

ИВАН КОРОБКО

СПРАВОЧНИК СИСТЕМНОГО АДМИНИСТРАТОРА по программированию Windows

**Объектная модель
Active Directory**

Интерфейсы ADO и IADs

**Идентификаторы безопасности
и NTFS**

**Групповые политики
и реестр**

Синтаксис командных файлов

Windows Script Host

Windows Installer

УДК 681.3.06
ББК 32.973.26-018.2
К68

Коробко И. В.

К68 Справочник системного администратора по программированию Windows. — СПб.: БХВ-Петербург, 2009. — 576 с.: ил. — (Системный администратор)

ISBN 978-5-9775-0296-2

Приведена исчерпывающая информация по устройству и управлению Active Directory. Описаны интерфейсы IADs, ADO, а также основные приемы программного управления каталогом на языке VBScript. Особое внимание уделено безопасности операционной системы: программному управлению NTFS, принципам построения и чтения идентификаторов безопасности и др. Подробно освещен вопрос управления групповыми политиками (ADM-файлы) и реестром (REG-файлы). Приведен синтаксис пакетных файлов (autorun.inf и др.), рассказано о технологии изменения дистрибутивов, созданных с помощью Windows Installer.

Для системных администраторов и программистов

УДК 681.3.06
ББК 32.973.26-018.2

Группа подготовки издания:

Главный редактор	<i>Екатерина Кондукова</i>
Зам. главного редактора	<i>Игорь Шишигин</i>
Зав. редакцией	<i>Григорий Добин</i>
Редактор	<i>Юрий Якубович</i>
Компьютерная верстка	<i>Натальи Смирновой</i>
Корректор	<i>Наталья Першакова</i>
Дизайн серии	<i>Инны Тачиной</i>
Оформление обложки	<i>Елены Беляевой</i>
Зав. производством	<i>Николай Тверских</i>

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 31.10.08.

Формат 70×100^{1/16}. Печать офсетная. Усл. печ. л. 46,44.

Тираж 2000 экз. Заказ №

"БХВ-Петербург", 194354, Санкт-Петербург, ул. Есенина, 5Б.

Отпечатано с готовых диапозитивов
в ГУП "Типография "Наука"
199034, Санкт-Петербург, 9 линия, 12

ISBN 978-5-9775-0296-2

© Коробко И. В., 2008
© Оформление, издательство "БХВ-Петербург", 2008

Оглавление

ОБ АВТОРЕ	3
ПРЕДИСЛОВИЕ	5
ВВЕДЕНИЕ	7
Для кого эта книга?	7
Какой язык программирования выбрать?	7
Как пользоваться книгой?.....	8
Какой редактор сценариев использовать?.....	11
Какова структура книги?.....	12
БЛАГОДАРНОСТИ	15
РАЗДЕЛ 1. ОСНОВЫ ПОСТРОЕНИЯ ACTIVE DIRECTORY	17
ГЛАВА 1. ВНУТРЕННЕЕ УСТРОЙСТВО КАТАЛОГА ACTIVE DIRECTORY	19
Основные термины и понятия	19
Нормативная документация по Active Directory.....	20
Общие сведения	20
RFC по LDAP v2	21
RFC по LDAP v3	21
Особенности и характеристики Active Directory	22
Active Directory как часть файловой системы.....	23
Архитектура службы каталогов Active Directory.....	24
DNS и Active Directory	25
Службы каталогов Active Directory.....	26
Глобальный каталог.....	27
Провайдеры ADSI.....	29
Схема объектной модели ADSI.....	30
Объекты в Active Directory	31
Доступ к объектам Active Directory.....	31

