Encr
79 70 74 69 6f 6e 20 43 65 72 74 69 66 69 63 61 yption.Certifica
74 65 30 81 9f 30 0d 06 09 2a 86 48 66 f7 0d 01 te0..0...*.H....

```

Совет Результаты работы программы Gpresult лучше всего выводить в файл, чтобы потом было удобно выполнять поиск нужных правил и параметров реестра. Если примененных правил не очень много, то, выводя результат в консольное окно, не забудьте установить размеры буфера консольного окна достаточными для приема всей информации.

GPOTool

Утилита командной строки Gpsoool входит в Windows 2000 Resource Kit и позволяет проверить, все ли хорошо с ОГП на контроллерах доменов. Так, в частности, можно проверить:

- однородность ОГП — считываются значения атрибутов контейнера групповой политики и данных в каталоге SYSVOL, сравниваются номера версий.
- * репликацию ОГП — при этом ОГП считываются с каждого контроллера и сравниваются между собой (можно сравнивать отдельные атрибуты и выполнять полное рекурсивное сравнение).

В домене можно указать, для каких контроллеров выполнять сравнение. Если этого не сделать, то сравниваться будут ОГП на всех доступных контроллерах домена. Кроме того, можно выполнять поиск нужного ОГП по его имени или номеру GUID. Ну и, наконец, можно сравнивать правила в разных доменах.

Посмотрим на пример анализа групповых правил на двух контроллерах. Чтобы получить максимум информации, запустим Gpotoool с параметром /verbose.

В первой части результата приводится информация обо всех контроллерах домена независимо от того, доступны они в данный момент или нет.

```

Domain: mycorp.ru
Validating DCs...
R00T1.mycorp.ru: OK
R00T2.mycorp.ru: OK
Available DCs:
R00T1.mycorp.ru
R00T2.mycorp.ru

```

Если контроллер домена в момент выполнения программы был недоступен, он исключается из дальнейшего анализа. Далее сообщается обо всех обнаруженных политиках:

Searching for policies...

Found 4 policies

А затем выполняется их тестирование и сообщается статус. Для политик, прошедших тестирование, выводится:

Policy {0DBEB430-79EB-4C3A-8118-A427B95E02BC}

Policy OK

Для политик, не прошедших тестирования, сообщение будет аналогично этому:

Policy {0DBEB430-79EB-4C3A-8118-A427B95E02BC}

Error: Version mismatch on R00T2.mycorp.ru, DS=4718592, sysvol=4718593

Наконец, для каждого из контроллеров домена выводится информация о каждом ОПП:

DC: flOOT1.mycorp.ru

Friendly name: Restrict Environment

Created: 12.05.2002 15:05:04

Changed: 12.05.2002 15:48:25

DS version: 72(user) 0(machine)

Sysvol version: 72(user) 0(machine)

Flags: 0

User extensions: [{25537BA6-77A8-11D2-9B6C-0000F8080861}{88E729D6-BDC1-11D1-BD2A-00C04FB9603F}][{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{0F6B957E-509E-11D1-A7CC-0000F87571E3}]

Machine extensions: not found

Functionality version: 2

На что здесь стоит обратить внимание? Я бы выделил:

- ◆ дату создания (Created) и последнего изменения (Changed);
- версии контейнера групповой политики (DS version) и Sysvol;
- ◆ значение флага (Flags), показывающего, что данная политика полностью или частично деактивизирована;
- ◆ перечень клиентских расширений (User extensions);
- ◆ версию функциональности (Functionality version); это значение должно быть не менее 2.

В случае прохождения теста групповой политикой ни на что и не стоит обращать внимания, а вот если для групповой политики сообщается об ошибке, следует сравнить содержимое правил на нескольких контроллерах. Например, увидев сообщение об ошибке, приведенное выше, стоит насторожиться, так как несовпадение версий ОПП в Active Directory и в каталоге Sysvol может свидетельствовать либо о банально незавершенной репликации файловой системы или Active Directory, либо о нарушениях в работе репликации. Подробная инфор-

мация, приведенная вслед за сообщением об ошибке, позволит косвенно понять источник проблем. Взгляните:

```
DC: ROOT1.mycorp.ru
Friendly name: Restrict Environment
Created: 12.05.2002 15:05:04
Changed: 13.05.2002 19:40:18
DS version: 72(user) 1(machine)
Sysvol version: 72(user) 1(machine)
Flags: 0
User extensions: [{25537BA6-77A8-11D2-9B6C-0000F8080861}
{88E729D6-BDC1-11D1-BD2A-00C04FB9603F}][{35378EAC-683F-11D2-A89A-
00C04FBBCFA2}{0F6B957E-509E-11D1-A7CC-0000F87571E3}]
Machine extensions: [{35378EAC-683F-11D2-A89A-00C04FBBCFA2}
{0F6B957D-509E-11D1-A7CC-0000F87571E3}]
Functionality version: 2
```

```
-----
DC: ROOT2.mycorp.ru
Friendly name: Restrict Environment
Created: 12.05.2002 15:05:04
Changed: 13.05.2002 19:15:14
DS version: 72(user) 0(machine)
Sysvol version: 72(user) 1(machine)
Flags: 0
User extensions: [{25537BA6-77A8-11D2-9B6C-0000F8080861}{88E729D6-BDC1-
11D1-BD2A-00C04FB9603F}][{35378EAC-683F-11D2-A89A-
00C04FBBCFA2}{0F6B957E-509E-11D1-A7CC-0000F87571E3}]
Machine extensions: not found
Functionality version: 2
```

Хорошо видно, что на контроллере **ROOT1** была выполнена модификация политики для компьютеров. Ее файловая часть уже «дошла» до контроллера **ROOT2**, а та, что находится в Active Directory, — еще нет. Именно этим объясняется отсутствие клиентских расширений для компьютерных правил на втором контроллере.

Если повторить выполнение **gpoutil** через некоторое время, причина возникновения проблемы станет ясна. Если дело в репликации, то она никуда не исчезнет, и тогда надо будет ее устранить средствами, описанными в главах «Active Directory и файловая система» или «Репликация Active Directory».

ADDIAG

Утилита **ADDIAG** из Windows 2000 Resource Kit предназначена для сбора информации обо всех программах, установленных на компьюте-

ре с помощью технологии Windows Installer. Эта программа имеет интерфейс командной строки и предоставляет сведения:

- о зарегистрированном пользователе, включая его полномочия, и также о типе платформы;
- ◆ о терминальном режиме работы
- об установленном или опубликованном ПО, почерпнутые из реестра;
- об опубликованном ПО, взятые из Active Directory;
- ◆ о Windows Installer.

У программы масса параметров командной строки (описание см. в справочном файле). А я приведу пример выводимой информации и прокомментирую отдельные моменты. Вывод начинается с информации о пользователе, способной повлиять на установку приложений:

```
User - NameSamCompatible: MYCORP\Administrator
User - NameFullyQualifiedDN: CN=Administrator,CN=Users,DC=mycorp,DC=ru
User - Logon Server: \\R00T1
User - SID: S-1-5-21-947463027-762207816-1681286078-500
User - Profile Type: LOCAL
User - Locale: 1049
Processor Architecture: x86
System Locale: 1049
```

Среди прочего обратите внимание на региональные параметры (Locale и System Locale). Они отвечают за язык интерфейса в системе и для данного пользователя. Если устанавливаемые приложения поддерживают режим многоязыкового интерфейса, то эти параметры служат для определения языка меню и диалоговых окон.

Далее приводится режим работы терминального сервера. Хорошо известно, что приложения на сервере, работающем в режиме сервера приложений, должны устанавливаться с применением модификаторов или специальных сценариев совместимости. В то же время, если сервер работает в режиме удаленного администрирования, то установка приложений администраторами ограничена. Например:

```
Running Remote Admin TS
```

Далее идет информация обо всех установленных приложениях, взятых из реестра. Иначе говоря, эти приложения установлены в соответствии с групповой политикой. Приложения перечисляются по их номерам GUID.

```
User dump for mycorp.ru
Dumping GPO list (1 items)...
  GPO GUID: {BB0B08E9-3E4F-4EAE-AA84-188CB97B3E8F}
  Name: Install Office
```

```

Microsoft Office 2000 SR-1 Premium
Object GUID: {4CA9546D-25B3-41EC-A809-CD787B06900D}
CN: fcec044f-8e20-4883-a862-c7ea71d38660
Package Flags;
    PostBeta3
    UserInstall
    OnDemandInstall
    Assigned
    UninstallOnPolicyRemoval
Deployed on: 05/11/2002 13:05:46
Changed on: 05/11/2002 13:07:31
MsiFileList: \\root1\software\Office_2000_SR1
\data1.msi
ProductCode: {00000409-78E1-11D2-B60F-006097C998E7}
Revision Count: 0
UI Level: Basic

```

Строка Package Flags указывает на флажок, связанный с данным приложением. Значение флажка указывает текущий статус приложения:

Величина	Обозначает
0x1	Приложение назначено
0x2	Приложение опубликовано
0x4	Удалять такое же приложение, установленное иным способом, перед применением политики
0x8	Оставлять приложение после отмены групповой политики
0x10	Удалять приложение после отмены групповой политики
0x20	Оставить приложение без управления
0x40	Удалить приложение

Полное значение флажка определяется комбинацией показанных величин.

Параметр UI Level указывает на степень взаимодействия пользователя с программой установки:

Величина	Обозначает
0x0	Уровень взаимодействия не изменяется
0x1	Уровень взаимодействия принятый по умолчанию
0x2	Полностью автоматическая установка
0x3	Индикаторы процесса установки и сообщения об ошибках
0x4	Настраиваемая установка, но с запретом программ-мастеров
0x5	Полностью настраиваемая установка
0x40	Показывать только индикаторы процесса установки
0x80	Сообщать об удачной или неудачной установке

Далее перечисляются приложения, установленные не с помощью групповых правил. Если для приложения в поле Product is указано Managed, то оно было установлено с помощью Windows Installer. Если указано Unmanaged, то установка была выполнена иначе, например с помощью Systems Management Server (SMS).

```
Windows 2000 Support Tools
Product GUID: {242365CD-80F2-11D2-989A-00C04F7978A9}
Install Name: Windows 2000 Support Tools
Install Source: \\10.1.1.3\SOFTWARE\W2KSUP\1\
Install Date: 20020513
Local Source: C:\WINNT\Installer\6bb94.msi
Product is: Managed
Transforms:
Language:
Version: 0.0
Install State: UseDefaultLocalOrSource
```

Если в командной строке указать параметр /verbose, будут приведены записи из журнала приложений. Вот, например, информационное сообщение:

```
EventID: 301
Type: INFO
Date: 20:13:20.0000 - 05/13/2002
User: MYCORP\u2
Computer: W2KPRO
Source: Application Management
Description: The assignment of application Microsoft Office Web
Components from policy Install Office succeeded.
Data:
```

А вот предупреждение:

```
EventID: 1001
Type: WARN
Date: 19:32:07.0000 - 05/12/2002
User: N/A
Computer: W2KPRO
Source: MsiInstaller
Description: Detection of product '{00000409-78E1-11D2-B60F-
006097C998E7}', feature 'ProductNonBootFiles' failed during request for
component '{CC29E9CD-7BC2-11D1-A921-00A0C91E2AA2}'
Data:
```

Наконец, приводится пример сообщения об ошибке. О том, что означает такая ошибка и как с ней бороться, я расскажу дальше:

EventID: 1000

Type: ERROR

Date: 12:38:53.0000 - 05/11/2002

User: NT AUTHORITY\SYSTEM

Computer: W2KPRO

Source: Userenv

Description: The Group Policy client-side extension Application Management was passed flags (1) and returned a failure status code of (1612).

Data:

SECEDIT

Устанавливается в Windows 2000 по умолчанию и в первую очередь предназначена для работы с политикой безопасности. Утилита позволяет:

- анализировать установленные параметры безопасности путем сравнения с шаблонами;
- конфигурировать параметры безопасности по шаблонам;
- экспортировать текущие параметры в виде шаблонов,

Эти функции полностью аналогичны оснастке MMC Security Configuration and Analysis и многократно подробно описаны. Но, помимо них, есть еще две важные функции, выполняемые этой программой, которые весьма полезны при анализе и отладке групповой политики. Это обновление политики и ее проверка.

Функция обновления политики позволяет принудительно выполнить обновление правил на компьютере, не дожидаясь наступления периода обновления и не выходя из системы с повторной регистрацией. Одной командой обновляется либо политика для пользователей, либо для компьютеров. Для обновления надо выполнить:

```
secedit /refreshpolicy machine_policy | user_policy
```

Если вы не изменяли правил, но хотите повторно применить политику, то к указанной выше команде добавьте параметр /enforce.

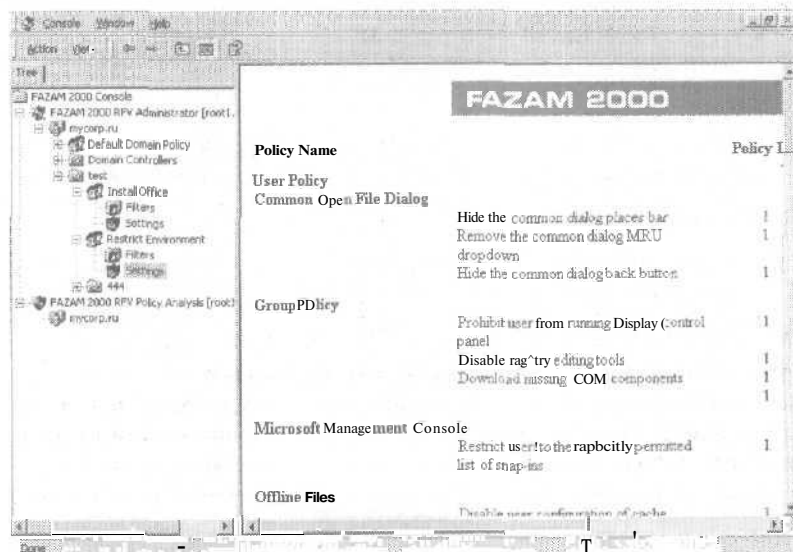
Замечание Клиент Windows XP больше не поддерживает применение команды secedit для обновления политики. Вместо этого следует использовать утилиту gpupdate.

FAZAM2000

FAZAM 2000 (Full Armor Zero Administration for Windows 2000) — очень удачный инструмент компании FullArmor. Он имеет две основные функции: диагностики и анализа. Диагностика выполняется как на локальном компьютере, так и на удаленном. Представьте, что вы за-

пускаете `gpresult`, но так, чтобы увидеть результирующий набор правил на другом компьютере и для другого пользователя.

Диагностика весьма информативна, так как не включает ничего лишнего. Сразу видно, какие правила и к каким объектам Active Directory применены.



Окно программы FAZAM2000

Функция анализа позволяет прогнозировать, что произойдет, если тот или иной пользователь будет перемещен в другое ОП или будет добавлен/исключен в какую-либо группу, а также если он зарегистрируется на другом компьютере. Такое моделирование ситуаций позволяет определить потенциальные проблемы и исключить их.

Еще одна полезная функция этого инструмента — резервное копирование и восстановление ОГП. Этой функции нет в Windows 2000, хотя без нее порой приходится трудно. Допустим, вы сформировали очень удачную групповую политику в тестовой зоне и хотите перенести ее в рабочую систему. FAZAM 2000 позволяет сделать копию политики в виде файла, перенести его в рабочую систему и там восстановить.

Журналирование

При поиске проблем важную информацию можно почерпнуть из журналов регистрации событий. Не является исключением и поиск проблем в инфраструктуре групповой политики. К счастью, в Windows 2000 хватает журналов, содержащих сведения о применении правил.

Я бы даже сказал, что журналов слишком много, поэтому далее показано, какую информацию и где искать.

Вам доступны следующие типы журналов:

- журнал событий приложений (Application Log) содержит достаточно общие сообщения о том, как выполняется обработка ОГП на рабочей станции или сервере;
- ◆ каталог %systemroot%\debug\Usermode содержит текстовые файлы с детальнейшим описанием процессов применения пользовательской политики;
- ◆ журналы Windows Installer содержат подробности установки приложений, размещенных с помощью групповой политики.

Журнал событий приложений

Журнал событий приложений должен быть первым источником информации при выявлении проблем с групповой политикой. К сожалению, по умолчанию в нем выводятся лишь самые общие сообщения — для анализа проблемы этого мало. Чтобы вывести подробную информацию, нужны изменения в реестре. В ветви HKLM\Software\Microsoft\Windows NT\Current Version надо создать еще один ключ — Diagnostics, а затем создать для него несколько параметров, определяющих степень детализации.

Параметр, тип, значение	Для чего служит
RunDiagnosticLogginGlobal REG_DWORD = 0x1	Подробная регистрация всех событий относящихся к групповой политике: перенаправление папок, обработка правил RIS, установка приложений
RunDiagnosticLogginGroupPolicy REG_DWORD = 0x1	Регистрация только общих сообщений групповой политики
RunDiagnosticLogginIntellimirror REG_DWORD = 0x1	Регистрация событий политики удаленной установки системы (RIS)
RunDiagnosticLogginAppDeploy REG_DWORD = 0x1	Регистрация событий установки приложений, определенных в политике

Эти параметры нужно добавить на всех серверах и рабочих станциях, на которых выполняется диагностика. Дабы облегчить труд, это можно сделать посредством административного шаблона. Шаблон добавляет параметр RunDiagnosticLogginGlobal (о том, как добавить этот шаблон, см. [1]):

```
CLASS MACHINE
    CATEGORY !!Custom
        POLICY !!GPOLogging
            KEYNAME "Software\Microsoft\Windows NT\CurrentVersion\Diagnostics"
            EXPLAIN !!GPOLogging_Help
```

```

VALUENAME "RunDiagnosticLoggingGlobal"
VALUEON NUMERIC 1
VALUEOFF NUMERIC 0
END POLICY
END CATEGORY; Custom

```

[strings]

GPOLogging="Включить подробное журналирование групповой политики"

GPOLogging_Help="Данная политика позволяет включить подробное журналирование всех событий, связанных с применением групповой политики."

Custom="Custom Preference"

События, связанные с групповой политикой, заносятся в журнал от имени одного из трех источников:

◆ *Userenv* отвечает за перечисление *ОПГ* и выявление всех, что не были применены;

- Application Management — источник событий, связанных с установкой приложений;

4 *Scecli* отвечает за события политики безопасности.

В ряде случаев в сообщении фигурирует фраза типа: «The Group Policy client-side extension Security was passed flags (17) and returned a failure status code of (1332)» [«Клиентскому расширению групповой политики был передан флаг (17) и получен код статуса ошибки (1332)»]. Такое сообщение исходит от источника *Userenv* и имеет Event ID=1000. Как его интерпретировать?

Начнем с выяснения того, что же за флаг был передан. Возможны следующие значения флага:

Значения флага групповой политики и их смысл

Значение флага (шестнадцатеричное и десятичное)	Смысл
0x00000001 (1)	Применяемая политика является компьютерной (не пользовательской)
0x00000010 (16)	Фоновое обновление политики
0x00000020 (32)	Политика применяется по медленному каналу
0x00000040 (64)	Установлена политика подробного вывода информации в журнал
0x00000080 (128)	С момента последнего цикла применения политики не обнаружено <i>никаких</i> изменений
0x00000100 (256)	Скорость канала связи изменилась с момента последнего применения групповой политики

Значения, приведенные в журнале регистрации, являются десятичными и получаются в результате побитового ИЛИ указанных в таблице величин. Так, в примере 17 образуется из сложения 16 и 1, т. е. это

сообщение о том, что компьютерные правила были применены в фоновом режиме.

Разобравшись с флагами, нетрудно понять и код статуса ошибки. Все, что нужно для этого сделать, — выполнить;

```
net helpmsg <номер кода>
```

В нашем примере код 1332 соответствует сообщению «No mapping between account names and security IDs was done» (Не было назначено соответствие между SID и именем учетной записи).

Если, даже раскрыв содержание ошибки, вы не поняли причины, по которой она произошла, то самое время заняться изучением журналов политики для пользователей.

Журналы политики для пользователей

Если не менять параметров в реестре, то в каталоге `Usermode` вы обнаружите только файл `userenv.log`, причем небольшого размера и совершенно неинформативный. Для целей диагностики нужно изменить значения параметров в реестре.

Замечание По умолчанию указанные параметры могут отсутствовать в реестре. Создавая их, учтите, что все они типа `REG_DWORD`.

Параметры, вносимые в реестр для активизации подробного журналирования

Что будет регистрироваться	Параметр и его величина
Трассировка применения групповой политики и обработка профиля пользователя. Данные заносятся в файл <code>userenv.log</code>	<code>HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\UserEnvDebugLevel = 0x10002</code>
Регистрация ошибок на клиентской стороне, возникающих при редактировании ОГП. Заносится в журнал <code>gpedit.log</code>	<code>HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GPEditDebugLevel = 0x10002</code>
Регистрация загрузки файлов административных шаблонов в файле <code>gpext.log</code>	<code>HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GPTextDebugLevel = 0x10002</code>
Регистрация событий, связанных с перенаправлением папок в файле <code>fdeploy.log</code>	<code>HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics\FDeployDebugLevel = 0x0f</code>
Регистрация событий, связанных с установкой ПО в файле <code>appmgmt.log</code>	<code>HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics\AppmgmtDebugLevel = 0x9b</code>

Вы можете удивиться: зачем модифицировать какие-то потайные параметры в реестре вместо того, чтобы использовать привычные элементы интерфейса или групповую политику! Затем, что поток инфор-

мации, который хлынет в журналы после модификаций, будет таков, что сразу скажется на производительности системы, а со временем — переполнит жесткие диски.

Не думайте, что, включив подробное журналирование, вы сразу обнаружите причину проблем с групповой политикой. Придется попотеть и, возможно, потратить не один час на то, чтобы продрасть сквозь дебри информации в этих файлах. Не верите? Тогда взгляните на пример выводимой информации в файле `userenv.log`. Я не привожу всей информации, так как это слишком много для этой книги.

Обратите внимание на такую неприятную вещь, как отсутствие дат: в тексте только время. Дабы понять, какие события произошли недавно, надо посмотреть в конец файла, так как в отличие от большинства журналов регистрации события здесь пишутся в конец.

Начинаются записи с сообщения о начале обработки групповой политики и определения роли компьютера. Фраза `PingComputer` означает, что эта функция вызвана на рабочей станции, чтобы определить скорость канала связи. В следующей строке дается заключение о том, что канал быстрый, т. е. будут обрабатываться все клиентские расширения политики.

```
USERENV(cc.580) 20:04:46:870 ProcessGPOs: Starting computer Group
Policy processing...
USERENV(cc.580) 20:04:46:680 EnterCriticalPolicySection: Machine
critical section has been claimed. Handle = 0x5d4
USERENV(cc.580) 20:04:46:980 ProcessGPOs: Machine role is 3.
USERENV(cc.580) 20:04:46:890 PingComputer: First time: 0
USERENV(cc.580) 20:04:46:890 PingComputer: Fast link. Exiting.
```

Теперь — регистрация имени учетной записи компьютера, имени домена и его контроллера и сообщение о вызове функции `GetGPOInfo` в нормальном режиме обработки политики.

```
USERENV(cc.580) 20:04:46:900 ProcessGPOs: User name is:
CN=ROOT1,OU=Domain Controllers,DC=mycorp,DC=ru, Domain name is: HYCORP
USERENV(cc.580) 20:04:46:900 ProcessGPOs: Domain controller is:
\\ROOT1.mycorp.ru Domain DN is mycorp.ru
USERENV(cc.580) 20:04:46:910 ProcessGPOs: Calling GetGPOInfo for normal
policy mode
```

Далее по очереди выполняется поиск **ОГП** в Active Directory и в каталоге SYSVOL.

```
USERENV(cc.580) 20:04:47:250 ProcessGPO: =====
USERENV(cc.580) 20:04:47:260 ProcessGPO: =====
USERENV(cc.580) 20:04:47:260 ProcessGPO: Searching <CN={6AC1786C-016F-
```

```

11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=mycorp,DC=ru>
USERENV(cc.580) 20:04:47:260 ProcessGPO: Machine has access to this GPO.
USERENV(cc.580) 20:04:47:260 ProcessGPO: Found functionality version
of: 2
USERENV(cc.580) 20:04:47:260 ProcessGPO: Found file system path of:
<\\mycorp.ru\\sysvol\\mycorp.ru\\Policies\\{6AC1786C-016F-11D2-945F-
00C04FB984F9}>
USERENV(cc.580) 20:04:47:280 ProcessGPO: Found common name of:
<{6AC1786C-016F-11D2-945F-00C04FB984F9}>
USERENV(cc.580) 20:04:47:280 ProcessGPO: Found display name of:
<Default Domain Controllers Poltcy>
USERENV(cc.580) 20:04:47:280 ProcessGPO: Found machine version of:
GPC is 2, GPT is 2
USERENV(cc.580) 20:04:47:280 ProcessGPO: Found flags of: 0
USERENV(cc.580) 20:04:47:280 ProcessGPO: Found extensions:
[{827D319E-6EAC-11D2-A4EA-00C04F79F83A}{803E14A0-B4FB-11D0-A0D0-
00A0C90F574B}]

```

Вся приводимая информация практически идентична той, что мы рассматривали в разделе, посвященном утилите GPOTool. И впрямь: в следующем фрагменте показано, как в реестре определяется, были ли изменения с момента применения правил в последний раз:

```

USERENV(cc.580) 20:04:47:310 ProcessGPOs: Processing extension Registry
USERENV(cc.580) 20:04:47:310 CompareGPOLists: The lists are the same.
USERENV(cc.580) 20:04:47:310 CheckGPOs: No GPO changes and no security
group membership change and extension Registry has NoGPOChanges set.
Далее идут сообщения об обработки клиентских расширений.
USERENV(cc.580) 20:04:47:321 ProcessGPOs: Processing extension Folder
Redirection
USERENV(cc.580) 20:04:47:321 ProcessGPOs; Extension Folder Redirection
skipped with flags 0x10007.

```

Заканчивает эту порцию информации сообщение о том, что политика была применена, и о том, когда она будет применена в следующий раз. Наш компьютер является контроллером домена, значит, Default domain controllers policy будет применена через 5 минут.

```

USERENV(cc.580) 20:04:47:371 ProcessGPOs: Computer Group Policy has
been applied.
USERENV(cc.580) 20:04:47:381 ProcessGPOs: Leaving with 1.
USERENV(cc.580) 20:04:47:381 GPOThread: Next refresh will happen in 5
minutes

```

И ничего страшного! Дело за малым — найти нужную информацию.

Журналы установки приложений

Рассмотрим последний тип журналов — журнал работы Windows Installer. Чтобы управлять объемом регистрируемой информации, не надо прибегать к модификации параметров реестра вручную. Для этого существует правило Logging из раздела Windows Components\Windows Installer шаблонов компьютерной политики. Оно хорошо документировано и не нуждается в дополнительных комментариях.

Выводимая информация идентична той, что выводит программа addiag. Только в отличие от последней вы можете управлять степенью подробности.

Общие проблемы групповой политики

Рассмотрим теперь характерные ошибки и способы борьбы с ними, отбросив те, что связаны с невнимательностью или забывчивостью администратора.

Зависание компьютера при регистрации пользователя или запуске компьютера

Возможная причина	Способы решения
Причин может быть несколько, но наиболее вероятная — неправильная политика сценариев. Например, вы определили сценарий запуска компьютера, требующий взаимодействия с пользователем, но забыли разрешить использование таких сценариев	Проверьте доступность файлов сценариев. Возможно, вы указали неверный путь к ним, или сервер, на котором они расположены, недоступен. Попробуйте выполнить сценарии в тестовом режиме. Посмотрите, требуют ли они взаимодействия с пользователем. Если да, то разрешите применение таких сценариев. Измерьте время выполнения каждого из сценариев. Возможно, оно превышает установленный тайм-аут. Если это так, подкорректируйте соответствующую политику

Определенная политика не обрабатывается полностью или частично

Возможная причина	Способ решения
Наиболее вероятные причины: неправильные права доступа к контейнеру (КГП) или шаблону (ШГП) групповой политики, КГП и ШГП рассинхронизированы, ОП сконфигурирован так, что обрабатывается только после внесения изменений	Проверьте права доступа к КГП и ШГП. В списках контроля доступа должны присутствовать учетные записи тех групп пользователей и компьютеров, для которых политика предназначена. Они должны иметь разрешения Read и Apply Group Policy. Для проверки синхронности КГП и ШГП примените Gpoutil. Если рассинхронизация имеет место, выясните причину. Используйте Replication

см. след. стр.

Возможная причина	Способ решения
Компьютер, к которому применяется политика, обнаружил медленный канал связи с контроллером домена	Monitor (см. главу «Репликация Active Directory»). Чтобы понять, выполняется ли какая-либо часть политики, посмотрите историю политики (раздел «История применения правил»). Если нужно, чтобы политика применялась независимо от того, был ли изменен ОПП, установите соответствующее правило (см. раздел «Применение неизменной политики»)
Испорчена/отсутствует динамическая библиотека, ответственная за обработку клиентского расширения групповой политики	Проверьте по файлу userenv.log, действительно ли это так. Если канал медленный, политика должна быть применена, измените соответствующее правило. (См. раздел «Обработка по медленным каналам связи») Проверьте, что все клиентские расширения зарегистрированы на компьютере путем сравнения содержимого ветви HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions на проблемном и исправном компьютерах. Убедитесь, что все указанные динамические библиотеки присутствуют в каталоге %systemroot%\system32

Обрабатывается не тот ОПП

Возможная причина	Способ решения
Причин может быть несколько. Например, компьютер может считать, что он находится в другом сайте и поэтому получать другую политику. Возможно, используются переключки правил (см. раздел «Переключки»)	Проверьте принадлежность компьютера к сайту, выполнив команду nltest. Если сайт не верен, то разрешите эту проблему с помощью оснастки Active Directory Sites and Services Проверьте, что для компьютера, на котором зарегистрирован пользователь, не установлена политика Loopback (переключка). Сделать это можно, посмотрев значение параметра UserPolicyMode в ветви реестра HKLM\Software\Policies\Microsoft\Windows\System. Если оно равно 1 или 2, то используется переключка
ОПП связан не с тем контейнером	Такое происходит по рассеянности администратора. Проверьте, с какими объектами в Active Directory связан указанный ОПП

Политика вообще не применяется

Возможная причина	Способ решения
Причин не так уж много. 1. Вы забыли связать ОПГ с каким-либо объектом Active Directory. 2. Рассинхронизация паролей между компьютером и контроллером домена. 3. Проблемы с разрешением имен DNS. 4. Проблемы с репликацией Active Directory или NTFRS	Для начала проверьте наличие связи. Если она все-таки есть, проверьте состояние компьютера используя утилиты netdom или nltest. При необходимости синхронизируйте пароли. Проверьте разрешение имен утилитой Nslookup (см. главу «Установка Active Directory»). Выясните как работает репликация (см. главы «Репликация Active Directory» и «Active Directory и файловая система»). Что касается рассинхронизации паролей, то она может возникать в парадоксальной ситуации. Положим, вы открыли терминальный сеанс на контроллере домена, зарегистрировавшись как администратор. Спустя некоторое время вы изменили пароль администратора, используя оснастку Active Directory Users and Computers на другом контроллере. Именно с этого момента возникнет рассинхронизация паролей между открытым терминальным сеансом и контроллером, на котором он открыт. Как следствие, пользовательская политика не будет применяться на этом контроллере к администратору. В журнале событий появится сообщение с Event ID=1000 и не содержащее упоминаний о флагах (см. выше) вообще. Для разрешения достаточно закрыть терминальный сеанс, а потом открыть его заново

Заключение

Ну вот, еще одна глава позади. Прочитав ее, кто-то скажет: «Зачем столько подробностей? Правила — они и в Африке правила. Надо будет — открою Windows 2000 Server Resource Kit и прочитаю». Так-то оно так, но есть вещи, которые теряются в таких толстых книгах. Я же собрал здесь в концентрированном виде то, без чего не стоит и думать о групповой политике. Но не вздумайте, что теперь вам море по колено! Упаси вас Бог братья за нее, не прочитав главу «Проектируем Active Directory». Я уж не говорю о главе «Репликация Active Directory», о системе безопасности, тиражировании NTFRS и т. д. Короче, читайте и разбирайтесь.

Active Directory и файловая система

Прочитав название главы, кто-то решит, что речь пойдет о файлах Active Directory, о том, как они хранятся на диске и как с ними работать. Но это не так. Во-первых, о файлах базы Active Directory рассказано в главе «Установка Active Directory», а о том, как поддерживать их целостность и исправлять, — в главе «Ищем и устраняем проблемы». Во-вторых, в Windows 2000 хватает *служб*, которые активно используют файловую систему и воздействуют на нее и в то же время неразрывно связаны с Active Directory. Можно, конечно, упомянуть службу безопасности Windows 2000, тесно интегрированную с Active Directory, но вопросы безопасности прекрасно разобраны в существующей литературе (см. [1], [3]). Та служба, без описания которой эта книга была бы неполной, — это служба репликации файловой системы NTFRS (далее — служба FRS). Она неразрывно связана со службой репликации Active Directory и частенько упоминалась в соответствующей главе. Не менее часто на нее я ссылался в главе «Групповая политика». Наконец, о ней я упоминал в главе «Установка Active Directory*». Пора поговорить о ней подробнее.

Очень тесно с FRS связана служба распределенной файловой системы (DFS). А так как DFS связана и с Active Directory, то не рассказать о ней в этой книге нельзя. Однажды я уже описывал работу DFS довольно подробно в [1], так что здесь я шире осветю те вопросы, о которых ранее лишь упоминал.

Служба репликации файловой системы

Как вы знаете, программа DCPROMO создает каталог SYSVOL в котором расположены файлы групповой политики Windows 2000, системной политики Windows 9x/NT, файлы сценариев и ряд других файлов, присутствие которых необходимо для нормальной работы Active Directory. Содержимое каталога SYSVOL должно быть идентичным на всех контроллерах в домене, а это значит, что должен существовать механизм репликации файлов.

В главе «Репликация Active Directory» я подробно разобрал механизм репликации объектов Active Directory. Механизм репликации файлов во многом похож на него, но не во всем.

Как распространяются изменения

При распространении изменений атрибутов объектов Active Directory используется номер последовательного обновления USN объекта, и практически не используется время изменения объекта. Репликация FRS осуществляется аналогично.

Когда на одном из контроллеров домена происходит изменение в файле, он передается всем партнерам по репликации (причем целиком, даже если изменился всего 1 байт). Партнеры должны решить, принять этот файл или отвергнуть.

Рассмотрим этот алгоритм на примере. Пусть в домене два контроллера: А и Б. Файл, измененный на контроллере А, передается на контроллер Б. Для каждого файла хранится метка в которой записано время его последней модификации. Итак, контроллер Б принял файл...

- Если на контроллере А файл изменился на 30 минут позже, чем на контроллере Б, то изменение (т. е. файл) принимается безоговорочно. Если на контроллере А файл изменился на 30 минут раньше, чем на контроллере Б, файл отвергается. Таким образом, если между двумя контроллерами не выполнялась репликация FRS более 30 минут, а изменения вносились на обоих контроллерах, то после восстановления репликации результирующими будут изменения, сделанные позже.
- ◆ Если разница во времени изменения на обоих контроллерах не превышает 30 минут, используется дополнительная проверка. Для начала сравниваются версии файлов. Под версиями понимается значение, аналогичное номеру USN и поддерживаемое на контроллерах для каждого файла. Если версия файла на контроллере А меньше версии на контроллере Б, изменение отвергается, если же больше — принимается. (Как видим, это в точности соответствует сравнению номеров USN при репликации атрибутов Active Directory.)

- ◆ Когда номера версий совпадают, сравнивается точное время изменения файла. Побеждает тот контроллер, на котором файл был изменен позже.
- ◆ Если случится (хоть это и маловероятно), что времена изменения файла совпадают, сравниваются размеры файлов на двух контроллерах — больший будет взят за основу.
- ◆ Наконец, если и размер файлов одинаков, сравниваются номера GUID контроллеров домена — чей номер GUID больше, тот и победит.

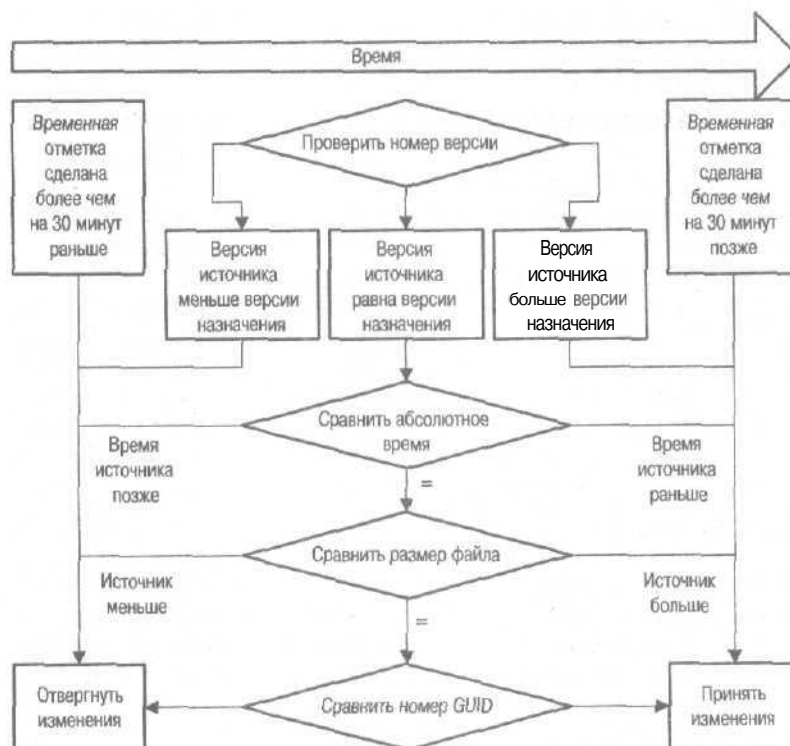


Схема распространения изменений

Описанный алгоритм отличается от алгоритма разрешения конфликтов при репликации Active Directory только в сравнении размера файла. Все остальные критерии совпадают.

Инициация тиражирования

Репликация FRS иницируется при изменении файла в каталоге SYSVOL. Это весьма похоже на инициацию репликации Active Directory. Если продолжить сравнение дальше, то репликация между сайтами иници-

ируется по расписанию. Как и репликация Active Directory, репликация FRS выполняется по умолчанию, конфигурировать ее не надо.

Совсем иное дело — репликация отказоустойчивых томов DFS. Репликация FRS используется и в этом случае, но имеет ряд особенностей.

- Репликация FRS применима только к доменным томам DFS (см. [1]).
- 4 Служба NTFRS установлена только на серверах Windows 2000; на контроллерах домена она запущена по умолчанию, а на членах домена запускается по требованию. Для репликации DFS надо явно указать, как ее выполнять.
- Изменение времени сохранения файла или каталога не инициирует репликации DFS,
- Изменение атрибута архивирования папки не инициирует репликации DFS. Это и предыдущие условия указывают на необходимость выполнения репликации по расписанию.
- + Репликация DFS выполняется по собственному расписанию. Окно репликации жестко определяет допустимое время тиражирования файлов. Если к моменту закрытия окна репликация не была завершена, то в отличие от репликации Active Directory тиражирование файлов будет прервано до следующего окна.
- Расписание тиражирования DFS можно создать как для объекта связи, так и для набора реплик. Расписание, созданное для объекта связи, имеет преимущество. Однако если набор реплик содержит большое число реплик, проще назначить расписание целому набору, чем заниматься этой работой для каждого объекта связи.

Чтобы репликация файлов DFS работала, надо соблюсти следующие условия.

- ◆ Совместно используемый каталог DFS должен находиться на томе с файловой системой NTFS v.5. Это связано с тем, что для работы FRS нужен журнал изменений NTFS, где записываются изменения файлов. Если компьютер был выключен до репликации, это не страшно, так как все изменения по-прежнему хранятся в журнале NTFS.
- ◆ Совместно используемый каталог DFS не должен располагаться на кластере.
- Компьютер с каталогом DFS должен быть членом домена Windows 2000.

Избыточность

Репликация FRS обеспечивает избыточность для каталога SYSVOL и для DFS. Избыточность заключается в следующем.

- Обеспечивается существование идентичных каталогов, доступ к которым, с точки зрения пользователя, непрерывен. Пользователь

не может определить в каждый момент времени, к какому каталогу он обращается. При выходе из строя любого каталога пользователь автоматически подключается к другому, входящему в избыточный набор.

- Может быть задействовано несколько путей тиражирования изменений в каталогах. Если один из путей недоступен, используется другой. Механизм демпфирования препятствует возникновению бесконечных циклов репликации и обеспечивает однократную передачу изменений между двумя контроллерами при наличии нескольких путей тиражирования.

Когда удобно использовать репликацию FRS

Дочитав до этого места, вы, наверное, задумались о практическом применении FRS и пришли к выводу, что обеспечиваемый доступ к данным далек от того, который предоставляют специализированные решения.

Обратите внимание на то, как **реплицируются** файлы. Если два пользователя одновременно работают над одним документом, хранящимся в разных репликах, то механизма, объединяющего сделанные ими **изменения**, не существует. Если в одной реплике пользователь А **добавил** к документу 10 страниц, а в другой пользователь Б **удалил** 4 страницы, но сделал это на 10 минут позже, то после репликации в документе будет на 4 страницы меньше.

Открытый файл не реплицируется, а это чревато неприятностями. Допустим, пользователь создавал документ в течение нескольких дней в Microsoft Word. Все это время он держал документ открытым. Наконец, сохранив его, **пользователь закрыл Word**. И тут же вспомнил, что забыл поставить многоточие в эпиграфе. Открыв документ, он ставит нужный знак, сохраняет файл и... теряет плоды своего многодневного труда. Вы, конечно, поняли, что, вторично открыв документ, пользователь обратился к другой реплике, до которой еще не дошли изменения. Так как ему было нужно самое начало документа, **пользователь** не удостоверился в том, что это тот файл, что ему нужен (точнее, ему и в голову это не пришло). Эта реплика стала авторитетной — ведь версии документа совпали, а время сохранения оказалось более поздним.

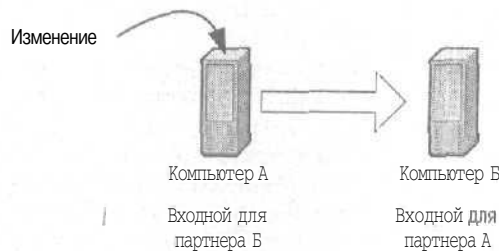
Следует обратить внимание и на то, когда выполняется репликация. Представим два **сайта**, связанных небыстрым каналом связи. В целях оптимального использования пропускной способности **расписание** репликации составлено так, что изменения файлов тиражируются только по ночам. А значит, все, что заносится в файл в одном сайте, станет доступно в другом только **ночью**, а реально — на следующее утро, когда пользователи выйдут на работу.

Что из всего сказанного следует? А вот что.

- Репликация **FRS** — идеальный вариант для редко изменяемых данных, например, файлов групповой политики, сценариев, обязательных профилей пользователей (все они расположены в каталоге **SYSVOL**), а также дистрибутивов программ, применяемых групповыми правилами для установки на клиентские компьютеры, всевозможных справочников и нормативных документов, размещенных в каталогах **DFS**.
- ◆ Репликация **FRS** не годится для тиражирования файлов БД (они обычно имеют большой размер и тиражируются полностью при любой модификации), персональных каталогов пользователей (документы пользователей часто изменяются) и любой иной часто обновляемой информации.

Работа службы **FRS** в подробностях

В первую очередь следует уяснить, какой партнер является входным для другого, а какой — выходным. Если имеются два компьютера — партнера по репликации А и Б и изменение выполняется на компьютере А, то он является *входным партнером* для компьютера Б, а тот — *выходным партнером* для компьютера А. (Выходной значит не «бездельник», а «стоящий на выходе».) Если изменение происходит на компьютере Б, то он становится входным партнером для компьютера А, а тот — выходным для компьютера Б.



Входной и выходной партнеры

Для тиражирования изменений между компьютерами должны существовать объекты связи. Объекты связи **однонаправленны**. Если изменение надо передавать от компьютера А к компьютеру Б и наоборот, то должны быть созданы два встречно направленных объекта связи.

Для каждого набора реплик должен быть создан список партнеров по репликации. Репликация каталога **SYSVOL** использует ту же топологию и тех же партнеров по репликации, что и **Active Directory**. То есть партнеры определяются **KCC** автоматически. Когда **FRS** используется

для репликации томов DFS, администратор вручную указывает партнеров и топологию.

До сих пор все было весьма похоже на репликацию Active Directory. А теперь различия.

Служба FRS является полностью многопоточной. Это значит, что один партнер по репликации способен одновременно принимать изменения от нескольких своих партнеров. Напомню, при репликации Active Directory многопоточной является только исходящая репликация, при которой изменения забираются одновременно несколькими партнерами. Входящая репликация является последовательной. В каждый момент времени принимаются данные только от одного партнера.

Служба FRS постоянно следит за журналом NTFS и отслеживает моменты закрытия файлов. Когда файл закрывается, партнеры по репликации оповещаются об изменении. Сам измененный файл при этом копируется в *подготовительный каталог*, в котором файлы временно хранятся, пока их не заберут партнеры по репликации. Необходимость в таком каталоге очевидна.

- ◆ Крупный файл тиражируется значительное время, в течение которого файл заблокирован для доступа. Дабы пользователи не испытывали неудобств, файл быстро копируется в подготовительный каталог.
- ◆ Если при тиражировании произойдет обрыв канала, пользователи могут получить неполный файл. Избежать этого позволяет промежуточное хранилище — подготовительный каталог.

После того как партнеры забирают файл из промежуточного каталога, тиражирование считается завершенным, и файл удаляется из промежуточного каталога.

Замечание Если какой-либо из партнеров длительное время не забирает причитающиеся ему изменения (например, выключен), то промежуточный каталог не очищается, и его размер растет, пока не достигнет максимально установленного значения. После этого работа службы FRS прекращается. Поскольку такая ситуация нежелательна, в SP3 внесено изменение, в соответствии с которым промежуточный каталог начинает освобождаться от «старых» файлов при достижении им 90% от максимально допустимого объема.

Выходная репликация

Выходная репликация начинается с момента занесения в журнал NTFS записи об изменении файла на *партнере-инициаторе* (для всех своих партнеров по репликации это входной партнер).

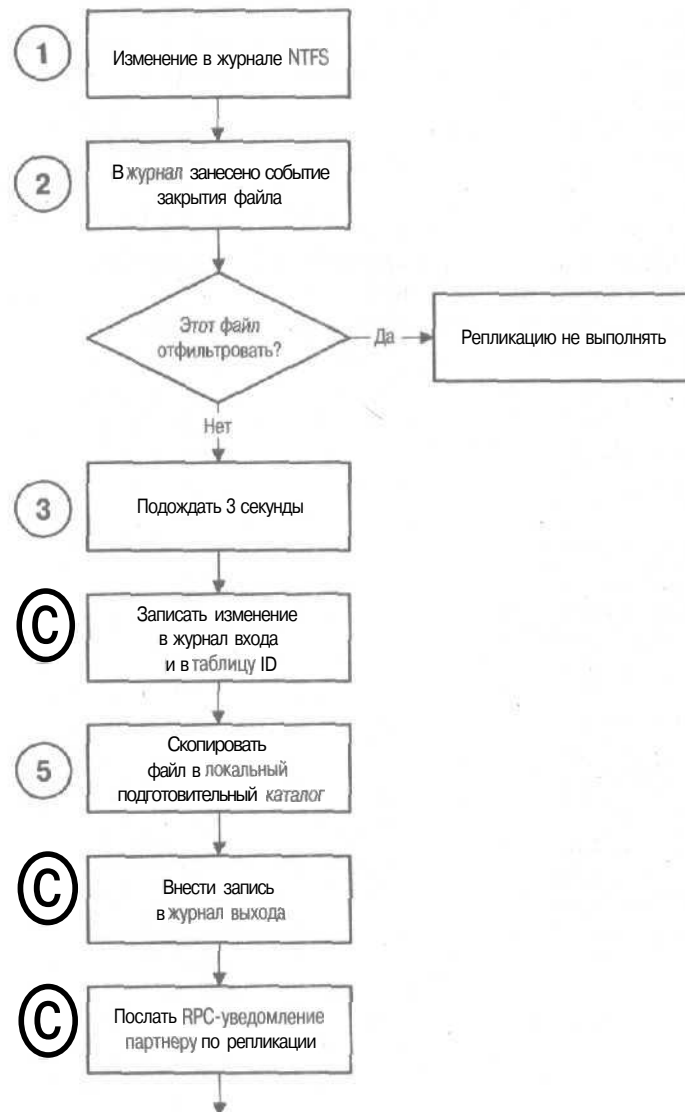
Все этапы показаны на рисунке.

1. Все, что заносится в журнал NTFS, сохраняется даже при перезагрузке и крахе ОС. Это обеспечивается транзакционностью записей. Объем этого журнала ограничен, но достаточен для работы службы FRS. При необходимости его можно увеличить.
2. Служба FRS выполняет постоянный мониторинг записей в журнале. Как только обнаруживается, что файл закрылся, выполняется проверка, нет ли его в списке исключаемых из процесса репликации. Все исключения записаны в фильтрах (см. о них ниже).
3. Если файла нет в фильтре, выдерживается пауза в 3 секунды, чтобы в файл были занесены последующие быстрые обновления.
4. В журнал входа заносится запись об изменении, указывающая, в каком порядке относительно других изменений было сделано данное. Это требует небольшого пояснения. Дело в том, что в этот журнал заносятся данные обо всех изменениях, поступивших от партнеров по репликации. Эти данные будут использованы для разрешения конфликтных ситуаций. Одновременно в таблицу идентификаторов заносятся сведения, необходимые для восстановления в случае краха ОС.
5. Копия измененного файла создается в подготовительном каталоге.

Замечание После установки SP2 поведение несколько изменяется. Если файл изменяется несколько раз в течение короткого срока, то в подготовительный каталог кладется только его последняя версия. Дополнительно файл в подготовительном каталоге сжимается.

6. Выполняется запись в журнал выхода, в котором регистрируется последовательность изменений, выполненных на локальном компьютере для определенной реплики. Источником изменений могут служить как локальные, так и поступившие с других партнеров по репликации.
7. Партнеры по репликации уведомляются об изменении. Для рассылки служит защищенный механизм RPC, использующий протокол Kerberos для аутентификации и шифрования передаваемых данных.

С этого момента забудем об источнике — переместимся на компьютер-приемник.



Алгоритм репликации на партнере-инициаторе

Входная репликация

Получив уведомление об изменении, партнер-приемник (для партнера-отправителя это выходной партнер) делает следующее.

1. Запрашивается файл. Файл передается по сети без сжатия.

Замечание После установки SP2 тиражируемый файл по сети передается в сжатом виде.

2. Информация о файле заносится в журнал входа и таблицу идентификаторов.
3. Файл копируется в локальный подготовительный каталог.
4. Информация заносится в журнал выхода для оповещения партнеров по репликации об изменении.
5. Измененный файл создается в предустановочном каталоге, а затем переносится в нужное положение на диске.

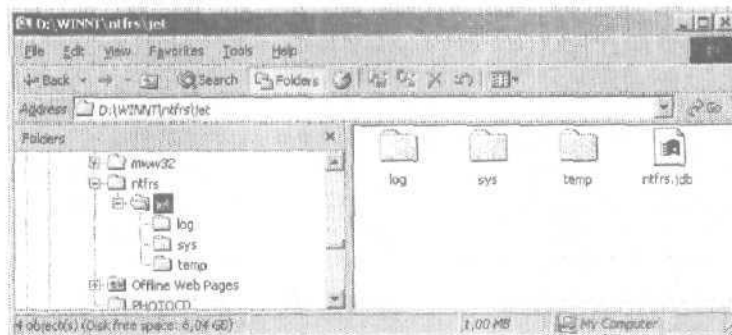
На этом репликация завершается. Как видите, процесс довольно прямолинеен. Пояснения требуют таблицы FRS и журналы в них.



Алгоритм репликации на партнере-приемнике

Таблицы службы FRS

В каталоге %systemroot%\ntfrs\jet хранятся файл ntfrs.jdb и ряд каталогов. Расширение .jdb указывает на то, что это файл БД Jet. Он содержит таблицы службы FRS для каждого набора реплик. В каталоге log расположены файлы edb.log (журнал транзакций) и два файла res1.log и res2.log, которые служат для резервирования места на жестком диске. В каталоге Sys лежит файл edb.chk — список контрольных точек. Такое устройство БД полностью аналогично устройству базы Active Directory ntds.dit.



В этом каталоге хранится база транзакций NTFRS

В файле ntfrs.jet хранятся следующие таблицы.

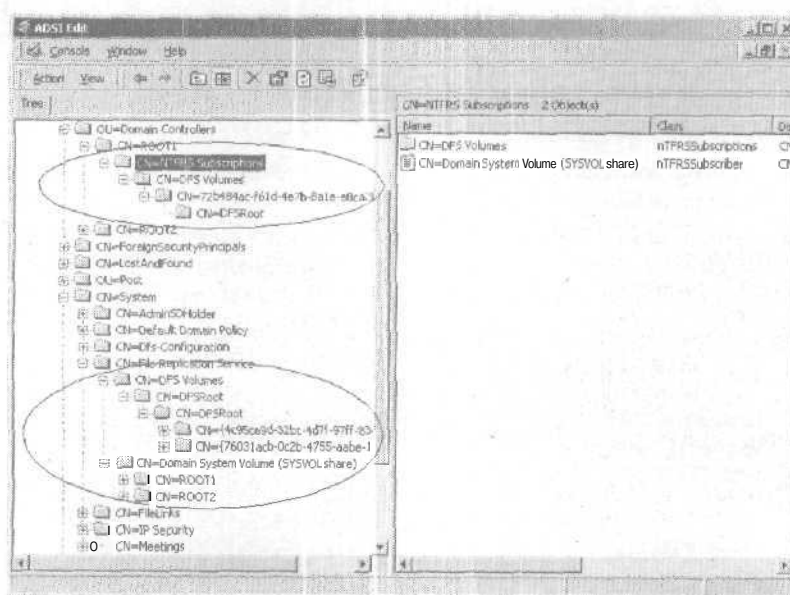
- ◆ **Таблица соединений** — по одной записи для каждого партнера по репликации
- **Журнал входа** содержит очередь изменений, которые должны быть сделаны на данном компьютере. Как только выполняется очередное изменение, партнерам по репликации рассылаются уведомления.
- ◆ **Журнал выхода** содержит очередь изменений, которые должны быть переданы всем партнерам по репликации. Записи остаются в журнале, пока все партнеры не сообщат о том, что приняли изменения. Очевидно, что при неблагоприятных условиях размер журнала может оказаться весьма большим.
- **Вектор версии (Version Vector)** аналогичен вектору обновленности репликации Active Directory. Представляет собой массив чисел, указывающих на изменения, полученные от каждого из партнеров — источников изменений. При определенных условиях вектор версии посылается входному партнеру, чтобы тот решил, какие изменения переслать, а какие нет.
- ◆ **Таблица D** содержит список всех файлов в наборе реплик, с которыми имеет дело служба FRS. Каждая запись состоит из номера

GUID, идентификаторов имени файла, родительского файла и объекта файла, а также номера версии и времени события.

Объекты **Active Directory**, используемые FRS

Служба FRS использует Active Directory для хранения нужных ей сведений о расположении файлов БД, каталогов, включенных в набор реплик, о фильтрах и т. п. Для хранения служат специальные объекты и атрибуты. Но прежде чем рассказать о них, я объясню пару терминов, используемых при рассмотрении службы репликации файлов.

Чтобы некоторые файловые объекты задействовали службу FRS, организуется *подписка* на услуги. Объекты реплик, использующие службу FRS для тиражирования данных, называются *подписчиками*. Каждый сервер, на котором работает служба FRS, имеет собственную подписку, а в каждой подписке может быть свое количество подписчиков. Сведения о подписках и подписчиках хранятся в контейнере <имя домена>\Domain Controllers\<имя сервера>\NTFRS Subscriptions. Контейнер является объектом класса ntFRSSubscriptions, а подписчики — объектами класса NtFrSubscriber. По умолчанию подписчиками являются объекты каталогов SYSVOL на контроллерах домена.



Объекты репликации FRS

Если вы **сконфигурировали** отказоустойчивую доменную DFS, то к подписчикам добавятся объекты реплик каталогов DFS. Причем рас-

полагаться они будут в том же контейнере, что и объекты SYSVOL, но не сразу, а во вложенных контейнерах \DFS Volumes\<номер GUID>\имя тома DFS. Все эти контейнеры также являются объектами класса ntFRSSubscriptions. Из атрибутов этих объектов интерес представляют, пожалуй, два:

- frsVersion может содержать номер версии;
- ◆ frsWorkingPath содержит путь к базе NTFRS.

Дополнительную информацию о подписчиках можно узнать, изучив атрибуты объектов класса NtFrsSubscriber:

- ◆ frsRootPath указывает путь к корню реплики;
- frsStagingPath указывает путь к подготовительному каталогу реплики;
- frsMemberReference указывает на объект — член набора реплик, которому он принадлежит.

Поясню на примере. Допустим, на контроллере домена root1.mycorp.ru система установлена в каталог c:\winnt, а остальные параметры приняты по умолчанию. Значения перечисленных атрибутов в этом случае:

```
frsWorkingPath = «c:\winnt\ntfrs»;
frsRootPath = «c:\winnt\sysvol\domain»;
frsStagingPath = «C:\WINNT\SYVOL\staging\domain»;
frsMemberReference = «CN=ROOT1,CN=Domain System Volume
(SYSVOL share),CN=File Replication Service,CN=System,DC=mycorp,DC=ru».
```

Как видите, последний атрибут указывает еще на один контейнер в Active Directory, содержащий сведения о службе FRS. Замечу, что это место более предсказуемо, так как контейнер System (а речь идет о нем) хранит данные о системных объектах. Именно в нем расположен контейнер File Replication Service. Если DFS не сконфигурирована, то в этом контейнере помещается только объект Domain System Volume (SYSVOL share). Большого интереса он не представляет. Другое дело, если сконфигурирована доменная DFS. Тогда к упомянутому объекту добавляется иерархия объектов:

```
сп=DFS Volumes (класс ntFRSSettings)
  сп=<имя корня DFS> (класс ntFRSSettings)
    сп=<номер набора реплик DFS> (класс ntFRSReplicaSet)
      сп=<номер GUID члена реплики> (класс ntFRSMember)
        сп=<номер GUID объекта связи> (класс ntDSCConnection)
      ...
    сп=<имя реплики DFS>
  ...
```

Эту информацию можно использовать для построения топологии репликации DFS.

Четыре атрибута связывают членов FRS с объектами-подписчиками:

1. Объект — член FRS использует атрибут `frsComputerReference` для указания на компьютерный объект.
2. Объект-подписчик использует атрибут `frsMemberReference` для указания на объект — член FRS.
3. Объект — член FRS использует атрибут `serverReference` для указания на объект NTDS Settings. В нормальных условиях эта связь формируется только для объектов `SYSVOL`.
4. Объект связи использует атрибут `fromServer` для указания на объект — член FRS.

Знание этих атрибутов и взаимосвязей между ними может пригодиться при выяснении причин проблем с репликацией FRS.

Настройка FRS

Зная, какие компоненты службы FRS и за что отвечают, службу можно настроить:

- изменить общие параметры службы FRS
- ◆ установить фильтры для реплик файлов и каталогов
- ◆ задать расписание репликации.

Изменение интервалов опроса Active Directory

Служба FRS постоянно сверяется с конфигурационной информацией, записанной в Active Directory. Первый раз это происходит при запуске службы. Затем FRS определяет партнеров по репликации для каждого набора реплик.

Служба периодически обращается к Active Directory, чтобы понять, не произошло ли изменений, способных повлиять на взаимоотношения компьютера с партнерами. Интервал обращения не постоянен.

Сначала используются 8 коротких интервалов (по умолчанию 5 минут). Если в течение этого срока конфигурация не меняется, происходит переключение на длинные интервалы (по умолчанию 5 минут для контроллеров доменов и 60 — для серверов-членов домена). Если же изменения произошли, счет коротких интервалов сбрасывается в 0. Счет интервалов сбрасывают такие события:

- ◆ добавление реплики;
- ◆ удаление реплики;
- ◆ добавление объекта связи;
- ◆ удаление объекта связи;
- ◆ изменение расписания;
- ◆ изменение фильтра файлов или папок.

Длительность коротких и длинных интервалов можно регулировать, изменяя в ветви реестра `HKLM\System\CurrentControlSet\Services\NtFrs\Parameters` значения параметров `DS Polling Short Interval in Minutes` и `DS Polling Long Interval in Minutes`. Устанавливаемое значение соответствует времени в минутах. Минимально возможная величина — 1 минута.

Установка фильтров

Фильтры устанавливаются на файлы и каталоги, чтобы исключить их из репликации. Фильтрация возможна как для набора реплик `SYSVOL`, так и для набора реплик корня `DFS` и томов `DFS`.

По умолчанию не выполняется *тиражирование*:

- зашифрованных файлов EFS — в Windows 2000 нет смысла копировать зашифрованные файлы куда бы то ни было, так как нельзя организовать к ним совместный доступ;
- точек перехода NTFS — поскольку они не являются файлами (см. [1]), а лишь указывают на какое-либо еще место на локальном компьютере или на съемном носителе;
- файлов с расширениями `.bak` и `.tmp` — они не представляют ценности, так как временно образуются в результате работы приложений таких, как Microsoft Word;
- файлов, начинающихся с символа «~». — они тоже, как правило, служат для временного использования и удаляются по окончании работы программ их породивших.

Внимание Действие фильтров распространяется только на файлы, добавляемые к набору реплик. Если файлы, описываемые фильтром, существовали до его добавления, действие фильтра не будет распространяться на них.

Допустим, вы заменили стандартные фильтры файлов с расширениями `.bak` и `.tmp` на новый фильтр файлов с расширением `.*?_`. При этом все файлы с расширением, заканчивающимся символом подчеркивания и существовавшие до установки фильтра, будут по-прежнему тиражироваться. Все вновь добавляемые файлы с такими расширениями тиражироваться не будут. Чтобы не выполнялось тиражирование всех файлов этого типа, их надо удалить вручную.

С другой стороны, все «старые» файлы с расширениями `.bak` и `.tmp` тиражироваться не будут, а вот новые файлы таких типов — будут. Если надо разрешить тиражирование прежних файлов, их надо модифицировать.

Почему используется столь «неудобная» логика? Допустим иную логику: действие добавленного фильтра распространяется на файлы

реплик, так и для объектов *связи*, причем расписание для объектов *связи* имеет преимущество,

А как лучше управлять репликацией SYSVOL? Вы знаете (а если нет, см. главу «Групповая политика»), что каталог SYSVOL в первую очередь служит для применения групповой политики. Хранимые в нем шаблоны групповой политики должны точно соответствовать контейнерам групповой политики в Active Directory. Рассогласование версий не позволяет применять групповую политику к клиентам. Значит, нужно обеспечивать согласованную репликацию Active Directory и каталога SYSVOL. Раз так, следует задать идентичное расписание тиражирования для Active Directory и службы FRS.

Расписание для межсайтовой репликации Active Directory определяется для объектов *связи*. Следовательно, расписание репликации FRS надо определять для тех же объектов *связи*: хотя это два разных процесса, они используют одни и те же объекты *связи*. Делается это, как вы помните, в оснастке Active Directory Sites and Services.

Замечание В то время как инициировать репликацию Active Directory позволяет команда Replicate Now контекстного меню объекта *связи* в оснастке Active Directory Sites and Services, а вот репликация FRS начинается только с открытием окна.

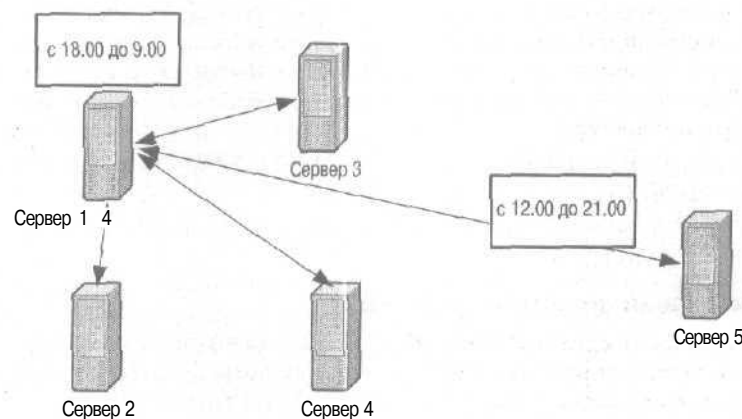
Совсем иное дело, когда речь идет о репликации DFS. Этот процесс не связан с репликацией Active Directory и использует собственную топологию и расписание. Кроме того, нет условий автоматической репликации — она всегда выполняется по расписанию. Если так, то вы получаете право выбора объекта, для которого надо определять расписание репликации.

Если в наборе реплик содержится значительное количество реплик, то удобнее расписание определить для набора. Я, правда, не встречал еще систем DFS, тиражирующих тома DFS более, чем на 2-3 компьютера. Однако это не значит, что такие системы нельзя создать.

Другой способ идентичен управлению расписанием репликации SYSVOL: вы указываете доступность репликации для объектов *связи*. И это расписание будет иметь преимущество над тем, что назначено для набора реплик в целом.

Рассмотрим, например, набор реплик DFS, состоящий из 5 серверов. Каналы между четырьмя свободны с 18.00 до 9.00, а вот канал с пятым сервером — только с 12.00 до 21.00. Если определять расписания для каждого из объектов *связи*, придется проделать эту операцию 10 раз (напомню, что объекты *связи* *однаправлены*), причем 8 раз — повторить одно и то же. Очевидно, оптимальным решением будет разрешение репликации с 18.00 до 9.00 всему набору реплик и отдель-

но — объекту связи с пятым сервером с 12.00 до 21.00. Иначе говоря, понадобится только три расписания.



Комбинирование расписания для всего набора реплик с расписанием для конкретного объекта связи

Чтобы изменить расписание репликации набора реплик, в оснастке Active Directory Users and Computers надо открыть последовательно контейнеры System a File Replication Service a DFS Volumes и т. д., пока не откроется нужный объект набора реплик. В окне его свойств надо щелкнуть кнопку Change Schedule и установить расписание.

Замечание Расписание устанавливается для каждого часа в течение недели. Если час отмечен синим прямоугольником, репликация разрешена, если нет — запрещена.

Чтобы изменить расписание репликации объекта связи, в оснастке Active Directory Users and Computers надо открыть последовательно контейнеры System a File Replication Service a DFS Volumes и т. д., пока не откроется *нужный* объект связи. Объект связи узнать легко: вместо имени для него записан номер GUID, а рядом указано, с какого компьютера и в каком домене он передает данные. В окне его свойств надо щелкнуть кнопку Change Schedule и установить расписание.

Замечание Изменить расписание можно, изменив значение атрибута schedule для объекта связи или объекта набора реплик, но это не очень удобно.

Напоследок несколько советов по планированию репликации FRS.

- Не планируйте межсайтовую репликацию очень часто. Это может вызвать перегрузку серверов-форпостов.

- Узкие окна репликации могут привести к прерыванию репликации на полпути; в отличие от репликации Active Directory репликация FRS прекращается, как только окно закрывается. Это может стать причиной переполнения подготовительных каталогов и журналов выхода. Улучшения, сделанные в SP2 (и планируемые к включению в SP3), частично снимают остроту этой проблемы, но она не исчезает полностью.
- Не запрещайте репликацию полностью. Она не начнется сама, пока окно закрыто.
- Старайтесь не делать расписания разнообразными — это усложнит поиск проблем.

Рекомендации по оптимизации FRS

Оптимизировать службу FRS необходимо в основном при использовании распределенной файловой системы. Об оптимальной конфигурации FRS для каталога SYSVOL заботится KCC. Однако и здесь есть над чем поработать. Ниже приведены некоторые рекомендации по оптимизации работы этой службы. Часть этих рекомендаций можно найти в [3], но я все же повторю и дополню их здесь, чтобы создать единую картину.

Журналирование

Итак, совет первый. Располагайте журналы регистрации FRS не на том диске, на котором находятся база FRS `ntfrs.jdb`, подготовительные каталоги и сами реплицируемые файлы. Это особенно актуально при высокой степени подробности регистрации событий. Для перемещения журнала регистрации в другое место надо указать его в параметре Debug Log File в ветви реестра `HKLM\System\CurrentControlSet\Services\Ntfrs\Parameters` и перезапустить службу FRS. По умолчанию этот файл расположен в каталоге `%systemroot%\debug`, т. е. как раз на том диске, где хранятся перечисленные выше файлы и каталоги.

Степень подробности регистрации событий регулируется другим параметром в этой же ветви реестра — Debug Log Seventy. Его величина может изменяться от 0 (минимальная степень детализации в журнале `Ntfrs_000x.log`) до 5 (максимальная). По умолчанию задано 4, однако если вы установили SP2, то значение равно 2.

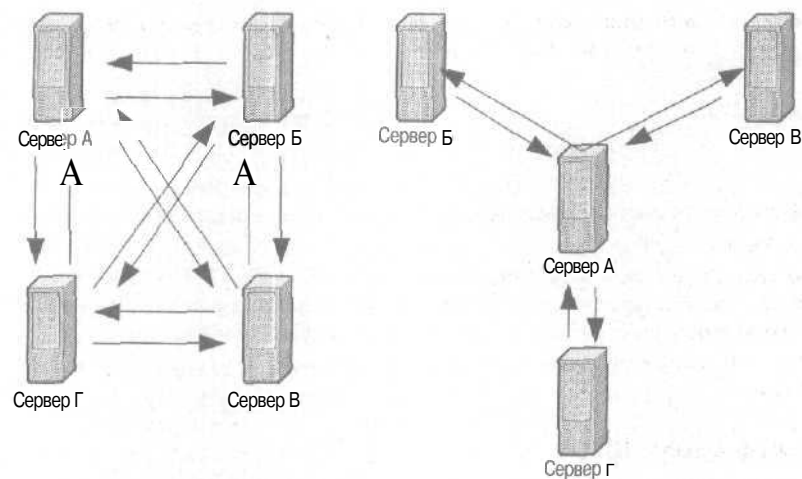
Чем выше степень подробности, тем быстрее заполняются файлы регистрации. Как только заполнится файл `Ntfrs_0001.log`, начинает заполняться файл `Ntfrs_0002.log`, потом `Ntfrs_0003.log` и так до 5. После заполнения пятого файла вновь заполняется первый. Если нужно отследить события за длительный период времени, пяти файлов может не хватить. Их число можно увеличить, указав нужное значение в параметре Debug Log Files.

Максимальный размер файла журнала определяется значением параметра Debug Maximum Log Messages, указывающим, сколько строк должно содержаться в каждом журнале. По умолчанию — 10000, но вы можете установить любое другое.

Второй совет относится к случаю, когда регистрация вообще не требуется. Ее можно отключить, и надобность в переносе журнала регистрации отпадет. Для этого в ветви реестра HKLM\System\CurrentControlSet\Services\Ntfrs\Parameters задайте 1 параметру Debug Disable.

Топология репликации

Третий совет относится к проектированию топологии репликации DFS. По мере того как вы добавляете новые реплики, образуется все больше объектов связей. При этом не используется никаких алгоритмов оптимизации — каждая реплика связывается с остальными репликами в наборе. В итоге получается каша из объектов связи и увеличивается сетевой трафик. Поэтому при большом числе реплик в наборе надо удалить ненужные связи. Так, при наличии четырех реплик по умолчанию создается 12 объектов связи. А ведь их можно сократить вдвое:



Пример топологий репликации: создаваемой по умолчанию и оптимизированной

Проектируя топологию репликации, надо учитывать пропускную способность каналов связи. Если один из компьютеров в наборе реплик связан со всеми партнерами, кроме одного, быстрыми каналами, а с оставшимся — медленным, не исключено, что очередь на репликацию и объем подготовительного каталога на нем будут расти. Поэтому

совет четвертый: проектируйте топологию так, чтобы балансировать нагрузку между репликами.

Подготовительный каталог

Пятый и шестой советы относятся к размеру и местоположению подготовительного каталога. Чтобы подготовительный каталог не разрастался, его объем можно ограничить. В этом случае после достижения им указанного объема входная репликация для данного партнера приостанавливается, пока подготовительный каталог не разгрузится за счет выходной репликации. Максимальный размер подготовительного каталога (в Кб) указывается в параметре Staging Space Limit in KB в ветви реестра HKLM\System\CurrentControlSet\Services\Ntfrs\Parameters.

Иногда стоит изменить местоположение подготовительного каталога. По умолчанию он находится на том же диске, что и реплицируемые файлы, а подчас и там же, где хранятся системные файлы. Изменить положение подготовительного каталога можно так.

- Остановите службу NTFRS на том компьютере, где собираетесь выполнить перенос каталога.
- Установите значение параметра BurFlags в ветви реестра HKLM\System\CurrentControlSet\Services\Ntfrs\Parameters\Backup/Restore\Process в 0xD2.
 - ◆ С помощью программы dp или ADSIEdit измените значение атрибута frsStagingPath для объекта-подписчика, соответствующего выбранному компьютеру.
 - ◆ Создайте или переместите подготовительный каталог в указанное место.
- + Запустите службу NTFRS.

Внимание Обязательно задайте параметру BurFlags значение 0xD2. Это инициирует обновление реплики и реинициализацию контрольной суммы файлов в подготовительном каталоге.

Размер журнала NTFS

Служба FRS постоянно просматривает журнал NTFS на предмет поиска в нем записей о закрытии файлов. Записи добавляются туда ОС при каждой операции над файлами; открытии, изменении, закрытии, удалении. Очевидно, что по мере добавления записей в журнал NTFS он достигнет своего максимального значения (по умолчанию 32 Мб) и начнет записывать новые данные в начало. Если скорость изменений файлов такова, что за время заполнения журнала репликация FRS не будет выполнена, часть данных будет безвозвратно потеряна для служ-

бы репликации файлов. А раз так, встает вопрос об увеличении объема журнала NTFS.

Размер журнала для всех томов, содержащих файлы, обслуживаемые FRS, задается в параметре `Ntfs Journal size in MB` в ветви реестра `HKLM\System\CurrentControlSet\Services\Ntfs\Parameters`. Минимальное значение — 8 Мб, максимальное — 128 Мб. Но учтите: если при увеличении размера журнала достаточно только перезапустить службу NTFRS, то при уменьшении нужно переформатировать все тома, содержащие реплицируемые файлы.

Использование FRS и удаленных хранилищ

Часть реплицируемых файлов может располагаться на магнитной ленте или ином носителе, используемом службой Remote Storage для организации удаленного хранилища (подробнее см. [1]). Ничего запретного в этом нет, только учтите, что компьютер, на котором установлено удаленное хранилище, может испытывать перегрузки. Дело в том, что всякий раз при полной репликации файлов (скажем, при добавлении нового компьютера в набор реплик) придется скачивать с ленты все файлы. Поэтому надо вручную конфигурировать топологию репликации так, чтобы минимизировать необходимость в полной репликации с этого компьютера.

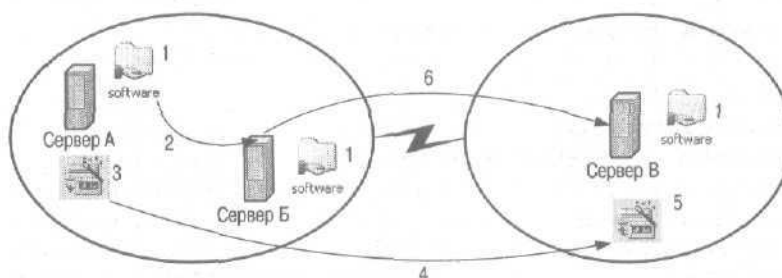
Использование резервного копирования для начальной конфигурации реплик

В главе «Планирование Active Directory» я рассказывал о конфигурировании контроллеров домена в удаленных сайтах, связанных с центральными медленными каналами связи. Думаю, стоит вернуться к этому вопросу еще раз и подумать, как оптимально сконфигурировать службу FRS для таких компьютеров.

Рассмотрим систему, в которой контроллеры домена А и Б расположены в центральном сайте, а В — в периферийном сайте, связанном медленным каналом. Вы планируете развернуть DFS для хранения дистрибутивов приложений. Доступ к ним должен быть максимально эффективным в любом сайте. Общий объем достигает нескольких гигабайт. Все три сервера должны входить в набор реплик. Понятно, что если В подключить к существующему набору реплик в центральном сайте, то все эти гигабайты потекут по медленному каналу. Как быть?

Есть два решения. Первое: вы привозите контроллер домена для удаленного сайта в центральный сайт, выполняете репликацию, а потом отвозите контроллер назад. Если такой возможности нет, можно использовать Windows Backup для организации транспортировки данных. Вот как сконфигурировать DFS.

1. На всех трех контроллерах домена создается каталог для хранения дистрибутивов и предоставляется в совместное использование.
2. Далее создается корень DFS и в нем каталог, в который включаются все три альтернативных тома с серверов А, Б и В. Репликация разрешается для серверов А и Б.
3. После того, как нужные дистрибутивы записаны на А и реплицированы на Б, выполняется резервное копирование каталога на съемный носитель.
4. Этот носитель по почте или с курьером доставляется в удаленный сайт.
5. На сервере В выполняется восстановление файлов с носителя в указанный каталог.
6. Серверу В также разрешается участвовать в репликации. Если за время доставки носителя в каталогах на А и Б произошли изменения, они будут реплицированы на В. Остальные файлы реплицироваться не будут.



Использование Windows Backup для начального тиражирования в удаленный сайт

По умолчанию после добавления сервера В в набор реплик между ним и серверами А-и Б образуются объекты связи. Поэтому тиражирование будет выполняться как с А, так и с Б. Пусть первым начнется тиражирование с Б. Сравнив свою таблицу ID с вектором версий сервера В, он станет пересылать измененные файлы. Но, как я уже сказал, репликация FRS — многопоточная, поэтому наряду с этим процессом то же самое начнет выполнять А. В результате В будет в сметанном порядке принимать файлы с обоих серверов в зависимости от того, с какого из них файл придет первым, В итоге В обновит свою таблицу ID и вектор версий так, чтобы отразить состояние на А и Б.

Не превышайте...

Напоследок несколько значений, которые не рекомендуется превышать. Ни одно из них не «зашито» в код; это экспериментальные значения для которых было сделано тестирование. Итак:

- максимальное число наборов реплик на одном компьютере — 50; при этом нельзя использовать топологию репликации по умолчанию.
- + максимальное число файлов и каталогов в одном наборе реплик — 64 000;
- ◆ максимальный объем данных в одном наборе реплик ограничен только объемом диска;
- максимальное число **входных** и выходных партнеров по репликации в одном наборе реплик — 32; при этом нельзя использовать топологию репликации по умолчанию;
- максимальное число членов в одном наборе реплик — 1 000; это значение не **тестировалось**, но для **SYSVOL** должно поддерживаться,

Поиск и устранение проблем FRS

Проблемы с репликацией FRS обычно возникают неожиданно. Неожиданно для вас, но не для системы. И система честно предупреждает вас об этом **заблаговременно**, занося сообщения об ошибках в журналы. Только ведь «плох тот администратор, который заглядывает в журналы и читает документацию»! Именно поэтому о маленькой неприятности узнают тогда, когда она вырастает в крупную проблему. Дабы не доводить систему до критически неработоспособного состояния, надо выполнять постоянный мониторинг журналов. Большую помощь в этом окажет Microsoft Operations Manager, который способен не только централизованно собирать все сообщения, заносимые в журналы на всех серверах, но и аккумулировать их и предупреждать администратора о надвигающейся опасности. Но уж коль этого не произошло, надо заняться поиском и устранением проблем.

Итак, если репликация файлов внезапно прекратила работать, надо сделать следующее.

Далее будем полагать, что есть два компьютера: А — источник данных репликации и Б — приемник.

1. В журнале регистрации событий File Replication System поищите сообщения с Event ID=13511 или 13522. Если они есть, проверьте свободное место на **дисках**, на которых находятся:

На компьютере А	На компьютере Б
Исходный каталог	Приемный каталог
Подготовительный каталог	Предварительный каталог
Файл ntfrs.jdb	Файл ntfrs.jdb

- Воспользуйтесь советами из раздела «Журналы» для данных сообщений. Полезно перечитать и «Рекомендации по оптимизации FRS». Возможно, переполнение подготовительного каталога вызвано тем, что между компьютерами долго не было соединения.
2. Создайте тестовый файл на компьютере Б и посмотрите, выполнится ли его тиражирование на компьютер А.
 3. Посмотрите, доступны ли оба компьютера в сети и разрешаются ли их имена DNS. Для этого лучше всего выполнить команду ping.
 4. Посмотрите, запущены ли службы FRS на обоих компьютерах. Если нет, загляните в журнал и выясните, почему это произошло. Если в журнале нет каких-либо сообщений об ошибках, запустите службу повторно.
 5. Проверьте связь по RPC между компьютерами с помощью утилиты RPC Ping из комплекта Windows 2000 Resource Kit. Если связь по RPC невозможна, а в журнале появилось сообщение 13508, постарайтесь выявить и ликвидировать причины, перечисленные в соответствующей части следующего раздела.
 6. Проверьте расписание репликации. Возможно, она просто запрещена в данное время.
 7. Проверьте, не заблокированы ли файлы. Если они открыты на любом из компьютеров, репликация невозможна.
 8. Проверьте фильтры репликации файлов и каталогов. Возможно, интересующие вас файлы просто исключены из разрешенных к тиражированию. Убедитесь, что они не зашифрованы и не являются переходами NTFS.
 9. Если ничто из перечисленного не помогает, обратитесь к рабочему журналу ntfrs (см. раздел «Журналы NTFRS»). Дополнительную информацию предоставит программа NTFRSUTL (см. ниже).
 10. В ряде случаев придется восстанавливать службу FRS на компьютере из резервной копии или из других реплик (см. разделы «Восстановление реплицируемых файлов» и «Восстановление конфигурации FRS»).

Журналы

Журналы — единственное средство диагностики проблем. К счастью для диагностики работы службы FRS, используются два вида журналов: журнал регистрации File Replication System, доступ к которому осуществляется через оснастку Event Viewer, и рабочий журнал NTFRS_0000x.log, содержащий отладочную информацию о работе модуля ntfrs. Этот журнал — ваше последнее средство диагностики, так как содержит избыточную информацию, через которую порой не так легко продаться к поискам истины.

Журнал регистрации File Replication System

Это первый и главный источник информации о работе службы FRS. Каждое сообщение имеет свой идентификатор (ID); основные перечислены ниже.

13501 — сообщение о запуске службы NTFRS.

Если в системе нет особенностей, влияющих на работу FRS, следующим и последним за весь сеанс работы будет сообщение **13516**. Оно появляется только на контроллерах домена и свидетельствует о том, что реплика каталога SYSVOL успешно инициализирована.

В промежутке между этими двумя может появляться сообщение **13512**. Для диска, на котором расположена база ntfrs.jdb, должно быть запрещено кэширование записи. Обычно при старте ОС кэширование диска запрещается. Если же ОС не удается этого сделать (скажем, если вы запустили Windows 2000 в виртуальной машине VMWare), выводится это сообщение. Это предупреждение о том, что в случае краха ОС или внезапного выключения питания служба репликации файлов может и не восстановиться.

Если компьютер не может выполнить репликацию со своим входным партнером, то в журнал записывается сообщение **13508**. Причин может быть много: и невозможность разрешения доменного имени партнера, и остановленная служба FRS на партнере, и незавершенная репликация сведений об объектах связи, и невозможность создания защищенного соединения между контроллерами, и элементарная недоступность партнера в сети.

Как только репликация с партнером становится возможной, в журнал заносится сообщение **13509**.

Сообщение **13562** может возникать в разных ситуациях, но всегда в результате наших ошибок. Так, следующее сообщение возникло из-за того, что вы создали дубликат объекта связи и назвали его «from root2».

Following is the summary of warnings and errors encountered by File Replication Service while polling the Domain Controller ROOT1.mycorp.ru for FRS replica set configuration information.

The nTDSConnection object cn=d489f659-bab5-4163-b6cb-c030db6715d4, cn=ntds settings, cn=root1, cn=servers, cn=default-first-site-name, cn=sites, cn=configuration, dc=mycorp, dc=ru is conflicting with cn=from root2, cn=ntds settings, cn=root1, cn=servers, cn=default-first-site-name, cn=sites, cn=configuration, dc=mycorp, dc=ru. Using cn=d489f659-bab5-4163-b6cb-c030db6715d4, cn=ntds settings, cn=root1, cn=servers, cn=default-first-site-name, cn=sites, cn=configuration, dc=mycorp, dc=ru

В этом нет ничего страшного. Гораздо хуже, когда в описании причины появляется:

```
The ntFRSMember object cn=dc1,cn=domain system volume (sysvol share),cn=file replication service,cn=system,dc=a,dc=com has a invalid value for the attribute ServerReference.
```

Это сообщение появилось скорее всего потому, что вы удалили объект NTDS Settings в контейнере Configuration — придется его восстановить.

Сообщение 13522 появляется при переполнении подготовительного каталога. При этом FRS приостанавливает свою работу до того, как объем подготовительного каталога не уменьшится либо вы не увеличите значение максимального объема подготовительного каталога (см. выше советы по оптимизации подготовительного каталога). Возможно, проверив объем свободного места на диске, вы будете удивлены тем, что его еще «много», а сообщение уже появилось и репликация остановилась. Скорее всего дело в том, что реплицируемый от входного партнера файл больше, чем свободного места на диске. Если это так, освободите диск и запустите службу репликации командой:

```
net start ntfrs
```

Служба FRS может остановиться и сообщить о событии 13511. Происходит это при переполнении диска, на котором расположена база NTFRS. Выходов может быть два:

- ◆ освободить место на диске и перезапустить службу FRS;
- ◆ переместить базу на другой диск (этот способ несколько сложнее первого).

Сообщение 13555 — не предупреждение, как все предыдущие, а ошибка. Оно свидетельствует о серьезной проблеме в работе службы FRS. Возможно, разрешит ее перезапуск службы:

```
net stop ntfrs
net start ntfrs
```

Если компьютер, на котором возникла данная ошибка, является контроллером домена и на нем нет реплик DFS, дальнейшие действия зависят от наличия других контроллеров домена. Если, кроме этого контроллера, есть еще хотя бы один, выполните неавторитетное восстановление состояния системы (см. раздел «Восстановление конфигурации FRS»). Если на всех прочих контроллерах та же ошибка, неавторитетное восстановление состояния системы выполняется на всех контроллерах, кроме того, на котором выполняется авторитетное восстановление. Если это единственный контроллер, выполните авторитетное восстановление состояния системы.

Если на контроллере домена также есть реплики DFS, то, прежде чем выполнять неавторитетное восстановление состояния **системы**, надо скопировать содержимое каталогов DFS в безопасное место и ликвидировать все объекты связи, которые могли сохраниться от прежних времен. Под этим термином подразумеваются бывшие контроллеры домена, статус которых был понижен до уровня серверов.

Журналы NTFRS

В разделе «Рекомендации по оптимизации FRS» описаны журналы, в которые служба FRS заносит всю информацию о своей работе с той степенью подробности, которую вы укажете. Количество файлов журналов и их объем также определяете вы (см. указанный раздел). Если вы занимаетесь поиском сложной проблемы, для идентификации которой надо просмотреть огромный объем информации, можете задать количество файлов журналов равным 50, а после того, как они заполнятся, — сделать резервную копию для последующего анализа.

Что же содержат журналы FRS? Подробно рассматривать каждую строку не имеет смысла — я **остановлюсь** на самых важных и характерных местах. Далее будем разбирать файл, степень подробности которого **установлена** равной 2 (**умолчание** при установленном SP2).

Для начала запомним общий формат выводимых сообщений:

Имя функции + ID потока + номер строки в коде + степень подробности + время + сообщение

Запуск службы начинается с регистрации в журнале информации о системе и о самой службе.

```
<DbgPrintInfo: 1328: 933: S2: 16:13:03> :H: Service running on
ROOT1 as SYSTEM at 16:13:03
<DbgPrintInfo: 1328: 935: S2: 16:13:03>
<DbgPrintInfo: 1328: 936: S2: 16:13:03> :H: ***** COMPILE
INFORMATION:
<DbgPrintInfo: 1328: 937: S2: 16:13:03> :H: Module
D:\nt\private\net\svcmgs \ntrepl\main\main.c
<DbgPrintInfo: 1328: 938: S2: 16:13:03> :H: Compile Date Nov 7
2000 11:01:45
<DbgPrintInfo: 1328: 942: S2: 16:13:03> :H: Latest changes:
<DbgPrintInfo: 1328: 942: S2: 16:13:03> :H: Windows 2000-SP2
<DbgPrintInfo: 1328: 946: S2: 16:13:03>
<DbgShowConfig: 1328: 741: S0: 16:13:03> :H: 08 Version 5.0 (2195) -
<DbgShowConfig: 1328: 745: S0: 16:13:03> :H: SP (2.0) SM: 0x0000
PT: 0x02
<DbgShowConfig: 1328: 755: S0: 16:13:03> :H: Processor: INTEL
Level: 0x0006 Revision: 0x0803 Processor num/mask: 1/00000001
```


Хочу обратить внимание на отсутствие в файле дат. Они и не нужны: дату можно узнать из самого файла журнала. Далее следует внушительный кусок отладочной информации, которая вряд ли пригодится при поиске проблем с репликацией. Многое можно узнать из реестра. Взгляните, например, на эти строки:

```
<DbgPrintInfo: 1328: 950: S2: 16:13:03> :H: ***** DEBUG INFORMATION:
<DbgPrintInfo: 1328: 951: S2: 16:13:03> :H: Total Log Lines: 202099
<DbgPrintInfo: 1328: 953: S2: 16:13:03> :H: Log Severity : 2
<DbgPrintInfo: 1328: 954: S2: 16:13:03> :H: Log Flush Int. : 20000
<DbgPrintInfo: 1328: 959: S2: 16:13:03> :H: Log File :
C:\WINNT\debug\NtFrs
<DbgPrintInfo: 1328: 960: S2: 16:13:03> :H: Max Log Lines : 20000
<DbgPrintInfo: 1328: 969: S2: 16:13:03> :H: Log Files : 5
<DbgPrintInfo: 1328: 971: S2: 16:13:03> :H: Force VvJoin : FALSE
```

Особое внимание надо уделить последней строке. Если бы компьютер, на котором регистрировались эти записи, подключался к новому набору реплик или параметр BurFlags был бы установлен равным 0xD2, то Force VvJoin равнялся бы TRUE. Это означает инициацию реплики и процесса VV-join (подробнее см. раздел «Оптимизация процессов восстановления»).

Далее в файле встретится запись:

```
<FrsNewDsFindComputer: 1220: 9762: S2: 16:22:38> :DS: Computer FQDN
is cn=root1,ou=domain controllers,dc=mycorp,dc=ru
<FrsNewDsFindComputer: 1220: 9768: S2: 16:22:38> :DS: Computer's
dns name is ROOT1.mycorp.ru
```

Это сведения об имени компьютера.

```
<FrsNewDsFindComputer: 1220: 9782: S2: 16:22:38> :DS: Settings
reference is cn=ntds settings,cn=root1,cn=servers,cn=default-first-
site-name,cn=sites,cn=configuration,dc=mycorp,dc=ru
```

А вот здесь ищется информация об объектах связи с партнерами по репликации.

```
<FrsNewDsGetSubscribers: 1220: 8980: SO: 16:22:38> :DS: No
NTRSSubscriber object found under cn=dfs volumes,cn=ntfrs
subscriptions,cn=root1,ou=domain controllers,dc=mycorp,dc=ru!
<FrsNewDsGetSubscribers: 1220: 8980: SO: 16:22:38> :DS: No
NTRSSubscriber object found under cn=72b484ac-f61d-4e7b-8a1e-
e8ca284ddae5,cn=dfs volumes,cn=ntfrs subscriptions,cn=root1,ou=domain
controllers,dc=mycorp,dc=ru!
```

Какая неожиданность: не обнаружено ни одного объекта-подписчика DFS! А раз так, то надобности в процессе VV-Join нет.

<MainVvJoin: 1326: 2343: S1: 16:24:51> :S: Vv Join Thread is exiting.

Если бы надобность в этом процессе возникла и он стал работать, в журнале появились бы такие записи:

<VvJoinSend: 1328: 1860: SO: 16:14:36> :v: MTXDM.DLL (9c0d0a84):
Vvjoin sending create

Запись свидетельствует о том, что файл MTXDM.DLL добавлен в реплику и его идентификатор 9c0d0a84 занесен в таблицу ID. Очевидно, что таких строк в журнале будет ровно столько, сколько добавляется файлов. Другое дело, что идти они могут не все сразу, а группами.

Подключение реплики завершается выводом сообщения вида:

<HainVvJoin: 1328: 2281: S1: 16:19:51> :V: vjoin succeeded for
DFSROOT\SOFTWARE\{4C95CE9D-32BC-4D7F-97FF-83EE1C828419}\
{4C95CE9D-32BC-4D7F-97FF-83EE1C828419} (3702 sent)

Оно означает, что для реплики DFS (DFSROOT\SOFTWARE), расположенной на члене FRS с GUID=4C95CE9D-32BC-4D7F-97FF-83EE1C828419, было успешно добавлено 3702 файла.

Если к существующей реплике добавить новый файл, в журнале появятся такие записи. Заметьте: в сообщениях впервые появляется дата.

<FrsStageCsSubmitTransfer:1400: 1357: S1: 12:47:38> Stage: submit
transfer Qxe4c490
5/26-12:47:39 :T: CoG: 3b9040ca CxtG: fb4f87bd [LclCo] Name: Copy of
small2-1.bmp
5/26-12:47:39 :T: EventTime: Sun May 26, 2002 12:47:35 Ver: 0
5/26-12:47:39 :T: FileG: fb0db575-f0a8-4b9c-bcf749cabcc1f0b7 FID:
009e0000 000c308c
5/26-12:47:39 :T: ParentG: e82cefbb-ec88-4c50-b7a6625515f43eb2 Size:
00000000 00001800
5/26-12:47:39 :T: OrigG: 3ae7eff6-10b7-4040-b99689cccd8490c5 Attr:
00000020
5/26-12:47:39 :T: LocnCmd: Create State: IBCO_COMMIT_STARTED
ReplicaName: DOMAIN SYSTEM VOLUME (SYSVOL SHARE) CD
5/26-12:47:39 :T: CoFlags: 0100042c [Content Locn LclCo NewFile
CmpresStage]
5/26-12:47:39 :T: UsnReason: 00008003 [DatOvrWrt DatExt Info]

Я специально выделил имя файла, его версию, а также причины, по которым нужно выполнить репликацию: новый файл (New File) и запись файловой системы (DatOvrWrt). Что произойдет при модификации файла? Изменится версия. Могут измениться размер или атрибуты, но не его идентификатор. И это действительно так:

<FrsStageCsSubmitTransfer: 1340: 1357: S1: 12:52:28> Stage: submit
transfer 0xe53770

```

5/26-12:52:28 :T: CoG: 988e323d CxtG: fb4f87bd [LclCo] Name: Copy of
                    small12-1.bmp
5/26-12:52:28 :T: EventTime: Sun May 26, 2002 12:52:25 Ver: 1
5/26-12:52:28 :T: FileG: fb0db575-f0a8-4b9c-bcf749cabcc1f0b7 FID:
                    009e0000 0000308c
5/26-12:52:28 :T: ParentG: e82cefbb-ec8-4c50-b7a6625515f43eb2 Size:
                    00000000 00001800
5/26-12:52:28 :T: OrigG: 3ae7eff6-10b7-4040-b99689cccd8490c5 Attr:
                    00000020
5/26-12:52:28 :T: LocnCmd: NoCmd State: IBCO_COMMIT_STARTED
                    ReplicaName: DOMAIN SYSTEM VOLUME (SYSVOL SHARE) (1)
5/26-12:52:28 :T: CoFlags: 01000024 [Content LclCo CmpresStage ]
5/26-12:52:28 :T: UsnReason: 00000001 [DatOvrWrt ]

```

Версия увеличилась на 1, хотя и размер, и атрибуты файла не изменились. Причиной репликации в этом случае стало изменение содержимого файла (Content). Как частный случай рассмотрим замещение файла другим с таким же именем. С точки зрения файловой системы, произойдет изменение содержимого файла, а значит, как минимум увеличится номер версии. Иное дело, если не просто заместить файл, а предварительно его удалить. После удаления в журнал будет занесено:

```

5/26-12:52:52 :T: CoG: 8ca26282 CxtG: fb4f87bd [LclCo ] Name: Copy of
                    small12-1.bmp
5/26-12:52:52 :T: EventTime: Sun May 26, 2002 12:52:52 Ver: 2
5/26-12:52:52 :T: FileG: fb0db575-f0a8-4b9c-bcf749cabcc1f0b7 FID:
                    009e0000 0000308c
5/26-12:52:52 :T: ParentG: e82cefbb-ec8-4c50-b7a6625515f43eb2 Size:
                    00000000 00001800
5/26-12:52:52 :T: OrigG: 3ae7eff6-10b7-4040-b99689cccd8490c5 Attr:
                    00000020
5/26-12:52:52 :T: LocnCmd: Delete State: IBCO_COMMIT_STARTED
                    ReplicaName: DOMAIN SYSTEM VOLUME (SYSVOL SHARE) (1)
5/26-12:52:52 :T: CoFlags: 00000028 [Locn LclCo ]
5/26-12:52:52 :T: UsnReason: 00000000 [<Flags Clear>]

```

Вы видите, что теперь версия файла стала равна 2, а ведь он удален! И об этом свидетельствует отсутствие флагов в журнале NTFS (UsnReason). Если теперь в каталог скопировать файл с таким же именем, то с точки зрения FRS, это будет иной файл. Его идентификатор (FID) будет отличаться от идентификатора только что удаленного файла, а версия будет равна 0.

Теперь рассмотрим сообщение об ошибке репликации,

```

<SndCsMain: 1464: 768: SO: 11:15:20> ++ ERROR - EXCEPTION
(000006ba) : WStatus: RPC_S_SERVER_UNAVAILABLE

```

```
<SndCsMain: 1464: 769: SO: 11:15:20> :SR: Cmd 00e1e200, CxtG  
4c71259c, WS RPC_S_SERVER_UNAVAILABLE, To ROOT2.mycorp.ru Len: (374)  
[SndFail - rpc exception]
```

Его появление связано с тем, что сервис RPC недоступен на партнере по репликации. Скорее всего компьютер выключен. Это, пожалуй, самое безобидное сообщение, так как вполне ясна причина. Если же вы уверены, что все партнеры доступны, а репликация тем не менее не идет, то для выявления причин выполните в журнале на входном партнере поиск строки «:: COG». На всех его выходных партнерах, с которыми нет репликаций, выполните поиск в журнале сообщений с его собственным номером GUID.

Сообщение «SHARING_VIOLATION» связано с тем, что один из реплицируемых файлов открыт. Как вы помните, выполняется репликация только закрытых файлов.

Если вы смотрите содержимое журнала сразу после запуска в первый раз контроллера домена либо после удаления файла ntfrs.jdb, появятся ошибки типа «jet attach db — 1811». Не стоит придавать им большого значения. Просто БД в момент старта службы FRS еще не была создана.

Поиск ошибок в журнале удобно осуществлять командой find:

```
find /I /n "error|warn|fail" ntfrs*.log >err.tmp
```

Вы получите сообщения обо всех ошибках и предупреждениях, собранные из всех файлов журнала.

Связь между монитором производительности и сообщениями в журнале

Если вы обратили внимание на формат выводимых в журнал сообщений, то заметили в нем идентификатор потока (thread ID). Его можно использовать при анализе причин снижения производительности с помощью монитора производительности. Рассмотрим пример.

Допустим, вы выполняете мониторинг загрузки процессора, так как вас удивляет его постоянно высокая загрузка. Анализ показывает, что большую часть времени процессор отводит на работу процесса ntfrs. Чтобы выяснить, чем занимается служба FRS, воспользуйтесь любой программой, показывающую загрузку потоков. Ниже показано окно программы qslice из Windows 2000 Resource Kit. В нем отображены перечень потоков процесса ntfrs и их текущая загрузка.

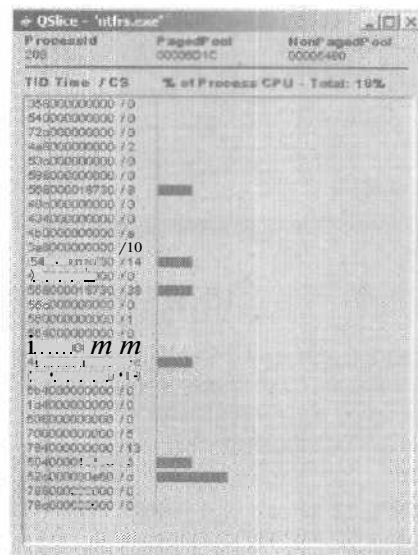
Допустим, вас заинтересовала высокая загрузка потока с ID=Qx52c. Без журнала ntfrs не выяснить, что именно вызвало повышенную загрузку. Если же такой журнал под рукой, сделаем поиск всех сообщений, относящихся к данному потоку. Так как шестнадцатеричному числу Qx52c соответствует десятичное 1324, выполним:

```
find /i /n "1324" ntfrs_000x.log > 1324.txt
```

и в файле 1324.txt обнаружим целую серию записей вида:

```
[198]>FrsGetOrSetFileObjectId: 1324: 4398: S1: 16:14:36> ++ ERROR - Set  
oid failed on file Policies; NTStatus: STATUS_DUPLICATE_NAME  
[199]>StuExecuteInstall: 1324: 1647: SO: 16:14:36> :: CoG 27272447,  
CxtG 9f8bf811, FV 0, FID 00570000 000030bb, FN: Policies, [Deleting  
conflicting file (ERROR_DUP_NAME)]
```

Сразу становится понятна причина возникновения проблемы.



Выяснение наиболее загруженного потока NTFRS

NTFRSUTL

Эта утилита из состава Windows 2000 Resource Kit может избавить вас от просмотра параметров в реестре или поиска необходимых атрибутов в Active Directory. Кроме того, только она позволяет отображать содержимое таблиц FRS. Хотя NTFRSUTL имеет интерфейс командной строки, предоставляемая ею информация весьма полна.

Общую информацию о службе FRS на любом компьютере вы получите, выполнив команду:

```
ntfsutl ds <имя компьютера>
```

Выводимая информация понятна без комментариев. Единственное, что нуждается в небольшом пояснении, — это вывод сведений о расписании репликации. В общем случае они имеют такой вид:

```

Schedule
Day 1: 111111111111111111111111
Day 2: ffffffffffffffffffffffff
Day 3: 000000000000000000000000
Day 4: ffffffffffffffffffffffff
Day 5: 555555555555555555555555
Day 6: ffffffffffffffffffffffff
Day 7: ffffffffffffffffffffffff

```

Первый день соответствует воскресенью, последний — субботе. Цифры (а их по 24 в каждой строке) соответствуют частоте репликации в течение часа:

- ◆ 0 — репликация не выполняется;
- 1 — репликация выполняется раз в час (значение для репликации DFS);
- 5 — репликация выполняется дважды в час;
- ◆ F — репликация выполняется четырежды в час (значение по умолчанию для репликации SYSVOL).

Ошибки, найденные в конфигурации, легко обнаружить по метке «WARN».

В предыдущем разделе рассказывалось, как обнаружить поток службы FRS, отбирающий процессорное время, с помощью журнала и утилиты `Qslic`. Статический снимок этой же информации позволяет получить и утилита `Ntfrsutl`, запущенная с ключом `threads`:

NTFRS THREAD USAGE:

```

FrsDs           2 CPUSeconds (2 kernel, 0 elapsed)
DelCs           0 CPUSeconds (0 kernel, 0 elapsed)
OutLog          0 CPUSeconds (0 kernel, 0 elapsed)
JRNL            0 CPUSeconds (0 kernel, 0 elapsed)
DBC             2 CPUSeconds (1 kernel, 0 elapsed)
COAccept        0 CPUSeconds (0 kernel, 0 elapsed)
ReplicaCs       0 CPUSeconds (0 kernel, 0 elapsed)
ReplicaCs       0 CPUSeconds (0 kernel, 0 elapsed)
ReplicaCs       0 CPUSeconds (0 kernel, 0 elapsed)
PROCESS        15 CPUSeconds (14 kernel, 0 elapsed)

```

Отличие в том, что вместо идентификаторов отображаются «дружественные» имена потоков.

В начале главы я много говорил о таблице идентификаторов файлов. Выполнив команду:

```
ntfrsutl idtable
```

вы получите список всех записей в этой таблице. Вот пример:

Table Type: ID Table for DOMAIN SYSTEM VOLUME (SYSVOLSHARE)

```

FileGuid           : 5c918aff-c623-4cc5-8f0e3bf7f340822a
FileID            : 00050000 00000071
ParentGuid        : 2f74c499-6780-4ecc-ae832a17fbbea463
ParentFileID      : 00060000 00000074
VersionNumber     : 00000000
EventTime         : Tue Jan 15, 2002 22:19:33
OriginatorGuid    : 7bca9f4d-b794-444a-ad7db40711f3ace1
OriginatorVSN     : 01c19df9 3c204cff
CurrentFileUsn    : 00000000 000feef8
FileCreateTime   : Tue Jan 15, 2002 22:19:33
FileWriteTime     : Tue Jan 15, 2002 22:19:33
FileSize         : 00000000 00000098
FileObjID        : 00000000-0000-0000-0000000000000000
FileName         : fddeploy.ini
FileIsDir        : 00000000
FileAttributes    : 00000022 Flags [HIDDEN ARCHIVE ]
Flags            : 00000000 Flags [<Flags Clear>]
ReplEnabled       : 00000001
TombStoneGC      : Sun Mar 17, 2002 22:00:39
OutLogSeqNum     : 00000000 00000000
Extension        : MD5: a6b54997 b18c9b2b 39382aa8 64ce0830
  
```

Последняя строка содержит контрольную сумму файла используемую при сравнении файлов в репликах.

Наконец, эта утилита позволяет управлять временем опроса Active Directory на предмет **внесения изменений** в конфигурацию. Если просто выполнить команду:

```
ntfrsutl poll
```

будет выведено **сообщение** о текущих интервалах опроса:

```

Current Interval:   5 minutes
Short Interval  :   5 minutes
Long Interval   :  60 minutes
  
```

Дополнительные ключи Now (сейчас). Quickly= (быстро) и Slowly= (медленно) позволяют задать быстрый и медленный интервал, а также выполнить опрос незамедлительно.

Пример диагностики проблем **репликации** каталога SYSVOL с помощью NTFRSUTL см. в Microsoft *Technet* в статье «Troubleshooting Missing SYSVOL and NETLOGON Shares [Q257338]».

Восстановление реплицируемых файлов

Когда заходит речь о файлах и их хранении, как **правило**, затрагивается тема резервного копирования и восстановления. Обычно для этих целей используют специальные программы вроде Windows Backup,

встроенной в ОС. Несомненно, что для резервного копирования файлов, тиражируемых службой FRS, используются те же программы. Резервное копирование не представляет какого-либо интереса (программе все равно, какие файлы сохранять), а вот восстановление — предмет отдельного разговора.

Служба FRS отслеживает изменения в файлах и хранит их версии — это основа работы механизма репликации. Однако версии файлов не сохраняются при резервном копировании, а значит, восстановленная информация оказывается в неопределенном положении: служба FRS должна получать указания, что делать с восстановленными файлами: заменить новыми или тиражировать их на все остальные партнеры по репликации в наборе реплик,

Эта дилемма существует и для объектов Active Directory. Там действуют понятия *авторитетного* и *неавторитетного* восстановления из резервной копии. Те же понятия актуальны и для механизмов восстановления FRS.

При неавторитетном восстановлении те файлы в восстановленной реплике, контрольная сумма которых совпадает с контрольной суммой файлов у партнера по репликации, остаются неизменными. Если же контрольная сумма различна, место восстановленного файла занимает файл, переданный партнером по репликации.

При авторитетном восстановлении восстановленные файлы являются истиной в конечной инстанции. Сведения о них передаются всем партнерам по репликации, и там, где наблюдается различие контрольных сумм, они заместят файлы в других репликах.

Неавторитетное восстановление — предпочтительный способ восстановления файлов. Он применяется, например, при восстановлении реплицируемого каталога на одном из серверов или при переносе содержимого реплицируемого каталога на удаленный сервер на магнитной ленте или ином съемном носителе. Авторитетное восстановление используется в крайних случаях, скажем, при полном крахе или порче всех реплик. К примеру, если вы случайно удалили все каталоги групповых политик и заметили это, только когда ваши действия были реплицированы на все компьютеры, без авторитетного восстановления не обойтись.

Замечание Файл ntfrs.jdb (БД FRS) не копируется. При его порче или уничтожении его восстанавливает ОС при сравнении файлов в разных репликах.

Неавторитетное восстановление

Неавторитетное восстановление применяется в случаях:

- нарушения в работе службы FRS;
- повреждения локальной базы `ntfrs.jdb`;
- ◆ ошибок, *связанных* с переполнением журналов и, как следствие, потери информации из-за *перезаписи*;
- ◆ ошибок при репликации.

Неавторитетное восстановление можно выполнить:

- ◆ с резервной копии;
- с других партнеров по репликации.

Первый способ предполагает, что вы следуете всем рекомендациям по обслуживанию ОС и поэтому у вас есть актуальная резервная копия. Поэтому данный способ и описан в [3], [6]. Здесь я только коротко скажу, что надо сделать.

1. Исключите из набора реплик компьютер, на котором нужно восстановить реплику.
2. Восстановите файлы из резервной копии в тот каталог, который должен реплицироваться.
3. Включите компьютер в набор реплик, указав при этом на восстановленный каталог как на реплицируемый.

После этого служба FRS обнаружит, что ее конфигурация изменилась и добавит новый член. Все вновь добавленные файлы будут перенесены во временный каталог. Далее будет запрошен входной партнер по репликации обо всех файлах в его реплике. В результате сравнения контрольных сумм будут выявлены отличающиеся файлы и заменены теми, что хранятся у партнера.

Второй способ пригоден для нерадивых администраторов, считающих роскошью регулярное резервное копирование. Основан он на том, что за счет изменения значения флага `BurFlags` можно инициировать авторитетное и неавторитетное восстановление реплики.

1. Остановите службу FRS на компьютере
2. Задайте параметру `BurFlags` в ветви реестра `HKLM\SYSTEM\CurrentControlSet\Services\NtFrs\Parameters\Backup\Restore\Process at Startup` значение `0xD2`. Это позволит выполнить неавторитетное восстановление всех реплик на компьютере. Если надо восстановить только конкретную реплику, измените этот параметр в ветви `HKLM\SYSTEM\CurrentControlSet\Services\NtFrs\Parameters\Cumulative Replica Sets\<Имя GUID реплики>`
3. Вновь запустите службу FRS

Далее произойдет следующее.

- ◆ Значение параметра `BurFlags` снова сбросится в 0.

- Файлы из реплицируемых каталогов будут перемещены в каталог `NtFrs_PreExisting` [See_EventLog](#). При этом в журнале службы репликации файлов появится сообщение с Event ID=13520 о выполненной операции.
- БД службы FRS будет перестроена заново.
 - ◆ Произойдет начальное подключение к набору реплик (создание вектора версий — процесс VV-join) того партнера, с которым имеется входной объект связи, либо того, что прописан в параметре `Replica Set Parent` для реплики `SYSVOL`. Сообщение об успешном добавлении к набору реплик появится в журнале регистрации под номером 13553. Как только откроется окно репликации, будет выполнена полная синхронизация реплик.

Зачем перемещать файлы в каталог `NtFrs_PreExisting` [See_EventLog](#)? Допустим, незадолго до того, как вы обнаружили, что реплика нуждается в восстановлении, в нее были внесены изменения, которые не были тиражированы на другие компьютеры. В таком случае после завершения синхронизации можно сравнить содержимое этого каталога с реплицируемым, выяснить различия и, если понадобится, повторить их путем копирования нужных файлов. Когда вы поймете, что репликация завершилась нормально и перенесете файлы из каталога `NtFrs_PreExisting` [See_EventLog](#), все файлы в нем можно удалить для освобождения диска.

Замечание Если указанный каталог не отличается от реплицируемого, он будет удален автоматически по завершении синхронизации.

Внимание Прежде чем выполнять неавторитетное восстановление этим способом, убедитесь, что вы уже ликвидировали причину сбоя, данный компьютер связан с «эталонным» компьютером, хранящим верную реплику и топология репликации такова, что неверные реплики с других партнеров по репликации не исказят данных.

Авторитетное восстановление

Авторитетное восстановление — последняя соломинка. К нему можно прибегнуть, только когда вы поняли, что уже ничто не поможет. Авторитетное восстановление выполняется двумя способами: из резервной копии и с партнера по репликации. Первый описан в [6] и здесь приведен вкратце. Второй способ описан полностью.

Восстановление с магнитной ленты. Магнитная лента, конечно, не единственный носитель: восстановление можно сделать с любого съемного носителя, используя `Windows Backup`. Эта программа устроена так, что при восстановлении реплицируемых файлов на кон-

троджере домена она позволяет указать, что восстанавливаемые данные являются первичным источником для всех реплик. Для этого отметьте флажок *When restoring replicated data sets, mark the restored data as the primary data for all replicas*. Иная картина на *сервере — члене домена*, где этот флажок использовать нельзя, Авторитетное восстановление возможно только на сервере, являющемся первым в наборе реплик. Для этого все файлы из реплицируемого каталога полностью удаляются, а потом восстанавливаются из резервной копии. Если сервер не первый в наборе реплик, возможно только неавторитетное восстановление.

Восстановление из реплики выполняется следующим образом.

1. Остановите службу FRS на всех компьютерах в наборе реплик.
2. На компьютере-эталоне задайте параметру *BurFlags* в ветви реестра *HKLM\SYSTEM\CurrentControlSet\Services\NtFrs\Parameters\Backup/Restore\Process at Startup* значение *0xD4*. Это позволит выполнить авторитетное восстановление всех реплик на компьютере. Если надо восстановить только конкретную реплику, измените этот параметр реестра в ветви *HKLM\SYSTEM\CurrentControlSet\Services\NtFrs\Parameters\Cumulative Replica Sets\<номер GUID реплики>*.
3. Запустите службу FRS на эталонном компьютере.

Далее произойдет следующее.

- ◆ Значение параметра *BurFlags* снова сбросится в 0.
- ◆ Файлы, расположенные в реплицируемом каталоге, останутся на своем месте и станут «авторитетными» для всех остальных партнеров по репликации.
- ◆ БД FRS будет перестроена на основании данных файлов.

Обязательно дождитесь появления в журнале событий службы репликации файлов сообщений о событиях 13553 и 13516. Далее можно по очереди включать службу FRS на партнерах по репликации, предварительно задав параметру *BurFlags* значение *0xD2*, т. е. инициализировав на них неавторитетное восстановление.

Восстановление конфигурации FRS

Говоря о конфигурации FRS, я подразумеваю те объекты Active Directory, что относятся к этой службе и были рассмотрены ранее. Восстановление объектов Active Directory возможно из резервной копии состояния системы (System State). В главе «Поиск и устранение проблем» я подробно описываю восстановление системного состояния. Здесь же я напомню, что, выбирая System State в программе резервного копирования, вы позволяете сохранять БД и журналы Active Directory, загрузочные файлы, зарегистрированные в системе COM+ объекты, реестр и... файлы каталога SYSVOL.

Ага, значит, из того, что относится к службе репликации файлов, в системное состояние включены объекты FRS и файлы SYSVOL! Возможно, что все, что сказано выше о восстановлении реплик, можно сделать иначе? Возможно... Но разберемся по порядку. Начнем с восстановления объектов FRS в Active Directory.

Допустим, вы удалили объекты FRS. Для восстановления объектов в AD, как известно, надо проделать авторитетное восстановление системного состояния из резервной копии:

- ◆ загрузите контроллер домена в режиме восстановления службы каталогов;
- восстановите самую свежую версию System State с помощью Windows Backup;
- отметьте удаленный контейнер как авторитетный с помощью программы ntdsutil;
- загрузите контроллер домена в нормальном режиме и дождитесь завершения репликации;
- ◆ если с момента выполнения резервного копирования состояния системы были добавлены новые реплики, добавьте их повторно.

А если удалены файлы в каталоге SYSVOL? Можно следовать алгоритму авторитетного восстановления объектов AD. Несомненно, этим способом удастся восстановить содержимое SYSVOL, но при этом восстановятся объекты Active Directory, соответствующие старому состоянию системы и, так как они восстановятся авторитетно, они перезапишут информацию на всех остальных контроллерах домена. То есть вы отбросите всю систему на какое-то время назад. Так значит, авторитетное восстановление в ntdsutil для восстановления SYSVOL использовать нельзя? Можно, но только делать это надо так:

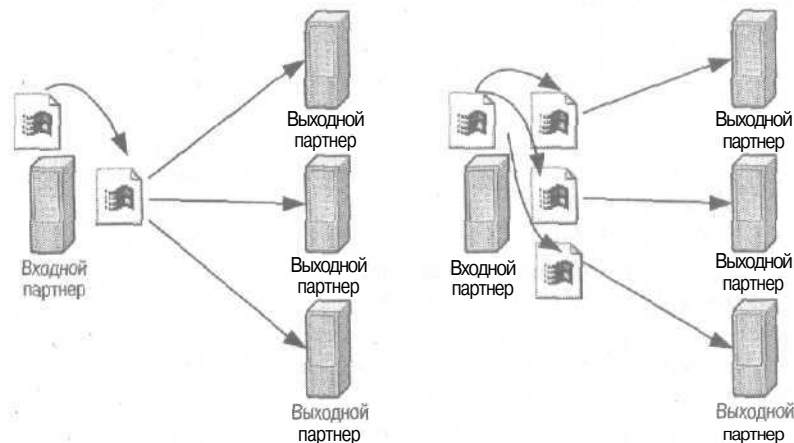
- ◆ загрузите контроллер домена в режиме восстановления службы каталогов;
- восстановите самую свежую версию System State с помощью Windows Backup в другое место на диске (поле Restore Files To);
- ◆ скопируйте удаленные файлы в каталог SYSVOL;
- ◆ если удалены были файлы групповой политики, синхронизируйте версии контейнеров групповой политики и файлов групповой политики.

Оптимизация процессов восстановления

Когда выполняется нормальная репликация файла, входной партнер создает один подготовительный файл для всех выходных партнеров. В случае выполнения восстановления файлов инициируется подключение вектора версий (Vector Version Join — VV-Join), при котором

для каждого реплицируемого файла создастся по 1 подготовительному файлу для каждого выходного партнера. Если надо тиражировать 10 файлов для 10 партнеров, будет создано 100 подготовительных файлов. Это может отрицательно сказаться на производительности серверов, поэтому данный процесс нужно **оптимизировать**, т. е.:

- ◆ копировать содержимое на новые члены набора реплик с помощью программы Windows Backup (см. выше);
- ◆ уменьшать число серверов создающих подготовительные файлы;
- сокращать число реплицируемых файлов в каталогах на время выполнения процесса WV-join.
- ◆ разрешать выполнение только одного подключения вектора версий на входном партнере.



Создание подготовительных файлов при обычной репликации и при инициации процесса W-join

Сокращение числа серверов, создающих подготовительные файлы

Сначала посмотрим на репликацию SYSVOL. При добавлении компьютера в домен репликация SYSVOL выполняется с того контроллера домена, с которого пришла информация об Active Directory. Его имя временно появляется в виде значения параметра Replica Set Parent в ветви реестра `HKLM\SYSTEM\CurrentControlSet\Services\NTFRS\Parameters\SysVol\<Имя домена>`. При неавторитетном восстановлении каталога SYSVOL можно принудительно указать, с какого сервера должна выполняться репликация, добавив этот параметр в реестр. Например, это может быть контроллер, расположенный в том же сайте.

Увы, такой механизм невозможен для реплик DFS, и приходится идти в обход.

- Остановка службы FRS на всех возможных входных партнерах, кроме того, что является предпочтительным. Идеальным это решение не назовешь: несмотря на остановку службы FRS, изменения в журнале NTFS будут накапливаться, и при длительной остановке журнал может переполниться, что приведет к возобновлению записи новых событий в начало, а значит будут потеряны сообщения об изменении файлов.
- Управление количеством объектов связи со входными серверами. Удаляя объекты, можно добиться того, что репликация будет выполняться только с одного сервера.
- ◆ Ограничение времени передачи файлов между серверами периодами наименьшей загрузки канала. По каналу с пропускной способностью 64 кбит/с и загрузкой 25% можно передавать до 21 Мб данных ежесекундно, или 506 Мб ежедневно. Значит, за выходной день можно передать около 2 Гб при степени сжатия 50%. Правда, надо учесть, что те серверы, что стоят в центральном сайте и «кормят» периферийные серверы данными репликации, должны иметь большой объем свободного пространства на диске и высокое значение предельной: емкости подготовительного каталога.

Сокращение числа реплицируемых файлов на время выполнения процесса VV-join

Чем меньше файлов в каталоге, тем меньше времени займет репликация, тем меньше объем подготовительного каталога и тем меньше подготовительных файлов будет создано.

Данный подход наиболее актуален при инициализации реплик DFS, так как для DFS характерны огромные объемы реплицируемых томов и большое число партнеров, попарно связанных между собой. В меньшей степени это актуально для репликации SYSVOL, так как топология репликации в этом случае оптимально задана KCC.

И все же как для DFS, так и для SYSVOL файлы из реплицируемого каталога надо переместить в безопасное место и инициировать процесс VV-join (реинициализации членов реплики). Если речь идет о каталоге SYSVOL, то из всех файлов нужно оставить каталоги, соответствующие политике домена и политике контроллеров домена по умолчанию, задать параметру BurFlags на эталонном компьютере значение 0xD4, а на всех остальных — 0xD2. По завершении реинициализации файлы возвращаются на прежнее место, и их репликация выполняется обычным путем.

Разрешение выполнения **только** одного подключения **вектора версий на входном** партнере

Для крупных реплик DFS, содержащих десятки гигабайт данных, следует рассмотреть возможность **добавления** не более одного члена за раз. Добавив новый компьютер, надо дождаться завершения **начальной** синхронизации и выхода из **процесса VV-join**. Проконтролировать это можно по исчезновению всех файлов из подготовительного каталога.

Предел объема подготовительного каталога надо задать равным объему 128 самых крупных файлов в реплицируемом каталоге.

Распределенная файловая система

Распределенная файловая система (Distributed File System — DFS), позволяет объединить серверы и **предоставляемые** в общее **пользование** ресурсы в однородное пространство имен. DFS обеспечивает однородный поименованный доступ к набору серверов, совместно используемых ресурсов и файлов, организуя их в виде иерархии. В свою очередь новый том DFS может **быть иерархично** подключен к другим совместно **используемым** ресурсам Windows 2000. Таким образом, DFS позволяет представлять физическое устройство хранения в виде логических элементов, доступ к которым прозрачен и для пользователей, и для приложений.

DFS подробно описана в [6]. Здесь же основной упор сделан на доменную DFS, репликацию отказоустойчивых томов DFS, оптимизацию работы и поиск проблем. Для начала рассмотрим общие концепции DFS, чтобы дальше использовать единую терминологию.

Немного о DFS

Любая DFS начинается с **корня**. Если речь идет об отдельно стоящей DFS, то корнем DFS является локальный **ресурс**, который **предоставляется** в **совместное** использование и применяется как точка отсчета для остальных ресурсов. Доступ к такому ресурсу осуществляется по имени сервера, на котором этот ресурс расположен:

```
\\server\DFSRoot
```

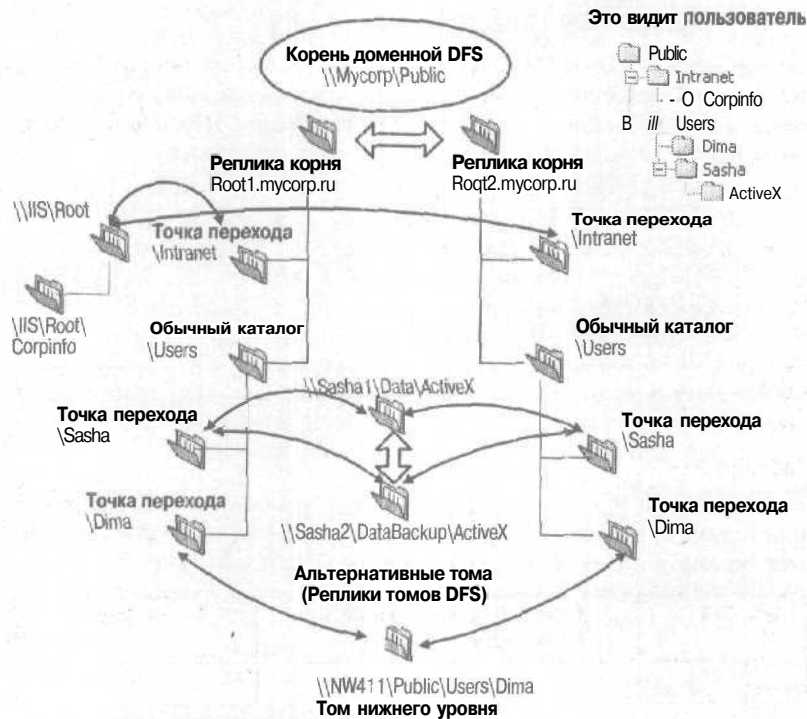
Если мы говорим о доменной DFS, то корнем также является совместно используемый ресурс на сервере, но доступ к нему осуществляется по имени домена независимо от того, на каком именно сервере расположен корень:

```
\\mycorp\DFSRoot
```

Замечание Доступ к доменной DFS возможен и по имени того сервера, который администратор выбрал в качестве *хоста* DFS.

В домене может быть несколько корней, но на одном сервере в домене может располагаться не более одного корня доменной DFS. Корни доменной DFS могут находиться либо на контроллере домена, либо на сервере — члене домена. Любой корень DFS может иметь несколько *корневых реплик*. Между репликами можно организовать тиражирование данных. По умолчанию репликации между корневыми репликами нет.

Как было сказано, информация о доменной DFS, в том числе обо всех репликах, хранится в Active Directory. Там же находится информация об *объектах связи* между репликами.



В доменной DFS может быть несколько реплик корня и альтернативных томов DFS

Под корнем находятся каталоги, часть которых является *точками перехода* DFS на другие ресурсы, как правило, на каталоги, предоставленные в совместное использование на любых других серверах, к которым есть доступ с любой реплики. Такую точку перехода совместно с каталогом, на который она указывает, называют *томом* DFS.

Замечание Под корнем могут храниться обычные каталоги, и их можно использовать для хранения данных точно так же, как в каталогах на любом другом сервере. Однако учтите, что в клиентской части DFS есть ошибка, которая не позволяет переименовывать каталоги в корне доменной DFS, названные по-русски. Эта ошибка исправлена только в .Net Server.

Если одна и та же точка перехода указывает на несколько альтернативных ресурсов с идентичным содержимым, эти точки перехода называются отказоустойчивыми томами DFS, а сами ресурсы — репликами тома DFS. Между репликами тома можно организовать тиражирование их содержимого. При запросе пользователем тома DFS с применением службы DNS на клиент передаются все реплики. Затем клиент выбирает ближайшую реплику, основываясь на сведениях о топологии узла в Active Directory. Если выбранная реплика недоступна, клиенту не надо выполнять повторный запрос к DFS.

Все тома, расположенные не на серверах Windows NT/2000, являются томами нижнего уровня. Они могут быть видны в структуре DFS, но сами не могут быть точками перехода или хостами DFS. К таким системам относятся Windows NT Workstation, Windows 9x, Windows for Workgroups, а также все сетевые ресурсы других производителей, к которым имеется доступ. Замечу, что DFS-клиент для Windows 95 может осуществлять доступ ко всем томам высокого уровня и всем SMB-томам нижнего, но не способен взаимодействовать не с SMB-томами.

Таблица PKT

Ключевую роль в работе DFS играет таблица знаний о разделах (Partition Knowledge Table — PKT), где хранится информация обо всех точках перехода. Структура таблицы такова:

Путь DFS	Список [Сервер + совместно используемый ресурс]	Время жизни

PKT существует на клиентской стороне, на сервере и в Active Directory.

Для отдельно стоящей DFS таблица PKT хранится в реестре сервера, являющегося хостом, тогда как PKT доменной DFS хранится в Active Directory. Доступ к PKT и его администрированию имеют все машины, участвующие в создании отказоустойчивого тома DFS.

PKT в Active Directory представляет собой атрибут pkt у объекта <имя корня DFS>,CN=Dfs-Configuration,CN=System,<имя домена>. Вообще именно этот объект хранит сведения о DFS. Это, скажем честно, не

лучшее решение, так как сказывается на масштабируемости отказоустойчивых корней DFS (см. раздел «Предельные возможности»).

На клиентской стороне существует одна РКТ для каждого тома DFS. После получения ссылки из серверной РКТ информация о ней остается в таблице в течение 30 минут. В случае повторного использования той же ссылки время жизни соответствующей строки таблицы обновляется. Если в течение 30 минут повторного обращения не происходит, соответствующая ссылка удаляется из таблицы РКТ. Если ссылка соответствует отказоустойчивому тому то кэшируется информация обо всех альтернативных ресурсах, и при повторном обращении к такой ссылке ОС произвольно выбирает один из них.

По умолчанию время кэширования — 30 минут. Но его можно изменить. Значение устанавливается для каждого тома DFS отдельно. Помните: если клиент обратится по ссылке, которую он выбрал из кэшированной таблицы РКТ до истечения срока хранения, он не узнает об изменениях. Если к этому времени физическое положение тома изменится, доступа к нему пользователь не получит.

Как видно из рисунка, в РКТ хранится соответствие логических имен DFS ссылкам на физические ресурсы. В случае альтернативных томов для точки перехода хранится список альтернативных ресурсов. Каждая строка в таблице занимает около 300 байт.

Пытаясь пройти точку перехода, клиент сначала обращается к РКТ, хранящейся в локальном кэше. Если описания этой точки там нет, он обращается к корню DFS. Если же при этом не происходит определение точки перехода, выдается сообщение об ошибке. Если ссылка разрешается, информация о ней заносится в локальную РКТ.

В РКТ хранятся сведения, позволяющие пользователям Windows 2000/XP подключаться к ресурсам в том сайте, в котором они находятся.

Внимание Данные о принадлежности к сайту заносятся в РКТ на этапе конфигурирования DFS. Если сервер переносится в другой сайт, DFS надо переконфигурировать. Помните об этом, используя подготовительный сайт в крупных компаниях (см. главу «Планирование Active Directory»).

Как известно, существуют две ревизии клиентской части DFS; 2 (реализована на клиентах Windows 9x/NT) и 3 (реализована на клиентах Windows 2000/XP). Между ними много различий, но я хочу обратить внимание на то, как данные об отказоустойчивых томах передаются клиентам из РКТ в зависимости от номера ревизии.

Для клиентов ревизии 2 таблица ссылок на все реплики передается в том виде, как она хранится на сервере. Записи предварительно не

сортируются. Клиент сам произвольно тасует полученные записи и выбирает первую попавшуюся.

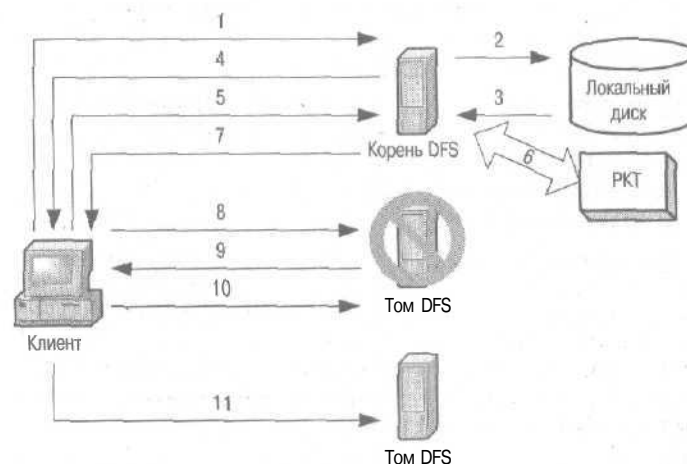
Для клиентов ревизии 3 таблица ссылок предварительно разбивается на две части: в первой перечисляются ссылки на реплики, расположенные в том же сайте, что и клиент, во второй — все остальные. Клиент перемешивает каждую из частей в произвольном порядке.

Описанный алгоритм обеспечивает балансировку нагрузки между репликами. И хотя такая балансировка весьма относительна, так как не принимает в расчет реальной загруженности реплик, она дает свой положительный эффект.

Замечание Принадлежность к сайту игнорируется в двух случаях: если доступ к корню или тому DFS осуществляется из консоли управления сервером DFS и из терминальной сессии, открытой на сервере DFS.

Взаимодействие клиента с сервером DFS

Как клиент взаимодействует с сервером DFS? Взгляните на рисунок:



Последовательность обращений клиента к корню DFS

1. Допустим, клиент обращается к серверу, на котором расположен корень DFS, и передает ему SMB запрос к ресурсу вида `\\server\public\file.txt`.
2. Первым делом сервер пытается обратиться к своему локальному ресурсу.
3. Довольно быстро обнаруживается, что такого локального ресурса нет.

4. Поэтому сервер посылает клиенту ответ `STATUS_PATH_NOT_COVERED`.
5. Если бы такой ответ получил обычный клиент (скажем, Windows 9x), он бы сообщил пользователю о неверно введенном имени файла. Иное дело, когда такой ответ получает клиент DFS. В ответ он посылает на сервер запрос `TRANS2_DFS_GET_REFERRAL`.
6. Обработывая этот запрос, сервер DFS обращается к PKT. Если для запрашиваемого файла имеется только одна ссылка на сервер, возвращается полное UNC-имя файла. Если есть ссылки на альтернативные тома, передается список альтернативных путей.
7. Сервер передает список клиенту.
8. Клиент выбирает из списка произвольный путь например `\\fsl\public\file.txt`, и обращается к указанному ресурсу.
9. Допустим, выбранный сервер недоступен в момент обращения либо на нем нет указанного файла. В первом случае клиент прервет обращение по тайм-ауту, во втором — сервер пошлет клиенту ответ `STATUS_PATH_NOT_COVERED`.
10. Это сообщение будет расценено клиентом иначе, чем при обращении к корню DFS. На этот раз клиент пошлет уведомление серверу `TRANS2_REPORT_DFS_INCONSISTENCY`.
11. Уведомив сервер, что у того не все в порядке, клиент выбирает из локальной PKT следующий путь к файлу, например `\\fs2\public\file.txt`, и обращается к нему. Если файл доступен, начинаются обычные операции чтения-записи.

Репликация DFS

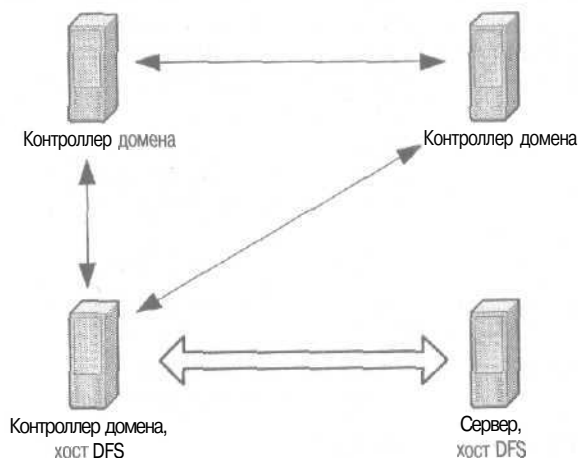
Первая часть этой главы практически полностью охватывает вопросы, связанные с репликацией DFS. Поэтому здесь я коротко рассмотрю те вопросы, которые обошел вниманием ранее.

Начну с того, что для репликации DFS не обязательно использовать службу FRS. Если у вас есть механизм, обеспечивающий большую эффективность, задействуйте его.

Как я неоднократно говорил, реплицировать можно как содержимое альтернативных томов DFS, так и сами корни доменной DFS.

Говоря о репликации корней доменной DFS, я имею в виду два различных механизма репликации. Первый — тиражирование объектов конфигурации DFS между контроллерами доменов. При этом задействован механизм репликации Active Directory. Второй — тиражирование содержимого корней на серверах-носителях корней. Если в домене три контроллера и два сервера — члена домена, на которых располагаются корни DFS, репликация выполняется по кольцу для

контроллеров домена и напрямую — между двумя серверами. И эти процессы между собой не связаны. Поэтому в определенные моменты после внесения изменений в конфигурацию DFS (а вносятся они всегда только на имитаторе PDC) будет существовать разное знание контроллеров о DFS, и клиенты, обращающиеся к разным контроллерам, будут получать разные сведения о DFS и ее структуре.



Топология репликации конфигурации DFS отличается от топологии репликации корней DFS

Следует учитывать и объем, занимаемый в Active Directory объектом конфигурации DFS. Для DFS, содержащей порядка 100 ссылок, он составит около 40 кб.

Репликация альтернативных томов по умолчанию не включается. Вообще можно содержимое альтернативных томов сделать различным, и DFS на это не отреагирует, так как не занимается проверкой идентичности. Если же тома включены в набор реплик, служба FRS обеспечит их идентичность.

Как я уже говорил, топология репликации между репликами томов DFS по умолчанию представляет собой набор попарных связей между членами набора реплик. Чем больше реплик в наборе, тем труднее администрировать такую топологию и тем более искать проблемы. С другой стороны, такая топология обеспечивает минимальное время распространения изменений. И все же топологию рекомендуется оптимизировать и делать ее подобной той, что используется при репликации Active Directory. Особое внимание следует обратить на существование сайтов.

Сайты и DFS

В главе «Репликация Active Directory» показана роль сайтов в формировании топологии репликации Active Directory. Но сайты влияют и на топологию репликации DFS, и на обращение клиентов к ресурсам.

- Репликация конфигурации доменной DFS идет в строгом соответствии с разбиением на сайты. То есть между сайтами репликация выполняется по расписанию, а значит, сведения о конфигурации DFS в удаленных филиалах могут существенно отличаться от реальных, так как изменения дойдут, только когда откроется окно межсайтовой репликации.
- ◆ При старте сервера — хоста доменной DFS происходит обращение к контроллеру домена для считывания конфигурации. При обращении учитывается сайтовая информация, так что выбирается ближайший контроллер.
- Пытаясь получить доступ к ресурсу DFS, клиент не только обращается к серверу, находящемуся в одном сайте с ним, но и к контроллеру домена в том же сайте.
- Когда администратор запускает оснастку управления DFS, она подключается к контроллеру домена, расположенному в том же сайте.

Предельные возможности и ограничения

Теперь обсудим масштабируемость DFS. В разных источниках приводятся противоречивые сведения и, чтобы исключить путаницу, я приведу данные, опубликованные в Microsoft Technet в статье «DFS Scalability in Windows NT 4.0 and Windows 2000 [Q232613]».

Масштабируемость DFS

Ресурс	Предел
Максимальное число отказоустойчивых корней в домене	1 на сервере, 16 в домене (рекомендуется)
Максимальное число отдельных корней на компьютере	1
Максимальное число точек перехода в доменной DFS	5 000
Максимальное число точек перехода в отдельно стоящей DFS	10 000
Максимальное количество корневых реплик	Рекомендуется не более 16
Максимальное количество реплик томов	256

Максимальное число корней на одном сервере будет увеличено в следующих после Windows 2000 версиях. Пока же приходится мириться с этим ограничением.

Отдельно стоящая DFS хранит сведения о конфигурации в реестре в ветви `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DfsHost`. Предел, установленный для размера файла реестра и равный 13 Мб, не является сдерживающим фактором. При числе точек перехода, превышающем 10 000, производительность ОС во время загрузки сильно снижается. После загрузки она продолжает работать в обычном режиме. Исходя из этого, рекомендуется создавать несколько корней, когда нужно использовать более 10 000 точек перехода.

Для доменной DFS вся информация о корне, точках перехода, репликах и их **сайтовой** принадлежности хранится, как я уже говорил, в атрибутах одного объекта Active Directory. Рекомендуемый размер этого объекта — не более 5 Мб. Размер можно рассчитать по формулам:

объем, занимаемый корнем (в байтах):

$180 + (\text{число символов в имени DFS} \times 4) + (\text{число символов в каждой реплике корня} \times 2)$

объем, занимаемый каждой точкой перехода:

$180 + (\text{число символов в имени точки перехода относительно доменного имени} \times 4)$

Объем занимаемый каждой репликой =

$20 + (\text{число символов в имени реплики} \times 2)$

объем, занимаемый каждым сервером, на котором располагается реплика:

$12 + (\text{число символов в имени сервера} + \text{число символов в названии сайта}) \times 2$

Узнать текущий размер объекта позволяет команда `dfsutil` (см. далее). Превышение указанного значения отразится на скорости загрузки компьютеров.

Вас может заинтересовать, почему доменная DFS поддерживает вдвое меньше точек перехода, чем отдельно стоящая DFS. Объяснений этому факту несколько.

- В доменной DFS сервер занимается рандомизацией ссылок в PKT, предоставляемой клиентам. Как ни мала нагрузка, она вносит свой вклад.
- ◆ Конфигурация DFS хранится в Active Directory как двоичный блок (blob) и в таком виде обновляется. Обращение к блокам требует больших процессорных ресурсов.
- ◆ Этот блок реплицируется за одну транзакцию при изменении конфигурации Active Directory. Если обновление одного из свойств срывается, происходит откат всей транзакции и ее последующее повторение.
- Отдельно стоящие DFS хранят данные в реестре и во время работы ОС располагаются в резидентной памяти. Active Directory хра-

нит информацию в базе NTDS.dit, загружаемой в нерезидентную область памяти. Доступ к объектам в резидентной памяти в общем случае выполняется быстрее доступа к объектам в нерезидентной. Значит, отдельно стоящая DFS должна обеспечивать большую производительность.

Один из показателей, характеризующим производительность сервера, — количество одновременно поддерживаемых сеансов. Для сервера DFS это 3 000–6 000. Столь большой разброс связан с тем, что это число зависит от загруженности сеансов. Для повышения числа сеансов можно оптимизировать параметр Autodisconnect командой:

```
net config server /autodisconnect:xx
```

где xx — время в минутах, диапазон — от -1 до 65 535. Этот параметр указывает время простоя в сеансе, по истечении которого сеанс отключается. При значении -1 отключение не выполняется.

Если пользователей, работающих с сервером, много, значение параметра можно уменьшить. Если же на DFS-сервере хранятся персональные каталоги пользователей, его стоит увеличить, чтобы пользователи не отключались в течение рабочего дня.

Ограничения доступа

С точки зрения пользователя, доступ к ресурсам DFS не отличается от доступа к ресурсам любого сервера. Можно использовать UNC-имена или назначать буквы подключаемым в виде сетевых дисков каталогам. Раскрывая любой каталог, пользователь прозрачно входит в него и продвигается по дереву в пространстве имен DFS, не задумываясь о том, на каком конкретно сервере он в данный момент «находится».

Такое поведение DFS наблюдают только пользователи, зарегистрированные в том домене, где создан корень DFS, либо в доменах, имеющих с этим доверительные отношения. Если пользователь не принадлежит к домену либо домен, в котором он зарегистрирован, находится в отдельном лесу, картина кардинально меняется.

По умолчанию пользователь не имеет доступа к корню DFS. Если же при подключении к корню он введет верные для данного домена имя учетной записи и пароль, то получит доступ к корню и к ресурсам этого сервера. Попытка обратиться к томам DFS, расположенным физически на других серверах, закончится неудачей, так как DFS не предложит ввести ему альтернативные параметры регистрации.

Рассмотрим пример. Пользователь, зарегистрированный в домене mycorp.ru, пытается обратиться к ресурсу Software\User на сервере fsl.test.com. Ресурс входит в пространство имен DFS. Между доменами mycorp.ru и test.com нет доверительных отношений, но поль-

зователь знает, что для доступа можно применить учетную запись TestU.

Пользователь набирает в окне Run строку `\\fs1.test.com\software`. Дальнейшее зависит от параметров сервера DNS в домене тусогр.ru и от параметров клиентской части DNS на компьютере пользователя. Очевидно, что, если на сервере DNS нет зоны test.com или перенаправления запросов на тот сервер, где эта зона определена, доступ к ресурсу по имени будет невозможен. (Предполагаем, что у клиента в параметрах TCP/IP указан только адрес «своего» сервера DNS.) Для преодоления этой препоны пользователь должен либо прописать в параметрах клиента дополнительный адрес сервера DNS, либо обращаться к нему по адресу IP.

Пусть и эта преграда преодолена, Появляется приглашение ввести альтернативные полномочия в формате «имя домена\имя учетной записи» и пароль. Если все введено верно, появляется окно Windows Explorer со списком папок, лежащих под корнем DFS. Пользователь щелкает папку User и... получает сообщение «Access denied».

Реальный выход из этой ситуации — напрямую подключиться к серверу, на котором физически размещен этот ресурс. Если известно, что на нем хранится много томов DFS, удобно подключиться к скрытому ресурсу IPCS, и тогда использование DFS вновь станет прозрачным.

Если переход DFS содержит ссылки на несколько альтернативных томов, придется напрямую подключиться ко всем либо не использовать DFS, а осуществлять прямой доступ к серверам. При этом, конечно, исключается какая-либо отказоустойчивость доступа.

Полезные советы

В этом разделе приведен ряд советов по эксплуатации DFS.

Работа DFS без NetBIOS

В главе «Установка Active Directory» мы обсуждали возможность отказа от поддержки имен NetBIOS и решили, что без поддержки NetBIOS клиенты Windows 2000 будут обладать полной функциональностью, кроме возможности обзора ресурсов сети. Но это не совсем так.

DFS использует имена NetBIOS для предоставления доступа к своему пространству имен. Это позволяет клиентам Windows 9x осуществлять доступ к ресурсам DFS (с установленным клиентом, конечно). Но вот если у клиентов Windows 2000 отключить поддержку NetBIOS, они не смогут подключиться к DFS по умолчанию.

Если использование только таких клиентов не планируется, перед конфигурированием DFS нужно модифицировать реестр на всех компьютерах, включаемых в пространство имен DFS. Параметру DFSDns-

Config в ветви реестра HKLM\System\CurrentControlSet\Services\DFS надо задать значение 1.

Внимание Если параметр DFSDnsConfig модифицировать не на всех компьютерах, включенных в пространство имен DFS, или доступ к DFS, кроме клиентов Windows 2000/XP с отключенной поддержкой NetBIOS, будут осуществлять клиенты, понимающие только NetBIOS-имена, это отрицательно скажется на доступе к DFS.

Резервное копирование пространства имен DFS

Выше, когда речь шла о службе FRS, я рассказал о резервном копировании реплицируемых файлов и каталогов. Это, несомненно, важно при работе с DFS, но не менее важно иметь возможность резервного копирования и восстановления пространства имен DFS.

Эти операции можно сделать двумя инструментами:

- Dfscmd;
- DfsUtil.

Работу с этими многофункциональными программами мы обсудим ниже. А здесь я расскажу, как их использовать для резервирования и восстановления пространства имен DFS.

Использование DfsCmd

Для сохранения пространства имен с целью его последующего восстановления команду DfsCmd следует выполнить с такими параметрами:

```
dfscmd /view \\Имя_домена\Имя_корня_DFS /batchrestore > DFS_backup.bat
```

В итоге в указанный файл будет записана последовательность команд, необходимых для воспроизведения при восстановлении. Вот пример такого файла, полученного при запуске на сервере root1, являющемся хостом доменной DFS в домене mycorp.ru. Для корня и тома Software существуют альтернативные реплики на сервере root2.

```
REM BATCH RESTORE SCRIPT
REM dfscmd /map \\MYCORP\DFSRoot \\ROOT1\DFSRoot "" /restore
REM dfscmd /add \\MYCORP\DFSRoot \\ROOT2\DFSRoot /restore
dfscmd /map \\MYCORP\DFSRoot\Software \\root1\software "" /restore
dfscmd /add \\MYCORP\DFSRoot\Software \\root2\software /restore
```

Чтобы восстановить DFS, достаточно просто выполнить этот файл.

Использование DfsUtil

Если для резервного копирования пространства имен DFS использовать DFSUtil, ее надо выполнить с такими параметрами;

```
dfsutil /view:\\Имя_DFS\Имя_корня_DFS /export:DFS_backup.txt
```

где:

имя DFS — либо имя сервера-хоста DFS, либо имя домена для доменной DFS;

имя корня DFS — имя, данное корню DFS на хосте.

Вот пример файла, получающегося в результате этой команды для той же DFS, что и выше.

```
// uncomment the addroot lines if
// you want the script to create the root
// ADDROOT:dfsroot SERVER:ROOT2 SHARE:DFSRoot
// ADDROOT:dfsroot SERVER:ROOT1 SHARE:DFSRoot
// Load the dfs information
LOAD:\\mycorp\dfsroot
// Link Information
LINK:Software /MAP GUID:C9B44B5EEB4EE64DAF6E3D0E132AADA TIMEOUT:1800
  ADD:\\root2\software
  ADD:\\root1\software
// Site Information
SITE:ROOT1 /MAP
  ADD:Default-First-Site-Name
SITE:ROOT2 /MAP
  ADD:Default-First-Site-Name
// Save the dfs information
SAVE:
```

В отличие от предыдущего этот файл нельзя использовать самостоятельно для восстановления DFS. Его нужно указать как файл импорта:

```
dfsutil /view:\\имя DFS\имя корня DFS /import:DFS_backup.txt
```

Делегирование полномочий по управлению DFS

Делегирование полномочий для доменной DFS отличается от предоставления тех же полномочий для отдельно стоящей DFS. Чтобы администрировать последнюю, пользователь должен иметь административные права на корневом сервере. По минимуму это означает включение его учетной записи в локальную группу **Administrators** на сервере — хосте DFS. Но это не все. Создание пространства имен подразумевает создание точек перехода к ресурсам на других серверах. Если эти ресурсы уже есть, дополнительных прав не требуется. Если нет, то пользователю надо предоставить локальные административные права и на всех серверах — носителях томов DFS.

Делегирование полномочий по управлению доменной DFS включает в себя предоставление полномочий на:

- + изменение конфигурации DFS (создание корней, добавление точек перехода, создание альтернативных корней и томов);

- настройку репликации томов и корней DFS (факультативно);
- создание ресурсов на других серверах, предоставление их в совместное использование для подключения к DFS, ограничение прав доступа.

Для выполнения этих трех категорий задач нужны разные полномочия.

Делегирование полномочий модификации конфигурации DFS

Конфигурация DFS хранится в свойствах объекта `имя.домена/System/Dfs-Configuration`. По умолчанию полномочия доступа к этому объекту установлены так:

Права доступа к объекту Dfs-Configuration

Группа	Полномочия
Authenticated Users	Чтение
Domain Admins	Чтение, запись, создание и удаление дочерних объектов
SYSTEM	Полный доступ
Administrators (доменная)	Чтение, запись, создание дочерних объектов
Enterprise Admins	Полный доступ
Pre-Windows 2000 Compatible Access	Просмотр содержимого, чтение объектов групп и пользователей

Для делегирования полномочий учетной записи надо предоставить соответствующие права доступа к этому объекту. Обычно достаточно прав, которыми обладает группа Administrators. Пользователь, права которому делегированы указанным способом, сможет управлять конфигурацией всех доменных DFS. Чтобы ограничить сферу его ответственности, права доступа надо предоставить не ко всему контейнеру Dfs-Configuration, а только к объекту, соответствующему нужному корню DFS.

Замечание Механизма более тонкого разграничения полномочий по управлению DFS не существует. Нельзя назначить администраторов для отдельных томов DFS.

Однако обеспечить возможность создания корней DFS предоставлением только доступа к объекту конфигурации нельзя. Пользователю нужны права на создание и модификацию каталогов на корневом сервере, а также права по предоставлению этих каталогов в совместное использование. Например, можно включить учетную запись пользователя в локальные группы администраторов на серверах — хостах DFS. Этого уже хватит, чтобы создать корень.

Делегирование полномочий **настройки** репликации томов DFS

В разделе «Объекты Active Directory, используемые FRS» я рассказал, какие объекты служат для хранения конфигурации службы репликации файлов, используемой в том числе и для репликации DFS. Объекты, относящиеся к репликации DFS, располагаются в контейнере имя-домена/System/File Replication Service и в контейнерах CN=NTFRS Subscriptions,CN=имя сервера,OU=Domain Controllers,<имя домена>. Следовательно, пользователю нужны права доступа к этим контейнерам.

По умолчанию права доступа к объекту File Replication Sendee в точности соответствуют правам доступа к объекту Dfs-Configuration, описанным выше. Изменить *эти* права можно в оснастке Active Directory Users and Computers. Права доступа к контейнеру подписчиков службы FRS по умолчанию таковы:

Права доступа к объекту NTFRS Subscriptions

Группа	Полномочия
Authenticated Users	Чтение
Domain Admins	Полный доступ
SYSTEM	Полный доступ
Administrators (доменная)	Чтение, запись, создание дочерних объектов
Enterprise Admins	Полный доступ
Pre-Windows 2000 Compatible Access	Просмотр содержимого, чтение объектов групп и пользователей

Изменить права доступа к этому контейнеру позволяет программа ADSIEdit.

Как видите, чтобы делегировать полномочия по управлению и модификации DFS, надо изменять полномочия доступа к большому числу объектов. Поэтому удобнее создать локальную группу домена DFS Admins, включить ее с соответствующими полномочиями в списки контроля доступа перечисленных выше объектов, а в нее включать глобальные группы или *пользователей*, которым надо делегировать соответствующие полномочия.

Делегирование полномочий по управлению томами DFS и разграничению доступа

Для создания томов DFS пользователь должен иметь возможность:

- ◆ создания каталога на **NTFS-разделе** сервера;
- предоставления этого каталога в совместное использование;
- ◆ разграничения прав доступа к этим каталогам.

Такие права имеют члены локальной группы Administrators на сервере. Можно включить учетную запись пользователя в эту группу. Если же это неприемлемо по соображениям безопасности, можно задей-

ствовать группу DFS Admins и предоставить ей нужные полномочия через групповую политику.

Поиск и устранение проблем DFS

Теперь можно перейти к животрепещущей теме поиска и устранения проблем. Как я уже говорил, DFS тесно связана со службой FRS (конечно, если вы используете альтернативные тома и несколько реплик корня). Значит, советы, которые я давал ранее в отношении устранения проблем этой службы, применимы и в данном случае. Но есть и своя специфика.

При работе с DFS могут возникнуть:

- проблемы доступа к пространству имен DFS;
- + проблемы доступа к томам DFS;
- задержки репликации содержимого альтернативных томов;
- + проблемы, связанные с безопасностью.

Администраторы часто чувствуют себя абсолютно беспомощными при возникновении элементарных проблем лишь потому, что не знают о DFSUtil — средстве избавления от головной боли с DFS.

DfsUtil

DFSUtil входит в состав Support Tools и является основным инструментом отладки и администрирования DFS из командной строки.

Внимание Рекомендуется применять DFSUtil из состава Support Tools, поставляемого с сервисным пакетом SP2 для Windows 2000, Стандартная утилита, поставляемая на диске с сервером Windows 2000, содержит серьезные ошибки.

Она имеет два варианта использования:

- ◆ выполнение отдельных команд, вводимых как параметры командной строки;
- выполнение сценариев, записанных в файле.

Синтаксис программы описан в справке к ней, поэтому здесь я остановлюсь только на приемах работы с ней. В разделе «Наиболее общие проблемы и их разрешение» я рассмотрю дополнительные примеры использования DFSUtil для разрешения конкретных проблем.

Внимание Не рекомендую использовать примеры, приведенные в справке к этой программе в Support Tools: они содержат неверную информацию.

/list

Аргумент /list позволяет вывести информацию обо всех DFS в домене. Если вместо «голового» аргумента использовать /list:имя.домена, будет выведен список всех корней DFS в указанном домене. В противном случае выводится список корней в том домене, где находится клиентский компьютер. Вот пример выводимой информации:

```
Getting DomDfs's in
Connecting to ROOT1.mycorp.ru
Found 1 DomDfs's
DFSRoot
The command completed successfully.
```

Если у вас есть сомнения в идентичности конфигурации DFS на разных контроллерах домена, можете дополнительно указать аргумент /dcname:имя.контроллера.домена. При этом будет предоставлена информация о конфигурации DFS на этом контроллере. Простое сравнение покажет, тождественны ли реплики.

/view

Аргумент /view позволяет не просто узнать, сколько корней DFS в домене, но и получить исчерпывающие сведения о каждом. Степень подробности данных можно изменять. По умолчанию выводится информация вроде этой:

```
C:\>dfsutil /view:\\mycorp\dfsroot

Здесь mycorp — это NetBIOS-имя домена (хотя ничто не запрещает
использовать DNS-имя), а dfsroot — имя корня,
\\mycorp\dfsroot is a DomDfs
Connecting to ROOT1

Итак, тип DFS — доменная. Сведения будут взяты с контроллера
ROOT1. По умолчанию берется информация с имитатора PDC. Если
бы надо было взять информацию с другого контроллера, то в коман-
дной строке надо указать аргумент /dcname:имя.контроллера.

--- Blob is 826 bytes...
```

Эта строка говорит о размере объекта конфигурации DFS в Active Directory.

```
Type is DomDfs
There are 2 dfs-links in this Dfs.
\\MYCORP\DFSRoot []
    Timeout is 300 seconds
    \\ROOT2\DFSRoot
    \\ROOT1\DFSRoot
\\MYCORP\DFSRoot\Software []
    Timeout is 1800 seconds
```

```

    \\root2\software
    \\root1\software

```

Приведенные данные свидетельствуют о том, что два альтернативных корня расположены на серверах ROOT1 и ROOT2 в каталогах DFSRoot. Период опроса Active Directory об изменениях в их конфигурации — 5 минут. Кроме того, два альтернативных тома имеют в пространстве имен DFS имя Software, они расположены также на серверах ROOT1 и ROOT2 в каталогах Software. Период опроса Active Directory об изменениях в их конфигурации — 30 минут.

Siteinformation:

ROOT1

Default-First-Site-Name

ROOT2

Default-First-Site-Name

The command completed successfully.

Завершается вывод информации сведениями о сайтовой принадлежности этих двух серверов.

Дополнительный аргумент /level:1 позволяет получить более подробные сведения, например:

```
C:\>dfsutil /view:\\mycorp\dfsroot /level:1
```

```
\\mycorp\dfsroot is a DomDfs
```

```
Connecting to ROOT1
```

```
— Blob is 826 bytes...
```

```
Type is DomDfs
```

```
There are 2 dfs-links in this Dfs.
```

До этого момента выводимая информация совпадает:

```
Version:1
```

```
remoteServerName:[\\ROOT2\DFSRoot][\\ROOT1\DFSRoot][*]
```

```
\\HYCORP\DFSRoot []
```

```
GUID: D642D0B5E77CB04B94B99EF486B4CD76
```

```
ShortPrefix: \MYCORP\DFSRoot
```

```
ObjectName: \domainroot
```

```
State:0x1 Type:0x81 Version:0x3
```

```
Timeout is 300 seconds
```

```
\\ROOT2\DFSRoot
```

```
State:0x2 (DFS_STORAGE_STATE_ONLINE) Type:0x1 (DFS_STORAGE_TYPE_DFS)
```

```
\\ROOT1\DFSRoot
```

```
State:0x2 (DFS_STORAGE_STATE_ONLINE) Type:0x1 (DFS_STORAGE_TYPE_DFS)
```

```
\\MYCORP\DFSRoot\Software []
```

```
GUID: C9B44B5EEB4EE64DAF6E3D0E132AADAFA
```

```
ShortPrefix: \MYCORP\DFSRoot\Software
```

```
ObjectName: \domainroot\C9B44B5EEB4EE64DAF6E3D0E132AADAFA
```

```
State:0x1 Type:0x1 Version:0x3
```



```

Timeout is 1800 seconds
\\root2\software
State:0x2 (DFS_STORAGE_STATE_ONLINE) Type:0x2 (DFS_STORAGE_TYPE_NONDFS)
\\root1\software
State:0x2 (DFS_STORAGE_STATE_ONLINE) Type:0x2 (DFS_STORAGE_TYPE_NONDFS)

```

Но на этом возможности применения аргумента /view не исчерпываются. Как я уже говорил, DFSUtil позволяет задействовать конфигурационные сценарии DFS. Сценарий можно написать самостоятельно, так как язык сценария прост и все доступные функции можно узнать, выполнив команду `dfsutil /scripthelp`. Однако чаще требуется сохранить текущую конфигурацию DFS для ее последующего воспроизведения. Сохранение конфигурации также выполняет команда `dfsutil /view`, но с аргументом /export:имя_файла. Пример выполнения этой команды см. в разделе «Резервное копирование пространства имен DFS». Сценарий запускается аргументом /import:имя_файла. В упомянутом разделе приведен пример использования и этого аргумента.

/pktinfo

Этот аргумент позволяет клиентской стороне узнать содержимое PKT, хранящееся в локальном кэше и на сервере, с разной степенью подробности. Эта информация позволяет сравнить содержимое кэшированной таблицы PKT с серверной, что поможет при поиске проблем. Запуск программы только с аргументом /pktinfo выводит сведения о PKT, хранящиеся в локальном кэше:

```

C:\>dfsutil /pktinfo
-mup.sys-

```

Вот это сообщение и говорит о том, что данные берутся из локального кэша, так как `mup.sys` — один из основных компонентов клиента DFS.

3 entries...

Entry: \mycorp.ru\sysvol

ShortEntry: \mycorp.ru\sysvol

Expires in 660 seconds

UseCount: 0 Type:0x81 (REFERRAL_SVC DFS)

0: [\ROOT1.mycorp.ru\sysvol] State:0x39 (ACTIVE)

1: [\ROOT2.mycorp.ru\sysvol] State:0x29 ()

Любопытно, да? Оказывается, ссылка на каталог SYSVOL тоже хранится в PKT! Таким образом, вы получаете лишнее подтверждение близости DFS и службы FRS.

Строка Expires in (Истекает через...) показывает срок, по истечении которого данная ссылка будет исключена из кэша PKT.

Entry: \mycorp\dfsroot

ShortEntry: \mycorp\dfsroot

```
Expires in 180 seconds
UseCount: 0 Type:0x81 ( REFERRAL_SVC DFS )
  0:[\ROOT2\DFSRoot] State:0x09 C )
  1:[\ROOT1\DFSRoot] State:0x19 ( ACTIVE )
Entry: \mycorp\DFSRoot\Software
ShortEntry: \mycorp\DFSRoot\Software
Expires in 1080 seconds
UseCount: 0 Type:0x1 ( DFS )
  0:[\root2\software] State:0x21 ( )
  1:[\root1\software] State:0x31 { ACTIVE }
```

Не совсем ясно, что значат фраза **State** и числа рядом с ней. Но если указать аргумент `/level:1`, та же информация будет выглядеть таю

```
C:\>dfsutil /pktinfo /level:1
-mup.sys-
3 entries...
Entry: \mycorp.ru\sysvol
ShortEntry: \mycorp.ru\sysvol
Expires in 900 seconds
UseCount: 0 Type:0x81 { REFERRAL_SVC DFS }
  0:[\ROOT1,mycorp.ru\sysvol] State:0x39 C ACTIVE MASTER REFERRAL DOWNLEVEL )
  1:[\ROOT2,mycorp.ru\sysvol] State:0x29 ( MASTER REFERRAL DOWNLEVEL )
Entry: \mycorp\dfsroot
ShortEntry: \mycorp\dfsroot
Expires in 180 seconds
UseCount: 0 Type:0x61 ( REFERRAL_SVC DFS )
  0:[\ROOT2\DFSRoot] State:0x09 ( MASTER REFERRAL )
  1:[\ROOT1\DFSRoot] State:0x19 ( ACTIVE MASTER REFERRAL )
Entry: \mycorp\DFSRoot\Software
ShortEntry: \mycorp\DFSRoot\Software
Expires in 1080 seconds
UseCount: 0 Type:0x1 { DFS }
  0:[\root2\software] State:0x21 ( MASTER DOWNLEVEL )
  1:[\root1\software] State:0x31 { ACTIVE MASTER DOWNLEVEL }
```

Теперь понятно, что значения **State** (состояние) соответствуют следующим элементам DFS:

Значение	Чему соответствует
0x09	Главная реплика ссылки на корень
0x19	Активная главная реплика ссылки на корень
0x21	Главная реплика тома нижнего уровня
0x29	Главная реплика ссылки на том нижнего уровня
0x31	Активная главная реплика тома нижнего уровня
0x39	Активная главная реплика ссылки на том нижнего уровня

Активность реплики означает, что именно к ней выполняется обращение.

Кстати, срок, по истечении которого сведения о томе SYSVOL будут удалены из кэша, изменился. Дело в том, что между последовательно выполненными командами dfsutil было выполнено обращение к SYSVOL и счетчик обновился.

Сравнить локальную таблицу РКТ с тем, что хранится на сервере, позволяет аргумент /dfs:

```
C:\>dfsutil /pktinfo /dfs
-dfs.sys-
```

Заметьте: предыдущая строка говорит о том, что информацию предоставил модуль dfs.sys — один из основных компонентов серверной части DFS.

```
2 entries...
Entry: \MYCORP\DFSRoot
ShortEntry: \MYCORP\DFSRoot
Expires in 0 seconds
UseCount: 0 Type:0x581 ( LOCAL PERMANENT REFERRAL_SVC DFS )
  0:[\ROOT1\DFSRoot] State:0x09 { }
  1:[\ROOT2\DFSRoot] State:0x09 ( )
Entry: \MYCORP\DFSRoot\Software
ShortEntry: \MYCORP\DFSRoot\Software
Expires in 0 seconds
UseCount: 0 Type:0x901 ( LOCAL_XPOINT PERMANENT DFS )
  0:[\root1\software] State:0x21 ( )
  1:[\root2\software] State:0x21 ( )
```

Первое, что бросается в глаза, — полное отсутствие информации о томах SYSVOL. И правильно: ведь формально они не имеют отношения к серверу DFS. Второе — величина времени в строке Expires in. Она равна 0. Это значит, что информация постоянно хранится и не может быть выброшена из РКТ на сервере, пока конфигурация не изменится. Наконец, в этой таблице РКТ не показано, какая из реплик активна. Сервер не может этого знать, так как для разных клиентов активной может быть своя реплика.

Аргументы управления конфигурацией

Для управления конфигурацией служат:

- оснастка MMC Distributed File System с графическим интерфейсом;
- программа DFSCmd с интерфейсом командной строки.

Однако и DFSUtil может оказаться полезной, так как выполняет эти операции по-другому. Например, удаление реплики корня и последу-

ющее его восстановление не приводят к запуску процесса начальной синхронизации VV-join.

Среди аргументов можно выделить группу тех, что позволяют управлять конфигурацией DFS (примеры их использования см. далее):

- /addroot создает корень отдельно стоящей или доменной DFS;
- ◆ /remroot удаляет корень отдельно стоящей или доменной DFS; если применить команду с этим аргументом к последней реплике корня, вся информация о DFS будет удалена;
- ◆ /reinit реинициализирует корень DFS на выбранном сервере;
- /clean обновляет записи в реестре сервера так, что оттуда удаляются все записи, свидетельствующие о том, что это корень DFS;
- /unmap удаляет точку перехода к совместно используемому каталогу на другом сервере.

Аргументы отладочного режима

Думаю, всем хорошо известно, что на диске с Windows 2000 Server есть каталог, в котором хранятся все файлы ОС, скомпилированные с отладочной информацией. Если их установить вместо обычных файлов, получается так называемая «checked»-сборка системы, которую удобно использовать при отладке системы.

Чтобы в отладочном режиме запустить DFS, надо заменить файл netapi32.dll. Это не так просто. Скорее всего потребуется загрузка с дискеты и утилита ntfsdos Марка Русиновича.

Далее надо изменить значение параметра NetAPIDfsDebug в ветви реестра HKLM\System\CurrentControlSet\Services\Dfs и задать ему значение 1. После перезагрузки компьютера станут доступны аргументы;

- /VERBOSE устанавливает степень подробности выводимой информации на клиенте;
- ◆ /DEBUG переводит DFSUtil в отладочный режим;
- ◆ /SFP показывает информацию о защите системных файлов; дополнительные аргументы /on или /off позволяют включать или отключать защиту;
- /DNS показывает значение параметра DfsDnsConfig на выбранном компьютере; дополнительный аргумент /VALUE: позволяет изменить это значение;
- /NETAPIDFSDEBUG показывает значение параметра NetApDfsDebug на выбранном компьютере; дополнительный аргумент /VALUE: позволяет изменить это значение;
- ◆ /DFSVCVERBOSE показывает значение параметра DfsSvcVerbose на выбранном компьютере; дополнительный аргумент /VALUE: позволяет изменить это значение;

- ◆ /LOGGINGDFS показывает значение параметра RunDiagnosticLoggingDfs на выбранном компьютере; дополнительный аргумент /VALUE: позволяет изменять это значение.
- /SYNCDINTERVAL показывает значение параметра SyncIntervalInSeconds на выбранном компьютере; дополнительный аргумент /VALUE: позволяет изменять это значение.
- /DFSREFERRALLIMIT показывает значение параметра DfsReferralLimit на выбранном компьютере; дополнительный аргумент /VALUE: позволяет изменять это значение.

Наиболее общие проблемы и их разрешение

Теперь самое время рассмотреть типовые проблемы и способы их разрешения. В основном для устранения проблем служит утилита DFSUtil. Но и на ней свет не сошелся клином. Другие инструменты администрирования DFS тоже не помешают.

Описанные ниже проблемы ни в коей мере не охватывают все множество затруднений, с которыми можно столкнуться. Это **всего** лишь характерные ошибки и сбои в работе DFS. Если ваша проблема не ассоциируется ни с одним из описанных ниже случаев, обратитесь к первому советчику в таких ситуациях — Microsoft Technet.

Обновление сервера до новой версии

Одна из тривиальных проблем — обновление версии. Пусть компьютер входит в пространство DFS (не будем уточнять, как именно: он может быть и корнем, и сервером, несущим том DFS). Вы хотите обновить на нем ОС. Непосредственное обновление никак не затрагивает конфигурации DFS — это похоже на установку сервисного пакета. Но есть любители переустанавливать ОС целиком с нуля. Очевидно, что переустановленная таким образом система не будет ничего знать о том, что когда-то на этом компьютере существовала DFS.

DFS, с другой стороны, не осведомлена о ваших действиях и будет по-прежнему пытаться обратиться к этому компьютеру (если вы дали ему то же имя). Результат — ошибка в работе.

Значит, прежде чем переустановить ОС, компьютер надо исключить из пространства имен DFS. Если же переустановка выполнялась не по вашей вине (скажем, произошел невосстанавливаемый крах ОС), выполните восстановление DFS с помощью команды DFSUtil.

В первую очередь надо исключить сервер из конфигурации DFS:

```
dfsutil /unmap:\\Имя_домена\Имя_корня DFS \\Имя_сервера\Имя_ресурса
```

Далее сервер нужно добавить вновь. Это можно сделать либо из стандартной оснастки управления DFS, либо командой:

```
dfsutil /addrroot:Имя_корня DFS /Server:Имя_сервера Share:Имя_ресурса
```

Изменение имени хоста DFS

Похожая проблема связана с переименованием серверов, входящих в пространство DFS. Этого надо, конечно, избегать, но уж если вы решились переименовать сервер, входящий в DFS, то удалите его из конфигурации DFS, переименуйте и после вновь включите в DFS.

Если переименование было сделано иначе, DFS надо восстановить. Думаете, администратор, понимая, что нельзя переименовывать сервер «в лоб», может на это решиться? Может: ведь бывают ситуации, когда могут происходить события, равносильные переименованию.

Рассмотрим пример. На сервер, входящий в пространство DFS в качестве одного из томов, установлено новое устройство, воспринимаемое системой как жесткий диск. На самом деле диском оно не является. До установки в качестве ресурса DFS предлагался каталог E:\Software. После установки устройства буквы дисков на сервере сдвигаются так, что каталог Software оказывается на диске F и, значит, он больше не предоставляется в совместное использование, о чем система вас и предупредит.

Замечание Стандартными средствами нельзя отменить предоставление ресурса в совместное использование, если этот ресурс принадлежит DFS.

Даже если вы отмените предыдущее предоставление и создадите ресурс с таким же именем, это будет, точки зрения DFS, другой ресурс, но поскольку БИ ее об этом не предупредили заранее, DFS будет пытаться обратиться по старому имени и сообщать об ошибке.

Для восстановления конфигурации следует выполнить описанные далее команды.

С любого клиента в домене:

```
dfsutil /unmap:\\Имя домена\Имя DFS \Старое имя сервера\ресурс
dfsutil /clean:Новое имя сервера
dfsutil /reinit:Новое имя сервера
```

На сервере надо перезапустить службы DFS:

```
net stop dfs
net start dfs
```

С этого момента сервер будет подхвачен службой DFS и вернется к нормальной работе.

Удаление последнего корня DFS

Иногда при удалении последней реплики корня DFS появляется сообщение о запрете доступа и невозможности администрирования DFS.

Подобная ошибка возникает, когда у пользователя нет нужных прав доступа к объекту конфигурации DFS в Active Directory (см. раздел «Делегирование полномочий модификации конфигурации DFS»). При этом корень DFS на сервере-хосте удаляется, а вот в Active Directory эта информация остается.

Для выхода из данной ситуации следует:

- ◆ зарегистрироваться в системе с надлежащими полномочиями;
- выполнить команду:

```
dfsutil /unmap:\\Имя домена\Имя корня DFS
```

Внимание Команда будет выполнена, даже если, помимо удаляемой реплики корня DFS, существуют другие реплики. В результате новые клиенты не получают доступа к DFS, но те клиенты, у которых в кэше осталась информация о корневых репликах, смогут по-прежнему к ним обращаться.

Для очистки «повисших» корней надо выполнить две команды:

```
dfsutil /clean:имя сервера  
dfsutil /reinit:имя сервера
```

Перемещение хоста DFS в другой сайт

При перемещении сервера — носителя реплики DFS в другой сайт информация о его сайтовой принадлежности не обновляется. Вследствие этого клиенты будут обращаться не к тому серверу по каналу связи между сайтами.

Чтобы уточнить, в каких сайтах находятся серверы с точки зрения DFS, выполните:

```
Dfsutil /view:Имя домена\Имя корня DFS
```

Такое поведение признается Microsoft в качестве проблемы, которая будет разрешена в следующей версии Windows. А пока... ее надо как-то решать.

Простейший вариант: используя графическую консоль управления DFS, исключить сервер из пространства имен DFS, а потом включить его снова. Это вынудит DFS обновить принадлежность сервера к сайту.

Это решение, однако, не лишено недостатков — они проявятся в случае использования службы FRS для репликации корня или томов DFS. Основной недостаток связан с тем, что, удаляя реплику DFS таким образом, вы удаляете ее и из топологии репликации FRS. При повторном подключении реплики начинается процесс VV-join, т. е. начинается полная синхронизация реплики с остальными.

Эту проблему позволяют решить следующие команды.

Для обновления информации о принадлежности к сайту реплики тома DFS (например, `\\Server\Share`) выполните:

```
Dfscmd /remove \\Имя_домена\Имя_DFS\Имя_перехода_DFS \\Server\Share
Dfscmd /add \\Имя_домена\Имя_DFS\Имя_перехода_DFS \\Server\Share
```

Для обновления информации о принадлежности к сайту реплики корня DFS (например, `\\RootServer\Share`) выполните:

```
Dfsutil /Remroot:Имя_корня_DFS /Server:RootServer /Share:Share
```

Внимание Эту команду нельзя использовать, если существует только одна реплика корня, так как это удалит всю конфигурацию DFS.

```
Dfsutil /Addroot: Имя_корня_DFS /Server:RootServer /Share:Share
```

Проблемы доступа к пространству имен DFS

Доступ к пространству имен DFS предоставляется без проблем, кроме тех случаев, когда;

- ◆ клиент работает на Windows 9x-компьютере без поддержки DFS — установите клиентскую часть;
- 4 корень отдельно стоящей DFS недоступен или выключен — выясните причины недоступности клиента и устраните их, и DFS вновь станет доступной;
- + доменное имя не разрешается правильно — проверьте зарегистрированные имена на сервере WINS и в DNS, а также выясните на клиенте причину неразрешения имен; скорее всего проблема связана с неверной конфигурацией сети или параметрами TCP/IP, полученными от сервера DHCP;
- клиент находится в рабочей группе или домене, с которым нет доверительных отношений — см. раздел «Ограничения доступа»;
- произошло рассогласование конфигурации DFS в Active Directory с реальной конфигурацией, например, при переименовании серверов-реплик DFS или при установке ОС с нуля — см. выше.

Невозможность администрирования DFS

Подобных случаев не так много, но вот один из них. При попытке запуска оснастки Distributed File System выводится сообщение «Distributed File System. The internal database maintained by the DFS service is corrupt». Если при этом попытаться запустить Dfscmd, то выводится сообщение об ошибке «System Error 2660 has occurred. The Internal database maintained by the DFS service is corrupt». Это случается только при соблюдении трех условий:

- ◆ в домене более одного контроллера домена (что бывает чаще всего);
- переходы DFS указывают на 3 и более серверов (альтернативных томов) — это встречается гораздо реже;
- вы не установили сервисный пакет Windows 2000.

Установите SP1, и данная проблема исчезнет.

Еще одна проблема: при попытке администрирования DFS выдается сообщение «System error 1355 has occurred. The specified domain either does not exist or could not be contacted».

Эта ошибка связана с тем, что DFS не может осуществить доступ к имитатору PDC в домене, так как все изменения в конфигурации DFS выполняются именно на нем. Проверить доступность контроллера домена позволяет команда:

```
nltest /dsgetdc:имя_домена /pdc
```

Удаление конфигурационной информации DFS

Порой всю информацию о DFS на компьютере надо удалить (обычно эта необходимость возникает, когда стандартные средства управления DFS уже не могут помочь). Это приходится делать вручную.

Удаление доменных корней

Вот как полностью удалить информацию о доменной DFS.

1. Остановите службу DFS. Откройте редактор реестра.
2. Найдите папку HKLM\Software\Microsoft\DfsHost\Volumes и удалите ее со всем содержимым.
3. Найдите папку HKLM\System\CurrentControlSet\Services\DfsDriver\LocalVolumes и удалите все вложенные в нее папки.
4. В оснастке Active Directory Users and Computers найдите контейнер DFS-Configuration. Удалите из него объект корня DFS.
5. Запустите службу DFS.

Удаление корней отдельно стоящих DFS

Чтобы полностью удалить информацию об отдельно стоящей DFS, сделайте так.

1. Остановите службу DFS. Откройте редактор реестра.
2. Найдите папку HKLM\Software\Microsoft\DfsHost\Volumes и удалите ее со всем содержимым.
3. Найдите папку HKLM\System\CurrentControlSet\Services\DfsDriver\LocalVolumes и удалите все вложенные в нее папки.
4. Запустите службу DFS.

Заключение

Как видите, репликация FRS и распределенная файловая система DFS играют важную роль в жизни ActiveDirectory. Первая обеспечивает поддержку групповой политики, вторая может оказаться подспорьем в реализации персональных каталогов пользователей и в удобном доступе к их ресурсам. Возможно, стоит перечитать главу «Групповая политика», чтобы понять все нюансы сосуществования этих функций.

Надеюсь, теперь вы поняли, как важно правильно спланировать Active Directory. Ведь стоит неверно определить сайты, как репликация каталогов SYSVOL сразу перегрузит ваши каналы. Поленитесь оптимизировать топологию репликации DFS — и все серверы, составляющие пространство имен DFS, окажутся загруженными процессами конвергенции репликации. Так что, если вы еще не ознакомились с главой «Планирование Active Directory», отсылаю вас к ней.

А вообще прочитанное должно подвигнуть вас смелее использовать DFS.

Поиск и устранение проблем

Ну, а теперь перейдем к рассмотрению общих вопросов, связанных с поиском и устранением проблем Active Directory. Вы можете спросить: а разве еще что-то осталось? **Ведь** в каждой главе, будь она посвящена установке Active Directory или репликации, рассказывалось о поиске и устранении проблем, связанных с той или функцией. Все так. Но в реальной жизни рядом с вами не окажется кого-то, кто напомним: «Эта ошибка связана с групповой политикой, открой книгу на **странице...**» Вам для начала придется понять, что явилось причиной возникновения нештатной ситуации. Записи об ошибках в журналах регистрации напоминают снежный ком: они стремительно растут, сигнализируя о проблемах в той или иной подсистеме. Но бросаться исправлять ошибки, не выявив первоисточник проблемы, бесполезно. Вот почему здесь я привожу общий алгоритм поиска и устранения неприятностей с Active Directory.

90% успеха при восстановлении ОС я отношу к наличию качественной и своевременно сделанной резервной копии. Это **ваша** страховка на случай катастрофы, и я искренне не **понимаю** администраторов, которые отсутствие резервных копий оправдывают нехваткой оборудования. Это то «**железо**», которое надо закупать в первую очередь! Ну, а если его действительно нет, то резервное копирование можно выполнять не только на магнитные ленты, но и на любые носители. Поэтому значительное внимание в этой главе я уделяю резервному копированию.

Но мало иметь резервную копию — надо уметь **правильно** ею распоряжаться в критической ситуации. Порой администратор, регулярно выполнявший резервное копирование с дрожью в коленках приступает к восстановлению системы при сбое. Его состояние понятно: он ведь до конца не уверен в том, что произойдет при **восстановлении**, не исчезнут ли очень важные данные, заработает ли система. Вот почему большой раздел посвящен восстановлению Active Directory.

Но резервная копия — не всегда единственный способ восстановления системы. Иногда в восстановлении из копии просто нет нужды. Поэтому далее мы обсудим механизмы восстановления системы без применения резервных копий.

Ну и, **наконец**, **самый** тяжелый случай. Это полный крах системы — когда в лесу доменов не остается ни одного «живого» контроллера, когда все мастера операций погибли. Но даже такую систему можно восстановить! Как? Об этом — последний раздел данной главы.

Алгоритм поиска и устранения проблем Active Directory

Проблемы с Active Directory можно разделить на четыре категории:

- повреждение базы Active Directory;
- искажение данных в Active Directory;
- ◆ нарушение работы репликации;
- ◆ проблемы с групповой политикой.

Причем, как я уже подчеркивал, все они могут возникать, конечно, по вине **оборудования** или **программ**, но источником большинства являются «кривые руки» и невнимательность.

Взять, например, повреждение базы. Оно может возникнуть при:

- ◆ внезапном отключении питания при включенном режиме отложенной записи;
- ◆ сбое диска;
- ◆ **сбое** контроллера домена.

Где тут человеческий фактор? Перечитайте-ка две первые главы. Написано **там**, что режим отложенной записи должен быть отключен? А что базу нужно разместить по крайней мере на массиве дисков RAID 0+1? И кто не знает, что выбор сервера, сделанного на Малой Арнаутской улице из соображений дешевизны, неминуемо приведет к краху? И чего же вы хотите?

А если рассмотреть проблему искажения данных в Active Directory, то на 99,9% это дело рук **человеческих**. Только администратор способен

одним движением уничтожить контейнер Active Directory или установить без предварительного тестирования приложение, делающее схему каталога малоприспособленной для дальнейшей работы!.. Но хватит об этом: книга эта ведь не чтобы корить, а чтобы учить.

Итак, есть четыре магистральных направления решения проблем. Каждое имеет свой алгоритм. Изобразив отправную точку на рисунке, отправимся по первому пути — Повреждение базы.



Возможные пути восстановления

Обычно эта проблема выражается в том, что контроллер домена не может загрузиться. В главе «Установка Active Directory» я говорил о том, что может явиться причиной долгой загрузки контроллера. Если же он не грузится совсем, надо попытаться загрузить его в режиме восстановления Active Directory. (Полагаю, вы отличите проблему, связанную с «железом» или «кривыми» драйверами, от проблемы, связанной с Active Directory.)

Если незадолго до этого печального события вы установили новое устройство или новый драйвер, то скорее всего причина в них, и восстанавливать Active Directory не надо.

Иное дело, когда контроллер домена, работавший до этого без перебоев, внезапно показал «синий экран» или молча ушел на перезагрузку. Вероятность повреждения базы при этом, особенно на дешевых компьютерах, весьма велика. Именно в этом случае загрузка в режиме восстановления Active Directory поможет найти источник проблемы. Что она дает? Немало. Например, при этом не стартуют службы, имеющие отношение к Active Directory, а значит, нет *причины*, пре-

пятствующей нормальной загрузке, и, что самое главное, файлы Active Directory при этом становятся доступны для анализа, замены, перемещения и пр.

Также вы получаете доступ к журналу регистрации. Именно здесь вы прочтете ID и описание ошибки, которая не дала загрузиться контроллеру. А дальше... ваш путь лежит на сайт <http://support.microsoft.com>, где стоит заняться поиском причин возникновения ошибки. Только помните, что искать надо первопричину, а не ее следствие.

Если поиск в базе знаний Microsoft не увенчался успехом и решение проблемы не обнаружено, стоит подумать о восстановлении базы. Наилучших результатов вы добьетесь, имея резервную копию базы: восстановление займет ровно столько времени, сколько потребуется на считывание файлов с ленты (или другого носителя). Перед восстановлением контроллера — мастера операций стоит поручить роли мастеров другим контроллерам в домене. Ну а после восстановления надо проверить его качество и приступить к нормальной работе.

Вы были столь беспечны, что резервной копии у вас нет или она сделана более 2 месяцев назад? Попробуйте восстановить контроллер с помощью утилиты NTDSUtil. Если же это был не единственный контроллер в домене, то так легко вы не отделаетесь.

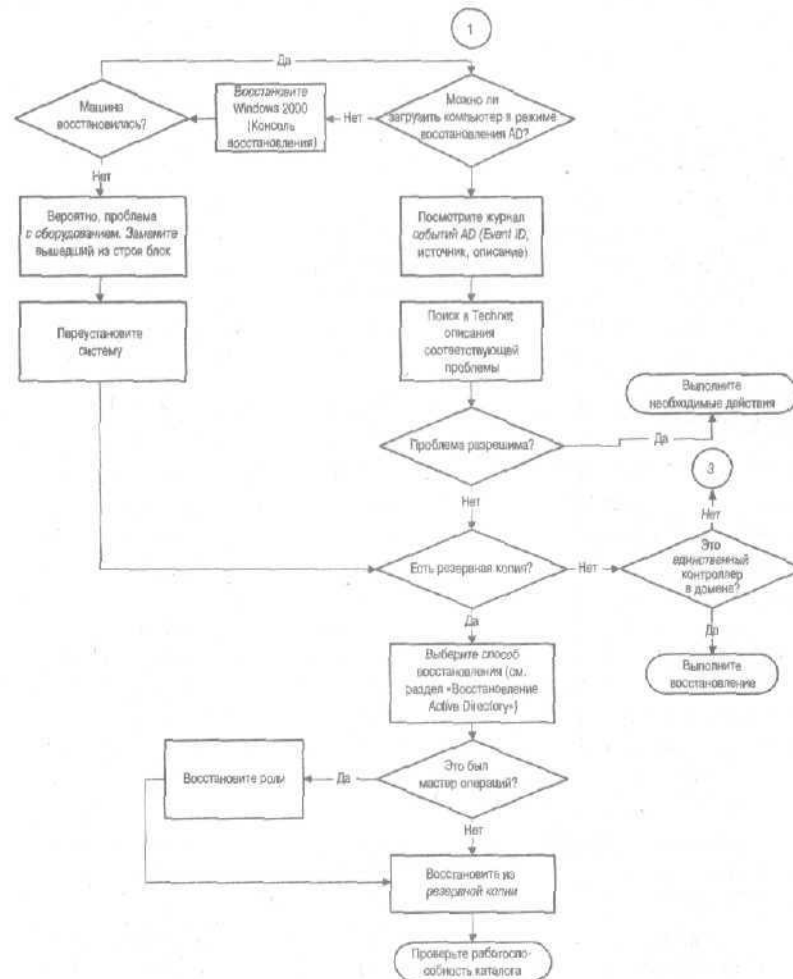
В первую очередь надо передать роли мастеров операций другим контроллерам в домене. Передать их, конечно, нельзя (ведь контроллер домена, их выполнявший, — мертв!), но можно принудительно назначить (см. об этом ниже). Затем Active Directory надо почистить, чтобы и духу от сбойного контроллера в ней не осталось. Этот процесс подробно описан в главе «Установка Active Directory» в разделе «А может, все переустановить?».

Теперь можно заняться «больным». Сначала замените компонент, вызвавший уничтожение контроллера. Менять его на аналогичный не стоит — лучше подобрать что-то понадежнее.

Далее установите ОС с нуля, потом сервер повышает свой статус до контроллера домена, и за счет нормальной репликации его база наполняется данными. Если до кончины сервер исполнял роль Глобального каталога (ГК), имеет смысл вернуть ее ему.

Теперь рассмотрим ситуацию, когда база цела, но хранится в ней совсем не то, что должно. В этом случае за счет механизмов репликации все неверные данные будут тиражированы по остальным контроллерам, так что борьбу придется вести на всех фронтах.

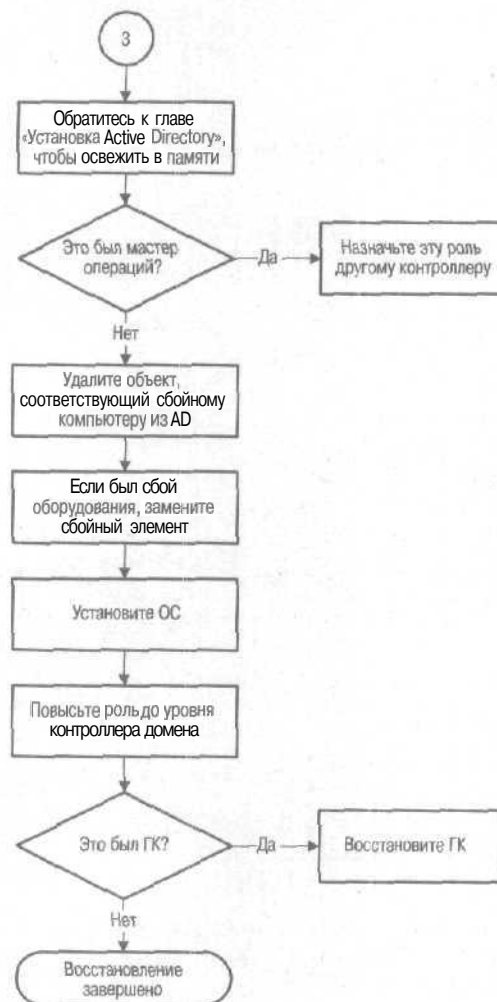
К счастью, это не так сложно, как кажется. Для начала прикиньте: а что, собственно говоря, восстанавливать? Может, это объект или несколько атрибутов, которые несложно создать заново? Если это так, то и воссоздайте их.



Последовательность действий при повреждении базы

Если количество утраченного и его значимость таковы, что заново его создать нельзя, то задаем традиционный вопрос: «Есть ли в нашем распоряжении актуальная резервная копия?» Если нет, увы, ручного воссоздания объектов не избежать. Счастье, коль она есть.

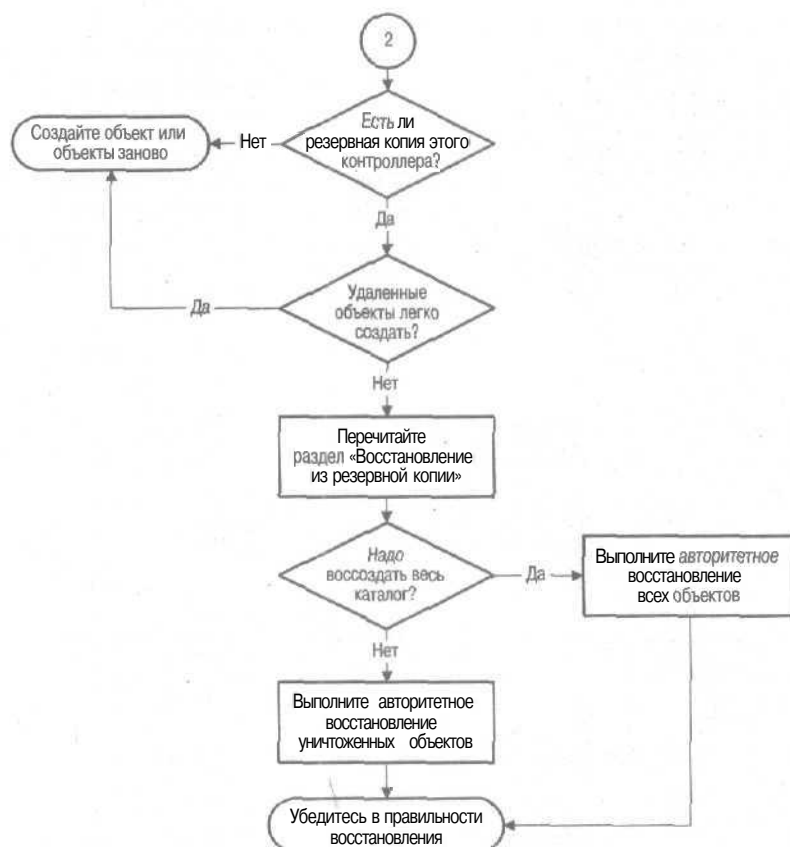
Теперь главное не переборщить, ведь речь пойдет об авторитетном восстановлении каталога. Хорошо подумайте: восстанавливать весь каталог или только одну-две ветви в нем. На ваш выбор должна оказать влияние дата резервной копии. Как много изменений было внесено в каталог с момента резервирования?



Восстановление контроллера домена после сбоя оборудования

После авторитетного восстановления данные будут реплицированы на другие контроллеры домена.

Таким образом, решается и эта проблема. Думаю, вы уже обратили внимание на важность сохранения актуальной резервной копии. Именно поэтому чуть дальше процесс резервного копирования и последующего восстановления Active Directory мы обсудим весьма подробно.



Восстановление поврежденных данных

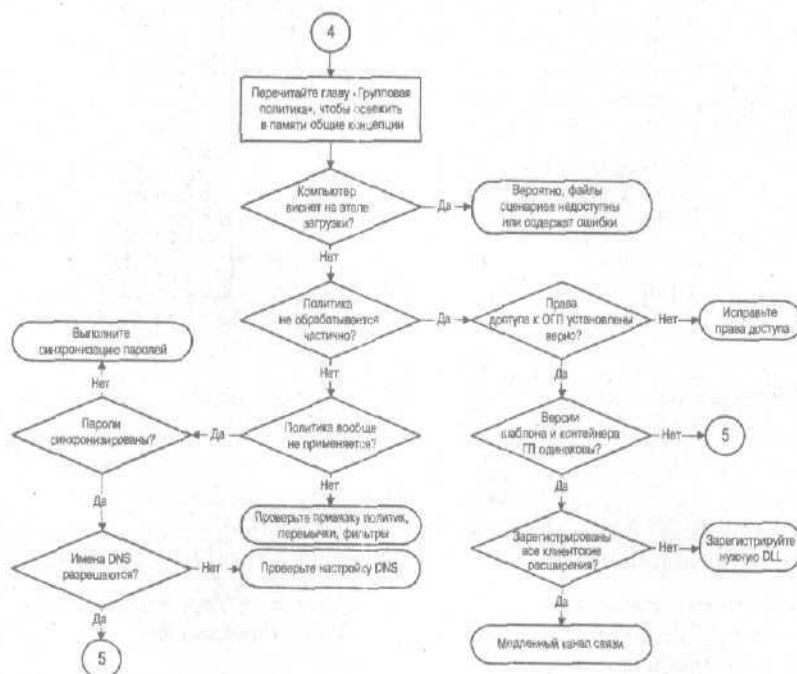
Проблемы, связанные с групповой политикой, и способы их разрешения подробно описаны в главе «Групповая политика». Здесь я позволю себе набросать лишь общий алгоритм.

Итак, если выяснилось, что групповая политика вызывает зависание компьютера на этапе загрузки, то причина скорее всего в сценариях загрузки. Посмотрите, какое изменение вы внесли в сценарии или в правила их обработки. Возможно, что они просто ждут реакции от пользователя, а «сказать» об этом не могут, так как соответствующая политика запрещает это.

Если политика применяется лишь частично, проверьте права доступа к компонентам ОПС, сверьте версии шаблона групповой политики и соответствующего контейнера. Если версии разные, то это следствие

нарушений в работе службы репликации. Еще одной возможной причиной может быть отсутствие или повреждение динамических библиотек, ответственных за определенные клиентские расширения. А может, и вообще все просто: клиентский компьютер находится на другом конце медленного канала?

Если политика не применяется вообще, то в первую очередь следует проверить, связали ли вы ее с: каким-либо объектом Active Directory. Кроме того, проверьте, нет ли фильтров, запрещающих применение данных правил к выбранной категории пользователей, не установлена ли перемычка правил и т. п.



Выявление проблем с групповой политикой

Если в этом плане все так, как вы и предполагали, стоит проверить, нет ли **рассинхронизации** пароля компьютера с тем, что хранится в Active Directory. Не лишне проверить параметры клиента DNS. Может, имя контроллера домена не разрешается? Если все верно, а групповая политика все же не **применяется**, следует приглядеться к репликации.

Проблемы, возникающие при тиражировании данных Active Directory, описаны в главе «Репликация Active Directory», а связанные с работой

службы FRS, — в главе «Active Directory и файловая система». Куда пойти, подскажет сравнение каталогов SYSVOL на контроллерах домена. Если они разные или на каких-то контроллерах их вообще нет, надо разбираться с репликацией FRS. Загляните в журнал регистрации событий этой службы. Если там есть ошибка 13508, ищите причину в репликации Active Directory. Если нет, обратите внимание на тот диск, где находятся каталог SYSVOL и подготовительные каталоги (обычно там же). Вполне возможно, что на нем осталось мало места. Освободите пространство или переместите каталог на другой диск.

Вероятно также, что кто-то из администраторов удалил объекты конфигурации FRS из Active Directory. Без резервной копии тогда не обойтись. Надо сделать авторитетное восстановление.

Наконец, некоторые непонятные на первый взгляд проблемы решаются простым перезапуском службы NTFRS.

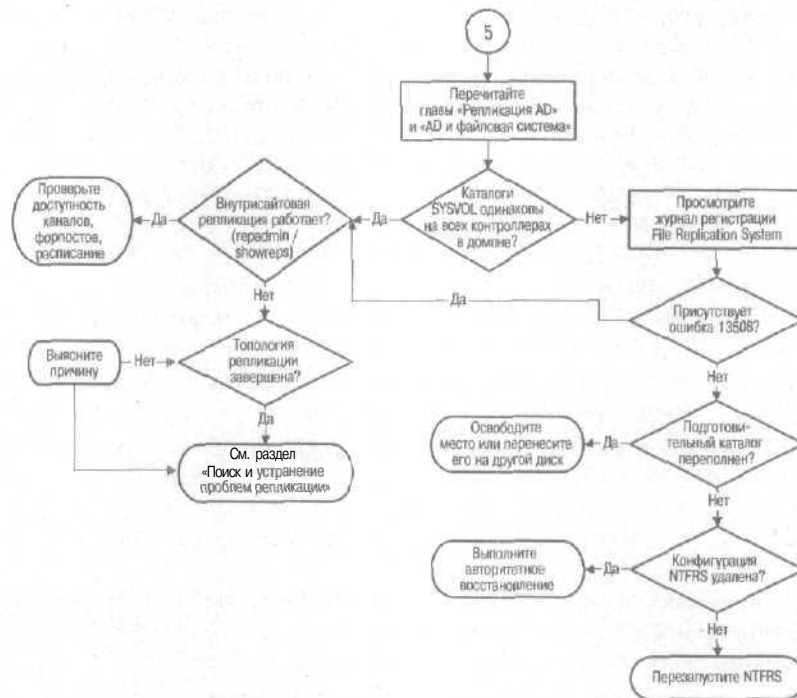
Проблемы репликации Active Directory надо разделить на те, что связаны с внутри- и межсайтовой репликациями. Если не работает только последняя, то причина скорее всего в недоступности канала связи, в закрытом «окне» репликации или в неправильном выборе выделенных форпостов.

Если проблемы связаны с внутрисайтовой репликацией, проверьте топологию и с помощью утилиты `gpadmin` или `Replication Monitor` выясните причину (см. главу «Репликация Active Directory»).

Резервное копирование Active Directory

Одним из условий создания отказоустойчивой системы является разработка стратегии резервного копирования. Цели этой стратегии таковы.

- Разработка методов резервного копирования и восстановления, позволяющих быстро восстанавливать утраченные данные.
- Обеспечение резервирования всех томов, на которых хранятся данные. В случае тотальной катастрофы это позволит восстановить данные полностью.
- Резервирование Active Directory, включающее весь домен и все контроллеры доменов. В резервной копии должны быть все учетные записи и вся информация о безопасности.
- Выявление файлов, которые не были скопированы из-за использования их другими приложениями, с помощью журналов резервного копирования. Эта информация пригодится для создания расписания копирования, учитывающего занятость файлов приложениями.
- Использование не менее трех резервных копий и постоянная их смена. Лучше всего иметь 5 или 7 резервных копий (по одной на



Устранение проблем с репликацией

каждый рабочий день или день недели). Одна из них должна храниться за пределами предприятия на случай крупной аварии, влекущей уничтожение всех копий на предприятии.

- Регулярное учебное **восстановление** данных. Учения помогают администраторам чувствовать себя уверенно в критических ситуациях, а также **выявляют** непредвиденные проблемы.
- 4 Ограничение доступа к устройству резервного копирования для предотвращения **восстановления** на сервере ложных данных посторонними людьми. Также следует охранять носители с данными.

Резервное копирование позволяет восстанавливать данные, уничтоженные как вследствие выхода из строя жестких дисков, так и вследствие ошибочных или преднамеренных действий администраторов или лиц, ответственных за работу с данными.

Планируя процесс резервного копирования и восстановления данных, надо иметь точное представление о **том**, какое время займет этот процесс. Это крайне важно, **так** как позволяет точно рассчитывать

«критическую точку» в процессе, после которой выполнение восстановления данных в заданное время становится невозможным.

На сроки выполнения резервного копирования существенно влияет загруженность сервера. В течение рабочего дня попытка копирования упрется в следующие факторы:

- сервер занят обработкой пользовательских запросов;
- многие файлы открыты и не будут скопированы в резервную копию;
- ◆ копируемые файлы недоступны для других процессов и для доступа пользователей;
- ◆ **копирование** по сети загружает сетевой адаптер.

Поэтому никогда не выполняйте резервное копирование в рабочее время.

Все сказанное выше в равной мере относится к резервному копированию как данных «вообще», так и Active Directory. **Теперь** посмотрим, что же особенного в копировании Active Directory.

Чем нужно копировать

Копирование Active Directory должно удовлетворять ряду условий.

- ◆ Резервное копирование нужно проводить в то время, когда контроллер домена активен и выполняет свои нормальные операции. С точки зрения многих программ резервного копирования, файл базы и другие сопутствующие файлы являются открытыми, а значит, копироваться не могут.
- Помимо файла базы, надо копировать ряд дополнительных системных файлов, которые также задействованы системными службами. Это и файлы, используемые службой FRS, и файлы службы сертификатов, и файл реестра системы, зарегистрированные объекты COM+, и др.
- + Желательно выполнить резервное копирование не только на магнитную ленту, но и на другие носители: жесткие диски, съемные диски, библиотеки дисков или лент, пул носителей.

Уверен, что существуют инструменты, удовлетворяющие этим условиям. Но стоит ли далеко ходить, когда в Windows 2000 встроено средство `ntbackup`! Помимо прочих видов резервного копирования (см. [1]), оно обеспечивает и *обычное* (normal), которое на сегодняшний день является единственно возможным для резервного копирования Active Directory. Особенности последнего являются:

- + выполнение во время обычной работы контроллера домена:
 - ◆ сброс атрибута файлов Archive, что помечает файлы как скопированные;

- файлы журналов баз данных обрезаются;
- ◆ восстановление данных выполняется с одного носителя за один проход.

NtBackup обладает графическим интерфейсом и имеет встроенные мастера резервного копирования и восстановления. Кроме того, она позволяет создавать диск аварийного восстановления. Но NtBackup имеет и интерфейс командной строки, что позволяет выполнять все операции и без графической оболочки. Следовательно, можно создавать командные файлы и запускать их по расписанию.

NtBackup способна работать с лентами, записанными иными программами резервного копирования. Почему это важно? Допустим, вы регулярно использовали некоторую программу для резервирования состояния системы. В результате катастрофы сервер, на котором была установлена эта программа, уничтожен. В условиях дефицита времени можно применить штатное средство для восстановления данных.

Замечание Чтение лент, записанных сторонними программами, возможно, только если не использовалось сжатие и формат записи был MTF (Microsoft Tape Format).

Кстати, справедливо и обратное: ленты, записанные с помощью NTBackup, могут быть прочитаны программами резервного копирования сторонних производителей.

Кстати о сторонних производителях. Среди программ, поддерживающих резервное копирование и восстановление Active Directory, стоит назвать;

- Veritas Backup Exec (www.veritas.com);
- Computer Associates ARCserveIT (www.cai.com);
- UltraBAC for Windows 2000 (www.ultrabac.com);
- Aelita Software ERDisk for Active Directory (www.aelita.com).

Еще одна особенность NtBackup в том, что она позволяет выполнять резервное копирование *состояния системы* (system state).

Что нужно копировать

Под состоянием системы на контроллере домена понимаются следующие компоненты:

- файлы Active Directory (ntds.dit, edb.chk, edb.log, resx.log);
- ◆ системные стартовые файлы;
- + системный реестр;
- база регистрации объектов COM+;

- каталог SYSVOL;
- ◆ база сертификатов (если развернута инфраструктура КИ);
- зоны DNS интегрированные с Active Directory;
- контрольные точки и кворумный журнал для кластерной службы в случае ее использования.

Помимо копирования состояния системы, для восстановления контроллера домена нужна резервная копия системного диска. Комбинация системного диска и состояния системы — одно из условий хорошей резервной копии. О других условиях поговорим далее.

Файлы базы Active Directory и журналы могут располагаться на разных физических дисках, и такое деление предпочтительно для нагруженных систем (см. главу «Установка Active Directory»). Но и в этом случае резервное копирование состояния системы будет выполнено в полном объеме.

Достаточно ли резервной копии только одного контроллера в домене? Да — для восстановления именно этого контроллера, но не других. Этот очевидно хотя бы уже потому, что каждый из контроллеров имеет свой номер GUID как партнер по репликации, свой SID как объект системы безопасности, а также может исполнять различные роли в домене. Поэтому, говоря о резервном копировании Active Directory, надо иметь в виду резервное копирование всех контроллеров.

Кто может копировать

Чтобы выполнять резервное копирование состояния системы, нужны соответствующие полномочия. По умолчанию ими обладают;

- члены группы Backup Operators;
- ◆ члены группы Administrators;

Это право можно делегировать любому обученному пользователю.

Для восстановления состояния системы на контроллере домена пользователь должен быть локальным администратором.

Файлы, игнорируемые при резервном копировании

Используя программу NtBackup, следует знать о тех файлах, которые по умолчанию не копируются и не восстанавливаются. Сведения о таких исключениях хранятся в реестре.

Файлы, исключаемые из процесса резервного копирования перечислены в виде параметров в ветви реестра HKLM\System\CurrentControlSet\Control\BackupRestore\FilesNotToBackup.

Файлы, исключаемые при резервном копировании

Параметр	Значение
Certificate Authority	%systemroot%\system32\certlog*.edb %systemroot%\system32\certlog*
ClientSideCache	%systemroot%\csc* /s
ComPlus	%systemroot%\registration*.crmlog /s
Internet Explorer	%UserProfile%\index.dat /s
Memory Page File	\pagefile.sys
MS Distributed Transaction Coordinator	%systemroot%\system32\dtclog\msdtc.log
Netlogon	%systemroot%\netlogon.chg
Ntfs	%systemroot%\ntfs\jet* /s %systemroot%\debug\ntfs* %systemroot%\sysvol\domain\DO_NOT_REMOVE_NtFrs_Preinstall_Directory* /s %systemroot%\sysvol\domain\NtFrs_PreExisting__See_EventLog* /s %systemroot%\sysvol\staging\domain\NTFRS.*
Power Management	\hiberfil.sys
Task Scheduler	%systemroot%\schedlg.txt
Temporary files	%temp%\ /s
Winlogon debug	%windir%\debug*

Ветви реестра, исключаемые из процесса резервного копирования, перечислены в виде параметров в ветви реестра HKLM\System\CurrentControlSet\Control\BackupRestore\KeysNotToBackup.

Ветви реестра, исключаемые при резервном копировании

Параметр	Значение
Active Directory Restore	CurrentControlSet\Services\NTDS \Restore In Progress CurrentControlSet\Services\NTDS\Parameters \New Database GUID
Certificate Authority	CurrentControlSet\Services\CertSrv \Configuration\Restore In Progress
Fault Tolerance	Disk\
Installed Services	CurrentControlSet\Services*
LDM Boot Information	CurrentControlSet\Services\dmio\boot info\
Mount Manager	MountedDevices\
Ntfs	CurrentControlSet\Services\Ntfs\Parameters \ Backup/Restore/Process at startup
Pending Rename Operations	CurrentControlSet\Control\Session Manager PendingFileRenameOperations
Plug And Play	CurrentControlSet\Enum\ CurrentControlSet\Control \CriticalDeviceDatabase\
Session Manager	CurrentControlSet\Control\Session
Windows Setup	Setup\SystemPartition

Актуальность резервной копии

В главе «Репликация Active Directory» я рассказал о времени жизни памятников удаленным объектам в Active Directory. По умолчанию это 60 дней. По истечении срока все удаленные и помеченные как памятники объекты будут удалены из Active Directory сборщиком мусора.

Этот параметр является значением аргумента `thombstoneLifitime` объекта службы каталогов. Например, в домене `mycorp.ru` отличительное имя этого объекта:

```
CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,  
DC=mycorp,DC=ru.
```

Но вдумайтесь в смысл этого атрибута. Раз через какое-то время сведения об объекте удаляются полностью из Active Directory, значит, этот объект не только больше не нужен, но и не может быть воссоздан! Все, что можно сделать, — это создать новый объект такого же класса, возможно, с таким же именем и значениями атрибутов, но... это будет другой объект, с уникальным номером GUID. Восстановление же объекта из резервной копии после указанного срока породит «зомби», само существование которого способно поставить под угрозу целостность каталога. Именно поэтому в момент выполнения резервной копии в нее записывается специальная метка, указывающая, до какого момента может использоваться данная резервная копия. По истечении этого срока восстановление из этой копии невозможно.

Но как быть, если единственная резервная копия, имеющаяся в вашем распоряжении, просрочена, а контроллер домена вышел из строя?

- Посмотрите, нет ли в сети хотя бы одного контроллера этого домена. Если «в живых» остался хотя бы один контроллер, этого вполне достаточно для воскрешения всех погибших. Об этом рассказано далее.
- Убедитесь, что резервная копия действительно просрочена. Не исключено, что вы успели увеличить время хранения памятников до выполнения резервной копии. Тогда, восстановив данные на одном контроллере в авторитетном режиме, их можно реплицировать на остальные контроллеры.
- Если вы поняли, что резервной копией воспользоваться не удастся, а этот контроллер единственный, придется его переустановить с нуля, создать заново все объекты на нем (хорошо, если это делалось с помощью сценариев) и... больше не забывать выполнять резервное копирование.

Правда, самые хитрые могут спросить, что будет, если перед выполнением резервного копирования передвинуть время на компьютере на год (два, три, десять) вперед? Ведь по идее тогда на ленту будет записана дата истечения срока годности с большим запасом.

Никогда не ставьте время на контроллере больше **текущего**

Название этого раздела — настоятельная рекомендация. Почему я столь категоричен? Судите сами:

Последствия перевода времени вперед

Репликация FRS

Памятники удаленным файлам в таблице ID удаляются раньше установленного времени. Реплицируемые данные с других контроллеров вступают в конфликт с ситуацией на контроллере. В итоге может оказаться, что файлы в каталоге SYSVOL или корне DFS на разных контроллерах и партнерах по репликации станут разными. Более того, выполнение репликации может прекратиться вовсе

Компьютер с переведенными вперед стрелками не сможет присоединиться к другим компьютерам в качестве партнера по репликации, так как процесс VV-join (см. главу «Active Directory и файловая система») выполняется только при условии рассинхронизации времени между компьютерами не более установленного значения

Изменения локальных файлов на компьютере с «убежавшим» временем заносятся в журнал выхода. При этом регистрируется текущее время изменения. В силу причин, изложенных выше, эти изменения не могут быть переданы на другие контроллеры. Когда время на компьютере вернется в заданные пределы, начнется репликация изменений на другие компьютеры. Однако те отвергнут эти изменения, так как время «неправильное» и указывает далеко в будущее. Файлы, измененные в период «будущего» времени, будут присутствовать только на одном компьютере и не будут тиражироваться на другие

Репликация Active Directory

При разрешении конфликтов выигрывает не тот партнер. Если, например, атрибут объекта был изменен на компьютере с «будущим временем», а потом — на компьютере с нормальным, то в итоге значение атрибута будет таким, как на первом компьютере, что неправильно (см. главу «Репликация Active Directory»)

Если два объекта с одним именем создаются на двух компьютерах, время на одном из которых ушло вперед, то победит его объект, а другому будет присвоен маркер дублированного имени

Восстановить резервную копию, сделанную в «будущем времени», на компьютер в «прошедшем» нельзя с помощью `ntbackup`. Если вы используете инструмент, позволяющий это сделать, возникнет конфликт «зомби»

Билеты аутентификации Kerberos окажутся просроченными, а значит, потребуются запросить новые. Однако это не удастся сделать, так как для протокола Kerberos требуется синхронизация по времени [1]

Как видите, последствия перевода времени вперед оказывают куда большее влияние на репликацию FRS. Поэтому, если вам все-таки нужно временно перевести часы вперед, то для исключения проблем со службой FRS сделайте это так.

1. Остановите службу ntfrs.
2. Переведите время вперед.
3. Выполните то, ради чего время переводилось вперед. При этом категорически запрещается вносить изменения в содержимое каталога SYSVOL или реплики DFS.
4. Верните время назад.
5. Запустите службу ntfrs.

Если все-таки реплика была изменена в период «будущего времени», то для избавления от последствий выполните неавторитетное восстановление реплики (см. раздел «Неавторитетное восстановление» в главе «Active Directory и файловая система»).

Резюмируя сказанное, повторю: никогда не ставьте время вперед при выполнении резервного копирования. Это принесет вам больше проблем, нежели выгод.

Восстановление Active Directory

Приступая к восстановлению Active Directory, ответьте на следующие вопросы:

- ◆ Есть ли актуальная резервная копия?
- ◆ Что повреждено? Это только локальная реплика на контроллере домена или все реплики имеют одинаковое состояние?
- ◆ Должны ли восстанавливаемые данные иметь преимущество и заместить текущие на всех контроллерах или нет?

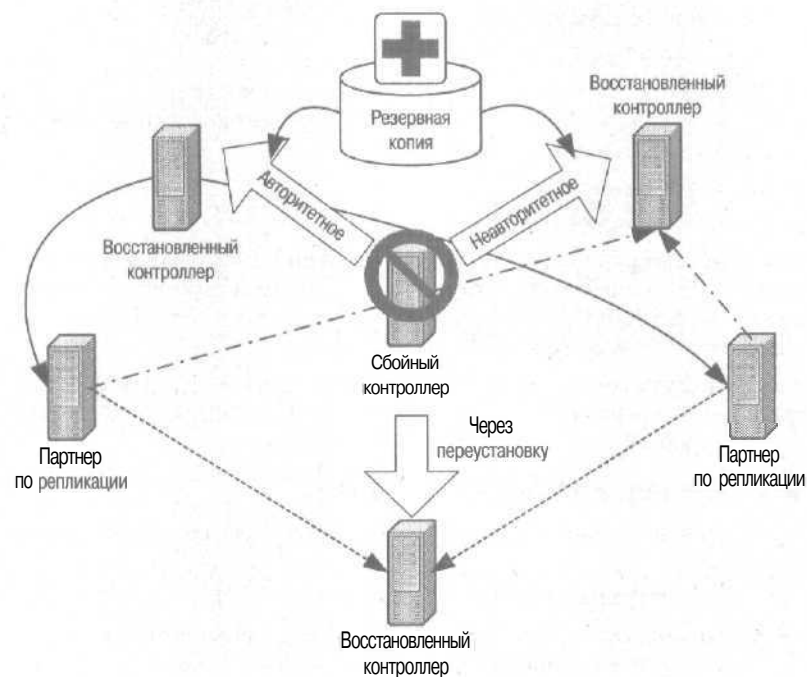
В зависимости от ответов выбирается способ восстановления. Очевидно, что если резервной копии нет, то выбирается восстановление, связанное с переустановкой контроллера и последующей репликацией с других контроллеров.

Если копия есть, то в зависимости от масштабов бедствия выбирается авторитетное или неавторитетное восстановление Active Directory. Механизмы, применяемые для восстановления Active Directory, заметно отличаются от используемых для восстановления службы FRS.

Восстановление через переустановку

Начнем с простейшего случая — восстановления через переустановку и репликацию. Как я уже говорил, для этого типа восстановления должны удовлетворяться такие условия:

- ◆ в домене, помимо восстанавливаемого, есть другие контроллеры;
- ◆ реплики на других контроллерах хранят адекватную информацию;
- нет резервной копии состояния системы для данного контроллера.



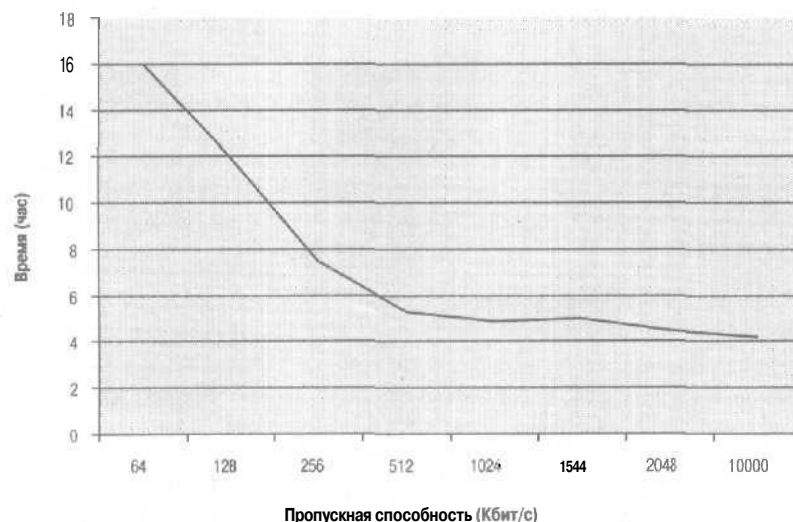
Три возможных способа восстановления. Тонкими линиями показано направление репликации

При этом следует учесть пропускную способность канала, связывающего данный контроллер с остальными. На рисунке приведена зависимость времени репликации базы Active Directory объемом 2 Гб от пропускной способности канала. Данная зависимость была получена на компьютере с двумя процессорами PII-266, объемом ОЗУ 256 Мб и одним жестким диском. Применение систем, рекомендованных в главе «Установка Active Directory», повлияет на эти результаты в сторону сокращения необходимого времени.

Чтобы выполнить восстановление, сделайте следующее.

1. Выясните причину, приведшую к необходимости восстановления. Если это был сбой оборудования, замените его.
2. Удалите из Active Directory всю информацию о сбойном контроллере (см. раздел «А может, все переустановить?» главы «Установка Active Directory»). Напомню, что при этом вам придется использовать утилиту Ntdsutil и оснастки Active Directory Users and Computers, Active Directory Sites and Services и DNS.

3. Если сбойный контроллер являлся мастером операций, передайте соответствующие роли другим контроллерам с помощью Ntdsutil.
4. Повторно установите контроллер домена. Имя нового контроллера и его IP-адрес могут совпадать с существовавшими ранее. Тогда выполняйте п. 2 с особой тщательностью.



Зависимость времени репликации Active Directory от пропускной способности канала

Принудительное назначение мастеров операций с помощью Ntdsutil

Ntdsutil — мощный инструмент для выполнения разнообразных операций с Active Directory. В главе «Установка Active Directory» я рассказывал о ее использовании для удаления компьютерных объектов из Active Directory. Теперь обсудим еще одну возможность — перемещение и принудительное назначение ролей мастеров операций контроллерам.

Известно, что роль любого мастера операций можно передать любому контроллеру домена с помощью оснасток Active Directory Users and Computers (роли мастера RID, инфраструктуры, имитатора PDC), Schema Management (роль мастера схемы) и Active Directory Domains and Trusts (роль мастера доменных имен). Такая передача возможна, если оба контроллера — и передающий, и принимающий роль — работают и доступны. В случае краха контроллера, выполнявшего роль одного или нескольких мастеров, передача роли невозможна автоматически. Можете себе представить человека, который через мгнове-

ние погибнет в автокатастрофе, вдруг позовет нотариуса, чтобы сделать последние распоряжения? То-то. Поэтому для разрешения такой ситуации используется Ntdsutil.

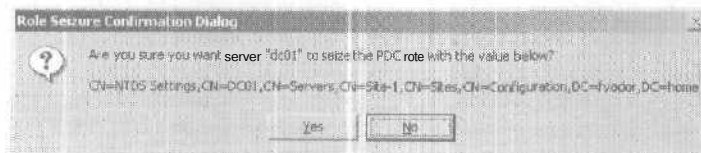
Эта утилита может выполнять как перенос ролей, так и принудительное назначение роли контроллеру домена. Для входа в режим переноса мастеров операций следует после запуска Ntdsutil выполнить команду roles.

Следующий шаг — подключение к тому контроллеру, которому роль будет передаваться или назначаться. Для этого выполняется команда Connections, а затем — Connect to server <имя сервера>

Замечание Нет нужды вводить команды полностью — достаточно использовать однозначное сокращение. Например, вместо команды Connect to server можно ввести «con to ser».

После подтверждения успешного присоединения к серверу надо вернуться в предыдущее меню Roles, для чего ввести команду Quit.

Теперь роль можно либо перенести, либо назначить. В первом случае используются команды, начинающиеся со слова Transfer. Далее следует имя роли, например Transfer PDC. Во втором — команды, начинающиеся со слова Seize, например Seize RID master. Для выполнения любой операции требуется подтверждение администратора. При этом обратите внимание, что, несмотря на отсутствие у программы Ntdsutil графического интерфейса, запросы на подтверждение действий выводятся в стандартных диалоговых окнах.



Запрос на подтверждение операции в программе Ntdsutil

Если выполняется команда назначения роли, то сначала Ntdsutil пытается передать роль от текущего мастера новому. Если контроллер—исполнитель роли недоступен, попытки передачи прекращаются через некоторое время, и роль передается.

Вот, например, перечень команд, которые необходимо выполнить для назначения роли имитатора PDC контроллеру DC01. В скобках для ясности указано продолжение имен команд.

```
ntdsutil: r(oles)
fsmo maintenance: c(onnctions)
server connections: con(nect) to ser(ver) dc01
```

Binding to dc01 ...

Connected to dc01 using credentials of locally logged on user
server connections: q(uit)
fsmo maintenance: seize pdc

В этом месте и возникает запрос на подтверждение. В зависимости от вашего ответа далее следует сообщение об отмене или успешном (или неуспешном) выполнении операции.

Замечание Так как роль мастера доменных имен может исполнять только контроллер, являющийся одновременно и ГК, принудительное назначение этой роли возможно только серверу ГК. С другой стороны, ничто не запрещает назначить роль мастера инфраструктуры серверу ГК, хотя это противоречит требованиям, предъявляемым к контроллерам, исполняющим эту роль.

Восстановление из резервной копии

Теперь рассмотрим восстановление из имеющейся резервной копии. Далее полагаем, что эта копия достаточно свежа, чтобы и Ntbackup, и аналогичные программы сторонних производителей смогли восстановить базу без негативных последствий. Восстановление из резервной копии отбрасывает состояние базы на момент резервирования. И вот тут-то и нужно знать, есть ли в домене другие контроллеры, сохранившие актуальную информацию, или эта резервная копия — все, что у вас осталось. В зависимости от этого делается вывод о методе восстановления. Как я уже говорил, доступны два альтернативных метода:

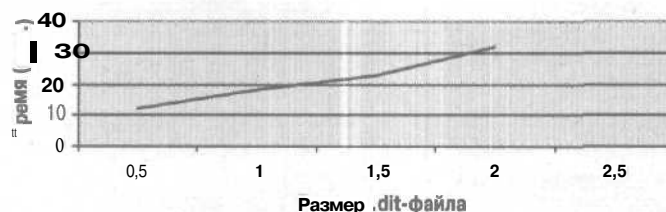
- ◆ неавторитетное восстановление;
- ◆ авторитетное восстановление.

Замечание Говоря о восстановлении Active Directory, нужно помнить, что одновременно надо восстанавливать и каталог SYSVOL (см. главу «Active Directory и файловая система»). Здесь же я буду лишь напоминать о необходимости восстановления этого каталога.

Неавторитетное восстановление

Неавторитетное восстановление состояния системы выполняется по умолчанию Ntbackup. Вообще это единственный способ восстановления, который можно выполнить, не прибегая к другим инструментам. Этот тип восстановления можно сравнить с предыдущим, использующим только механизм репликации Active Directory. Там новые данные в базу передаются по сети с других контроллеров. При этом тиражируется полный объем базы. При восстановлении из резервной

копии большая часть данных заносится в базу локально, а по сети передается только разница, возникшая с момента выполнения резервного копирования. Следовательно, нагрузка на сеть существенно снижается, что наглядно демонстрирует следующий график. На нем показана зависимость времени восстановления базы в зависимости от ее размера на компьютере с процессором PII-400, ОЗУ 256 Мб и ленточным накопителем 4/SGb DAT.

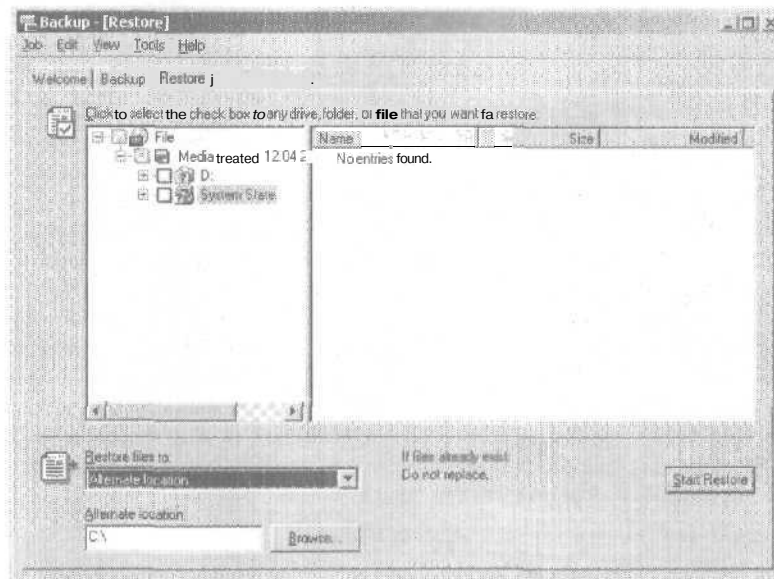


Зависимость времени восстановления состояния системы от размера базы Active Directory

В отличие от резервного копирования, которое можно выполнять в нормальном режиме работы Active Directory, восстановление выполняется только в специальном режиме работы контроллера домена — Directory services restore mode (Режим восстановления службы каталога). Входя в этот режим, вы обязаны зарегистрироваться как локальный администратор компьютера. Заметьте: поскольку Active Directory в этом режиме не функционирует, то и авторизоваться в ней вы не сможете. Единственный механизм авторизации — база SAM, хранящая учетную запись локального администратора. Помните: пароль для этой записи был введен вами во время работы DCPROMO при установке контроллера домена и скорее всего не совпадает с паролем администратора домена.

Ntbackup позволяет восстановить файлы в новое место. Если указать эту возможность, то в иное место будут восстановлены только загрузочные файлы, каталог SYSVOL, файлы реестра и, если восстанавливается кластер, то его база. Ни база Active Directory, ни база сервера сертификатов, ни база регистрации объектов COM+ восстановлены не будут!

Это не значит, что данный режим не годится для восстановления Active Directory. Если, например, надо восстановить только отдельные файлы групповой политики, этот метод весьма удобен, так как позволяет выбрать нужные ОГП после восстановления и скопировать их в «настоящий» каталог SYSVOL.



Восстановление состояния системы в иное место на диске

Внимание Безусловным требованием для восстановления состояния системы является сохранение корня системы. Если на момент резервного копирования это был диск C:, то и при восстановлении корневым должен быть тот же диск.

Хочу предостеречь от ошибки. При восстановлении состояния системы восстанавливается не только база Active Directory, но и реестр. Вследствие этого все службы, установленные или переконфигурированные на контроллере после резервного копирования, но до его краха, будут возвращены к прежней конфигурации или удалены. То же произойдет и с объектами COM+. Я уж не говорю о том, что если вы меняли адрес IP контроллера, то он вновь станет прежним, что может вызвать цепочку неприятных последствий. Так что, прежде чем выполнять восстановление, подумайте, как это отразится на работоспособности контроллера и системы.

Теперь посмотрим, что происходит с базой Active Directory, когда она заполняется новыми данными из резервной копии.

После перевода в нормальный режим работы Active Directory обнаруживает, что находится в состоянии восстановления. На это указывает параметр `RestoreInProgress` в ветви реестра `HKLM\System\CurrentControlSet\Services\NTDS`. Зачем это надо? Дело в том, что само по себе

восстановление не гарантирует целостности БД. Поэтому надо проверить целостность и выполнить реиндексирование средствами, которые обычно используются Active Directory. Вот именно этим система и станет заниматься довольно долго.

И только когда Active Directory будет готова, запускается обычный механизм репликации. Тут-то и кроется опасность. В главе «Репликация Active Directory» я говорил, что последовательный номер обновления (USN) является критерием, определяющим, какие данные на контроллере должны быть тиражированы партнерам по репликации. После восстановления должен восстановиться и тот номер USN, что существовал на момент резервного копирования. Раз так, то именно этот номер и должен использоваться. Однако он уже был однажды использован, и его повторение может привести к непредсказуемым результатам. Для избавления от этой неприятной ситуации на этапе восстановления формируется новый номер USN, не противоречащий известному на остальных контроллерах. И вот уже после этого может начинаться репликация с партнерами.

Проверка восстановления с помощью Ntdsutil

Представьте себе, что вы выполнили восстановление, загрузились в нормальный режим работы и... с ужасом обнаружили, что в резервной копии были ошибки или что это была не та копия, на которую вы рассчитывали. Короче, репликация, возможно, уже разнесла ошибки по остальным контроллерам в домене.

Очевидно, до перевода контроллера в нормальный режим надо выполнять проверку. Как? Очень просто. Надо запустить утилиту Ntdsutil, войти в режим Files и выполнить команду Info. Если Active Directory была восстановлена без ошибок, на экране появится информация о конфигурации, например:

```
ntdsutil: files
file maintenance: info
Drive Information:
      C:\ NTFS (Fixed Drive ) free(133.2 Mb) total(1.9 Gb>
DS Path Information:
Database   : C:\WINNT\NTDS\ntds.dit - 10.1 Mb
Backup dir : C:\WINNT\NTDS\dsadata.bak
Working dir: C:\WINNT\NTDS
Log dir    : C:\WINNT\NTDS - 30.0 Mb total
              res2.log - 10.0 Mb
              res1.log - 10.0 Mb
              edb.log  - 10.0 Mb
```

Конечно, эти сведения не дают представления о том, какие именно данные **восстановлены**, но это не позволит внести в структуру фатальных ошибок.

Восстановление на другую технику

Все сказанное выше относится к восстановлению того же самого контроллера домена либо его полного «тезки», т. е. одной модели с идентичным набором системных ресурсов. Но это справедливо и для случая восстановления на иной компьютер. Возможно, что причиной краха контроллера была его постоянная перегруженность и вы решили заменить его на новую современную технику. Конечно, можно сконфигурировать новый контроллер и позволить репликации самой наполнить его данными. Но, как вы видели, этот процесс может **затянуться**. Поэтому считаем, что новый компьютер конфигурируется с тем же именем и готовится к восстановлению резервной копии.

Замечание Так как новый компьютер будет иметь то же имя, что и вышедший из строя, позаботьтесь об удалении из Active Directory соответствующих объектов.

Как указано в [3], новый компьютер должен иметь столько же дисков, сколько и предыдущий. Кроме того, если он имеет другие видеоадаптер и сетевую плату, то перед восстановлением их надо отключить. Далее их подключит функция Plug and Play. На этом все рекомендации в [3] кончаются. А жаль, потому что самое интересное дальше.

Чтобы восстановленный на новом компьютере контроллер заработал, придерживайтесь такой последовательности.

1. У вас должна быть полная резервная копия как состояния системы, так и системного диска.
2. Установите сервер на новый компьютер. При этом убедитесь, что:
 - сервер не входит в домен;
 - системный диск тот же самый;
 - **файловая** система — NTFS;
 - каталог, в который устанавливается система, имеет то же имя, что и в предыдущем контроллере.
3. Запустите NtBackup, выберите нужную резервную копию, укажите восстановление в то же место и установите переключатель в положение Always replace the file on the disk. Начните восстановление.
4. По завершении восстановления перезагрузите компьютер. Дальнейшие ваши действия зависят от **того**, по какому из трех возможных сценариев **начнут** развиваться события:

- система загрузится;
- система не сможет загрузиться в обычном режиме, но загрузится в **безопасном** режиме;
- система **не** загрузится ни в одном из режимов.

Если система загрузилась

То, что система загрузилась после **восстановления**, не гарантирует, что все службы запустились и работают. На проблемы укажет сообщение о том, что одна или несколько служб не смогли запуститься. Посмотрите в **журнале** регистрации, что вызвало это сообщение.

Вполне возможно, что данное сообщение не имеет отношения к работоспособности службы **каталогов**, а связано с отсутствием какого-то драйвера устройств. Тогда достаточно установить нужный драйвер. Возможна и прямо противоположная проблема — драйвер оборудования, присутствовавшего в **прежнем** компьютере, не сможет запуститься из-за **отсутствия** такого устройства в новом компьютере.

Иное дело, если прежний компьютер был, например, сервером DNS, WINS или DHCP. Тогда надо сконфигурировать эти службы (см. главу "Установка Active Directory»). Особое внимание надо уделить серверу и клиенту DNS. Если тип сетевой карты отличается от того, что использовался на прежнем компьютере, все параметры TCP/IP будут **потеряны**, и их надо восстановить. Если контроллер был сервером DNS, клиенту надо указать использовать самого себя. Затем надо перезапустить службу Netlogon и проверить наличие записей о домене в DNS. Если к этому времени вы уже сконфигурировали другой сервер **DNS**, клиент должен указывать на него в качестве первичного сервера. Тогда перезапуск службы Netlogon должен отразиться **появлением записей** в этом сервере.

После проверки работы всех **служб** и устройств, установки нужных драйверов систему надо перезапустить и проверить по журналу регистрации отсутствие ошибок.

Если в журнале регистрации появится сообщение об ошибке с Event ID=1656 и его источником будет **NTDS**, значит, не все в порядке с протоколом RPC на компьютере. Откройте в реестре ветвь **HKLM\Software\Microsoft\Rpc\ClientProtocols** и убедитесь, что там присутствуют пять параметров:

- ncacn_http;
- ncacn_ip_tcp;
- ncacn_nb_tcp;
- ◆ ncacn_np;
- ncadg_ip_udp.

Тип этих параметров — REG_SZ, а значение у всех одинаковое — `rpert4.dll`

Совет Для надежности рекомендую открыть эту ветвь реестра на другом, работоспособном контроллере и посмотреть значение параметров. Если оно отличается, то и вам следует установить иное значение.

Далее выполните команду `Dcdiag`. В зависимости от ошибок, которые она сообщит, надо выполнить соответствующие действия. Они описаны в предыдущих главах.

Наконец, если этот контроллер выполнял роли мастеров операций, то их ему надо восстановить (см. раздел «Принудительное назначение мастеров операций с помощью `Ntdsutil`»).

Если система загружается только в безопасном режиме

Загрузка системы только в безопасном режиме свидетельствует скорее всего о том, что ее архитектура или набор микросхем отличаются от тех, что использовались в предыдущем компьютере. Поэтому систему при загрузке надо перевести в режим восстановления/обновления, загрузив компьютер с установочного диска Windows 2000 Server и выбрать команду `R(epair)`,

В этом режиме будут добавлены драйверы нужных устройств, а также предложено установить дополнительные компоненты. Проверьте, установлена ли служба DNS (конечно, если восстанавливаемый сервер исполнял ранее эту функцию).

По окончании обновления/восстановления системы компьютер должен перегрузиться, и система запустится без проблем. В этом случае переходите к предыдущему разделу и следуйте приведенным в нем инструкциям.

Если система не загружается

Если система не загружается даже в безопасном режиме, то наиболее вероятная причина — использование несоответствующего уровня абстракций HAL (см. [1]). Для изменения типа HAL надо загрузиться с установочного диска, войти в режим восстановления и нажать F7 для загрузки стандартного HAL. Подробнее об этом см. в базе знаний Microsoft статью Q237556.

Замечание Если восстановление не помогло, загрузитесь в консоль восстановления, выполните команду `«disable acpi»`, перезагрузите компьютер и войдите в режим восстановления.

После восстановления и загрузки системы обратитесь к разделу «Если система загрузилась» и следуйте приведенным в нем инструкциям.

Авторитетное восстановление

Авторитетное восстановление применяется обычно, когда из каталога случайно удаляется объект(ы). Тогда эти объекты можно восстановить из резервной копии, в которой они присутствуют, а далее они будут тиражированы по остальным контроллерам. И это будет сделано, даже если эти объекты старше, чем объекты на партнерах по репликации,

Авторитетное восстановление возможно только для объектов, находящихся в доменном контексте имен или в контексте конфигурации. Авторитетное восстановление схемы невозможно, так как в противном случае нарушается целостность данных (см. раздел «Политика изменения схемы» главы «Проектируем Active Directory»).

Чтобы лучше понять возможности авторитетного восстановления, рассмотрим пример. В пятницу вечером администратор создал два ОП. В воскресенье было выполнено резервное копирование состояния системы. В понедельник утром он получил команду разнести пользователей из одного ОП по другим. Выполняя эту операцию, администратор случайно удалил оставшееся ОП вместе со всем, что в нем было. К счастью, это было вовремя замечено, и начался процесс авторитетного восстановления. Прежде чем его начать, были проанализированы все действия, совершенные после последнего резервного копирования. Их можно условно разделить на две категории: полезные (те, результат которых должен остаться в Active Directory) и вредные (те, что надо отменить). Вредным, разумеется, является удаление ОП, а полезным — разнесение пользователей из одного ОП по другим. Если выполнить авторитетное восстановление всей базы Active Directory, то наряду с ликвидацией последствий вредного действия (удаленный ОП восстановится), будут удалены плоды созидательного труда (пользователи вновь вернутся из ОП, в которые они были разнесены). Значит, требуется авторитетное восстановление только части базы. К счастью, это выполнимо.

Авторитетное восстановление выполняется в два этапа:

- ◆ обычное восстановление данных из резервной копии с помощью NtBackup.
- авторитетное восстановление с помощью Ntdsutil.

Авторитетное восстановление с помощью Ntdsutil

При авторитетном восстановлении Ntdsutil лишь помечает базу или отдельные ее части как авторитетные. Остальное — дело репликации. Чтобы пометить данные объекта как авторитетные, версия его должна быть значительно больше, чем известная остальным контроллерам домена.

Для выполнения авторитетного восстановления нужно после запуска Ntdsutil дать команду Authoritative restore. Далее вы можете выбрать один из четырех режимов восстановления:

Режимы авторитетного восстановления

Команда	Назначение
Restore database	Помечает все содержимое базы как авторитетное
Restore subtree %s	Помечает только указанную часть базы как авторитетную
Restore database verinc %d	Помечает все содержимое базы как авторитетное, но увеличивает номер версий на указанную величину. По умолчанию — это 100000. Применяется в основном при повторном авторитетном восстановлении одного и того же объекта
Restore subtree %s verinc %d	Помечает только указанную часть базы как авторитетную, но увеличивает номер версий на указанную величину. Применяется обычно при повторном авторитетном восстановлении одного и того же объекта

Покажем использование режима восстановления отдельной ветви на примере. Пусть на момент резервного копирования в каталоге имелось ОП Test (ou=test,dc=mycorp,dc=ru). В нем находились учетные записи пользователей и компьютеров, в том числе ОП ToBeDeleted, в котором в свою очередь находился пользователь ToBe Deleted.

После выполнения резервного копирования администратор внес:

- в ОП Test добавил ОП PostBackupExt;
- в ОП ToBeDeleted также добавил ОП PostBackup;
- ◆ ОП ToBeDeleted удалил со всем содержимым.

Далее система была перезагружена в режим восстановления Active Directory. Было выполнено восстановление из резервной копии с помощью Ntbackup, затем запущена Ntdsutil.

```
ntdsutil: auth res
```

```
authoritative restore: re sub "ou=ToBeDeleted,ou=Test,dc=mycorp,dc=ru"
```

Последняя команда предписывает выполнить авторитетное восстановление удаленного ОП ToBeDeleted.

```
Opening DIT database... Done.
```

```
The current time is 06-08-02 16:40.19.
```

```
Most recent database update occurred at 06-08-02 16:20.31.
```

```
Increasing attribute version numbers by 100000.
```

Утилита определила, что последнее обновление было выполнено 20 минут назад, и увеличила номера всех атрибутов на 100000.

Counting records that need updating...

Records found: 0000000002

Done.

Found 2 records to update.

Обнаружено, что надо обновить две записи. Резонно предположить, что это ОП ToBeDeleted и учетная запись пользователя ToBe Deleted в нем.

Updating records...

Records remaining: 0000000000

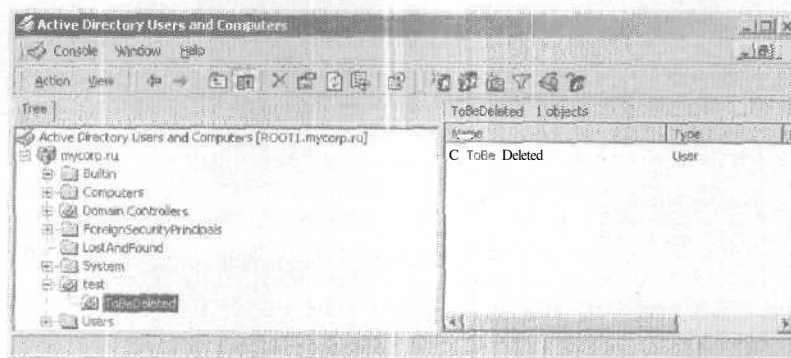
Done.

Successfully updated 2 records.

Authoritative Restore completed successfully.

Обновление выполнено, перегружаем компьютер в нормальный режим и смотрим на результат.

Кажется, цель достигнута: ОП ToBeDeleted с пользователем внутри вновь в Active Directory! То, что в этом ОП нет ОП PostBackup, легко объяснимо. Его ведь не было в резервной копии — оно находилось в удаленном контейнере. Так как последний восстановлен авторитетно, то восстановилось состояние на момент резервирования, т. е. без вложенного ОП.

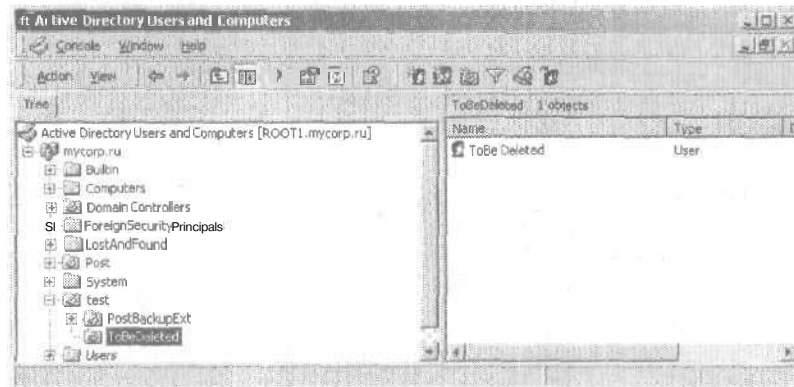


*Результат авторитетного восстановления
до репликации с партнерами*

Но куда делось ОП PostBackupExt? Ведь оно располагалось в ОП Test, которое должно было восстановиться неавторитетно, т. е. не восстанавливая своего состояния на момент резервного копирования. Рас-

суждая так, вы забываете, что неавторитетное восстановление означает не то, что объект не восстанавливается из резервной копии, а то, что объект будет замещен на более актуальную версию при репликации.

Состояние, изображенное на предыдущем рисунке, соответствует моменту сразу после загрузки контроллера домена в нормальный режим. Репликация с партнерами еще не выполнена. А вот после репликации все придет в норму;



*Результат авторитетного восстановления
после репликации с партнерами*

Обеспечение правильности авторитетного восстановления

Выполняя авторитетное восстановление ОП, доменов и сайтов, помните, что с ними могут быть связаны ОГП. А значит, надо уделить особое внимание восстановлению каталога SYSVOL. Во-первых, его нельзя сразу восстановить в исходное положение. При этом вы рискуете нарушить синхронизацию между КГП и ШГП (см. главу «Групповая политика»). Поэтому его следует восстановить в другой каталог на диске, а потом вручную скопировать нужные каталоги групповых правил для авторитетно восстанавливаемых объектов.

Во-вторых, процесс восстановления SYSVOL выполняется так, что каталог SYSVOL после него публикуется не сразу, а только после репликации с партнерами. Теперь представьте, что вы авторитетно восстановили Active Directory на всех контроллерах в домене одновременно. Начнется репликация SYSVOL, увы, бесконечная. Чтобы этого избежать, восстановите Active Directory изначально только на одном контроллере, дождитесь публикации SYSVOL и только потом начинайте восстановление на остальных контроллерах.

Чтобы убедиться в выполнении авторитетного восстановления объекта, достаточно выполнить команду `repadmin /showmeta <имя восстанавливаемого объектов>`

```
repadmin /showmeta ou=tobedeleted,ou=test,dc=mycorp,dc=ru
```

8 entries.

Loc. USN	Originating DSA	Org. USN	Org. Time/Date	Ver	Attribute
9645	Default-First-Site-Name\ROOT1	16:20.04 1	9645 2002-06-08		objectClass
9665	Default-First-Site-Name\ROOT1	17:59.22200001	9665 2002-06-08		ou
9665	Default-First-Site-Name\ROOT1	17:59.22200001	9665 2002-06-08		instanceType
9665	Default-First-Site-Name\ROOT1	17:59.22200001	9665 2002-06-08		whenCreated
9665	Default-First-Site-Name\ROOT1	17:59.22200000	9665 2002-06-08		isDeleted
9665	Default-First-Site-Name\ROOT1	17:59.22200001	9665 2002-06-08		nTSecurityDescriptor
9665	Default-First-Site-Name\ROOT1	17:59.22200001	9665 2002-06-08		name
9665	Default-First-Site-Name\ROOT1	17:59.22200001	9665 2002-06-08		objectCategory

Номер версии атрибутов наглядно показывает, на какую величину было выполнено изменение версии при авторитетном восстановлении.

Влияние авторитетного восстановления

Авторитетное восстановление — вещь опасная, так как может восстановить в каталоге те объекты и атрибуты, которые могут негативно сказаться на работе контроллера домена или системы в целом. Среди прочего я хотел бы остановить внимание на восстановлении:

- паролей компьютерных учетных записей;
- ◆ членства в группах.

Первое может привести к неработоспособности контроллера, второе — к нарушению правильного функционирования всей системы,

Влияние на доверительные отношения и учетные записи компьютеров

Пароли учетных записей компьютеров и доверительных отношений периодически изменяются. Для компьютеров и доверительных отно-

шений Windows 2000 этот интервал равен 30 дням, для Windows NT 4.0 — 7 дням. Кроме того, хранится история двух паролей, что позволяет системам взаимодействовать даже при рассинхронизации последних паролей. Для Windows 2000 этот период равен 60 дням, а вот для Windows NT 4.0 — всего 14.

Замечание В [3] эта информация приведена довольно невнятно, и можно подумать, что максимальный срок синхронизации для компьютеров Windows 2000 равен 14 дням, но это не так.

Теперь представьте, что вы восстанавливаете систему авторитетно из резервной копии, срок которой превышает 60 дней. (Выше я показал, что стандартными средствами это сделать нельзя. Но ведь есть же и нестандартные...) При этом будут восстановлены старые пароли доверительных отношений и учетных записей контроллера, которые не позволят ему связаться со своими партнерами по репликации, а клиентским станциям — подключиться к контроллеру. В журнале регистрации появится одно или оба следующих сообщения:

```
The session setup from the computer DOMAINMEMBER failed to
authenticate. The name of the account referenced in the security
database is DOMAINMEMBER$. The following error occurred: Access is
denied.
```

NETLOGON Event ID 3210:

```
Failed to authenticate with \\DOMAINDC, a Windows NT domain controller
for domain DOMAIN.
```

Если рассинхронизированы пароли, появится сообщение:

NETLOGON Event 5722:

```
The session setup from the computer %1 failed to authenticate. The
name of the account referenced in the security database is S2. The
following error occurred: %n%3
```

В таком случае надо сбросить пароль учетной записи контроллера домена с помощью утилиты Netdom (см. раздел «Поиск и устранение проблем репликации» главы «Репликация Active Directory» или статью Q216393 в Microsoft Technet).

Наиболее вероятно авторитетное восстановление паролей для связи с доменами Windows NT, так как они гораздо чаще изменяют свои пароли. Поэтому, если в сети есть такие домены либо в домене Windows 2000 есть контроллеры Windows NT 4.0, надо внимательно относиться к дате резервной копии при авторитетном восстановлении.

Влияние на членство в группах

Последствия авторитетного восстановления групп могут быть куда более серьезными. Наихудший вариант — потеря информации о членстве в восстановленной группе.

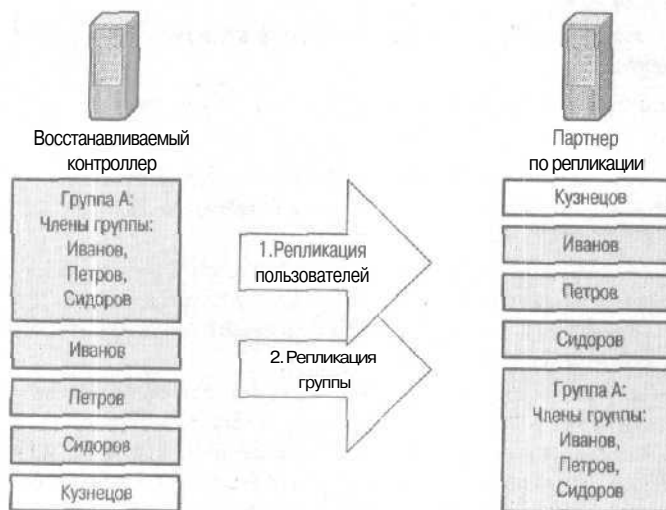
Допустим, вы случайно удалили группу и несколько ее членов. Члены группы представлены в атрибуте `member`, имеющем много значений. К тому же связи, обратные связи и удаления распределены по Active Directory. Это все приводит к тому, что результат авторитетного восстановления группы зависит от того, какой из объектов будет реплицирован первым: группа или пользователи в ней.

Если первой произойдет репликация восстановленных пользователей, членство в группе будет отражено правильно как в атрибутах группы, так и в атрибутах пользователей.

Если первой выполнится репликация восстановленной группы, то на партнерах по репликации пользователи будут исключены из группы, так как на этот момент их с локальной точки зрения контроллеров нет. А раз так, они и не могут быть членами группы.

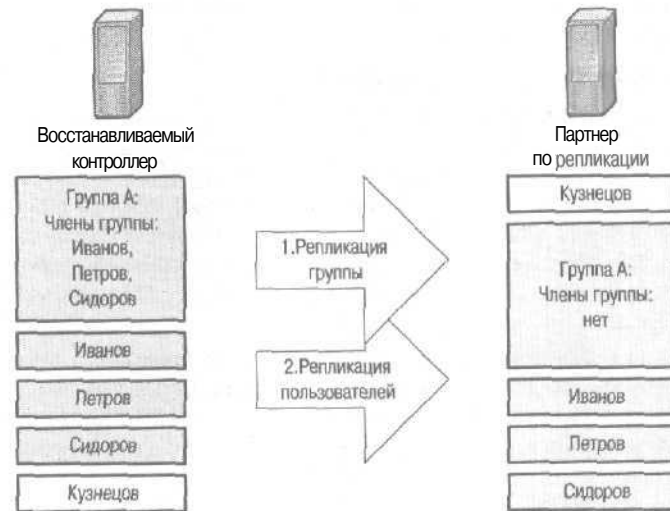
К сожалению, нет способа указать, какие объекты должны реплицироваться первыми. Значит, конечный результат будет правильным с вероятностью 50%. Можно ли с этим бороться?

Можно. После авторитетного восстановления группы вы добавляете в нее фиктивного пользователя. Сразу же после добавления вы его

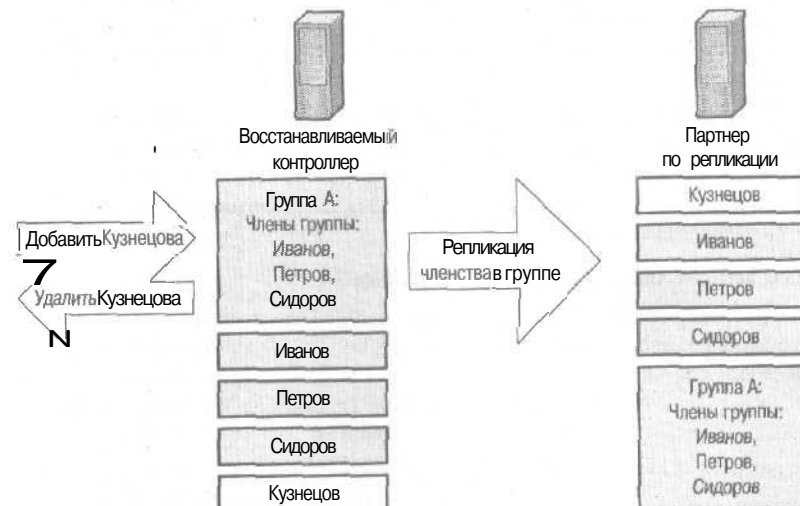


Если первой прошла репликация пользователей, то восстановление правильное

удаляете. Это нехитрое действие укажет, что членство в этой группе должно быть обновлено на остальных контроллерах домена. Так как к этому моменту учетные записи восстановленных пользователей уже будут присутствовать на остальных партнерах по репликации, членство в группе восстановится совершенно правильно.



Если первой прошла репликация группы, членство в ней теряется



Добавление и удаление фиктивного члена в группы исправляет положение

Тут есть небольшая опасность: если до того, как вы добавите и удалите фиктивного пользователя на восстанавливаемом контроллере, другой администратор внесет изменение на другом контроллере в членство этой группы или для любого ее члена, вы **вновь** получите неверный результат. Тогда авторитетное восстановление группы придется повторить, дополнительно увеличив при этом номер версии с помощью аргумента `verinc`.

Восстановление Глобального каталога

Способ восстановления ГК зависит от способа восстановления Active Directory. Если оно **выполнялось** путем полной переустановки контроллера с последующей репликацией, ГК по умолчанию восстановлен не будет. Вам придется отметить соответствующий флажок в оснастке Active Directory Sites and Services для преобразования контроллера в сервер ГК. Естественно, при этом надо уделить внимание пропускной способности канала, так как объем ГК может быть весьма велик при большом числе доменов.

Иное дело, когда восстановление выполнялось из резервной копии. Независимо от вашего желания вместе с состоянием системы будут восстановлены все разделы Active Directory и в том числе ГК. Уже после его **восстановления** вы можете **решить**, нужен ли он вам на этом контроллере.

Восстановление мастеров операций

Я уже рассказывал об этом в разделе «Принудительное назначение мастеров операций с помощью `Ntdsutil`». Здесь же остановимся на том, когда восстанавливать мастер и что будет, если его нельзя восстановить.

Если сервер, выполнявший одну или несколько ролей мастеров **операций**, восстанавливается из резервной копии, восстанавливаются и соответствующие роли. Если же восстановление выполнялось путем полной переустановки и последующей репликации, роли мастеров надо назначать принудительно.

Кто может быть мастером операций?

Странный вопрос! Им может быть любой контроллер в домене, скажете вы. Но это **утверждение** справедливо для нормально работающего домена, а не для восстанавливаемого после аварии. Ведь при этом нельзя гарантировать, что репликация завершена и все контроллеры имеют одинаковую информацию о домене.

Выяснить, какой из них **обладает** самыми последними данными, позволяет утилита `repadmin` (см. главу «Репликация Active Directory»). Я перечислю здесь лишь выполняемые команды.

Пусть в домене mycorp.ru два контроллера домена root1 и root2, один из них был восстановлен. В данный момент ни тот, ни другой не является мастером операций. Чтобы выяснить, какой обладает самыми точными знаниями о домене, выполним команды:

```
C:\>repadmin /showvector dc=mycorp,dc=ru root2.mycorp.ru
Default-First-Site-Name\ROOT2      9 USN 7214
Default-First-Site-Name\ROOT1      @ USN 9261
```

```
C:\>repadmin /showvector dc=mycorp,dc=ru root1.mycorp.ru
Default-First-Site-Name\ROOT2      @ USN 7208
Default-First-Site-Name\ROOT1      9 USN 9261
```

Как видно из результата, сервер root2 имеет более полные сведения о себе (7214 > 7208) и одинаковые сведения с партнером о нем (USN=9261). Значит, наиболее актуальная информация хранится на root2, и его имеет смысл принудительно сделать мастером операций,

Восстановление мастера схемы

Мастер схемы требуется, только когда должна быть модифицирована схема (см. главу «Проектируем Active Directory»). А часто ли вы изменяете схему? Думаю, это случалось один-два раза — при установке приложений, вносящих в схему собственные атрибуты или объекты. В остальных случаях мастер схемы и не нужен.

Так, может, от него вообще избавиться? Я бы не был столь категоричен. Допустим, вышел из строя контроллер, бывший мастером схемы. То, как быстро вам его надо восстановить, зависит от необходимости модификации схемы. В принципе можно не торопясь собрать и протестировать новый сервер, поднять на нем контроллер домена и уж потом восстановить исполняемую роль.

Иное дело, когда авария произошла в самый ответственный момент, когда вы устанавливали, например, Microsoft Exchange 2000. Тратить время на восстановление контроллера — значит, сорвать план установки почтовой системы. В такой ситуации можно принудительно назначить другой контроллер мастером схемы и продолжить работу. Потом, когда аварийный контроллер будет восстановлен, ему можно будет вновь передать эту роль от «и. о. мастера схемы».

Восстановление мастера доменных имен

Аналогичная ситуация наблюдается и для мастера доменных имен. Как известно, он нужен при добавлении в домен или удалении контроллеров домена. В нормальных рабочих системах это происходит довольно редко. (Конечно, если вы не занимаетесь расширением сети и добавлением новых территорий.) Значит, можно не торопясь собрать

и протестировать новый сервер, поднять на нем контроллер домена и потом восстановить исполняемую роль.

Если мастер доменных имен нужен позарез, можно принудительно назначить другой контроллер мастером доменных имен и продолжить работу. Передача этой роли возможна, только если контроллер-адресат является сервером ГК. Восстановленному контроллеру можно вновь передать эту роль.

Восстановление мастера RID

Отсутствие мастера RID серьезно сказывается на домене. Так, если один из контроллеров домена полностью исчерпал свой пул RID, а это 512 идентификаторов, то при попытке создать объект системы безопасности появится сообщение об ошибке: «Windows cannot create the object because: The directory sendee has exhausted the pool of relative identifiers». Дополнительно к этому в журнал регистрации событий того контроллера, на котором выполнялась попытка добавления объекта, будет занесено сообщение с ID=16645.

Значит ли это, что надо все бросить и спешно восстанавливать мастера RID? Все зависит от того, сколько контроллеров в домене и насколько они исчерпали свои пулы RID. Три контроллера в домене обеспечивают до 1536 идентификаторов. Поэтому в крайнем случае объекты можно продолжить создавать на них.

Иное дело, если вы переносите объекты безопасности из других доменов. Тогда отсутствие мастера RID не позволит вам это сделать, так как нет обходных путей.

Решение о принудительном назначении контроллера домена мастером RID должно приниматься, исходя из того, что потом он и только, он будет исполнять роль мастера RID. Если вы надеетесь восстановить аварийный контроллер, выполнявший эту функцию, то принудительно назначать роль мастера RID другим контроллерам категорически запрещено. Дело в том, что восстановленный впоследствии мастер RID потенциально может выдать пул ID, выданный однажды временным мастером RID, что приведет к появлению в системе объектов безопасности с одинаковыми SID.

Восстановление имитатора PDC

Отсутствие имитатора PDC в домене может привести к следующим последствиям.

- В домене, работающем в смешанном режиме, при наличии контроллеров Windows NT 4.0 станет невозможно выполнять администрирование этих контроллеров. Попытка использования User manager for domains или Server manager будет заканчиваться выводом сообщения о недоступности PDC.

- В домене, работающем в естественном режиме, учащаются отказы в доступе. В частности, при смене пароля пользователя на одном из контроллеров регистрация пользователя на другом контроллере будет невозможна, пока репликация не передаст новое значение пароля. Если нужна срочная регистрация пользователя в домене, пароль можно изменить прямо на том контроллере, где он будет регистрироваться.
- ◆ Неудобство редактирования групповой политики. Как известно редактирование ОГП выполняется на имитаторе PDC, а потом тиражируется на остальные контроллеры (см. главу «Групповая политика»). Поэтому отсутствие имитатора PDC приведет к выводу сообщения о том, что контроллер домена не обнаружен, и будет предложено выбрать иной контроллер. Это сообщение будет выводиться при каждой операции редактирования ОГП.
- + Невозможность внесения изменений в конфигурацию DFS. Модификация конфигурации DFS выполняется только на имитаторе PDC (см. главу «Active Directory и файловая система»).

Раз так, то имитатор PDC должен постоянно присутствовать в домене. В отличие от мастера RID нет принципиальной разницы, какие контроллеры домена и в какой последовательности выполняют эту роль. Главное условие: имитатор должен быть один. Поэтому после аварии контроллера, являвшегося имитатором PDC, достаточно выбрать другой контроллер и принудительно назначить ему эту роль. После восстановления аварийного контроллера эта роль ему может быть возвращена.

Замечание В смешанном режиме работы контроллер, назначаемый имитатором PDC, необходимо синхронизировать с остальными.

Восстановление мастера инфраструктуры

Недоступность мастера инфраструктуры на конечных пользователях не сказывается. Более того, это проблема администраторов. Выражается она в том, что при различных манипуляциях с группами операции будут выполняться чрезвычайно медленно. Но будут. Есть ограниченное число операций, которые не могут быть выполнены без мастера инфраструктуры.

Поэтому в случае аварии контроллера, исполняющего эту роль, его восстановления можно подождать. Если же ждать невозможно, эту роль можно принудительно передать любому контроллеру, на котором нет ГК.

Проверка целостности и восстановление базы

Ntdsutil позволяет выполнять проверку целостности базы Active Directory. Не могу сказать, что это полезно. На мой взгляд, поиск статьи, описывающей вашу конкретную ситуацию в базе знаний Microsoft, принесет больше практической пользы, чем такой анализ. Но иногда для самоуспокоения (мол, с Active Directory-то все в порядке — проблема в чем-то другом) имеет смысл выполнить эти тесты. Помните только, что их выполнение может затянуться.

Среди предлагаемых тестов следует выделить:

- «Мягкое» восстановление журналов базы;
- ◆ проверка целостности базы;
- семантический анализ базы.

«Мягкое» восстановление журналов базы

В случае внезапного отключения контроллера домена (например, при аварии электропитания) его перезагрузка сопровождается проверкой журнала базы и повторным воспроизведением транзакций, записанных в нем (см. главу «Установка Active Directory»). Эту же операцию можно выполнить самостоятельно. Для этого достаточно в Ntdsutil войти в режим File Maintenance и выбрать команду Recover. Вот пример такого восстановления.

```
C:\>ntdsutil
ntdsutil: files
file maintenance: recover
Executing Command: C:\WINNT\system32\esentutl.exe /r /8 /o
/1"C:\WINNT\NTDS" /s"C:\WINNT\NTDS" /i10240
```

```
Initiating RECOVERY mode...
    Log files: C:\WINNT\NTDS
    System files: C:\WINNT\NTDS
```

```
Performing soft recovery...
```

```
Operation completed successfully in 7.851 seconds.
Spawned Process Exit code 0x0(0)
```

If recovery was **successful**, it is recommended you **run** semantic database analysis to insure semantic database consistency as well.

Проверка целостности базы

Команда Integrity позволяет проверить структуру базы на низком уровне. Также проверяется целостность таблиц, правильность заголовков и т. д. Эта операция может занимать длительное время. Примерная скорость проверки — 2 Гб/час. При этом на экран выводится информация о том, какая часть работы уже выполнена, обнаруженные ошибки заносятся в журнал. Например:

```
file maintenance: integrity
```

```
Opening database [Current].
```

```
Executing Command: C:\WINNT\system32\esentutl.exe /g
```

```
"C:\WINNT\NTDS\ntds.dit" /!10240 /8 /v /x /o
```

```
Initiating INTEGRITY mode...
```

```
Database: C:\WINNT\NTDS\ntds.dit
```

```
Temp. Database: INTEG.EDB
```

```
got 6107 buffers
```

```
checking database header
```

```
checking database integrity
```

```
Scanning Status ( X complete )
```

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

```
checking SystemRoot
```

```
SystemRoot (OE)
```

```
SystemRoot (AE)
```

```
checking system table
```

```
MSysObjectsShadow
```

```
MSysObjects
```

```
Name
```

```
RootObjects
```

```
rebuilding and comparing indexes
```

```
checking table "datatable" (6)
```

```
checking data
```

```
.....checking long value tree (48)
```

```
checking index "LCL_ABVIEW_index00000419" (89)
```

```
checking index "DNT_IsDeleted_Index" (88)
```

```
checking index "INDEX_000901FD" (87)
```

```
checking index "INDEX_000901F6" (86)
```

```
checking index "INDEX_000900DE" (85)
```

```
checking index "INDEX_000201D5" (84)
```

```
checking index "INDEX_000902BB" (83)
```

```
checking index "INDEX_0000002A" (24)
```

```

checking index "INDEX_00000004" (23)
checking index "NC_Acc_Type_Name" (22)
checking index "PDNT_index" (21)
checking index "INDEX_00090001" (20)
checking index "Ancestors_index" (13)
checking index "DRA_USN_CREATED_index" (12)
checking index "DRA_USN_index" (11)
checking index "del_index" (10)
checking index "INDEX_00090002" (9)
checking index "NC_Acc_Type_Sid" (8)
checking index "INDEX_00090092" (7)
rebuilding and comparing indexes
checking table "hiddentable" (16)
checking data
rebuilding and comparing indexes
checking table "link_table" (14)
checking data
checking index "backlink_index" (15)
rebuilding and comparing indexes
checking table "MSysDefrag1" (90)
checking data
checking index "TablesToDefrag" (91)
rebuilding and comparing indexes
checking table "sdproptable" (17)
checking data
checking index "clientid_index" (19)
checking index "trim_index" (18)
rebuilding and comparing indexes

```

integrity check completed.
Operation completed successfully in 11.26 seconds.

Spawned Process Exit code 0x0(0)

If integrity was successful, it is recommended
you run semantic database analysis to insure
semantic database consistency as well.

Семантический анализ базы

Позволяет протестировать логическую целостность базы. Вот что проверяется.

- Счетчик ссылок Проверяется, что у каждого объекта есть номер GUID, отличительное имя и ненулевое число ссылок на него. Для

удаленных объектов проверяется, что у них есть дата и время, но нет номера GUID и отличительного имени. Проверяется и целостность таблиц ссылок (см. [3]).

- ◆ Удаленные объекты. Проверяется, какое именно **время** имеют удаленные объекты и **есть** ли у них специальное отличительное имя.
- ◆ Описатели безопасности. Проверяется наличие у каждого дескриптора контрольного поля и списка контроля доступа. Если у удаленных объектов нет списка контроля доступа, выводится предупреждение.
- ◆ Правильность репликации. Проверяется вектор **обновленности** для раздела каталога. Также **проверяются** метаданные объектов.

Для выполнения семантического анализа надо в утилите Ntdsutil войти в режим Semantic database **analysis**, включить подробный вывод (**Verbose on**) и запустить проверку командой Go:

```
ntdsutil: sem da an
semantic checker; ver on
Verbose mode enabled.
semantic checker: go
Fixup mode is turned off
Opening database [Current]. . . .Done.
```

```
Getting record count...2678 records
Writing summary into log file dsdit.dmp.0
Records scanned:      2600
Processing records..Done.
```

Результаты анализа можно найти в файле dsdit.dmp.xx, где xx — порядковый номер. Ниже приведен пример результатов анализа. Этот анализ выполнялся на контроллере домена **myscorp.ru**, который был также и сервером ГК. Помимо него, имелся дочерний домен **msk**.

```
INFO: UpToDate vector found for NC head 1162(mycorp)
INFO: UpToDate vector found for NC head 1163(Configuration)
WARNING: Deleted object 1175 has timestamp[12/30/9999] later than now
WARNING: Deleted object 1177 has timestamp[12/30/9999] later than now
INFO: UpToDate vector found for NC head 1179(Schema)
```

Данные строки указывают на то, что обнаружен вектор обновленности для контекстов **myscorp.ru**, схемы и конфигурации.

```
Warning SE_DACL_PROTECTED for 1337(VolumeTable)
Warning SE_DACL_PROTECTED for 1343({31B2F340-016D-11D2-945F-00C04FB984F9})
Warning SE_DACL_PROTECTED for 1346({6AC1786C-016F-11D2-945F-00C04FB984F9})
Warning SE_DACL_PROTECTED for 1396(AdminSDHolder)
Warning SE_DACL_PROTECTED for 1402(Administrator)
Warning SE_DACL_PROTECTED for 1421(Schema Admins)
```

Warning SE_DACL_PROTECTED for 1422(Enterprise Admins)

Warning SE_DACL_PROTECTED for 1424(Domain Admins)

Подтверждено существование непустых списков контроля доступа к основным учетным записям домена mycorp.ru.

INFO: UpToDate vector found for NC head 2622(msk)

INFO: Partial Attributes List found for NC head 2622(msk)

WARNING: Deleted object 2652 has timestamp[12/30/9999] later than now

Обнаружен ГК и в нем — контекст msk.

Warning SE_DACL_PROTECTED for 2664(VolumeTable)

Warning SE_DACL_PROTECTED for 2670({31B2F340-016D-11D2-945F-00C04FB984F9})

Warning SE_DACL_PROTECTED for 2673({6AC1786C-016F-11D2-945F-00C04FB984F9})

Warning SE_DACL_PROTECTED for 2768(AdminSDHolder)

Warning SE_DACL_PROTECTED for 2769(Domain Admins)

Warning SE_DACL_PROTECTED for 2770(Administrator)

Warning SE_DACL_PROTECTED for 2810({BB0B08E9-3E4F-4EAE-AA84-188CB97B3E8F})

Warning SE_DACL_PROTECTED for 2824({0DBEB430-79EB-4C3A-8118-A427B95E02BC})

Подтверждено существование непустых списков контроля доступа к основным учетным записям домена msk.mycorp.ru в ГК.

2678 total records walked.

Summary:

Active Objects 2651

Phantoms 12

Deleted 15

Информация достаточно исчерпывающая, но повторюсь: в повседневной практике от нее мало толку. В основном применение этих функций имеет смысл при восстановлении базы Active Directory *не с* помощью резервной копии.

Ремонт базы

Данную операцию я назвал «ремонт», чтобы указать на отличие от процессов *восстановления*, описанных ранее. Пойти на ремонт можно только в крайнем случае, когда у вас нет возможности восстановить базу из резервной копии или путем репликации.

Ремонт также выполняется с помощью утилиты Ntdsutil. Но это не гарантирует, что база останется работоспособной. Это последняя надежда, когда терять больше нечего.

Для выполнения ремонта надо войти в режим File maintenance и выбрать команду *repair*. Процесс ремонта может *затянуться*, но в любом случае надо дождаться его завершения. А затем надо обязательно выполнить проверку *целостности* и семантический анализ.

Перенос базы Active Directory

Когда в главе «Установка Active Directory» мы обсуждали конфигурирование контроллеров домена, я подчеркивал, что файлы базы и журналов транзакций в нагруженных контроллерах нужно разнести на разные физические диски. Жизнь показывает, что не все верят этому либо верят, но не имеют возможности так поступить при развертывании Active Directory. Когда же осознается необходимость разнесения этих файлов или появляется такая возможность, требуется использовать **Ntdsutil**. При этом:

- ♦ уточните, на каких дисках в настоящее время размещаются файлы базы и журналов;
- перенесите файл базы/файлы журналов на новый (желательно отказоустойчивый) диск.

Выяснение местоположения файлов

Для выяснения текущего положения файлов базы Active Directory и журналов транзакций надо запустить утилиту **Ntdsutil**, войти в режим **File maintenance** и выбрать команду **Info**.

Замечание Данная команда выполняется только в режиме восстановления Active Directory.

При этом проверяется свободное место на диске и сообщаются текущие размеры файлов:

```
file maintenance: info
Drive Information:
    C:\ NTFS (Fixed Drive ) free(534.6 Mb) total(1.9 Gb)
DS Path Information:

Database   : C:\WINNT\NTDS\ntds.dit - 10.1 Mb
Backup dir : C:\WINNT\NTDS\dsadata.bak
Working dir: C:\WINNT\NTDS
Log dir    : C:\WINNT\NTDS - 40.1 Mb total
              res2.log - 10.0 Mb
              res1.log - 10.0 Mb
              REPAIR.TXT - 0.0 Kb
              ntds.pat - 16.0 Kb
              edb00001.log - 10.0 Mb
              edb.log - 10.0 Mb
```

Перенос файлов базы

Файлы базы нельзя перенести простым копированием. Дело в том, что система должна как-то узнать, куда файлы перенесены. Поэтому перенос может осуществить одним из двух способов.

- + Файлы базы копируются на новый диск. В режиме File maintainance выберите команду Set path DB %s, указав в ней новый путь к базе. Я бы рекомендовал этот способ при добавлении новых жестких дисков. При этом сами файлы базы никуда не перемещаются, а вот буква, присвоенная диску может измениться.
- Второй способ удобнее именно при физическом переносе базы на другой диск. В режиме File maintainance выберите команду Move DB to %s, подставив в нее путь к каталогу с базой. Программа сама скопирует файлы в новое положение и обновит свою информацию.

В любом случае после переноса файлов надо произвести мягкое восстановление журналов либо просто перезагрузить контроллер. Восстановление будет выполнено автоматически при загрузке компьютера,

Внимание Мягкое восстановление журналов занимает длительное время после переноса файла базы на другой диск. Так, для базы размером всего 10 Мб оно может выполняться 15-20 минут на машине с процессором PIII-866 и объемом памяти 512 Мб.

Перенос файлов журналов

Как перенос файлов базы нельзя выполнить простым копированием файлов, так и для переноса журналов нужна Ntdsutil. Это связано с тем, что система должна как-то узнать, куда файлы перенесены. Перенести журналы можно одним из двух способов.

- ◆ Файлы журналов копируются на новый диск. В режиме File maintainance выберите команду Set path logs %s, указав в ней новый путь к журналам.
- ◆ Переноса журналы на другой диск, в режиме File maintainance выберите команду Move logs to %s, указав в ней путь к каталогу с журналами. Программа сама скопирует файлы в новое место и обновит свою информацию.

После переноса выполните мягкое восстановление журналов либо просто перезагрузите контроллер. Восстановление будет выполнено автоматически во время загрузки компьютера.

Если надо переустановить домен в лесу

Не часто, но случается, что в дереве доменов появляется полностью «расстроенный» домен. Причин тут может быть несколько, например, желание администратора постоянно экспериментировать с рабочей системой. Как бы там ни было, приходит день, когда в домене перестают устанавливаться приложения, те, что работают, начинают сбоить, а пользователи чаще и чаще сталкиваются с проблемами регистрации и входа в домен. Несомненно, опытный администратор может

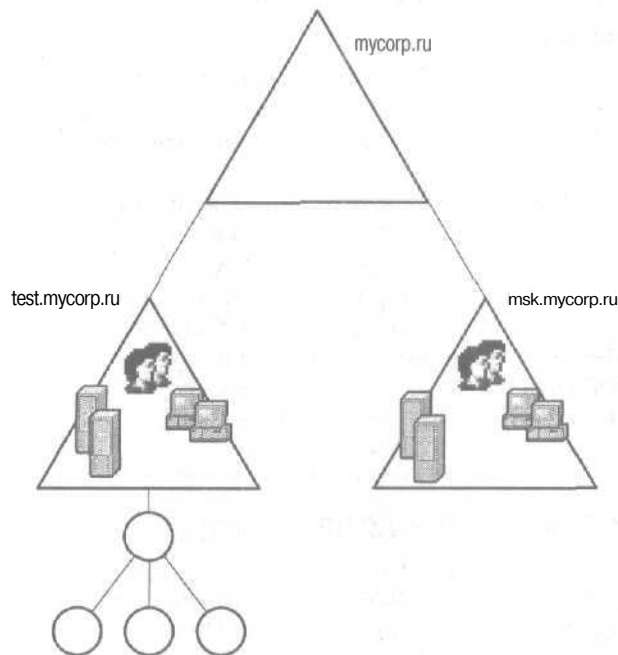
проанализировать поведение системы и восстановить нормальное функционирование. Вот только времени на это уйдет гораздо больше, чем того заслуживает такая система. Поэтому можно предложить альтернативный способ решения проблемы — обновление домена.

Он применим только к тем доменам, которые не имеют дочерних, либо дочерние домены являются небольшими ресурсными доменами и могут быть расформированы с переносом ресурсов в другие домены в дереве.

Для обновления домена все учетные записи групп и пользователей нужно перенести во временный домен, затем существующий домен уничтожить и воссоздать. Проверив корректную работу воссозданного домена, сохраненные учетные записи нужно вернуть назад.

Постановка задачи

Рассмотрим обновление на примере. Допустим, лес состоит из трех доменов. К корневому домену mycorp.ru подключены дочерние: test.mycorp.ru и msk.mycorp.ru. Проблемным является домен test.



Начальная топология леса

В корневом домене нет учетных записей пользователей и ресурсов. Все пользователи находятся в доменах test и msk. В обоих есть серверы.

ры — члены домена, где размещены файлы и принтеры. Доступ пользователей к ресурсам регулируется через членство в локальных и глобальных группах. В домене test есть иерархия ОП, к некоторым из них применяется групповая политика.

К обновлению предъявляются следующие условия:

- ◆ после обновления текущая конфигурация должна быть сохранена;
- пользователи домена msk не должны испытать неудобств при обновлении домена test;
- пользователи домена test должны сохранить свои права доступа к ресурсам домена и свою групповую политику.

Общая последовательность действий

Начать надо с резервного копирования одного из контроллеров того домена, обновление которого планируется, т. е. test. Нужно сделать копию состояния системы и системного диска одного из контроллеров домена. Лучше выбрать мастер операций в домене и ГК. Далее надо принять ключевые решения, определяющие ход обновления.

Определение правил переноса

Так как обновление начинается с переноса объектов из одного домена в другой, определимся с его порядком.

1. Какой домен выбрать в качестве временного: корневой (mycorp.ru) или дополнительный?

Можно рассмотреть и третий случай — задействовать в качестве временного пристанища домен msk, но пользователи не должны испытывать неудобств при обновлении домена test.

При использовании корневого домена дополнительное оборудование не требуется. Во втором случае нужно задействовать дополнительный контроллер домена. Для понимания сути не важно, какой домен выбрать, — будем считать, что у нас нет лишних компьютеров и использование корневого домена в качестве временного «перевалочного пункта» — единственно возможный вариант. В дальнейшем будем называть его доменом-приемником.

Теперь выполним резервное копирование всех контроллеров в этом домене. Необходимо сохранять состояние системы.

2. Когда выполнять обновление? Лучше всего в выходные: пользователей в домене test будет минимум. Кроме того, это позволит избежать проблемы открытых, а значит, перемещаемых файлов.
3. Какие ОП переносить? Для них надо создать такие же в домене-приемнике. Удобнее создать новую структуру внутри специально выделенного ОП, например Temp Migration.

4. Какие группы перенести? Не переносятся встроенные группы, расположенные в контейнере Users. Если в этом контейнере есть группы, отличные от встроенных, удобно их переносить в ОП Temp Migration\Users в домене-приемнике.
5. Каких пользователей перенести? Не переносятся встроенные учетные записи (Administrator, Guest). Если в контейнере Users есть пользователи, они переносятся отдельно от своего контейнера. Удобно их переносить в ОП Temp Migration\Users в домене-приемнике.
6. Какие учетные записи служб, выполняемых не от имени локальной системы, перенести? Если они располагались в отдельном контейнере, надо создать такой же контейнер в домене-приемнике, если же в контейнере Users — они переносятся в контейнер Temp Migration\Users.

Последовательность действий с первого взгляда

Следующий шаг — документирование текущей конфигурации обновляемого домена. Иерархию ОП нужно сохранить. Желательно написать сценарий для воссоздания такой же иерархии.

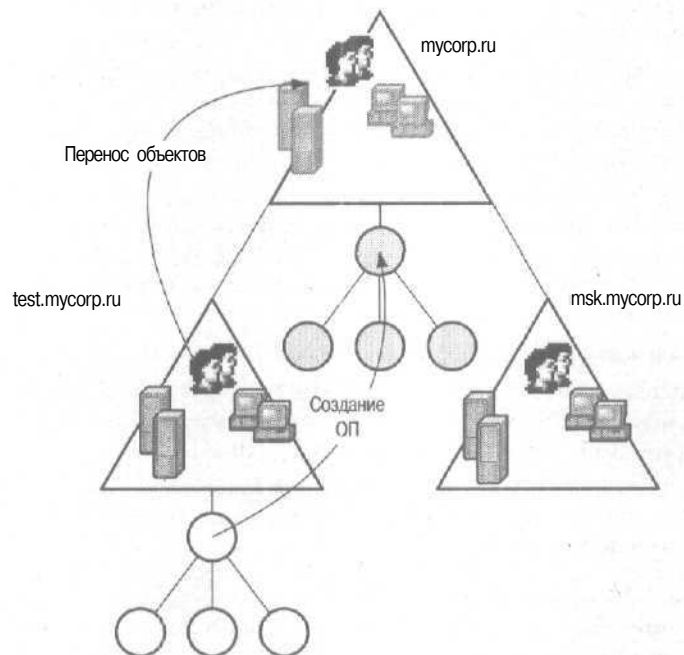
Если использовались групповые правила и их надо перенести в обновленный домен, то соответствующие ОГП должны быть применены к ОП в домене-приемнике.

Замечание К переносу групповых правил надо подходить с большой осторожностью, так как возможно, что именно они явились одной из причин некорректной работы домена.

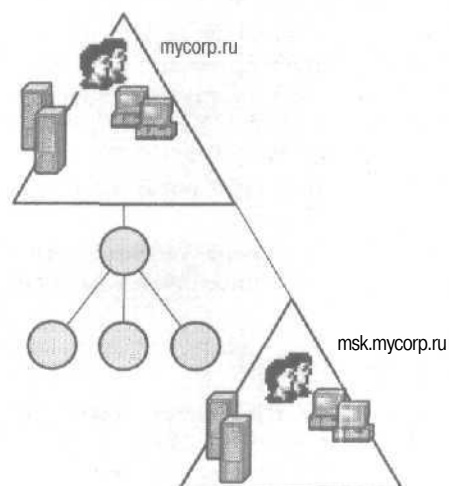
Дальнейшая последовательность действий в общих чертах такова.

1. Перенос серверов-членов домена в домен-приемник. Если на контроллерах домена размещались файловые и принтерные ресурсы, их надо перенести в домен-приемник. Перенос должна выполнять программа, сохраняющая права доступа, например хсору /o /x. Доступ пользователей к этим ресурсам временно будет потерян.
2. Перенос учетных записей служб в соответствующий контейнер в домене-приемнике.
3. Перенос локальных и глобальных групп домена. Удобно совместить эту операцию с переносом учетных записей пользователей, входящих в эти группы.
4. Перенос пользователей, не входящих в уже перенесенные группы, и перенос их блуждающих профилей.
5. Понижение статуса всех контроллеров в обновляемом домене до статуса серверов. С этого момента пользователи не смогут регистрироваться в домене test под прежними именами и паролями.

- б. Переустановка ОС на бывших контроллерах домена. Проверка правильности работы системы.

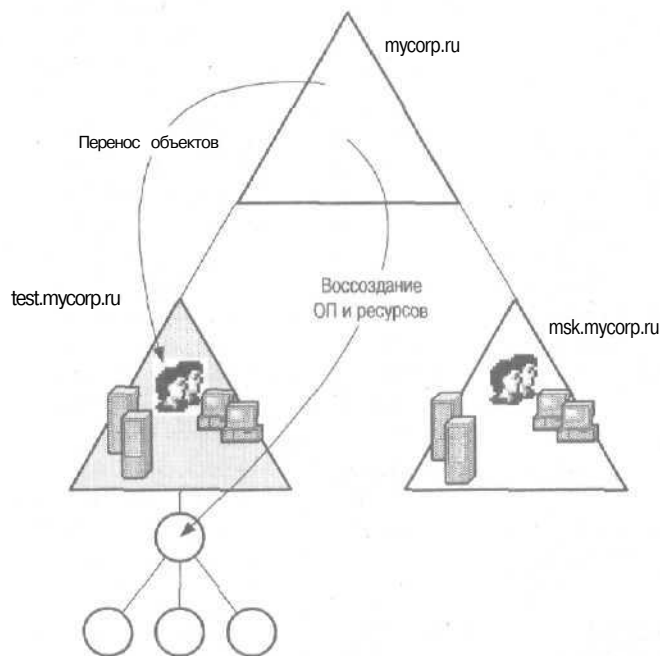


Все объекты переносятся в домен-приемник



Домен временно прекращает свое существование

7. Повышение статуса одного из серверов до контроллера домена `test.mycorp.ru`. Воссоздание в нем структуры ОП. Обратный перенос файловых и принтерных ресурсов, ранее перенесенных в корневой домен. Назначение ОПП воссозданным ОП.
8. Обратный перенос учетных записей служб из корневого домена по завершении репликации.
9. Перенос назад локальных и глобальных групп.
10. Перенос назад пользователей, не входящих в группы.
11. Резервное копирование воссозданного контроллера после проверки работоспособности домена, работоспособности репликации и правильности доступа к ресурсам и отработки профилей.



После установки первого контроллера в домене все перенесенное возвращается назад

12. Переустановка второго контроллера домена.

Перенос пользователей и групп в деталях

Из перечисленных выше операций детального описания требует перенос групп и пользователей. Удобнее всего выполнять его с помощью Active Directory Migration Tool (ADMT).

ADMT, распространяемая свободно на Web-сайте Microsoft, помимо миграции пользователей и групп, позволяет переносить компьютеры, параметры безопасности, доверительные отношения, учетные записи служб, а также готовить отчеты о выполненных операциях.

Замечание При переносе домен-приемник должен работать в естественном режиме.

Перенос может выполняться в двух режимах: тестовом и рабочем. Рекомендуется предварительно выполнить тестовый перенос, а потом, если ошибок нет, — рабочий.

ADMT содержит набор программ-мастеров. Для переноса групп служит *мастер переноса групп*. Запустив его, выберите переносимые локальные и глобальные группы в домене-источнике. Затем укажите, в какой контейнер (к этому моменту он должен существовать) в домене-приемнике их поместить.

Укажите свойства переноса. Так как нам важно сохранить права доступа к ресурсам обновляемого домена, надо выполнить перенос групп с сохранением атрибута SID history. С этой целью в диалоговом окне мастера отметим флажок Update User rights.

С другой стороны, нужно сохранить членство в группах. Поэтому отметим флажок Copy group membership. При этом переносятся не только указанные, но и все группы и учетные записи пользователей — члены переносимых групп. Так мы убиваем двух зайцев: переносим и группы, и пользователей. Например, если в локальную группу LG1 входит глобальная GG1, а в нее — ряд пользователей, то при переносе групп будут перенесены все пользователи из группы GG1.

Переносимые группы можно переименовать, добавив к именам префикс или суффикс. Так, при переносе группы Password resetters ее имя можно преобразовать в Test_Password Resetters. Это актуально, если:

- ◆ группы переносятся в общий контейнер с другими группами в домене-приемнике,
- ◆ перенос выполняется «навечно», т. е. не ставится задача возвращения групп в исходный домен после его обновления.

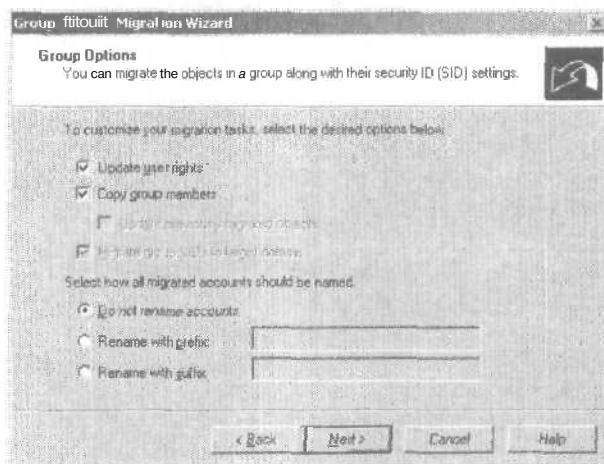
Поскольку выбран перенос групп в специальные контейнеры на время, переименовывать группы нет смысла. Поэтому соответствующий переключатель остается в том же положении, что и на рисунке.

Если бы в домене-приемнике имелись учетные записи и группы, надо было бы позаботиться об уникальности переносимых имен. В нашем случае в этом нет нужды, но когда есть вероятность обнаружения одноименных групп, можно определить правило, предписывающее

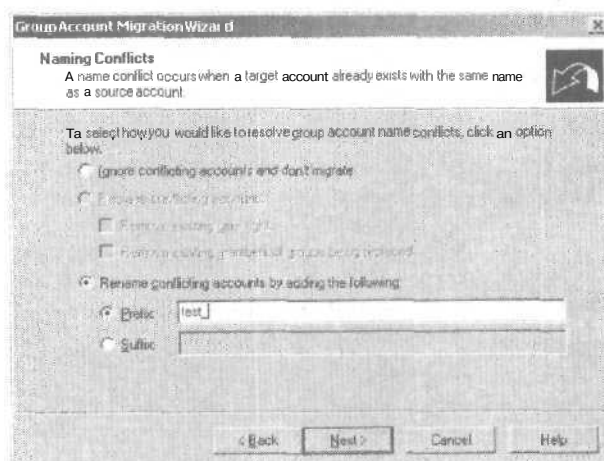
добавлять к именам префикс или суффикс при обнаружении в домене-приемнике «тезки» переносимой группы.

Если такой способ разрешения конфликта не подходит, можно выбрать один из следующих.

- ◆ При обнаружении конфликтных имен перенос таких групп не выполняется. Это самый безопасный вариант, однако впоследствии вы должны проверить, какие группы перенесены, а какие нет,



Управление параметрами переноса групп



Разрешение конфликтов именования групп

- ◆ Перенос сопровождается замещением одноименных групп домене-приемнике. При этом можно лишать прав пользователей в группах и исключать членов замещаемых групп. Как видите, это жесткий вариант, который не оставляет группам в домене-приемнике шансов на выживание.

В нашем примере наиболее удачным является путь переименования.

После определения начальных параметров начинается процесс переноса. Чтобы понять, не было ли ошибок, достаточно взглянуть на финальное окно мастера с кратким отчетом о проделанной работе. А вот если ошибки были, то, чтобы понять, в чем они заключались, надо открыть файл `migration.log`. Взгляните на пример такого файла. Сначала сообщается, что именно должно быть сделано. В нашем примере из домена Test в домен Мусопр переносятся две глобальные группы GG01 и GG02, две локальные — LG01 и LG02, а также включенные в них учетные записи пользователей.

2002-06-07 02:56:41-

2002-06-07 02:56:41-Active Directory Migration Tool, Starting...

2002-06-07 02:56:41-Starting Account Replicator.

2002-06-07 02:56:42-Account MigrationWriteChanges:No TEST MYCORP

CopyUsers:Yes CopyGlobalGroups:Yes CopyLocalGroups:Yes CopyComputers:No

2002-06-07 02:56:48-User account CN=Fy01 will be moved.

2002-06-07 02:56:48-User account CN=Fy02 will be moved,

2002-06-07 02:56:48-User account CN=Fyt01 will be moved.

2002-06-07 02:56:48-User account CN=fyt02 will be moved.

2002-06-07 02:56:48-Group CN=GG01 will be moved.

2002-06-07 02:56:48-Group CN=GG01 will be moved.

2002-06-07 02:56:48-Group CN=GG02 will be moved.

2002-06-07 02:56:48-Group CN=GG02 will be moved.

2002-06-07 02:56:48-Group CN=LG01 will be moved.

2002-06-07 02:56:48-Group CN=LG02 will be moved.

После этого перечислены все действия по переносу. Я не стал воспроизводить все строки журнала, так как они одинаковы для каждого переносимого объекта, а оставил только некоторые, дающие представление о ходе переноса. Сначала сообщается, что пользователь Fy02 был перенесен из домена Test в домен Мусопр. Перенос пользователей — членов групп должен выполняться первым, иначе будет потеряна информация о членстве.

2002-06-07 02:56:49-Moved

LDAP://TEST/CN=Fy02,CN=Users,DC=test,DC=mycorp,DC=ru to

LDAP://MYCORP/CN=Fy02,OU=Test Unit,DC=mycorp,DC=ru

А вот эта строка говорит, что этот же пользователь удален из глобальной группы GG01 в домене Test:

2002-06-07 02:56:50- Removed

LDAP://TEST/CN=Fy02, CN=Users, DC=test, DC=mycorp, DC=ru from

LDAP://DC01/CN=GG01, OU=Test, DC=test, DC=mycorp, DC=ru

После переноса всех пользователей-членов группы и их исключения из нее сообщается о переносе глобальной группы GG01;

2002-06-07 02:56:50-Moved

LDAP://test.mycorp.ru/CN=GG01, OU=Test, DC=test, DC=mycorp, DC=ru to

LDAP://MYCORP/CN=GG01, OU=Test Unit, DC=mycorp, DC=ru

И вслед за этим удаляются остальные члены этой группы:

2002-06-07 02:56:50-Removing members from group CN=GG01

CLDAP://DC01/CN=GG01, OU=Test, DC=test, DC=mycorp, DC=ru).

Далее идут аналогичные операции для оставшейся глобальной группы и для локальных групп. Так как с информационной точки зрения в них ничего нового, я их опустил.

А вот следующая операция — добавление пользователей в перенесенные группы, но уже в домене-приемнике.

2002-06-07 02:56:51-Readding members to group CN=GG01

(LDAP://MMS-SERVER/CN=GG01, OU=Test Unit, DC=mycorp, DC=ru).

2002-06-07 02:56:51-Readding members to group CN=LG01

(LDAP://MMS-SERVER/CN=LG01, OU=Test Unit, DC=mycorp, DC=ru).

И под конец сообщается об обновлении прав доступа, т. е. об изменении атрибута SID history для перенесенных групп и занесении в него SID пользователей, перенесенных из домена Test.

2002-06-07 02:56:52-Updated user rights for CN=Fy02

2002-06-07 02:56:52-Updated user rights for CN=GG01

2002-06-07 02:56:52-Updated user rights for CN=LG01

2002-06-07 02:56:53-Operation completed.

Если при переходе возникает ошибка, она также заносится в этот журнал. Наиболее вероятная причина ошибки — использование учетной записи, не имеющей административных прав в обоих доменах. Учетная запись запрашивается мастером на начальных этапах. Удобнее всего применять учетную запись администратора предприятия.

Помимо журнала регистрации, рассмотренного выше, для контроля можно использовать мастер создания отчетов. Он выводит ту же информацию наглядно.

Если после переноса групп остаются пользователи, не входящие в группы или расположенные в контейнере Users, то перенести их поможет специальный мастер переноса пользователей. Его работа аналогична работе мастера переноса групп.

В ADMT есть ряд других мастеров, в том числе мастер **откатов**, позволяющий отменить результат последнего переноса. Мастер работает так, что все параметры последней операции берет из своей базы и воспроизводит их в обратном направлении.

Проверка результата

Обновив домен, надо проверить правильность действий.

- Включив клиентскую машину в обновленный домен, надо зарегистрироваться в домене под именем любого пользователя этого домена. (Например, под именем `Test\FY02` в нашем примере.) Невозможность регистрации свидетельствует об одной из двух проблем:
 - учетные записи пользователей не были перенесены или перенос был выполнен некорректно;
 - учетные записи **компьютеров** не были повторно созданы в обновленном домене.
- Далее с помощью утилиты Gpresult (см. главу «Групповая политика») надо проверить, применены ли к этому пользователю определенные для него групповые правила. Если правила отличаются от ожидаемых:
 - » проверьте привязку ОПП к домену и ОП; если используется фильтрация, проверьте списки контроля **доступа** к ОПП;
 - проверьте содержимое каталога SYSVOL — возможно, вы забыли перенести шаблоны групповой политики.
- ◆ Теперь надо проверить доступ **пользователя** к его ресурсам. Если доступа к ним нет:
 - возможно, вы забыли отметить флажок `Update User rights` при переносе пользователей и групп — следовательно, атрибут `Sid History` не был обновлен;
 - возможно, вы забыли при переносе сохранить членство пользователя в группах;
 - возможно, вы забыли указать на необходимость сохранения списков контроля доступа при **переносе** ресурсов.
- Наконец, надо проверить работу служб и приложений, действующих от имени несистемных учетных записей и существовавших в домене до **обновления**. Если приложения не запускаются или работают некорректно:
 - возможно, учетные записи служб не были перенесены или перенос был выполнен некорректно;
 - возможно, вы забыли отметить флажок `Update User rights` при переносе учетных записей служб — следовательно, атрибут `Sid History` не был обновлен;

- возможно, вы не применили групповую политику, определяющую права данных учетных записей; как правило, это права локальной регистрации, работы от имени ОС, работы в пакетном режиме и т. п.;
- возможно, вы забыли при переносе сохранить членство служебных учетных записей в группах, в частности, в группе Administrators;
- возможно, вы забыли указать сохранение списков контроля доступа при переносе ресурсов; если приложение осуществляет доступ к файлам от имени своей учетной записи, он будет невозможен.

План аварийного восстановления

Теперь несколько слов о том, как поступать, если что-то пойдет не так. Работы лучше начать в пятницу вечером или в субботу утром. Сам перенос начинаем только после выполнения резервного копирования контроллера домена-источника.

Если перенос пользователей завершился неудачно либо внезапно сообщено о большом числе ошибок, надо запустить мастер откатов. В случае его нормальной работы перенесенные учетные записи возвратятся назад. Если этого не произошло, рекомендуется на контроллере-источнике переустановить Active Directory и сделать авторитетное восстановление из резервной копии. На контроллере-приемнике надо проверить, не осталось ли перенесенных учетных записей и при их обнаружении — удалить.

Если после обновления домена пользователи нормально входят в домен и имеют доступ к ресурсам, а приложения не работают, надо выяснить причину (см. выше). Если причину не удастся обнаружить и ликвидировать, следует авторитетно восстановить в домене данные из резервной копии и отложить перенос до выяснения причин неудачи и повторной попытки обновления домена.

Если в лесу все перестало работать

В заключение рассмотрим ситуацию, когда в лесу доменов Active Directory перестало работать все. Как этого добиться — разговор отдельный: это под силу не каждому. Но уж коли это произошло, надо как-то выходить из создавшегося положения.

Далее предполагаем, что условия таковы.

- В лесу не осталось нормально работающих контроллеров домена. Под этим будем понимать, что базы на контроллерах рассинхронизированы, репликация FRS работает не так или с перебоями, контроллеры периодически или постоянно не видят друг друга, поль-

зователи не могут регистрироваться в домене, приложения не работают или работают с ошибками.

- ◆ У вас есть копии, недавно выполненные на нормально работающей системе.
- Вы пробовали восстановить работоспособность системы всеми способами, но увы... Ни один из контроллеров не годится на должность идеального. Авторитетное восстановление базы из резервной копии не помогает. Ремонт Active Directory с помощью Ntdsutil не дал положительного результата. Вы уже проконсультировались со всеми знакомыми и прочитали массу литературы — все бесполезно. Даже специалисты Microsoft не смогли вам помочь и рекомендовали «жесткое» восстановление системы.

Остается последовать совету спецов. Итак, «жесткое» восстановление...

Общая последовательность действий

Жестким восстановление называется потому, что сопровождается массой неприятных последствий.

- Вы отбрасываете систему назад во времени. Все изменения, внесенные в Active Directory в последнее время, аннулируются. Учетные записи пользователей и компьютеров, добавленные после последнего резервного копирования, придется добавлять заново.
- Приложения, работавшие на контроллерах домена, придется переустановить. Остальные приложения, возможно, тоже придется переустанавливать, хотя это может и не потребоваться.
- ◆ Если использовалась служба DNS, интегрированная с Active Directory, то ее также придется восстанавливать. Возможно, сначала ее придется восстанавливать в иной конфигурации и лишь потом, по завершении восстановления части леса, можно будет перейти к оригинальной конфигурации DNS.

Последовательность ваших действий приведена на диаграмме.

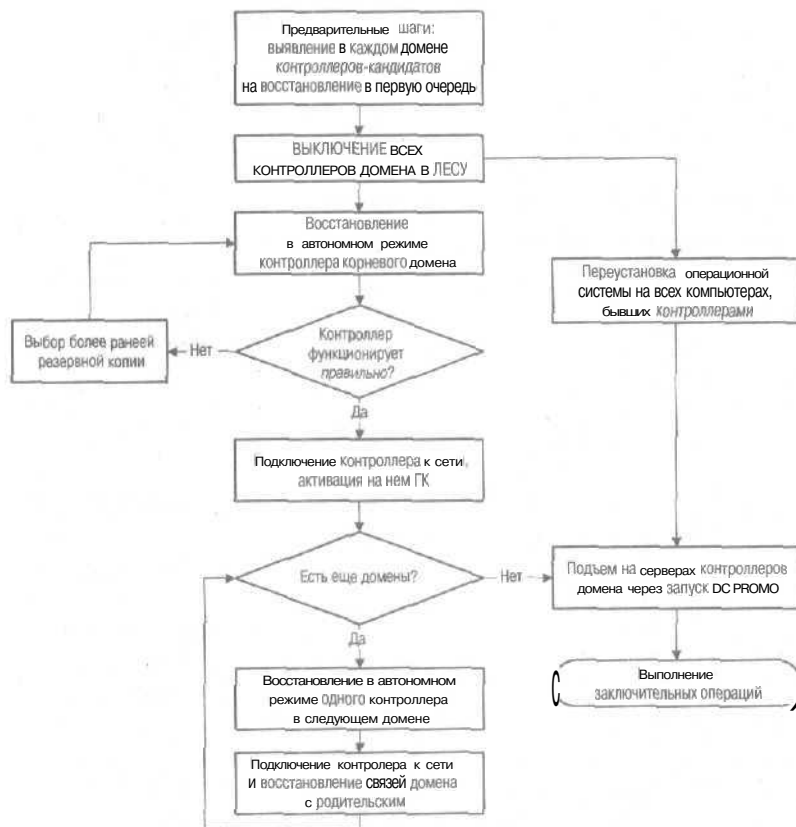
Как видите, восстановление начинается с предварительных шагов, которые помогут понять, какие серверы восстанавливать первыми, а также порядок дальнейших действий.

Помните: восстановление леса, как и установка нового, всегда выполняется с корневого домена. Именно здесь находятся группы Enterprise Admins и Schema Admins. Кроме того, только отсюда можно устанавливать отношения с дочерними доменами.

Убедившись, что корневой домен восстановлен, можно браться за остальные домены. Если вы обладаете достаточным количеством ресурсов, восстановление доменов можно выполнять параллельно, но при этом помните;

- в каждом домене восстанавливается не более одного контроллера;
- ◆ нельзя восстанавливать домены с нарушением их родительно-дочерних взаимоотношений.

Параллельно с выполнением предыдущего шага можно переустанавливать ОС на оставшихся контроллерах, устанавливать сервисные пакеты и заплатки системы безопасности, которые будут рекомендованы к установке на тот момент времени.



Алгоритм выполнения жесткого восстановления леса Active Directory

Убедившись, что все домены в лесу восстановлены и работают (т. е. выполняется репликация Active Directory и FRS, все базы синхронны, тестовые подключения пользователей показывают отсутствие проблем с регистрацией в сети) можно на оставшихся переустановленных серверах выполнить команду `DCPROMO` для повышения их статуса до контроллеров нужных доменов.

Замечание В Windows .Net Server эта операция может выполняться с использованием резервной копии базы Active Directory, сделанной на самом первом контроллере в домене.

Предварительные шаги

От того, как тщательно вы их выполните, зависит успех операции. Вот что надо сделать:

- задокументировать текущую конфигурацию леса;
- разработать процедуру восстановления текущей конфигурации в случае неудачи;
- выявить в каждом из доменов тот компьютер, с которого начинать восстановление;
- выключить VCE контроллеры домена в лесу.

Документирование текущей структуры леса

Документируя структуру леса, надо зафиксировать такую информацию.

- + Иерархия доменов. Ее нужно запомнить как с целью определения порядка восстановления, так и с целью разработки плана отката в случае неудачи.
- Имена контроллеров в каждом домене, их роли и список приложений, исполняемых на них.
- Пароль администратора каждого из доменов. При восстановлении это единственная учетная запись, которую можно будет применять.
- ◆ Структура сайтов. Это необязательное условие, но если структура перед этим была тщательно протестирована и не вызывала нареканий, то лучше восстановить именно ее. Особое внимание стоит уделить расположению серверов-форпостов, связям, их расписанию и стоимости.

Информацию занесите в таблицу вроде показанной ниже. Далее мы воспользуемся данными из нее.

Рассмотрим лес, состоящий из двух доменов: mусогр.ru и дочернего msk.mусогр.ru. В первом 4 контроллера, а во втором — 3. В обоих находятся учетные записи пользователей, работа которых в последнее время осложнилась. После бесплодных попыток восстановления доменов принято решение восстановить весь лес. Конфигурация доменов собрана в таблицу. Поскольку структура сайтов не является в этом примере определяющей, сведения о ней не сохранялись.

Пример документирования текущей конфигурации леса

Имя конт- роллера	Мастер	Наличие резервной копии	Наличие разделов для приложений	ГК	DNS
<i>Домен mycorp.ru</i>					
root1	схемы, имитатор PDC	Да	Нет	Да	Нет
root2	нет	Да	DNS, DHCP	Да	Да
root3	инфраструктуры	Нет	Нет	Нет	Нет
root4	доменных имен, RID	Да	DNS	Да	Да
<i>Домен msk.mycorp.ru</i>					
mid1	RID, инфраструктуры	Да	WINS	Нет	Нет
mid2	Нет	Да	DNS, WINS	Да	Да
mid3	имитатор PDC	Нет	Нет	Нет	Нет

Разработка процедуры отката назад

Возможно, вы спросите: *зачем возвращаться* в состояние, которое и так рассматривалось как критическое? Оно, конечно, так. Только не стоит забывать, что, несмотря на всю сложность ситуации, система продолжала работать, а пользователи, хоть и с трудом, но могли осуществлять доступ к ресурсам. Если процесс восстановления окажется неудачным или затянется, пользователи вообще не смогут работать.

Для разработки процедуры отката надо иметь представление о том, что может произойти при восстановлении. Из очевидных последствий отмечу следующие.

- Система вообще не может быть восстановлена и потребует полной реконфигурации. Это может произойти в том случае, когда вы не делали резервных копий либо все копии плохие или уничтожены.
- После восстановления состояние системы далеко от требуемого. Многих учетных записей нет, свойства объектов устарели. Это может случиться, когда последняя хорошая копия делалась довольно давно и с тех пор в систему было внесено много изменений.
- ◆ ОС может быть восстановлена, но на это уйдет больше времени, чем вы предполагали. Значит, надо вернуться на исходные позиции, разработать новый план (возможно, с привлечением дополнительных ресурсов) и выполнить обновление в другой раз.

Раз так, то в плане процедуры восстановления надо выделять критические точки. Например, если на одном из этапов предполагается отключение всех контроллеров всех доменов, то критическая точка здесь — момент выключения последнего контроллера в домене: ведь с этого момента ни один пользователь больше не имеет доступа к ресурсам. Следующая критическая точка — переустановка ОС на кон-

троллере: пока контроллер не возобновит работу, его нельзя включить в сеть для обработки запросов пользователей.

Для каждой критической точки нужно определить действия, которые вы должны выполнить, если что-то вдруг идет не так. Скажем, для первой из описанных выше критических точек действия весьма просты: вновь включить контроллеры домена. Для второй — восстановление прежней конфигурации контроллера из резервной копии.

Помимо описанных критических точек, надо учитывать критическое время. Допустим, вы планируете восстановить систему за выходные. Предварительное тестирование позволило узнать, сколько времени занимает та или иная процедура. Просуммировав время и распараллелив, где надо, процесс, вы решили, что к 12 часам дня воскресенья вы завершите всю работу. Предполагая, что что-то может пойти не так, надо определить точку, после которой все ваши действия должны быть остановлены. Например, тестирование показывает, что для восстановления исходного состояния системы требуется 8 часов, а пользователи начинают работу с 9.00 в понедельник. Это значит, что если к 1 часу ночи в воскресенье система не восстановлена, то все работы нужно прекратить и начать откат к прежнему состоянию. Никакие соображения типа «еще полчаса» принимать в расчет нельзя. Система должна быть работоспособна к началу рабочего дня.

Действия, выполняемые в случае неудачи в критических точках, определение критического времени и действий в случае его наступления и составляют план отката. В итоге алгоритм восстановления системы с учетом плана отката можно составить так (см. рис. на стр. 471).

Выявление лучшего кандидата на восстановление

Вернувшись к плану восстановления, вы увидите, что первоначально восстанавливается только по одному контроллеру в каждом домене. Они заложат основу вашей восстановленной системы.

При отборе наилучших кандидатов необходимо учитывать:

- ◆ наличие резервной копии контроллера;
- ◆ качество резервной копии;
- функции, выполнявшиеся контроллером до краха.

Вполне очевидно, что если резервная копия для какого-то контроллера не существует, то он не может быть кандидатом на восстановление. Это справедливо, даже если этот контроллер был установлен всего день назад.

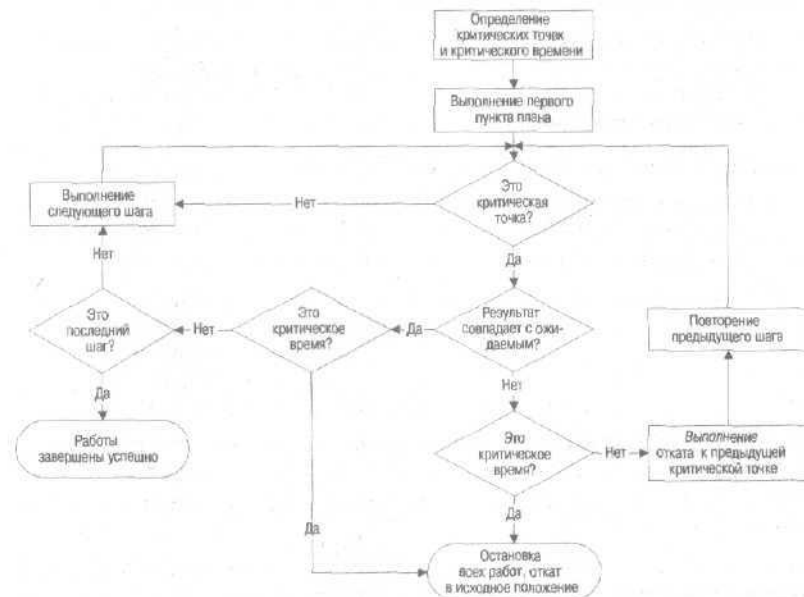
Качество резервной копии определяется сроком ее давности. Наверняка вы подозреваете, что явилось причиной тотального сбоя в лесу. А если нет, то примерно знаете время, когда появились первые при-

знаки проблемы. Следовательно, дата резервной копии должна быть не позже этого времени. Но и очень далеко назад уходить не стоит, так как чем дальше вы отбросите систему назад, тем больше корректив вам придется вносить после восстановления.

Выполняемые контроллером функции оказывают противоречивое влияние на выбор кандидата. Так, если контроллер являлся сервером ГК, его восстановление займет гораздо больше времени в многодоменной организации. Поэтому вряд ли стоит выбирать этот контроллер в качестве базового. С другой стороны, если он являлся и сервером DNS, то, восстанавливая контроллер, вы восстановите и DNS, что упростит вам дальнейшие действия.

В нашем примере контроллеры root3 и mid3 отпадают сразу, так как для них нет резервных копий. Из оставшихся в домене mусорг.ru идеальным кандидатом является контроллер root2, так как он является сервером DNS и DHCP. Он, правда, еще и сервер ГК, но так как имеются всего два домена, объем ГК невелик. В домене msk наилучшим кандидатом является контроллер mid2: ведь он еще и сервер DNS и сервер WINS.

Вместе с тем ни один из выбранных контроллеров не является мастером каких-либо операций. Вообще это не имеет значения за исклю-



Алгоритм выполнения работ

чением, пожалуй, мастера RID. Так как он будет в итоге создан заново, есть вероятность, что он выдаст пулы ID, которые уже использовались. Чтобы избежать этого, надо предпринять некоторые меры.

Выключение всех контроллеров доменов

Зачем выключать все контроллеры в лесу? Как вы помните, каждый восстановленный контроллер подключается к корпоративной сети в строго определенном порядке. Если не все контроллеры выключены, после подключения первого восстановленного контроллера может начаться репликация. В данном случае эта репликация нежелательна, так как она будет выполняться с контроллеров, содержащих испорченные данные. Поэтому все контроллеры должны быть выключены.

А если у вас большая распределенная сеть с множеством сайтов, разбросанных по огромной территории? Все их выключить одновременно затруднительно. В таком случае надо принять меры, препятствующие взаимодействию с такими сайтами. Возможно, связь с ними придется временно порвать на физическом уровне, запретив, например, маршрутизацию.

Восстановление

Итак, восстановление состоит из трех блоков работ:

- 4 восстановление корневого домена;
- ◆ восстановление остальных доменов;
- ◆ добавление переустановленных контроллеров в домены.

Восстановление корневого домена

Внимание Восстановление корневого домена выполняется на контроллере, отключенном от корпоративной сети.

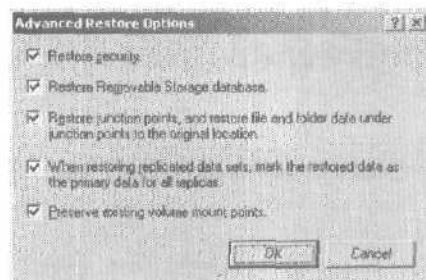
Восстановление начинается с контроллера домена, выбранного в качестве наилучшего кандидата.

Шаг 1 На этом контроллере домена выполните неавторитетное восстановление состояния системы и каталога SYSVOL (см. раздел «Неавторитетное восстановление»). Восстановление выполняется из резервной копии, признанной наилучшей.

Убедитесь, что восстановление выполняется:

- ◆ в то же самое место;
- * с восстановлением параметров безопасности;
- с восстановлением точек перехода ntfs;
- + с сохранением точек монтирования томов;

- с пометкой восстанавливаемых реплик как первичных для набора реплик.



При выполнении восстановления должны быть отмечены эти флажки

Шаг 2 Выполните проверку контроллера после перезагрузки. Вполне возможно, что загрузка займет длительное время, так как не будет обнаружен сервер DNS (см. главу «Установка Active Directory»). Это не страшно. Хуже, если структура Active Directory будет содержать ошибки, которые перед этим привели к краху всего леса. В этом случае надо воспользоваться еще более ранней резервной копией и повторить восстановление контроллера.

Внимание Это первая критическая точка.

Шаг 3 Если данный компьютер был сервером DNS, на котором содержалась зона, интегрированная с Active Directory, надо войти в оснастку DNS и посмотреть на содержимое зоны `_msdcs.<имя леса>`. В этой зоне надо удалить все записи, относящиеся к контроллерам в домене за исключением только что восстановленного. Также удалите все SRV-записи, относящиеся к остальным контроллерам. Это позволит предупредить нежелательную репликацию с партнерами, которые остались невыключенными. Клиентская часть DNS на этом контроллере должна указывать только на **этот** контроллер. Если это не так, внесите соответствующее изменение.

Если вы использовали зоны DNS, интегрированные с Active Directory, но восстанавливаемый сервер не был сервером DNS, то на нем надо установить и сконфигурировать службу DNS:

- создайте необходимые зоны с теми же именами, что и ранее;
- ◆ разрешите защищенные динамические обновления зон;
- настройте делегирование зон и переадресацию неразрешенных запросов,

Настроив службу DNS, перезапустите службу Netlogon (см. раздел «Что делать с DNS» главы < • Установка Active Directory »).

Замечание Указанные действия выполняются, только если контроллеры домена выступали серверами DNS. Если же используется специализированный сервер DNS (не обязательно Windows 2000), очистите зоны от указанных записей.

Шаг 4 Если восстановленный контроллер был сервером ГК, сбросьте соответствующий флажок в оснастке Active Directory Sites and Services. Зачем? Как я уже говорил, для восстановления каждого контроллера в разных доменах используется своя резервная копия. Не факт, что все копии делались в один день. А это значит, что при восстановлении каждого из доменов будут восстанавливаться данные, соответствующие разным периодам. Если восстановленный ГК содержит сведения о каком-то разделе более позднюю, чем та, что будет восстановлена для этого раздела на «его» контроллере, то эти данные будут неактуальны и, что хуже всего, навсегда останутся в ГК и будут тиражированы по остальным серверам ГК. Поэтому после восстановления контроллера, бывшего ГК его надо лишить этой функции.

Шаг 5 Назначьте все роли мастеров операций в лесу и в домене этому контроллеру (см. раздел «Принудительное назначение мастеров операций с помощью Ntdsutil»).

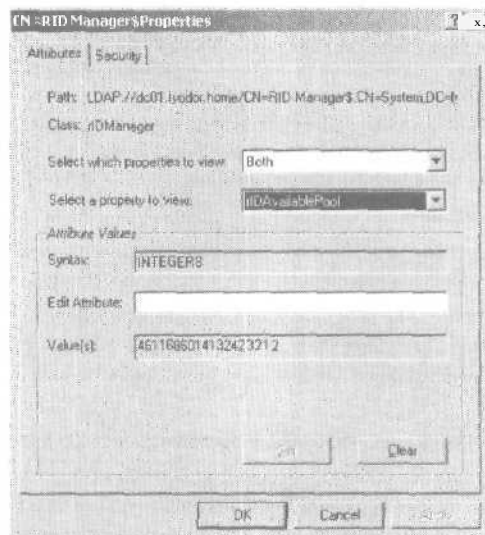
Шаг 6 Вычистите из Active Directory все метаданные, имеющие отношение к остальным контроллерам домена (см. раздел «А может, все переустановить?» главы «Установка Active Directory»). Это необходимо, чтобы КСС не попытался задействовать объекты связи с несуществующими партнерами по репликации.

Шаг 7 Откройте оснастку Active Directory Users and Computers и удалите все объекты, соответствующие остальным контроллерам в домене. То же проделайте и в оснастке Active Directory Sites and Services.

Шаг 8 Увеличьте значение текущего пула RID на 100000. Как я уже говорил, принудительное назначение контроллеру роли мастера RID чревато неприятными последствиями. Так, если после выполнения резервной копии, с которой произошло восстановление контроллера, некоторым объектам системы безопасности были предоставлены какие-то права доступа или полномочия, они сохранятся и после восстановления контроллера. Так как новый мастер RID не знает о SID объектов, существовавших до него, он может выдать точно такие же ID новым объектам. В результате в системе появятся объекты с одинаковыми SID, что, с точки зрения системы безопасности, расценивается как один и тот же объект. А значит, возникает угроза несанкционированного доступа к ресурсам.

Для предотвращения такой ситуации надо изменить пул относительных ID.

- ◆ На восстановленном контроллере запускается ADSIEdit или Ldp. Лучше использовать обе эти утилиты. Далее ищется объект `cn=RID Manager$,cn=System,<имя домена>`, а у него — атрибут `rIDAvailPool`. Тип этого атрибута — `INTEGER8`, т. е. длинное целое.



Атрибут указывающий на текущий пул RID

- ◆ Старшая часть указывает на количество объектов безопасности, которые можно задействовать в системе. Младшая — текущее значение пула номеров RID. Чтобы их вычислить, лучше всего использовать преобразователь длинных целых чисел в программе Ldp. Так, для значения, показанного на рисунке, младшая часть равна 2604. Учитывая, что каждый раз контроллеру домена выдается пул в 512 номеров ID, увеличение пула на 100000 застрахует вас от появления объектов с одинаковыми SID.

Шаг 9 Дважды сбросьте пароль учетной записи компьютера и секрет LSA, выполнив команду:

```
netdom resetpwd имя.домена
```

Внимание Сброс паролей надо обязательно выполнить дважды, чтобы исключить даже потенциальную возможность репликации с контроллерами, не прошедшими через восстановление. Так как в истории хранится не более двух паролей, такой сброс позволяет исключить из истории пароли, использовавшиеся в проблемном домене.

Шаг 10 Дважды сбросьте пароль для учетной записи krbtgt. Это делается точно так же, как и для любой учетной записи пользователя.

Шаг 11 Сделайте контроллер домена сервером ГК. Это позволит пользователям авторизоваться в домене. Однако сервер не будет себя объявлять ГК, пока не будет выполнена синхронизация с другими разделами Active Directory. Это возможно только после установки по одному контроллеру в других доменах.

Теперь можно подключить контроллер домена к корпоративной сети.

Внимание Это вторая контрольная точка. Пользователи корневого домена (если они есть) могут регистрироваться в домене, однако этого не следует пока допускать, разве только в тестовых целях.

Восстановление остальных доменов

Восстановление остальных доменов похоже на процедуру восстановления корневого, но есть и некоторые отличия, их мы и обсудим.

Восстановление дочерних доменов можно выполнять одновременно — главное, не нарушать порядок наследования: для одного родителя одновременно могут восстанавливаться только его непосредственные дочерние домены.

В каждом восстанавливаемом домене поступаем следующим образом.

Шаг 1 Кандидат на восстановление отключен от корпоративной сети. Он загружается в режиме восстановления Active Directory, и выполняется неавторитетное восстановление каталога из резервной копии. Каталог SYSVOL помечается как первичный для остальных реплик.

Шаг 2 Проверьте контроллер после перезагрузки. Если структура Active Directory содержит ошибки, воспользуйтесь более ранней резервной копией и повторите восстановление.

Внимание Это третья критическая точка.

Шаг 3 Если компьютер был сервером DNS, на котором содержалась зона, интегрированная с Active Directory, войдите в оснастку DNS и удалите SRV-записи, относящиеся к восстанавливаемому домену, кроме тех, что относятся к службам текущего контроллера. Клиентская часть DNS на контроллере должна указывать на сервер DNS в корневом домене и на этот контроллер. Если это не так, внесите соответствующее изменение. Проверьте, есть ли в зоне корневого домена делегирование зоны, соответствующей восстанавливаемому домену.

Если вы использовали зоны DNS интегрированные с Active Directory, но восстанавливаемый сервер не был сервером DNS, то на нем надо установить и сконфигурировать службу DNS,

Замечание Указанные действия нужны, только если контроллеры домена были серверами DNS. Если же используется специализированный сервер DNS (не обязательно Windows 2000), то выполните очистку зон от указанных записей.

Шаг 4 Если восстановленный контроллер был сервером ГК, сбросьте соответствующий флажок в оснастке Active Directory Sites and Services.

Шаг 5 Назначьте все роли мастеров операций в домене этому контроллеру.

Шаг 6 Удалите из Active Directory метаданные, относящиеся к прочим контроллерам домена.

Шаг 7 Удалите все объекты, соответствующие остальным контроллерам в домене.

Шаг 8 Увеличьте значение текущего пула RID на 100000.

Шаг 9 Дважды сбросьте пароль учетной записи компьютера и секрет LSA.

Шаг 10 Дважды сбросьте пароль для учетной записи krbtgt. Это делается так же, как и для любой учетной записи пользователя.

Шаг 11 Подключите восстановленный контроллер к корпоративной сети. Иницилируйте его репликацию с контроллером в родительском домене. Репликация должна выполняться в обоих направлениях для каждого контекста имен. Для ее инициации служит команда:

```
repadmin /sync <контекст имен> <DNS.имя.контроллера.назначения>  
<номер GUID контроллера-источника> /force.
```

Следовательно, ее нужно дать трижды на дочернем контроллере и дважды — на родительском. Такая асимметричность связана с тем, что контроллер в родительском домене является ГК, а в дочернем — нет.

Например, в рассмотренном ранее случае восстановления доменов mycorp.ru и msk.mycorp.ru на контроллере mid2 выполняются команды:

```
repadmin /sync cn=configuration,dc=mycorp,dc=ru root2.msk.mycorp.ru  
19c9dbc3-d5d2-47cc-94e3-5135adfc4bcb /force  
Sync from 19c9dbc3-d5d2-47cc-94e3-5135adfc4bcb to root2.msk.mycorp.ru  
completed successfully.  
repadmin /sync cn=schema,cn=configuration,dc=mycorp,  
dc=ru root2.msk.mycorp.ru 19c9dbc3-d5d2-47cc-94e3-5135adfc4bcb /force  
Sync from 19c9dbc3-d5d2-47cc-94e3-5135adfc4bcb to root2.msk.mycorp.ru  
completed successfully.  
repadmin /sync dc=msk,dc=mycorp,dc=ru root2.msk.mycorp.ru  
19c9dbc3-d5d2-47cc-94e3-5135adfc4bcb /force  
Sync from 19c9dbc3-d5d2-47cc-94e3-5135adfc4bcb to root2.msk.mycorp.ru  
completed successfully.
```

На контроллере root2 выполняются команды:

```
repadmin /sync cn=configuration,dc=mycorp,dc=ru mid2.msk.mycorp.ru
a4818f4f-bd9a-4dd9-b8f9-f4e26a84eb7a /force
Sync from a4818f4f-bd9a-4dd9-b8f9-f4e26a84eb7a to mid2.msk.mycorp.ru
completed successfully.
repadmin /sync cn=schema,cn=configuration,dc=mycorp,
dc=ru mid2.msk.mycorp.ru a4618f4f-bd9a-4dd9-b8f9-f4e26a64eb7a /force
Sync from a4818f4f-bd9a-4dd9-b8f9-f4e26a84eb7a to mid2.msk.mycorp.ru
completed successfully.
```

Выполнять команды надо по очереди: сначала выполняется репликация контекста на контроллере в корневом домене, потом — репликация того же контекста на контроллере в дочернем домене.

После успешного восстановления по одному контроллеру домена в каждом из доменов можно переходить к установке дополнительных контроллеров в домены.

Восстановленный контроллер домена можно сделать сервером ГК.

Внимание Это четвертая критическая точка. В зависимости от конкретной конфигурации сети на этом этапе можно говорить об удачном восстановлении леса Active Directory.

Шаг 12 Проверьте содержимое Active Directory. Если вы обнаружите, что некоторых принципиально важных объектов или учетных записей нет, их можно добавить. Это просто сделать, если вы документировали все ваши действия в домене до его краха,

Добавление дополнительных контроллеров

Установку дополнительных контроллеров домена можно продолжить в рабочее время, когда пользователи выйдут на работу. И все же ее лучше выполнить до этого момента, по крайней мере установить по одному дополнительному контроллеру.

К установке контроллеров специальных требований не предъявляется — вы используете программу DCPROMO (см. главу «Установка Active Directory»).

Замечание Если вы хотите задействовать в качестве источника данных для вновь устанавливаемых контроллеров только тот, что был восстановлен первым, выберите автоматический режим установки и укажите в качестве параметра ReplicationSourceDC нужное имя (см. раздел «Автоматическая установка контроллера» главы «Установка Active Directory»).

Если контроллеры домена располагаются в других сайтах, то при подключении их к основному сайту создайте соединения, восстано-

вите расписание репликации и стоимость, предоставьте возможность КСС создать объекты связи.

Заключительные шаги

Последними шагами в восстановлении леса Active Directory должны стать следующие.

- Переустановите приложения, выполнявшиеся ранее на контроллерах. В то время как на тех контроллерах, что были установлены заново с применением DCPROMO все приложения должны быть установлены с нуля, на восстановленных контроллерах они сохранились. Если информация этих приложений хранилась в реестре, она там сохранилась и была восстановлена во время неавторитетного восстановления из резервной копии. Об этом следует помнить при запуске приложений.
- ◆ Выполните резервное копирование всех контроллеров доменов. С этого момента именно эти копии станут для вас «хорошими» копиями, которые будут использоваться для восстановления системы.
- ◆ Модифицируйте конфигурацию DNS, чтобы обеспечить оптимальную для сети схему разрешения имен.
- Перераспределите роли мастеров операций между контроллерами доменов.
- Проверьте доступ пользователей в сеть. Если какие-то пользователи не могут войти, повторно включите их рабочие станции в домен.
- ◆ Проверьте функционирование групповых политик. Если групповые политики восстановились в «раннем» состоянии, переопределите их и проверьте их привязку к доменам, сайтам и подразделениям.
- Проверьте возможности доступа пользователей к файловым и принтерным ресурсам. Если ресурсы располагались на выделенных серверах, то невозможность доступа к ним или неправильный вид доступа связан с тем, что не восстановились группы или учетные записи, появившиеся в Active Directory после создания резервной копии, использованной для восстановления. Если ресурсы располагались на контроллерах домена, установленных с нуля, восстановите файловые ресурсы из резервной копии и предоставьте в совместное использование; установив соответствующие драйверы, предоставить в совместное использование и принтеры.

На этом восстановление можно считать завершенным. И начинается ежедневное сопровождение системы. Если вы не хотите повторения описанной процедуры, рекомендую на сайте Microsoft найти все, что относится к Microsoft Operations Framework (MOF). Поверьте, это весьма полезные указания по ежедневному управлению Active Directory,

Заключение

Как бы мне хотелось, чтобы, дойдя до этого места, вы сказали, что теперь готовы самостоятельно бороться с любой проблемой в Active Directory!

Возможно, что кто-то так и решит, что вот она, волшебная книга, которая открывает путь к выходу из любой трудной ситуации. Увы, это не так. Здесь я описал только общий подход к решению проблем, а также затронул некоторые конкретные случаи. Увы, в реальности случается такое, что не приснится и в страшном сне. Порой решение одной проблемы порождает другую, третью и т. д. Да, описанный подход, позволит в конечном итоге найти решение, но путь может быть долог и тернист. Чтобы его сократить, настоятельно рекомендую использовать базу знаний Microsoft. Она доступна либо по подписке на диски Technet, выходящих ежемесячно, либо на сервере <http://technet.microsoft.com>. Только тут вы отыщете решение своей проблемы среди нескольких сотен тысяч статей.

Словарь терминов

А

Автономная папка - offline folder

Папка на сервере, все документы в которой *кэшируются* на клиентской стороне. При *отсутствии* связи между клиентом и сервером работа с документами остается возможной в автономном режиме. При восстановлении связи выполняется синхронизация документов.

Авторизация - authorization

Процесс проверки полномочий доступа к ресурсу системы.

Авторитетное восстановление - authoritative restore

В *Active Directory* такое восстановление данных из резервной *копии*, при котором они имеют *преимущество* перед *данными*, хранимыми в Active Directory.

Агент восстановления - recovery agent

Лицо, уполномоченное выполнять *восстановление зашифрованных файлов*. Должно обладать соответствующим сертификатом. По умолчанию это *администратор* системы. Рекомендуется переопределять с помощью *групповой политики*.

Администратор-administrator

Лицо, ответственное за управление учетными записями пользователей локального компьютера или домена, конфигурирование системных служб, управление политикой безопасности и групповой политикой. Входит в группу *Administrators* и обладает всеми полномочиями в рамках домена или локального компьютера.

Администратор предприятия - enterprise administrator

Лицо, ответственное за исполнение административных задач в пределах *леса доменов*. Входит в группу Enterprise Admins, расположенную в *корневом домене леса*.

Администратор схемы - schema administrator

Лицо, ответственное за модификацию *схемы Active Directory*. Входит в группу Schema Admins, расположенную в *корневом домене леса*.

Атомарная транзакция - atomic transaction

В *Active Directory* транзакция, выполняемая как единое целое. Если один из компонентов транзакции не выполнен, происходит **откат** всей транзакции, т. е. возврат к *состоянию*, предшествовавшему началу транзакции.

Атрибут объекта - object attribute

Характеристика **объекта** в *Active Directory*. Иногда называется свойством **объекта**. Атрибуты имеют одно или несколько значений и бывают нескольких типов.

Атрибут файла - file attribute

Флаг, устанавливающий определенное свойство файла. В Windows 2000 существуют следующие атрибуты файлов: R (файл доступен только для чтения), H (скрытый файл), S (системный файл), A (архивный файл), C (сжатый файл), E (**зашифрованный** файл). Атрибуты применимы и к каталогам файлов.

Аудит - audit

Отслеживание работы отдельных компонентов системы и регистрация результатов в *журнале событий*.

Аудит доступа к: службе каталогов - Active directory service access audit

Регистрация удачных и неудачных попыток доступа к службе каталогов *Active Directory*.

Аудит каталогов - folder audit

Отслеживание *использования* одного или нескольких *каталогов файловой системы*. Отслеживаются попытки удачного и неудачного доступа.

Аудит печати - print audit

Функция, позволяющая отслеживать доступ к указанным *принтерам*.

Аудит приложений - application audit

Регистрация событий, связанных с процессами ввода, обработки и **вывода** внутри приложений.

Аудит реестра - registry audit

Отслеживание *событий*, связанных с попытками открыть *ветвь реестра* или извлечь из нее данные.

Аудит событий регистрации **учетных записей** - **account logon events** audit
Регистрация удачных и неудачных попыток регистрации *учетной записи* в системе.

Аутентификация - authentication

Проверка регистрационной информации о пользователе. Если пользователь регистрируется к *Windows 2000 Professional* или на отдельно стоящем сервере, аутентификация выполняется на этом компьютере. Если пользователь регистрируется в *домене*, аутентификация выполняется на *контроллере домена* с применением данных, хранящихся в каталоге *Active Directory*.

Аутентификация Kerberos - Kerberos authentication

Аутентификация по протоколу *Kerberos*. В основе метода лежит использование *инфраструктуры открытых ключей*. Для проверки доступа применяются *билеты*. Аутентификация выполняется в несколько этапов. 1. *Начальная аутентификация*. 2. Получение *сеансового билета*. 3. *Имперсонация*. В трехъязысных системах клиент — сервер дополнительно выполняется *делегирование аутентификации*.

Аутентификация NTLM - NTLM authentication

Механизм аутентификации в Windows NT. Имеются две версии этого механизма. Вторая обеспечивает повышенный уровень криптозащиты. Обе версии поддерживаются в Windows 2000 для обеспечения совместимости с Windows NT.

Б

База данных SAM - SAM database

База данных информации безопасности, содержащая имена учетных записей пользователей и пароли, а также параметры политики безопасности в Windows NT. В Windows 2000 используется либо на отдельно стоящих *серверах*, либо на контроллерах домена для защиты доступа в режиме восстановления *Active Directory*.

Безопасный режим - safe mode

Режим загрузки Windows 2000, при котором загружается только минимально необходимое число проверенных драйверов устройств. Применяется для восстановления системы после установки некорректно работающего драйвера устройств.

Билет - ticket

Объект Kerberos, содержащий данные об участнике системы безопасности и служащий для его аутентификации. В Windows 2000 два вида билетов: TGT (билет на право получения билетов) и билет для доступа к службе.

Блокирование политики - policy blocking

Определяя групповую политику для подразделения, можно установить запрет на применение всех правил, наследуемых от вышестоящих

контейнеров. Запрет не распространяется на те правила, для которых установлен запрет блокировки.

Блокировка учетной записи - account lockout

Функция, позволяющая блокировать определенную *учетную запись* на заданный срок при превышении указанного количества неудачных попыток регистрации в системе.

В

Ветвь - branch

Часть дерева службы каталогов, исходящая из *узла* дерева и содержащая все дочерние объекты узлового контейнера.

Взаимная аутентификация - mutual authentication

Процесс *аутентификации*, характерный для *аутентификации Kerberos*. При этом не только сервер проверяет подлинность клиента, но и клиент проверяет подлинность сервера.

Видимость объекта - object visibility

Свойство объекта в каталоге *Active Directory* быть видимым для пользователей. Объекты, размещенные в контейнерах, к которым пользователи не имеют доступа, считаются невидимыми.

Владелец - owner

Владелец объекта имеет над ним полный контроль и может изменять права доступа к нему. По умолчанию владельцем объекта является создавший его пользователь. Владелец *ресурса* является лицом, использующим ресурс в данный момент.

Время жизни билета - ticket lifetime

Время, в течение которого *сеансовый билет* считается действительным и может применяться для доступа к серверу. **Время жизни билета** определяется доменной политикой и обычно равно 8 часам. По истечении времени жизни билета *поставщик функций безопасности Kerberos* возвращает соответствующую ошибку, что позволяет клиенту и серверу обновить билет.

Встроенные группы - built-in groups

Группы, входящие в Windows 2000 по умолчанию. Встроенные группы обладают набором *привилегий* и *прав*.

Вторичная зона DNS - DNS secondary zone

Зона DNS, являющаяся копией *первичной зоны*. Не позволяет вносить изменения в записи.

Г

Глобальная группа - global group

Глобальные группы могут включать в себя *учетные записи* из своего домена и могут быть включены в *локальные группы* других доменов. Используются для *предоставления* прав доступа и *делегирования ад-*

министративных полномочий. Информация о членстве в глобальных группах не тиражируется в глобальный каталог.

Глобальный каталог - Global Catalog

Хранит реплики всех объектов Active Directory, но с сокращенным числом атрибутов. К хранимым относятся атрибуты, используемые наиболее часто при выполнении операций поиска (например, имя пользователя, имя входа в систему и т. д.) и достаточные для обнаружения полной реплики объекта. ГК позволяет быстро находить объекты, не требуя указания того, в каком домене хранится объект, а также использования смежного расширенного пространства имен на предприятии.

Глобальный уникальный идентификатор - Globally Unique ID (GUID)

Уникальное 128-разрядное число, характеризующее любой объект в Active Directory.

Горизонтальное доверие - horizontal trust

Доверительные отношения, установленные между двумя доменами в разных деревьях в одном лесу. Используются для сокращения пути доверия.

Гостевая учетная запись - guest account

Учетная запись, применяемая для регистрации в домене при отсутствии в нем или в доверяемых доменах личной учетной записи. По умолчанию использовать учетную запись запрещено.

Группа - group

Объект службы каталогов Active Directory, включающий в себя учетные записи, называемые членами группы. Права и привилегии группы предоставляются и ее членам, что удобно для определения общих свойств ряда учетных записей пользователей. Группы могут находиться как в домене, так и в организационных подразделениях домена. Группы делятся на почтовые и группы безопасности.

Групповая политика - group policy

Набор правил, определяющих параметры системы: безопасность, работу приложений и служб, установку ПО и т. п. Групповая политика применяется к объектам Active Directory в следующем порядке: сайм, домен, подразделение. Объект, стоящий последним, имеет приоритет групповой политики.

Группы безопасности - security groups

Группы, используемые для разграничения доступа к ресурсам и делегирования административных полномочий. Бывают локальными, глобальными и универсальными. В противоположность им существуют почтовые группы.

Д**Двунаправленные доверительные отношения - two-way trust relationships**

Вид доверительных отношений между доменами, при котором каждый из двух доменов доверяет друг другу.

Делегирование зон - zone delegation

Механизм передачи управления *зоной DNS* с одного сервера на другой. Сервер, отвечающий за зону, называется авторитетным для нее. Делегирование используется для эффективного разрешения имен.

Делегирование полномочий - delegation

Возможность предоставления отдельных административных полномочий пользователям или *группам в домене*. Применяется для распределения административных обязанностей и позволяет избавиться от всемогущих *администраторов*. Полезно наделить администраторов филиалов частичными полномочиями, не противоречащими полномочиям центральной службы информационных технологий.

Демилитаризованная зона - DMZ

Часть корпоративной сети, отделенная от корпоративной сети и от Интернета межсетевыми *экранами* так, что доступ в нее *возможен*, а сквозной проход — нет. Позволяет предоставлять доступ к ресурсам как из корпоративной сети, так и из Интернета. Предназначена для размещения общедоступных ресурсов.

Дерево - tree

Иерархическая структура, состоящая из *объектов*. Объекты на концах дерева называются *листьями*. В листьях не содержится других объектов. Узловые точки дерева (места, из которых *выходят* ветви) являются контейнерами. Внешний вид дерева показывает *взаимосвязи* между объектами.

Дерево доменов - domain tree

Дерево доменов состоит из нескольких *доменов*, использующих *одну* и ту же *схему* и *конфигурацию* и образующих единое пространство имен. Домены в дереве связаны между собой *доверительными отношениями*. Служба каталогов *Active Directory* состоит из одного или нескольких доменных деревьев.

Дескриптор безопасности - security descriptor

Атрибуты безопасности для объекта: идентификатор владельца (*SID*), идентификатор *группы*, *список контроля доступа* (*ACL*) и системный список контроля доступа.

Динамически подключаемая библиотека - dynamically loaded library (DLL)

Процедура *API*, доступ к которой из приложений осуществляется путем вызова обычных *процедур*. Код этой процедуры не входит в ис-

полняемый образ приложения. ОС автоматически изменяет исполняемый образ в процессе работы так, чтобы он указывал на DLL

Дистрибутивный диск - distribution disk

Диск, на котором записаны файлы и каталоги, необходимые для установки Windows 2000. При создании собственных дистрибутивных дисков рекомендуется использовать программу Setup Manager.

Доверительные отношения - trusted relationships

Разновидность связи между *доменами*, предусматривающая выполнение *аутентификации*, когда *пользователь* имеет *учетную запись* только в одном домене, но может обращаться ко всей *сети*. *Доверяющий домен* предоставляет право аутентификации *доверяемому домену*. Доверительные отношения бывают *транзитивными* и *нетранзитивными*.

Доверяющий домен - trustee domain

Домен, предоставляющий доступ к своим *ресурсам* пользователям других, *доверяемых доменов*.

Доверяемый домен - trusted domain

Домен, пользователи которого могут осуществлять доступ к ресурсам других, *доверяющих доменов*.

Домашний каталог - home directory

Каталог на диске, доступный пользователю и содержащий файлы и программы этого пользователя. Домашний каталог можно назначить *либо* отдельному пользователю, *либо* нескольким сразу.

Домен - domain

Организационная единица безопасности в сети. Active Directory состоит из одного или нескольких доменов. Домен может охватывать несколько физических *сайтов*. В каждом домене своя политика безопасности и отношения с другими доменами. Домены, объединенные общей схемой, конфигурацией и *глобальным каталогом*, образуют *дерево доменов*. Несколько доменных *деревьев* можно объединить в *лес*.

Дочерний домен - child domain

Домен, стоящий в иерархии *дерева доменов* ниже, чем родительский. Дочерний домен связан с родительским двусторонними *транзитивными доверительными отношениями*.

Драйвер устройства - device driver

Программа, позволяющая определенному устройству взаимодействовать с Windows 2000. Хотя устройство физически может быть установлено в компьютер, Windows 2000 не использует его, пока не будет установлен необходимый драйвер.

Е**Естественный режим работы домена - native mode**

Режим работы домена Windows 2000, в котором в домене не могут существовать *машины*, не поддерживающие работу с Active Directory. В этом режиме в домене могут существовать *универсальные группы*. Альтернативой является *смешанный режим работы*.

Ж**Журнал событий - event log**

Файл, содержащий *информацию* о событиях *аудита*, таких как попытки регистрации, попытки использования *ресурсов* и т. п.

Журнал безопасности - security log

Файл, содержащий ошибки, предупреждения и *информацию*, порожденные системой безопасности при включенном *аудите* безопасности Windows 2000

Журнал изменений NTFS - change journal

Функция *NTFS*, позволяющая *отслеживать* все изменения файлов в *томе*. Используется механизмом *репликации FRS* для определения *измененных* файлов.

Журнал приложений - application log

Файл, содержащий ошибки, предупреждения и *информацию*, порожденные прикладными программами, исполняемыми в Windows 2000.

Журнал системы - system log

Файл, содержащий ошибки, *предупреждения* и *информацию*, порожденные системой Windows 2000.

Журнал Active Directory - Active Directory log

Файл, содержащий *записи*, *связанные* с регистрацией работы службы каталогов.

З**Загрузочный раздел - boot partition**

Раздел диска, отформатированный в *NTFS*, *FAT* или *FAT32* и содержащий файлы ОС Windows 2000 и файлы поддержки. Загрузочный раздел может совпадать с *системным разделом*.

Запись DNS - DNS record

Ресурсная запись в базе сервера DNS.

Запись DNS типа A - A record

Запись в базе сервера *DNS*, ставящая в соответствие имя хоста и его адрес IP.

Запись DNS типа CNAME - CNAME record

Запись в базе *DNS*, используемая для идентификации хоста по разным именам. В *Active Directory* служит для обнаружения и регистрации партнеров по репликации.

Запись DNS типа SRV - SRV record

Ресурсная *запись DNS*, используемая для регистрации и обнаружения информации о хорошо известных службах. В Windows 2000 служит для поиска информации о контроллерах *доменов*.

Запрет наследования - inheritance blocking

Механизм, позволяющий дочерним объектам не наследовать все или часть *свойств* родительского объекта.

Зона - zone

Часть пространства имен DNS, *администрируемая* как самостоятельная сущность. Зона имеет имя и содержит ресурсные записи DNS. Имя домена Active Directory совпадает с одной из зон DNS.

Зона интегрированная с Active Directory - Active Directory integrated zone

В отличие от стандартной зоны DNS, хранящей информацию в текстовом файле, зона интегрированная с *Active Directory* хранит информацию в базе AD. Использует механизмы тиражирования Active Directory для передачи информации между серверами DNS. Позволяет вносить динамические изменения в защищенном режиме.

И**Идентификатор безопасности - security identifier (SID)**

Уникальный *номер*, идентифицирующий пользователя или группу в домене Windows NT/2000.

Имя~name

Имена служат для идентификации объектов в *Active Directory*. Существует несколько видов имен: полное имя, отображаемое имя, общее имя, отличительное имя и прочие.

Имя компьютера - computer name

Имя компьютера однозначно определяет конкретный компьютер в сети. Не может быть двух компьютеров с одинаковыми именами. Компьютеры с Windows 2000 имеют два типа имен: NetBIOS и полное. NetBIOS-имя служит для совместимости с существующими системами. Полное имя *является* полностью квалифицированным и состоит из имени компьютера и имени домена. NetBIOS-имя компьютера не может совпадать с именем любого пользователя в домене.

Имя учетной записи пользователя - user account name

В домене однозначно характеризует *пользователя* при регистрации. Иногда его называют именем регистрации. В зависимости от типа системы, в которой выполняется регистрация, применяется один из двух видов имен: имя_домена\имя_пользователя или имя_пользователя@полное.имя.домена.

Имитатор PDC - PDC simulator

Мастеропераций, выполняющий роль главного контроллера домена. В *смешанном режиме* работы домена играет роль PDC для всех ре-

зервных контроллеров домена Windows NT. В *естественном режиме* работы хранит сведения обо всех изменениях в домене до завершения *тиражирования*.

Интерактивная регистрация - interactive logon

Пользователь должен ввести учетную информацию с клавиатуры того компьютера, на котором регистрируется. Исключение составляет регистрация в терминальном *режиме*, которая также является интерактивной для *терминал-сервера*. Противоположна *удаленной регистрации*.

Интерфейс NetBIOS - NetBIOS interface

Интерфейс программирования, позволяющий посылать и принимать запросы ввода/вывода удаленного компьютера. Скрывает *техническую* часть сети от программ.

Интернет - Internet

Глобальная сеть компьютеров, *взаимодействующих* посредством набора общих протоколов, таких как HTTP и TCP/IP.

Интрасеть - intranet

Термин относится к любой *сети TCP/IP*, не связанной с *Интернетом*, но использующей коммуникационные стандарты и средства Интернета для предоставления данных пользователям частной сети.

Инфраструктура открытых ключей - public key infrastructure

Термин, используемый для описания законов, *стандартов*, правил и ПО для регуляции или управления *открытыми* и *личными ключами*. На практике представляет собой набор *сертификатов* и *центров сертификации*, удостоверяющих подлинность участников защищенного обмена информацией.

К**Каталог - catalog**

Хранилище чего-либо нужного или интересного. Отличительной особенностью каталогов является возможность систематизации хранимой в них информации, быстрого поиска данных, возможности добавления и расширения его *возможностей*. Служба каталогов хранит сведения об объектах системы и позволяет манипулировать ими.

Квотирование дискового пространства - disk quoting

Ограничение дискового пространства, выделенного пользователю. Квотирование выполняется относительно каждого пользователя и каждого дискового тома

Клиент - client

Компьютер, осуществляющий доступ к ресурсам другого компьютера (называемого *сервером*), предоставленным в совместное использование.

Клиентский сертификат - client certificate

Термин относится к использованию сертификатов для аутентификации клиентов. Так, Web-браузер можно рассматривать в качестве клиента сервера Web. Пытаясь осуществить *защищенный* доступ к серверу Web, Web-браузер должен послать клиентский сертификат для подтверждения подлинности клиента.

Ключ - key

В *инфраструктуре открытых ключей* это некоторая *величина*, используемая для шифрования и дешифрации. Ключи бывают *открытыми* или *личными*.

Ключ восстановления - recovery key

Ключ, который наряду с *личным ключом пользователя*, применяется для шифрования ключа, которым зашифрован файл. Этот ключ принадлежит *агенту восстановления* и применяется в экстремальных ситуациях.

Командный файл - batch file

Неформатированный текстовый файл, содержащий одну или *несколько* команд Windows 2000. Командный файл имеет расширение .CMD или .BAT. Его команды выполняются последовательно.

Консоль восстановления - recovery console

Режим загрузки Windows 2000, в котором доступна лишь текстовая консоль с ограниченными правами доступа к ресурсам ОС. *Позволяет* восстановить ОС в случае невозможности ее нормальной загрузки.

Консоль управления MMC - Microsoft Management Console

Программа, являющаяся *контейнером* для загрузки *оснасток*. Позволяет путем комбинации оснасток создавать специализированные *инструменты*, решающие определенные административные задачи в системе. Может использоваться для управления как локальным, так и удаленным компьютером.

Контейнер - container

Объект, который может содержать в *себе* другие объекты. Например, папка — контейнер для документов, а шкаф — *контейнер* для палок. Контейнер каталога является *контейнером* объектов каталога.

Контейнер групповой политики - group policy container

Контейнер Active Directory, в котором хранятся объекты групповой политики.

Контроллер домена - domain controller

В Windows 2000 — *сервер*, на котором находится служба каталогов Active Directory. В предыдущих версиях Windows NT — сервер, на котором хранится база учетных записей SAM и который выполняет авторизацию доступа.

Конфигурация - configuration

Специальный контейнер *Active Directory*, в котором хранится конфигурация леса доменов,

Корень DFS - DFS root

Начальная точка доступа к пространству имен DFS. Для доменной DFS может быть отказоустойчивым, т. е. состоять из нескольких реплик

Корневое доверие - root trust

Вид поперечного доверия, используемый для связи всех *корневых доменов в лесу*; является *двунаправленным* и *транзитивным*.

Корневой домен - root domain

Самый первый *домен* в иерархии. Различают корневой домен дерева, являющийся первым доменом в дереве, и корневой домен леса — самый первый домен в лесу. В корневом домене леса находятся такие группы, как Enterprise Admins и Schema Admins.

Кэширование диска - disk caching

Метод повышения производительности файловой системы. Вместо того чтобы постоянно обращаться к диску для выполнения операций чтения и записи, файлы хранятся в кэше в памяти. Все операции чтения/записи выполняются со скоростью обращения к памяти, что гораздо быстрее, чем обращение к диску.

Л**Лес - forest**

Набор несмежных деревьев, которые не образуют единое пространство имен. В то же время деревья используют одну и ту же *схему, конфигурацию* и *Глобальный каталог*. Деревья в лесу связаны между собой *доверительными отношениями* Kerberos. Для обращения к лесу используется имя самого первого домена,

Личный ключ - private key

Служит для шифрования и дешифрации данных, хранится в секрете и известен только одному человеку. Для хранения личного *ключа* используются *сертификаты* или *смарт-карты*.

Логический диск - logical drive

Подраздел расширенного раздела жесткого диска.

Локальная группа - local group

Может содержать учетные записи своего домена, а также учетные записи и *глобальные группы* из других доменов. Служит для предоставления доступа к ресурсам своего домена. Информация о членстве в локальных группах не тиражируется в *Глобальный каталог*.

М**Максимальный срок жизни пароля - maximum password lifetime**

Период, в течение которого можно использовать *пароль*, прежде чем система потребует его изменить.

Мастер домен - master domain

Домен, хранящий учетные записи всех пользователей в доменной структуре Windows NT.

Мастер операций - operations master

Контроллер домена, исполняющий одну из функций, выполняемую только одним контроллером. В *домене* три мастера операций, а в *лесу* — два. Функция мастера операций может быть передана любому контроллеру.

Мастер доменных имен - domain naming master

Мастер операций, ответственный за добавление новых доменов в *лес* или их удаление. Обеспечивает уникальность имен.

Мастер инфраструктуры - infrastructure master

Мастер операций, ответственный за уникальность объектов и за поддержание связей между ними. В каждом домене один мастер инфраструктуры.

Мастер схемы - schema master

Мастер операций, ответственный за внесение изменений в *схему Active Directory*. Эту роль выполняет единственный контроллер в *лесу*.

Мастер RID - RID master

Мастер операций, в рамках домена выделяющий *пулы RID* другим контроллерам.

Минимальный срок жизни пароля - minimum password lifetime

Период, в течение которого будет использоваться установленный *пароль*, прежде чем его можно будет изменить.

Н**Наследование - inheritance**

Механизм, позволяющий дочерним объектам наследовать все свойства родительского объекта.

Набор реплик - replica set

Совокупность *компьютеров*, между которыми выполняется *репликация* раздела *Active Directory* или содержимого каталога файлов.

Назначение приложений - application assignment

Процесс, используемый Windows Installer для принудительной установки приложений пользователям или группам *пользователей*.

Неавторитетное восстановление - non-authoritative restore

В Active Directory процесс восстановления данных из резервной копии, при котором данные, хранящиеся в Active Directory и измененные после выполнения резервной копии, замещают восстановленные данные в процессе репликации.

Неактивная учетная запись пользователя ~ disabled account

Учетная запись *пользователя*, которому запрещено регистрироваться; появляется в списке учетных записей и может быть активизирована в любое время.

Нетранзитивные доверительные отношения - non-transitive trust relationships

Доверительные отношения, при которых доверие устанавливается только между двумя доменами. Если один из них доверяет третьему, то второй не будет доверять третьему домену. Нетранзитивные доверительные отношения устанавливаются либо с доменами Windows NT, либо между доменами в разных лесах.

О**Объект - object**

Отдельный набор атрибутов, соответствующих чему-либо конкретно, например, пользователю, компьютеру или приложению. В атрибутах содержатся данные о субъекте, представленном данным объектом. Так, атрибуты пользователя могут включать его имя, фамилию, домашний адрес, адрес электронной почты, семейное положение и т. п.

Объект связи - connection object

Объект, создаваемый между двумя контроллерами доменов для репликации от одного к другому. Всегда направлен только в одну сторону. Направление объекта соответствует направлению репликации.

Общее имя - common name

Обязательный атрибут любого объекта Active Directory. Служит для идентификации объекта.

Организационное подразделение - organizational unit

Контейнерный объект внутри домена. Может содержать в себе другие объекты, объединенные в древовидную структуру. Внутри могут быть как контейнеры, так и листья. Используется для отслеживания организационной структуры предприятия.

Оснастка - snap-in

Программный компонент, являющийся минимальной единицей расширения консоли ММС. Одна оснастка соответствует единице возможностей управления. Технически оснастки являются In-proc-серверами OLE.

Отказоустойчивость - reliability

Способность компьютера и ОС адекватно реагировать на катастрофические события (например, пропадание напряжения или отказ техники). Обычно под отказоустойчивостью понимается способность системы продолжать функционировать без потери данных или закрытие системы с перезапуском и последующим восстановлением всех процессов, имевших место до момента аварии.

Открытый ключ - public key

Ключ, используемый для шифрования данных и не являющийся секретом. Данные, зашифрованные открытым ключом пользователя, можно расшифровать только его личным ключом.

Отличительное имя - distinguished name (DN)

Содержит имя домена, в котором находится объект, а также полный путь к этому объекту в иерархии контейнера

П**Пакет - package**

Специальным образом подготовленный набор файлов, необходимых для установки приложения службой Windows Installer. Содержит сведения о типе установки и необходимые параметры.

Пароль - password

Уникальная строка символов, которую нужно ввести для аутентификации доступа при регистрации. Является средством защиты для ограничения входа в систему и доступа к компьютерным системам и ресурсам,

Партнер по репликации - replication partner

При репликации службы каталогов — контроллер домена, оповещаемый об изменениях на другом контроллере и запрашивающий у него эти изменения. Один контроллер может иметь несколько партнеров по репликации. При репликации FRS — сервер, получающий уведомления от другого об измененных файлах в реплике. При репликации DFS партнерами по репликации являются все компьютеры, входящие в набор реплик.

Первичная зона DNS - DNS primary zone

Зона DNS, авторитетная для остальных зон. Позволяет вносить изменения в записи. Тиражирует информацию во вторичные зоны.

Переадресация запросов - forwarding

В DNS процесс перенаправления запросов неразрешенных на данном сервере другим серверам DNS.

Перенаправление папок - folder redirection

Правило *групповой политики*, позволяющее перенаправлять обращения к некоторым системным каталогам на сетевые файловые ресурсы.

Полная реплика - full replica

В Active Directory — набор *объектов* пространства имен, содержащих все *атрибуты*. На каждом контроллере домена хранятся полные реплики *схемы*, *конфигурации* и того домена, которому принадлежит контроллер.

Поставщик функций безопасности (ПФБ) - Security provider

Часть ПО, выполняющая функции безопасности. Взаимодействие с ПФБ выполняется через стандартные интерфейсы (например, *Crypto-API*), что позволяет сделать систему независимой от типа ПФБ.

Право доступа - access right

Разрешение процессу определенным образом воздействовать на определенный *объект*. Разные типы объектов поддерживают разные права доступа, хранящиеся в *списках контроля доступа*.

Предоставление файлов в совместное использование - file sharing

Способность Windows 2000 использовать часть (или всю) своей локальной файловой системы совместно с другим компьютерами.

Привилегия - privilege

Позволяет пользователю выполнять определенные действия в системе. *Привилегии* предоставляются к системе в целом в отличие от *прав доступа*, применимых к определенным *объектам*.

Проверка доступа - access verification

Проверка информации об *учетной записи пользователя* для определения возможности предоставления субъекту права выполнения запрашиваемой операции.

Программа-мастер - wizard

Специальная программа, предназначенная для облегчения выполнения рутинных операций. Использует пошаговый подход к выполнению последовательности *действий*. Не позволяет пропустить ввод или определение важных параметров.

Пространство имен - namespace

Упорядоченный список всех узлов, доступных для данного инструмента, *отформатированный* в виде дерева. Изображение пространства имен аналогично изображению структуры файлов и каталогов на жестком диске.

Протокол - protocol

Набор правил и соглашений, используемых двумя компьютерами для передачи сообщений по сети. В сетевом ПО обычно несколько уровней протоколов, расположенных один над другим.

Публикация приложений - application publishing

Процесс, применяемый Windows Installer для предложения пользователям программ, доступных для установки. Пользователи могут отказаться от установки опубликованных приложений.

Пул адресов - address pool

Диапазон адресов IP, используемый сервером DHCP для назначения регистрирующимся клиентам.

Пул RID - RID pool

Диапазон относительных идентификаторов (RID), выделяемых *мастерам RID* другим контроллерам в домене для генерации уникальных идентификаторов безопасности (SID).

Путь доверия - trust path

Путь, который проходит при *аутентификации* в домене *учетной записи* из другого домена в том же *лесте*.

Р**Рабочая поверхность - desktop**

Фоновая поверхность *экрана*, над которой располагаются окна, значки и диалоговые окна. На рабочей поверхности располагаются такие значки, как My Computer, My Network Places, Recycle bin.

Рабочая станция - workstation

Компьютеры, на которых исполняется *Windows 2000 Professional*, называются рабочими станциями **в отличие** от *серверов*, на которых выполняется *Windows 2000 Server*.

Рабочий стол - desktop

См. *рабочая поверхность*.

Распорядитель локальной безопасности - Local Security Authority (LSA)

Создает маркер безопасного доступа для каждого *пользователя*, обращающегося к системе.

Распределенная файловая система - distributed file system (DFS)

Сетевое расширение, позволяющее представлять совместно используемые ресурсы сети в виде единого дерева с общим корнем. Доступ к ресурсам выполняется без *уточнения* того, какому конкретному серверу в сети они принадлежат. Обладает возможностью балансировки нагрузки и предоставления альтернативных ресурсов в случае сбоев.

Редактор Реестра - Registry Editor

Системное приложение Windows 2000, позволяющее просматривать и редактировать записи в *реестре*. Имеются две версии редактора: regedit и regedt32.

Редиректор - redirector

Сетевая программа, принимающая запросы ввода/вывода для удаленных файлов, именованных каналов или почтовых слотов и передаю-

щзя их сетевым *службам* на другом компьютере. В Windows 2000 ре-директоры выполнены как драйверы файловой системы.

Реестр - registry

Архив баз данных Windows 2000 для хранения информации о конфигурации компьютера, включая аппаратные средства, установленное ПО, параметры окружения и др.

Режим восстановления Active Directory - Active Directory repair mode

Такой режим загрузки контроллера домена, при котором *Active Directory* переводится в автономный режим и перестает взаимодействовать с остальными контроллерами и отвечать на запросы LDAP. Позволяет выполнять восстановление целостности базы, перемещение файлов и другие ремонтные операции.

Резервное копирование - backup

Сохранение данных на магнитной ленте, в файле или ином носителе с целью восстановления в случае искажения или потери данных. Восстановление бывает *авторитетным* и *неавторитетным*.

Реплика - replica

Составляющая часть *набора реплик*. Все реплики в наборе имеют идентичный набор данных. Идентичность обеспечивается механизмом *репликации*.

Репликация - replication

Процесс копирования данных с одного компьютера, называемого *репликой*, на остальные, называемые *партнерами по репликации* и составляющие *набор реплик* с целью поддержания идентичности хранимой информации.

Репликация службы каталогов - directory services replication

Процесс копирования модификаций, внесенных в *Active Directory* на одном контроллере домена, на *партнеры по репликации*. Различают репликацию внутри *сайта* и между сайтами.

Репликация FRS - FRS replication

Процесс копирования измененных файлов с одной *реплики* на другие в пределах *набора реплик* с помощью службы NTFRS. Позволяет синхронизировать каталоги SYSVOL на разных контроллерах домена, а также отказоустойчивые тома DFS.

Ресурс - resource

Любая часть компьютерной системы или сети (например, диск, принтер, память), которая может быть предоставлена программе или процессу во время работы.

Родительский домен - parent domain

Домен, являющийся вышестоящим в дереве доменов по отношению к рассматриваемому.

Родительский класс - parent class

Класс объекта в каталоге, выступающий старшим по отношению к рассматриваемому. **Классы**, образованные от родительского, наследуют от него все обязательные и вспомогательные **атрибуты**.

С

Сайт ~ site

Место в сети, все части которой связаны быстрыми **соединениями**. Сайт **обеспечивает** надежность связи всех **серверов** и быстрый поиск необходимой информации.

Свободное пространство - free space

Неиспользуемая и неформатированная часть жесткого диска, которая может быть разбита на разделы или подразделы. Свободное пространство внутри расширенного раздела **доступно** для создания **логических дисков**. Пространство, не используемое расширенным разделом, доступно для создания **раздела**. Максимальное число разделов — 4.

Сеансовый билет - session ticket

Билет, выдаваемый **кличенту** *Центром* **распределения ключей** для доступа к серверу в течение одного сеанса работы. Сеансовый **билет** хранится в кэше билетов и может быть использован неоднократно в течение *времени жизни билета*.

Сервер - server

В *Windows 2000 Professional* — компьютер, предоставляющий свои **ресурсы** для совместного **использования** в сети. См. также *клиент*.

В *Windows 2000 Server* — компьютер, содержащий копию базы данных защиты **домена** и идентифицирующий регистрацию по сети. См. также *контроллер домена*.

Сервер-форпост - bridgehead server

Контроллер домена в сайте, через который выполняется репликация с другими сайтами. Сервер-форпост выбирается **KCC** из числа доступных контроллеров домена. Форпост, **назначенный** администратором, называется выделенным форпостом.

Серверный сертификат - server certificate

Термин относится к использованию сертификата для **аутентификации** сервера. Например, сервер Web может послать свой серверный сертификат **браузеру**, чтобы последний удостоверился в подлинности сервера.

Сетевой интерфейс - network interface

Сетевая плата, устройство удаленного доступа, виртуальный канал **PPTP** и др. Устройство, **через** которое **компьютер** подключен к сети. В одном компьютере может быть несколько сетевых **интерфейсов**, с каждым из которых **могут** быть связаны различные *протоколы*.

Сетевой каталог ~ network directory

См. *совместно используемый ресурс*.

Системный раздел - system partition

Том, содержащий файлы, зависящие от типа техники, необходимые для загрузки *Windows 2000*.

Скрипт - script

См. *сценарий*.

Служба - service

Процесс, выполняющий определенные функции системы и часто предоставляющий *API* для вызова других процессов. Службы *Windows 2000* поддерживают *RPC*, что подразумевает возможность вызова процедур *API* с удаленных компьютеров.

Служба каталогов Active Directory

Служба, интегрированная с *Windows 2000 Server* и обеспечивающая иерархический вид сети, наращиваемость и расширяемость, а также функции распределенной безопасности. Содержит информацию обо всех объектах системы и их свойствах, а также о взаимосвязях между объектами.

Смешанный режим работы - mixed mode

Режим работы домена *Windows 2000*, допускающий наличие в домене контроллеров домена старых версий. В этом режиме не существуют универсальных групп и запрещено вложение групп.

Событие - event

Любое значительное происшествие в системе или в приложении, о котором надо оповестить пользователя или занести запись в журнал.

Совместно используемый ресурс - shared resource

Ресурс (каталог, принтер, страница книги обмена и т. п.), доступный пользователям сети.

Сокращение пути доверия - shortcut trust

Использование горизонтальных доверительных отношений для уменьшения длины пути доверия.

Список контроля доступа - Access Control List (ACL)

Часть дескриптора безопасности, перечисляющая защитные функции, примененные к объекту. Владелец объекта может изменять список контроля доступа к объекту для предоставления или запрещения доступа к объекту другим. Список контроля доступа состоит из строк контроля доступа.

Строка контроля доступа - access control entry (ACE)

Элемент в списке контроля доступа (*ACL*). Строка содержит идентификатор безопасности пользователя (*SID*) и набор прав доступа.

Процесс с совпадающим идентификатором имеет либо разрешающие права, либо *запрещающие*, либо *разрешающие* права с *аудитом*. См. *список контроля доступа*.

Сфера влияния службы каталогов - directory services scope

Может включать любые объекты (пользователи, файлы, принтеры и т. д.), серверы в *сети*, *домены* и даже глобальные сети.

Схема - schema

Набор экземпляров классов объектов, хранящихся в каталоге. Приложения могут динамически изменять схему, добавляя в нее новые атрибуты и классы. Модификация схемы сопровождается созданием или модификацией объектов, хранящихся в каталоге. Все внесенные изменения моментально становятся доступны для других приложений. Доступ к любому объекту схемы (впрочем, как и к любому объекту в *Active Directory*) защищен *списками контроля доступа*, что гарантирует внесение изменений только *лицами*, уполномоченными делать это.

Сценарий - script

Последовательность команд, написанных на некотором языке *сценариев*. Для исполнения сценариев применяется хост или процессор. Сценарии служат для определения среды пользователя при его регистрации, для выполнения функций на серверах Web по запросу клиентов, для автоматизации административных задач и т. п.

Сценарий загрузки - startup script

Обычно командный файл. Исполняется на этапе загрузки ОС, используется для запуска приложений или служб исполняемых от имени компьютера.

Сценарий регистрации - logon script

Обычно командный файл, автоматически выполняемый при каждой регистрации пользователя в системе. Может служить для настройки окружения пользователя или рабочей среды. Сценарий регистрации назначается одному или нескольким пользователям сразу.

Т**Терминальный сеанс работы - terminal session**

Сеанс работы с *Windows 2000 Server* с использованием Terminal Services. На экране удаленного терминала *отображается* окно сеанса Windows 2000 *независимо* от версии ОС клиента. Служит для удаленного администрирования и для исполнения приложений на сервере.

Тиражирование с несколькими мастерами - multi master replication

Процесс *репликации* службы каталогов подразумевающий, что изменения могут выполняться на нескольких контроллерах домена. Использует специальный алгоритм для разрешения конфликтных ситуаций.

Тиражирование службы каталогов - directory replication

См. *репликация службы каталогов*.

Том - volume

Раздел диска или несколько разделов, форматированных для использования файловой системой.

Том DFS - DFS volume

Совокупность переходов DFS и совместно используемых ресурсов, на которые они указывают. Характеризуется именем, по которому осуществляется доступ к ресурсам.

Топология репликации - replication topology

Набор объектов связи между контроллерами доменов, определяющий последовательность репликации изменений между контроллерами. Топология, формируемая внутри сайта по умолчанию, — двунаправленное кольцо.

Точки перехода NTFS - NTFS junction points

Места в файловой системе NTFS, позволяющие переходить из текущего каталога в другой каталог или на другой диск.

Транзитивные доверительные отношения - transitive trust relationships

Двусторонние доверительные отношения между доменами, установленные так, что если один из них доверяет третьему домену, то второй также доверяет ему. Устанавливаются автоматически при включении нового домена в дерево доменов.

Транспорт TCP/IP

См. *TCP/IP*.

У**Удаленная регистрация - remote logon**

Когда пользователь устанавливает связь с удаленного компьютера, проверка доступа осуществляется на компьютере, не имеющем маркера доступа для данного пользователя. (Маркеры доступа создаются при интерактивной регистрации.)

Удостоверяющий центр - Certificate Authority

См. *Центр сертификации*.

Узел - node

Любой управляемый объект, задание или вид: компьютеры, пользователи, страницы Web и т. д.

Универсальные группы - universal groups

Группы безопасности или почтовые группы, в которых могут быть учетные записи пользователей, глобальных или универсальных групп из любого домена в лесу. Членство в глобальных группах публикуется

в *Глобальном каталоге*. Универсальные группы могут менять свой статус и переходить из групп безопасности в почтовые и наоборот.

Уникальность пароля - password uniqueness

Элемент *групповой политики*, определяющий число *паролей*, которые необходимо сменить, прежде чем сможет быть использован первоначальный пароль.

Учетная запись пользователя - user account

Объект *каталога Active Directory*, содержащий всю информацию о пользователе Windows 2000: имя и *пароль*, необходимые для регистрации, *группы*, в которые входит *данная* учетная запись, *права* и *привилегии* при работе в системе и доступе к ресурсам.

Ф

Файловая система с шифрованием - encrypting file system (EFS)

Расширение *файловой системы NTFS*, позволяющее прозрачно для пользователя шифровать/расшифровывать данные, хранимые на диске. Для шифрования применяется произвольный ключ. Текущая реализация не позволяет совместно использовать зашифрованные файлы.

Файловая система NTFS - NTFS file system

Файловая система Windows NT, разработанная для использования специально с Windows NT и Windows 2000. Поддерживает средства восстановления файловой системы и допускает применение чрезвычайно больших носителей данных, а также различные функции подсистемы POSIX. Также поддерживает *объектно-ориентированные* приложения, обрабатывая все файлы как объекты с определяемыми пользователем и системой атрибутами.

Фильтр групповой политики - group policy filter

Список контроля доступа к объекту групповой политики. Среди стандартных прав доступа содержит Apply, позволяющее регулировать применение политики к пользователям и группам.

Форпост - bridgehead

См. *сервер-форпост*.

Ц

Центр сертификации - Certificate authority

Институт, ответственный за выдачу сертификатов. Это может быть организация, сертификатам которой вы доверяете, например Verisign. Также это может быть программный компонент *системы*, такой как Microsoft Certificate Server.

Цифровая подпись - digital signature

Цифровая последовательность, связанная с документом и применяемая для подтверждения истинности передаваемой информации. Со-

здается с использованием *личного ключа* отправителя. Для проверки подлинности применяется *открытый ключ* отправителя.

Ч

Частичная реплика - partial replica

В Active Directory — копия объектов пространства имен, содержащих только часть атрибутов. Частичные реплики всех доменных пространств имен хранятся в *Глобальном каталоге*.

Членство в группе - group membership

Принадлежность к *группе*. *Права и привилегии*, предоставленные группе, распространяются на ее членов. Обычно действия, которые может совершить пользователь Windows 2000, определяются принадлежностью к той или иной группе.

Ш

Шаблон групповой политики - group policy template

Часть объекта групповой политики, хранящаяся на диске в каталоге SYSVOL. Тесно связан с соответствующим ему *контейнером групповой политики*.

Шифрование данных - data encryption

Изменение формата данных, так чтобы их *нельзя было* прочитать. См. *файловая система с шифрованием*.

Я

Язык сценариев - script language

Язык, на котором пишется *сценарий*. Это может быть обычный набор команд системы, собранных в командный файл, либо некоторый стандартный язык программирования. В Windows 2000 стандартно поддерживаются два языка сценариев: VB Script и Jscript.

А

ACE

См. *строка контроля доступа*.

ACL

См. *список контроля доступа*.

Active Directory

См. *служба каталогов Active Directory*.

ADSI (Active Directory Services Interface)

Интерфейс программирования, позволяющий приложениям использовать *службу каталогов Active Directory* и обращаться к объектам каталога. Также позволяет добавлять новые *классы* и *атрибуты* объектов путем *модификации схемы*.

ADSI Editor

Мощный инструмент просмотра объектов *Active Directory* и их атрибутов. Позволяет модифицировать атрибуты. Имеет графический интерфейс. Входит в состав Windows 2000 Support tools.

С**CA (Certification Authority)**

См. *центр сертификации*.

Certificate server

См. *сервер сертификатов*.

CRL (Certificate Revocation List)

Документ, публикуемый и обслуживаемый *центрами сертификации* и содержащий список сертификатов им аннулированных.

D**DCPROMO**

Программа-мастер, используемая для повышения статуса сервера Windows 2000 до контроллера домена.

DDNS (Dynamic DNS)

Динамический сервер DNS. Клиенты Windows 2000 динамически обновляют информацию о своих адресах в базе DNS.

DFS (Distributed File System)

См. *распределенная файловая система*.

Dfsutil

Инструмент для диагностики и управления службой распределенной файловой системы. Имеет интерфейс командной строки. Входит в состав Windows 2000 Server Resource Kit.

DHCP (Dynamic Host Configuration Protocol)

Протокол автоматического предоставления адресов IP клиентским компьютерам. В Windows 2000 реализована соответствующая служба. Кроме того, позволяет динамически регистрировать имена компьютеров в базе DNS. Требуется обязательная *авторизация* в *Active Directory*.

DLL (Dynamic Link Library)

См. *динамическая библиотека*.

DNS (Domain Name System)

Система имен домена. База данных, обеспечивающая соответствие имен компьютеров и IP-адресов.

E**EFS (Encrypted File System)**

См. *файловая система с шифрованием*.

F

FAZAM 2000

Мощный инструмент компании FullArmor, позволяет анализировать результирующий набор групповых правил на клиенте, а также выполнять планирование групповой политики.

FSMO (Flexible Single Master Object)

Главная копия для некоторых функций каталога *Active Directory*, исполняемых только на одном контроллере домена. Контроллер, хранящий объект FSMO, называется *мастером операций*.

FTP (File Transfer Protocol)

Протокол передачи данных, позволяет перемещать файлы с одного компьютера в *Интернете* или в *интрасети* на другой. Серверы, предназначенные для предоставления файлов для загрузки на другие компьютеры, называются серверами FTP,

I

ISTG (Inter-site Topology Generator)

Генератор *межсайтовой* топологии — процесс ответственный за создание объектов *связи* между сайтами. По своей сути это функция *KCC*.

K

KCC (Knowledge Consistency Checker)

Процесс, выполняемый на контроллерах домена и ответственный за формирование топологии *репликации*. KCC создает объекты связи между контроллерами внутри *сайта*. Один из KCC выполняет роль генератора межсайтовой топологии (*ISTG*).

KDC (Key Distribution Center)

См *центр распределения ключей*.

Kerberos

См. *аутентификация Kerberos*.

L

Ldp

Мощный инструмент просмотра, поиска и редактирования объектов *Active Directory* и их атрибутов. Имеет графический интерфейс. Требует знания языка запросов *ШАР*. Входит в состав Windows 2000 Support tools.

LDAP (Lightweight Directory Access Protocol)

Протокол доступа к службе каталога, основанный на стандарте X.500.

M

MMC (Microsoft Management Console)

См. *консоль управления MMC*.

MMS (Microsoft Metadirectory Services)

Сервер, позволяющий синхронизировать несколько разнородных служб каталогов. Может служить для объединения нескольких лесов с целью создания единого пространства имен.

N**Ntdsutil**

Основной инструмент диагностики и исправления базы *Active Directory*.

NTFRS (NT File Replication System)

Служба репликации файлов, применяемая в Windows 2000 для репликации каталогов *SYSVOL* и *томов DFS*.

Ntfrsutil

Основной инструмент диагностики и исправления службы NTFRS.

NTFS (New Technology File System)

См. *файловая система NTFS*.

NTLM

См. *аутентификация NTLM*.

P**PKT (Partition Knowledge Table)**

Таблица, используемая сервером *DFS* для хранения информации о соответствии между переходами *DFS* и совместно используемыми ресурсами, на которые они указывают. Клиенты кэшируют PKT для ускорения доступа к ресурсам *DFS*.

R**Repadmin**

Один из основных инструментов диагностики репликации *Active Directory*. Имеет интерфейс командной строки. Входит в состав Windows 2000 Support tools.

Replication Monitor

Один из основных инструментов диагностики репликации *Active Directory*. Имеет графический интерфейс. Входит в состав Windows 2000 Support tools.

RID (Relative Identifier)

Компонент SID. Каждый контроллер в домене использует свой пул *KID* для идентификации своих объектов.

S**SID (Security Identifier)**

См. *идентификатор безопасности*.

SSPI (Security Support Provider Interface)

Интерфейс поставщика функций безопасности. Набор функций, которые приложения могут использовать для доступа к механизмам аутентификации *Kerberos* или *NTLM*.

U**UNC (Universal Naming Convention)**

Универсальное соглашение об именовании, используемое в сетях Microsoft. Синтаксис соглашения: \\сервер\ресурс\каталог\файл.

UPN (User Principal Name)

Дружественное имя пользователя, определяющее его в каталоге Active Directory. Состоит из регистрационного имени пользователя и суффикса. Суффиксом может быть полное имя домена либо виртуальное имя домена.

USN (Update Sequence Number)

64-разрядное уникальное число, применяемое для отслеживания изменений свойств объектов в *Active Directory*. Используется механизмом тиражирования при разрешении конфликтных ситуаций.

W**Windows 2000 Professional**

Младшая система в семействе Windows 2000. Предназначена для настольных и мобильных компьютеров в качестве клиентской рабочей станции.

Windows 2000 Server

Младшая система в семействе серверных продуктов Windows 2000. Поддерживает работу с оперативной памятью до 4 Гб и до 4 процессоров.

Windows 2000 Advanced Server

Средняя система в семействе серверных продуктов Windows 2000. Поддерживает работу с оперативной памятью до 8 Гб и до 8 процессоров. Поддерживает кластеры серверов и кластеры с сетевой балансировкой нагрузки.

Предметный указатель

A

Active Directory
— FRS 350
— авторизация серверов 122
— восстановление
— — аварийное 465
— — авторитетное 436
— — базы 448
— — из резервной копии 429
— — на другой компьютер 433
— — неавторитетное 429
— — через переустановку 425
— журнал транзакций 134
— именование объектов 6
— контейнер 38
— лес 2
— объект 38
— объем базы 155
— ограничение 133
— перенос базы 453
— планирование 2
— проектирование 1
— резервное копирование 417
— — обычное 419
— — состояния системы 420
— сайт 47
— система именования 4
— срочное тиражирование
изменений 67
— стратегия именования 2
— тиражирование изменений 47
— установка 91
— ~~устранение~~ проблем 410
— целостность базы 449
Active Directory Domains and Trusts 427

Active Directory Migration Tool CM. ADMT
Active Directory Sites and Services
203, 214
Active Directory Sizer 152
Active Directory Users and
Computers 395, 427
ADMT (Active Directory
Migration Tool) 170, 459
ADSI 36
ADSIEdit 203, 395
Aelita Software ERDisk for Active
Directory 420
AH (authenticated header) 78
AutoSiteCoverage 115

B

BDC 167, 173
BIND 92, 100
BOOTP relay agent
см. агент передачи BOOTP

C

CGP 267
CNAME 4, 106, 111
Computer Associates ARCServeIT 420

D

Dcdiag 222
DCPROMO 94, 130, 340
DFS (Distributed File System) 47, 339,
381
— делегирование полномочий 393
— доменная 381, 407
— доменный том 342
— доступ 390
— имена NetBIOS 391

- конфигурация 394, 402
- корень 381, 390, 404
- корневая реплика 382
- масштабируемость 388
- пространство имен 392, 406
- резервное копирование 360
- сервер 385
- том 382
- — отказоустойчивый 383
- — реплика 383
- — создание 395
- точка перехода 382
- устранение проблем 396
- хост 381, 404
- DfsCmd 392
- DFSCmd 401
- DfsUtil 392, 396
- DFSUtil 401, 403
- DHCP 54, 122, 125, 153
- авторизация в Active Directory" 122
- контроль 130
- сервер
- — авторизация 122
- — размещение 122
- DHCPDISCOVER 123
- distinguished name •
- см. имя, отличительное объекта
- Distributed File System см- DFS
- DLL 257
- DMZ см. демилитаризованная зона
- DN 67, 68
- DNS (Domain Name Service) 2, 54, 76, 78, 91, 153
- динамическая регистрация имен 122, 125
- зона 4
- имя 4
- пространство имен 2
- сервер 4
- стратегия именования 6
- DSA 185
- DsaStat 213, 220
- E
- EAP 82
- encapsulated security payload см. ESP
- ESE (Extensible Storage Engine) 130
- ESP (encapsulated security payload) 78
- Event Viewer 363
- Extensible Storage Engine CM. ESE
- F
- FRS 47, 339
- Active Directory 350
- восстановление конфигурации 377
- журнал 366
- журналирование 357
- интервал опроса Active Directory 352
- механизм восстановления 374
- — авторитетное 374, 376
- — из реплики 377
- — неавторитетное 374
- — с магнитной ленты 376
- оптимизация 357
- таблица 349
- устранение проблем 362
- фильтр 353
- G
- GPC (Group Policy Container) 251, см. также групповая политика
- GPT (Group Policy Template) 251, см. также групповая политика
- GUID 59, 68, 185
- H
- high watermark см. репликация, Active Directory, «верхняя ватерлиния»
- HTTP 75
- HTTPS 75
- I
- IAS (Internet Authentication Server) 81
- ICANN 3
- ID 67
- IEAK (Internet Explorer Authorization Kit) 298
- IKE (Internet Key Exchange) 78
- Integrity 449
- InternetAuthenticationServer CM. IAS
- Internet Explorer 298
- Internet Explorer Authorization Kit CM. IEAK
- Internet Key Exchange CM. IKE
- IP (Internet Protocol) 4
- IPSec 75, 78
- ISTG 49, 59, 63, 153, 204
- K
- KCC (Knowledge Consistency Checker) 49, 60, 153, 193, 198, 202, 344, 380
- KDC 244
- Kerberos 76, 78, 346
- Knowledge Consistency Checker CM. KCC
- L
- L2TP/IPSec 82
- LAN Manager 117
- LDAP 39, 76
- Ldp 203
- LMHOSTS 118
- LSDOU 263

M

master browser *см.* домен, обозреватель
 Microsoft Consulting Services 153
 Microsoft Exchange 2000 45, 66
 Microsoft Identity Integration Server (MIIS) 2003 25
 Microsoft Installer 278
 Microsoft Tape Format *СМ.* MTF
 MMC 328, 401
 MTF (Microsoft Tape Format) 420

N

NAT (Network Address Translation) 5, 76, 106
 NetBIOS 67, 76, 116, 391
 — имя 116
 — отключение поддержки 120
 — разрешение имени 118
 Netdiag 158
 Netlogon 9", 114
 Network Address Translation *СМ.* NAT
 Novell Netware 92
 ntbackup 419
 Ntbackup 429
 Ntdsutil 427, 432, 436
 NTFRSUTL 371
 NTFS v.5 342

O

originating update *ом.* объект, исходное обновление

P

Partition Knowledge Table *см.* PKT
 PDC 138, 167, 171
 PKI 24, 78
 PKT (Partition Knowledge Table) 383
 PPTP 82

R

RADIUS 5, 81
 Remote Storage 360
 repadmin 213, 215, 225
 Replication Monitor 218, 227
 replmon 213
 RID 67, 174, 427, 446
 Routing and Remote Access Server *см.* RRAS
 RPC 76, 78
 — динамическое назначение портов TCP 195
 — поверх IP 194, 195
 RRAS (Routing and Remote Access Server) 125

S

SAM 67, 130, 171
 Schema Management 427
 Server 157
 SID 67, 68, 131, 174
 SID history *см.* история SID
 Simple Network Time Protocol *см.* SNTP
 single master replication *см.* тиражирование с одним мастером
 SMB 76
 SMTP (Simple Network Time Protocol) 59, 63, 137, 194, 196
 special identities *см.* особые объединения
 SPN 238
 SRV 4, 92
 subscription forest *см.* лес, подписки
 SYSVOL 135, 340

T

TCP 195
 TCP/IP 111, 125, 158
 thread ID *см.* идентификатор потока

U

UGP 267
 UltraBAC for Windows 2000 420
 UNC 278
 update sequence number *СМ.* USN
 updateness vector *см.* вектор, обновленности
 USN (update sequence number) 166, 183, 189, 340
 — исходный 184
 — локальный 184
 — сохранение 183
 UTF-8 100

V

Vector Version Join (VV-Join) *СМ.* подключение вектора версий
 Veritas Backup Exec 420
 Version Vector *см.* вектор версии
 VPN 75

W

W32Time 137
 Web-интерфейс 36
 Windows 2000 100, 119, 121, 211, 247
 Windows Backup 360
 Windows Installer 335
 Windows Internet Naming Service *СМ.* WINS
 Windows NT 6, 26, 39, 92, 211
 Windows NT 4.0 167

Windows Scripting Host 280, 299
 Windows XP 119, 121
 WINS 54, 116, 153
 WINS (Windows Internet Naming Service) 76

A

авторизация 80
 агент передачи BOOTP 125
 административный шаблон 294, 303
 адресная книга 45
 аргумент
 — /addroot 402
 — /clean 402
 — /DEBUG 402
 — /DFSREFERRALLIMIT 403
 — /DFSVCVERBOSE 402
 — /DNS 402
 — /list 397
 — /LOGGINGDFS 403
 — /NETAPIFSDEBUG 402
 — /pktinfo 399
 — /remit 402
 — /remroot 402
 — /SFP 402
 — /SYNCINTERVAL 403
 — /unmap 402
 — /VALUE 402
 — /VERBOSE 402
 — /view 397
 аренда адреса 127

B

вектор
 — версии 349
 — обновленности 166
 виртуальный туннель 64

G

генератор межсайтовой топологии
 см. ISTG
 глобальный каталог (ГК) 32, 68, 103, 444
 группа 32
 — Administrators 37
 — Authenticated Users 268
 — Domain Admins 37
 — Enterprise Admins 37, 38
 — Everyone 132
 — Pre-Windows 2000 Compatible Access 132
 — Schema Admins 38
 — Windows 2000 32
 — административная 37, 38

— глобальная 28, 32, 37
 — размер 34
 — формирование 34
 — локальная 28, 32, 35, 37
 — правило Restricted Groups 38
 — универсальная 32
 — содержимое 32
 — сортировка учетных записей 33
 — членство 32
 — членство 442
 групповая политика 38, 165, 247
 см. также групповые правила
 — ADDIAG 324
 — ADDIAG 316
 — FAZAM 2000 328
 — FAZAM2000 316
 — Gpoutil 322
 — GPOTool 316
 — GPRESULT 316
 — SECEDIT 316, 328
 — журналирование 329
 — контейнер см. GPC
 — объект (ОПТ) 251, 276, 248
 — планирование 306
 — список контроля доступа 268
 — сценарий 299
 — устранение проблем 315
 — фильтрация 267
 — флаг 331
 — фоновое применение 259
 — хранение параметров 252
 — шаблон см. GPT
 групповые правила
 см. также групповая политика
 — делегирование полномочий 274
 — для домена 249
 — для компьютеров 250
 — для организационных подразделений 249
 — для пользователей 250
 — для сайта 248
 — изменение последовательности применения
 — блокировка наследования 263, 264
 — деактивация 267
 — перемишка 265
 — принудительное наследование 265
 — история применения 270
 — контейнер 248
 — локальные 248
 — применение 263
 — редактирование 272
 — создание 272
 — шаблон 248

Д

- делегирование административных полномочий 39, 46
- демилитаризованная зона 75, 80, 100
- демпфирование 188
- дерево 10, 20, 106
- динамическая библиотека 249
- дисковая подсистема 163
- доверительные отношения
 - нетранзитивные 10
 - попарные 30
 - транзитивные 10
- документ
 - печать 45
 - поиск 44
 - редактирование 44
 - совместное использование 45
- домен 1, 10
 - административная политика 11
 - безопасность 11
 - глобальный 12
 - дочерний 10
 - имя 2, 4
 - контекст имен 53
 - контроллер 4, 10, 27
 - корневой 1, 2, 10, 14, 112
 - пустой 38
 - миграция 26, 31
 - с несколькими мастер-доменами 30
 - с одним мастер-доменом 27
 - модель
 - полностью доверительных отношений 10
 - с несколькими мастер-доменами 9
 - с одним доменом 9, 11
 - обозреватель 67
 - объединение 30
 - отношения доверия 10
 - переустановка 454
 - плоское имя 112
 - подключение через VPN 75
 - подразделение 1
 - политика 19
 - промежуточный 1
 - пул идентификаторов 67
 - размер 11
 - родительский 10
 - уникальное имя 66
- доступ к файловым ресурсам 35

Ж

- журнал
 - NTFS 345, 359
 - входа 346, 349
 - выхода 346, 349

- политики для пользователей 332
- регистрации 136
- File Replication System 364
- системных событий 163
- событий 95
- событий приложений 330
- транзакций 134, 349
- установки приложений 335

З

- зона 4, 93
 - демилитаризованная 5
 - динамическое обновление 95
- имя 102

И

- идентификатор безопасности см. SID
- идентификатор потока 370
- имитатор PDC 67, 138, 153, 174, 273, 427, 446
- имя
 - Cn 6
 - DisplayName 6
 - NetBIOS 27
 - SamAccountName 6
 - UserPrincipalName (UPN) 7
 - компьютера 8
 - общее 6
 - отличительное объекта 9
 - подразделения 9
 - пользователи 6
- инфраструктура открытых ключей см. PKI
- история SID 28

К

- каталог
 - восстановление 413
- коммутируемая линия 64
- контроллер домена 51
 - Windows 2000 123
- генератор межсайтовой топологии 203
- главный си. РОС.
- понижение статуса 165
- проверка 156
- резервный см. BDC.
- установка 138, 178
- кэширование 384

Л

- лес 1, 10, 20, 32
 - добавление домена 66
 - имя 2
 - корень 10
 - подписки 25
 - структура 468
- логическое имя 116

М

- маршрутизатор 125
- мастер
 - доменных имен 66, 445
 - **инфраструктуры** 61, 447
 - операций 427, 444
 - относительных идентификаторов *см.* RID
 - переноса групп 460
 - подготовки 66
 - схемы 65, 445
 - установки Active Directory 93
- межсайтовая связь 56
 - интервал репликации 58
 - объект 59
 - имя 59
 - направление 59
 - создание 59
 - протокол репликации 59
 - расписание 58
 - создание 55
 - стоимость 57
 - топология 55
 - транзитивная 57
- межсайтовый мост 57
- межсетевой экран 75
- миграция 39
- мультисеть 123

О

- объект
 - NTDS Settings 193
 - исходное добавление 187
 - исходное обновление 183, 188
 - модификация 187
 - ограничение числа 39
 - памятник 186
 - рассортировка 39
 - реплицированное добавление 187
 - реплицированное обновление 183, 188
 - связи 59
 - создание 186
 - удаление 186
- ОГП *см.* групповая политика, объект
- организационное подразделение (ОП) 10, 38
 - глубина вложения 39
 - иерархия 39
 - модель
 - административная 41
 - географическая 40
 - объектная 40
 - организационная 40
 - проектная 41
 - первого уровня 39
 - принцип построения 39

- ресурсное 47
- учетное 46
- особые объединения 37
 - категория
 - Authenticated Users 37
 - Everyone 37
 - Interactive Users 37
 - Network Users 37
- относительный идентификатор *см.* RID

П

- пакет установки 278
- пароль учетной записи 211
- плоская сеть 122
- подготовительный каталог 345
- полноключные вектора версий 378
- подписка 350
- пользовательский идентификатор 122, 128
- последовательный номер обновления *см.* USN
- правила
 - IPSecurity 293
 - безопасности 300
 - выполнения сценариев 281
 - групп с ограниченным членством 290
 - журнала регистрации 289
 - локальные 284
 - параметры безопасности 286
 - правила аудита 284
 - правила пользователей 285
 - открытых ключей 292
 - реестра 291
 - системных служб 291
 - **учетных записей** 282
 - правила Kerberos 283
 - правила блокировки учетных записей 283
 - правила паролей 282
 - файловой системы 292
- прокси-сервер 5
- пропускная способность каналов связи 48
- пространство имен 10
- протокол трансляции сетевых адресов *см.* NAT

Р

- распределенная файловая система *см.* DFS
- регистрация 47
- редактор реестра 203
- резервное копирование 392
- реплика
 - базы объектов домена 180

- домена 180
- доменного контекста имен 180
- конфигурации 180
- локальная 180
- мастер 179
- полная 180
- резервная 179
- схемы 180
- частичная 180
- репликация 10, 32, 227
 - см. также тиражирование
- Active Directory 47, 72, 163, 179, 424
 - асинхронная 195
 - «вектор обновленности» 188
 - «верхняя ватерлиния» 188
 - внутрисайтовая 195, 198
 - входящее соединение 194
 - выделенный сервер-форпост 194
 - ГК 208
 - конвергенция 179
 - контроллер домена 193
 - межсайтовая 195
 - пакет 197
 - с несколькими мастерами 179
 - сайт 193
 - связь 194
 - сервер-форпост 194
 - сетевой протокол 194
 - синхронная 195
 - слабая связанность 179
 - топология 181, 192
 - штамп 184
 - DFS 342, 355, 386
 - объект 395
 - сайт 388
 - топология 358
 - FRS 47, 164, 174, 340, 424
 - избыточность 342
 - инициация 341
 - объект 350
 - планирование 356
 - расписание 354
 - список партнеров 344
 - журнал NTFS 359
 - SYSVOL 379
 - внутри сайта 194
 - входная 347
 - выходная 345
 - ГК 208
 - диагностика 212
 - интервал 58
 - контроллер домена 48
 - критических событий 209
 - между сайтами 194
 - механизм LMRepl 174
 - механизм NTFRS 252
 - отказоустойчивых томов DFS 342
 - ошибка
 - LDAP 49, 244
 - внутренняя ошибка системы 243
 - Отсутствие конечной точки (No more end-point) 244
 - Ошибка поиска в DNS (DNS Lookup failure) 240
 - по SMTP 195
 - пропускная способность канала связи 358
 - пропускная способность каналов 48
 - протокол 59
 - Разница во времени (Ошибка LDAP 82) 242
 - расписание 49, 58, 65
 - связь 235
 - Служба каталогов перегружена (Directory service too busy) 240
 - список партнеров 214
 - схемы 72
 - трафик 47, 48
 - файла 378
 - файловая 174
 - файловой системы 168
- С
 - сайт 47, 193
 - планировка 1
 - топология репликации 1
 - сегментированная сеть 125
 - сервер
 - DFS 385
 - DHCP 122
 - DNS 54, 92, 121
 - ISA 77
 - Windows NT 4.0 122
 - WINS 118, 120
 - аутентификации 81
 - ГК 54, 66, 68
 - обновление 403
 - терминальный 52
 - файловый 52
 - форпост 54, 59, 194
 - автоматический 60
 - выделенный 60, 194
 - репликация 62
 - тиражирование 61
 - сертификат 78, 292
 - системная политика 247
 - служба
 - распределенной файловой системы см. DFS
 - репликации
 - Active Directory 339
 - файловой системы NTFRS см. FRS
 - каталогов Windows NT 1
 - синхронизации времени 137

смарт-карта 14, 82
 список
 — контрольных точек 349
 — контроля доступа 132, 149
 — совместимого оборудования 151
 суперобласть 122, 123
 схема
 — модификация 73
 — политика изменения 72
 сценарий 203, 280
 -ADSI 36

T

таблица
 — знаний о разделах *см. РКТ*
 -ID 349
 — идентификаторов 34й
 — соединений 349
 тиражирование
 см. также репликация
 — с одним мастером 168
 топология сети 55
 — звезда 55
 — кольцо 55
 — сложная (комбинированная) 56
 точка перехода NTFS 353
 транзакция атомарная 183
 трафик
 — LDAP-запросов 52
 - SMTP 197
 — компрессия 49
 — межсайтовый 49
 — регистрации 52
 — репликации 47
 — управление 49
 — шифрование 75
 туннелирование 76

У

удаленное хранилище 360
 удаленный вызов процедур *см. RPC*
 учетная запись 440

Ф

файл
 — config.pol 248
 — DCPromo.log 137, 145
 — DCPromos.log 137, 151
 — DCPromoUI.log 137, 146
 — edb.chk 134, 349
 — edb.log 134, 349
 — Lbridge.cmd 175
 — netapi32.dll 402
 - Netsetup.log 137, 150
 — ntconfig.pol 248
 — NTDS.DIT 133
 — ntfrs.jdb 349
 - ntfrs.jet 349
 - res1.log 133, 349
 — res2.log 133, 349
 — userenv.log 332
 — восстановление 373
 — ответов 142
 — резервное копирование 373

X

хост 4

Ш

широковещательная рассылка 118
 штамп 184

Список литературы

1. Зубанов Ф. Microsoft Windows 2000. Планирование, развертывание, управление. 2-е изд., испр. и доп. — Русская Редакция. М., 2000 г.
2. Межсетевое взаимодействие, Ресурсы Microsoft Windows 2000 Server. — Русская Редакция. М., 2001 г.
3. Распределенные системы. Книга 1, Ресурсы Microsoft Windows 2000 Server. — Русская Редакция. М., 2000 г.
4. Сети TCP/IP. Ресурсы Microsoft Windows 2000 Server. — Русская Редакция. М., 2000 г.
5. Active Directory Branch Office Planning Guide. <http://www.microsoft.com/windows2000/techinfo/planning/activedirectory/branchoffice/default.asp>
6. Windows 2000 Server Distributed Systems Guide. — Microsoft Press, 2000 г.
7. Windows 2000 Server Operations Guide. — Microsoft Press, 2000 г.
8. Windows 2000 Server Deployment Planning Guide. — Microsoft Press, 2000 г.
9. Зубанов Ф. Windows NT: выбор «профи». 2-е изд. — Русская Редакция. М., 1997 г.

Об авторе

Федор Зубанов работает в Российском отделении корпорации Microsoft. За 10 лет он прошел путь от системного инженера до старшего консультанта службы Microsoft Consulting Services. Долгое время занимался популяризацией системы Windows. Последние 5 лет занимается планированием и внедрением систем на базе Windows NT/2000. Его конек — построение службы каталогов Active Directory. Федор принимал активное участие в проектах по развертыванию сетевой инфраструктуры на базе Windows 2000 в таких компаниях, как Альфа-банк, Вымпелком, Лукойл, Роснефть, Юкос и др. В последнее время привлекается российскими компаниями в качестве эксперта по Active Directory.

Попав под сильное давление издательства «Русская Редакция» Федор написал в 1995 г. свою первую книжку — о Windows NT 3.51. Последовавшие за ней книги по администрированию Windows NT 4.0 и Windows 2000 сразу стали бестселлерами. Настоящая книга — пятая по счету, обобщает многолетний опыт работы с Active Directory. Все книги были написаны в свободное от основной работы время. Так что вопрос о хобби отпадает сам собой.

Зубанов Федор Валерианович

Active Directory: подход профессионала

Издание 2-е, исправленное

Компьютерная верстка **В. Б. Хильченко, Е. Б. Сярая**

Технический редактор **О. В. Дергачева**

Дизайнер обложки **Е. В. Козлова**

Оригинал-макет выполнен с использованием
издательской системы Adobe PageMaker 6.0

TypeMarketFontLibrary
легальный пользователь

ПОЛЬЗОВАТЕЛЬ
Para(-)Type
FOR LEGAL USE

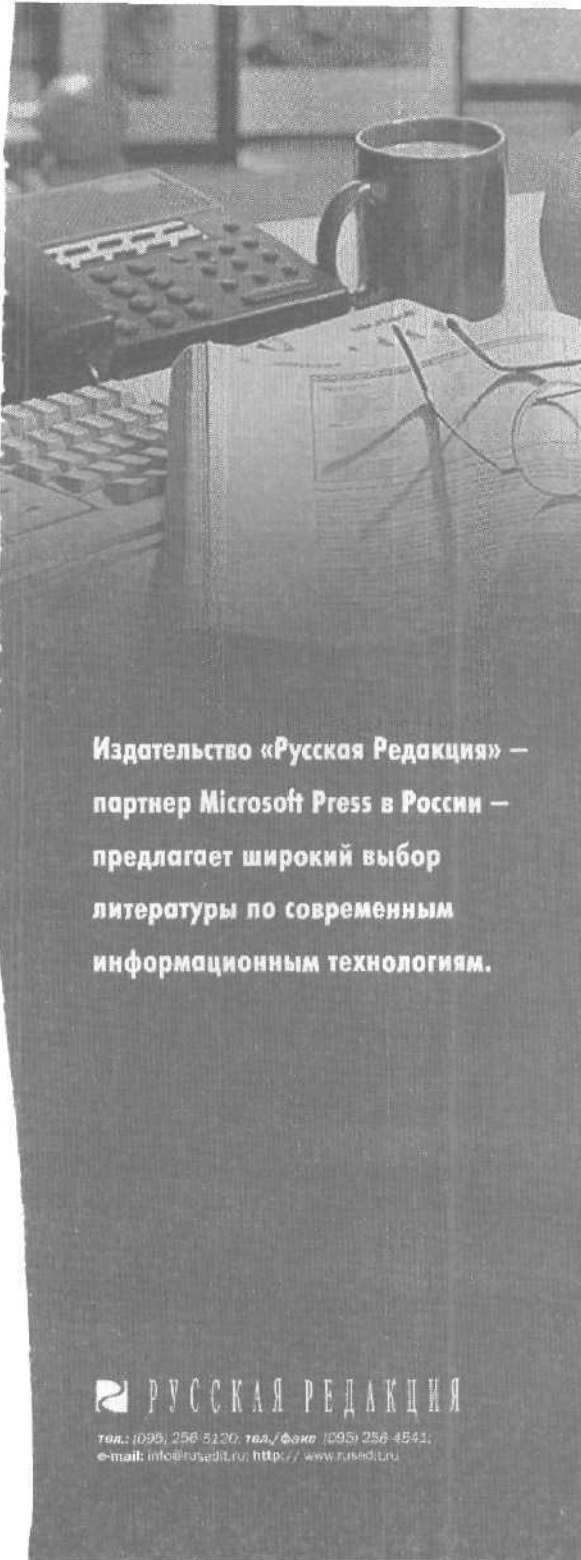
Главный редактор **А. И. Козлов**

Подготовлено к печати издательством «Русская Редакция»
123317, Москва, ул. Антонова-Овсеенко, д. 13
тел.: (095) 256-5120, тел./факс: (095) 256-4541
e-mail: info@rusedit.ru, <http://www.rusedit.ru>

 **РУССКАЯ РЕДАКЦИЯ**

Подписано в печать 20.10.2003 г. Тираж 2 000 экз.
Формат 60х90/16. Физ. п. л. 34

Отпечатано в ОАО «Типография «Новости»»
105005, Москва, ул. Фр. Энгельса, 46



**Издательство «Русская Редакция» —
партнер Microsoft Press в России —
предлагает широкий выбор
литературы по современным
информационным технологиям.**

 **РУССКАЯ РЕДАКЦИЯ**

тел.: (095) 256-5120; тел./факс: (095) 256-4541;
e-mail: info@rusedit.ru; <http://www.rusedit.ru>

Наши книги Вы можете приобрести

• в Москве:

Специализированный магазин
«Компьютерная и деловая книга»
Ленинский проспект, *строение 38*,
тел.: (095) 778-7269

«Библио-Глобус» ул. Мясницкая, 6,
тел.: (095) 928-3567

«Московский дом книги» ул. Новый Арбат, в.
тел.: (095) 290-4507

«Дом технической книги» Ленинский пр-т, 40,
тел.: (095) 137-6019

«Молодая гвардия» ул. Большая Полянка, 28,
тел.: (095) 238-5001

«Дам книги на Соколе» Ленинградский пр-т,
78, тел.: (095) 152-4511

«Дом книги на Войковской» Ленинградское ш.,
13, стр. 1, тел.: (095) 150-6917

«Мир печати» ул. 2-я Тверская-Ямская, 54,
тел.: (095) 978-5047

Торговый дом книги «Москва» ул. Тверская, 8,
тел.: (095) 229-6483

• в Санкт-Петербурге:

СПб Дом книги, Невский пр-т., 28
тел.: (812) 318-6402

СПб Дом *военной книги*, Невский пр-т., 20
тел.: (812) 312-0563, 314-7184

Магазин «Подписные издания»,
Литейный пр-т., 57, тел.: (812) 273-5053

Магазин «Техническая книга», ул. Пушкинская,
2, тел.: (812) 164-6565, 164-1413

Магазин «Буквоед», Невский пр-т., 13,
тел.: (812) 312-6734

ЗАО «Торговый Дом «Диалект»,
тел.: (812) 247-1483

Оптово-розничный магазин «Наука и техника»,
тел.: (812) 567-7025

• в Екатеринбурге:

Магазин «Дом книги»,
ул. *Валекс*, 12,
тел.: (3432) 59-4200

• в Великом Новгороде:

«Наука и техника»,
ул. Большая Санкт-Петербургская, 44,
Дворец Молодежи, 2-й этаж

• в Новосибирске:

ООО «Топ-книга», тел.: (3832) 36-1026

• в Алматы (Казахстан):

ЧП Болат Амреев,
моб. тел.: 8-327-908-28-57, (3272) 76-1404

• в Киеве (Украина):

ООО Издательство «Ирина-Пресс»,
тел.: (+1038044) 269-0423

«Техническая книга на Петровке»,
тел.: (+1038044) 268-5346