Типы объектов Active Directory	32
Типы данных объектов в Active Directory	33
ГЛАВА 2. УСТАНОВКА ДОМЕНА WINDOWS 2003/2008.....	35
Основные термины и понятия	35
Подготовка к установке Active Directory.....	36
Запуск мастера установки Active Directory	36
Синтаксис файла ответов утилиты <i>dcpromo.exe</i>	37
Описание процесса установки Active Directory	41
Мастер установки домена Windows 2008	50
РАЗДЕЛ 2. ПРИНЦИПЫ ПРОГРАММНОГО УПРАВЛЕНИЯ	
ACTIVE DIRECTORY	53
ГЛАВА 3. ОСНОВЫ ПРОГРАММНОГО УПРАВЛЕНИЯ ACTIVE DIRECTORY.....	55
Основные термины и понятия	55
Идентификаторы Active Directory	56
Типы объектов в Active Directory.....	57
Способы доступа к объектам Active Directory	59
LDAP-путь к объекту.....	60
Развернутая форма записи	61
Сокращенная форма записи.....	61
Способы доступа к каталогу Active Directory	62
Диалект LDAP	62
Диалект SQL.....	66
Прилинкованный SQL-сервер	69
Чтение данных из Active Directory	75
Тип данных: длинное целое число (<i>VarType = 3</i>)	77
Тип данных: дата-время (<i>VarType = 7</i>)	79
Тип данных: строка (<i>VarType = 8</i>).....	82
Тип данных: объект (<i>VarType = 9</i>)	85
Тип данных: булево значение (<i>VarType = 11</i>).....	87
Тип данных: массив элементов (<i>VarType = 8192+x</i>).....	88
ГЛАВА 4. ОБЪЕКТНАЯ МОДЕЛЬ ИНТЕРФЕЙСОВ <i>IADs</i>*	90
Основные термины и понятия	90
Типы данных, поддерживаемые интерфейсами <i>IADs</i> *	91
Классификация интерфейсов <i>IADs</i> *	93
Основные интерфейсы	93

Объектная модель <i>IADs</i>	93
Объектная модель <i>IADsContainer</i>	105
Объектная модель <i>IADsNamespaces</i>	111
Объектная модель <i>IADsOpenDSObject</i>	112
Интерфейсы свойств объектов.....	113
Объектная модель <i>IADsPropertyList</i>	114
Объектная модель <i>IADsPropertyEntry</i>	120
Объектные модели <i>IADsPropertyValue</i> и <i>IADsPropertyValue2</i>	124
Интерфейсы объектов.....	127
Методы интерфейсов объектов.....	128
Свойства интерфейсов объектов.....	128
Использование <i>IADs</i> *-интерфейсов на практике.....	129
Способы доступа к объектам Active Directory.....	131
Управление атрибутами с помощью интерфейса <i>IADs</i>	133
Управление атрибутами с помощью интерфейса <i>IADsUser</i>	133
ГЛАВА 5. ОБЪЕКТНАЯ МОДЕЛЬ ADO DB.....	135
Основные термины и понятия.....	135
Объекты ADO.....	135
Объект <i>Connection</i>	137
Объект <i>Command</i>	146
Объект коллекции <i>Properties</i>	153
Объект <i>Recordset</i>	155
РАЗДЕЛ 3. ОБЪЕКТЫ ACTIVE DIRECTORY.....	169
ГЛАВА 6. ВИРТУАЛЬНЫЙ ОБЪЕКТ ROOTDSE.....	171
Основные термины и понятия.....	171
Назначение объекта RootDSE.....	171
Объектная модель RootDSE.....	172
Атрибуты, характеризующие структуру домена.....	172
Атрибуты, характеризующие конфигурацию домена.....	173
Атрибуты, характеризующие конфигурацию контроллера домена.....	175
Управляющие объекты.....	175
Получение сведений об объекте RootDSE.....	178
Утилиты для просмотра характеристик RootDSE.....	178
Программное управление RootDSE.....	188
Определение имени домена.....	189

ГЛАВА 7. АТРИБУТЫ ОСНОВНЫХ ОБЪЕКТОВ ACTIVE DIRECTORY	191
Основные термины и понятия	191
Условные обозначения	192
Обязательные атрибуты для всех объектов Active Directory	193
Основные объекты Active Directory	194
Пользователь	195
Группа безопасности	204
Контейнер	207
Компьютер	208
ГЛАВА 8. УПРАВЛЕНИЕ УЧЕТНОЙ ЗАПИСЬЮ ПОЛЬЗОВАТЕЛЯ	214
Основные термины и понятия	214
Производимые операции	214
Создание пользователя	215
Работа мастера. Теория	216
Работа мастера. Практика	219
Программное создание учетной записи пользователя	224
Поля учетной записи, создаваемой мастером	227
Удаление пользователя	227
Удаление с помощью мастера	227
Удаление программным способом	227
Чтение свойств пользователя	229
Вкладка <i>General</i>	229
Вкладка <i>Address</i>	233
Вкладка <i>Account</i>	235
Вкладка <i>Profile</i>	242
Вкладка <i>Telephones</i>	245
Вкладка <i>Organization</i>	247
Вкладка <i>Member Of</i>	251
Вкладка <i>Dial-in</i>	253
Вкладка <i>Environment</i>	258
Вкладка <i>Sessions</i>	261
Вкладка <i>Remote control</i>	265
Вкладка <i>Terminal Services Profile</i>	267
Вкладка <i>COM+</i>	270
ГЛАВА 9. УПРАВЛЕНИЕ УЧЕТНОЙ ЗАПИСЬЮ ГРУППЫ БЕЗОПАСНОСТИ	271
Основные термины и понятия	271
Производимые операции	271
Создание группы	272

Работа мастера. Теория	272
Работа мастера. Практика	275
Программное создание группы	277
Поля создаваемой мастером учетной записи	278
Удаление группы	279
Удаление с помощью мастера	279
Удаление программным способом.....	280
Чтение параметров группы безопасности	280
Вкладка <i>General</i>	281
Вкладка <i>Members</i>	284
Вкладка <i>Member Of</i>	285
Вкладка <i>Managed By</i>	287
ГЛАВА 10. УПРАВЛЕНИЕ КОНТЕЙНЕРОМ	289
Основные термины и понятия	289
Создание контейнера.....	289
Работа мастера. Теория	290
Работа мастера. Практика	291
Программное создание учетной записи контейнера	293
Поля контейнера, создаваемого мастером	293
Удаление контейнера	294
Удаление с помощью мастера	294
Удаление программным способом.....	294
Чтение свойств контейнера.....	296
Вкладка <i>General</i>	296
Вкладка <i>Managed By</i>	299
Вкладка <i>COM+</i>	300
Вкладка <i>Group Policy</i>	301
ГЛАВА 11. УПРАВЛЕНИЕ УЧЕТНОЙ ЗАПИСЬЮ КОМПЬЮТЕРА	304
Основные термины и понятия	304
Создание учетной записи компьютера	304
Создание учетной записи компьютера в MMC-консоли	305
Программное создание учетной записи компьютера	312
Удаление компьютера	315
Удаление с помощью мастера	315
Удаление программным способом.....	316
Чтение свойств компьютера	316
Вкладка <i>General</i>	317
Вкладка <i>Operating System</i>	319

Вкладка <i>Member Of</i>	321
Вкладка <i>Delegation</i>	323
Вкладка <i>Location</i>	325
Вкладка <i>Managed By</i>	325
Вкладка <i>Dial-in</i>	326
Публикация компьютера в домене.....	331
РАЗДЕЛ 4. БЕЗОПАСНОСТЬ.....	335
ГЛАВА 12. ИДЕНТИФИКАТОРЫ БЕЗОПАСНОСТИ ACTIVE DIRECTORY	337
Основные термины и понятия	337
Идентификаторы в Active Directory	337
Globally Unique Identifier	338
Структура GUID.....	338
Определение типа GUID	339
Алгоритм создания GUID v.1	339
Получение нового GUID	341
Особенности глобального идентификатора GUID	342
Security Identifier	342
Структура SID	342
Чтение SID из Active Directory	343
Определение SID пользователя с помощью утилиты <i>GetSID</i>	346
Особенности SID.....	347
Широко известные идентификаторы SID.....	348
ГЛАВА 13. ПРОГРАММНОЕ УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ ФАЙЛОВОЙ СИСТЕМЫ.....	355
Основные термины и понятия	355
Виды файловых систем.....	356
FAT	356
HPFS.....	357
VFAT	357
FAT32	357
NTFS.....	358
Главная файловая таблица.....	359
Метафайлы NTFS.....	359
Особенности NTFS	362
Сравнение файловых систем	362
Управление правами доступа на файлы и папки.....	364
Организация доступа к параметрам безопасности	364

Объектная модель NTFS	364
Объектная модель <i>IADsSecurityUtility</i>	365
Методы интерфейса <i>IADsSecurityUtility</i>	366
Свойства интерфейса <i>IADsSecurityUtility</i>	369
Объектная модель <i>IADsSecurityDescriptor</i>	370
Объектная модель <i>IADsAccessControlList</i>	373
Методы интерфейса <i>IADsAccessControlList</i>	374
Свойства интерфейса <i>IADsAccessControlList</i>	380
Объектная модель <i>IADsAccessControlEntry</i>	381
Свойства интерфейса <i>IADsAccessControlEntry</i>	382
Стандартный набор параметров безопасности	387
Технология Access-based Enumerator	388
Установка ABE.....	389
Ограничения технологии ABE	391
Способы настройки ABE	392
Удаление ABE.....	393
Недостатки технологии ABE.....	393
Практика использования ABE	393
РАЗДЕЛ 5. УПРАВЛЕНИЕ КОМПЬЮТЕРОМ.....	395
ГЛАВА 14. РЕЕСТР WINDOWS 2K	397
Основные термины и понятия	397
Историческая справка	397
Основы построения реестра.....	398
Синтаксис REG-файлов.....	400
Редакторы реестра	401
Программное управление реестром.....	402
Управление реестром с помощью WSH	402
Управление реестром с помощью групповых политик	404
Синтаксис ADM-файлов	405
Управление интерфейсом групповых политик.....	410
Примеры использования административных шаблонов на практике	418
ГЛАВА 15. WINDOWS SCRIPT HOST	421
Основные термины и понятия	421
Сервер сценариев Windows Script.....	421
Запуск сценариев WSH из командной строки.....	422
Возможности WSH-сценариев	424
Объектная модель WSH	424

Объект <i>WScript</i>	426
Свойства объекта <i>WScript</i>	426
Методы объекта <i>WScript</i>	430
Объект <i>WshArguments</i>	433
Объект <i>WshShell</i>	433
Метод <i>AppActivate()</i>	435
Управление ярлыками методом <i>CreateShortcut()</i>	436
Свойство <i>Environment</i>	436
Метод <i>ExpandEnvironmentStrings()</i>	441
Метод <i>LogEvent()</i>	441
Метод <i>Popup()</i>	442
Метод <i>Run()</i>	444
Метод <i>SendKeys()</i>	446
Свойство <i>SpecialFolders</i>	448
Объект <i>WshShortcut</i>	450
Создание ярлыка	451
Чтение и изменение свойств ярлыка.....	453
Удаление ярлыка.....	453
Объект <i>WshURLShortcut</i>	454
Объект <i>WshNetwork</i>	455
Методы <i>AddWindowsPrinterConnection()</i> и <i>AddPrinterConnection()</i>	456
Метод <i>RemovePrinterConnection()</i>	458
Метод <i>EnumPrinterConnections()</i>	459
Метод <i>SetDefaultPrinter()</i>	459
Метод <i>MapNetworkDrive()</i>	460
Метод <i>EnumNetworkDrives()</i>	461
Метод <i>RemoveNetworkDrive()</i>	461
Ошибки выполнения сценариев в WSH	461
ГЛАВА 16. ЗАГРУЗКА ОПЕРАЦИОННОЙ СИСТЕМЫ.....	464
Основные термины и понятия	464
Процесс запуска	465
Предварительная загрузка.....	465
Загрузка.....	466
Загрузка ядра	467
Инициализация ядра	467
Регистрация	468
Варианты загрузки операционной системы	468
Безопасный режим	469
Режим протоколирования загрузки.....	470
Режим VGA	470
Загрузка последней удачной конфигурации.....	471

Восстановление службы каталогов	471
Режим отладки	472
Обычный режим.....	472
Файл Boot.ini	472
Компоненты файла Boot.ini	473
ARC-путь	474
Параметры настройки загрузки ОС	475
ГЛАВА 17. ОСОБЕННЫЕ ФАЙЛЫ WINDOWS	486
Основные термины и понятия	486
Файл подкачки	486
Размер файла подкачки	486
Снятие ограничения в 4096 Мбайт на размер файла подкачки.....	487
Размещение файла подкачки	487
Включение нескольких файлов подкачки	488
Файл Autorun.inf.....	489
Синтаксис	489
Пакетный файл.....	493
Различие между BAT и CMD	493
Формальные параметры	493
Команды пакетного файла	494
ГЛАВА 18. WINDOWS INSTALLER.....	502
Основные термины и понятия	502
Пакетная установка программного обеспечения.....	502
Windows Installer	503
Параметры командной строки для Msiexec.....	504
Windows Installer SDK	506
Доступ к MSI-файлам с помощью графической оболочки Orca.exe	506
Структура MSI-файлов	508
Доступ к MSI-файлам программным способом.....	511
Работа с таблицами в Orca.exe.....	511
ПРИЛОЖЕНИЯ	517
ПРИЛОЖЕНИЕ 1. ТАБЛИЦА ASCII	519
Назначение служебных символов	520
Форматирование	521

Передача данных.....	521
Разделительные знаки при передаче информации	522
Другие символы	522
ПРИЛОЖЕНИЕ 2. ИЗМЕРЕНИЯ В БАЙТАХ	524
ПРИЛОЖЕНИЕ 3. СИСТЕМЫ СЧИСЛЕНИЯ.....	525
Десятичная система счисления.....	525
Двоичная система счисления.....	525
Шестнадцатеричная система счисления.....	526
ПРИЛОЖЕНИЕ 4. ПЕРЕМЕННЫЕ СРЕДЫ.....	528
ПРИЛОЖЕНИЕ 5. БУКВЕННЫЕ СОКРАЩЕНИЯ СТРАН.....	531
ПРИЛОЖЕНИЕ 6. ИНТЕГРИРОВАНИЕ СОБСТВЕННЫХ ШАБЛОНОВ В PRIMALSCRIPT	542
ОТВЕТСТВЕННОСТЬ.....	547
ЛИТЕРАТУРА	548
ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ.....	549



Внутреннее устройство каталога Active Directory

В этой главе кратко описываются основы построения Active Directory. Рассматриваются основные службы каталогов, подробно рассказывается об объектах и соответствующих им типах данных. Приводятся нормативные документы, касающиеся структуры каталога Active Directory и основных правил доступа к нему.

Основные термины и понятия

- **Active Directory** — служба каталогов, обеспечивающая централизованное управление сетью. Она содержит информацию об объектах сети и обеспечивает к ней доступ пользователей, компьютеров и приложений в соответствии с установленными правилами безопасности.
- **Глобальный каталог** — централизованное хранилище информации об объектах дерева или домена.
- **Лес** — объединение одного или нескольких деревьев. Деревья в лесу обеспечивают однородный доступ к схеме и правилам совместной работы объектов.
- **Дерево** — группировка или иерархия одного или нескольких доменов Windows 2000, предоставляющих совместный доступ к объектам.
- **Доверительные отношения** — связующее звено между двумя или большим числом доменов. При этом каждый доверяющий домен предоставляет аутентификацию входа в систему доверяемому.
- **Домен (Windows 2000)** — логическая группировка сетевых компьютеров, объединенных общей базой данных каталога, которая содержит учетные записи объектов и правила безопасности.

- ❑ **Контроллер домена** — это компьютер под управлением Windows Server, хранящий реплику раздела каталога.
- ❑ **Пространство имен** — набор правил именования, обеспечивающих иерархическую структуру.
- ❑ **Схема Active Directory** — формальное описание объектов в хранилище Active Directory.

Нормативная документация по Active Directory

Нормативная документация (RFC, Request for Comments) по Active Directory содержит информацию о внутренней структуре каталога и поддерживаемых протоколов (provider); описание типов данных объектов и т. д.

Общие сведения

RFC (Request for Comments, запрос комментариев) — пронумерованный информационный документ, содержащий технические спецификации и стандарты, широко применяемые в сети Интернет. Первый RFC опубликован 7 апреля 1969 г. и называется "Host Software". Несмотря на название, запросы комментариев RFC сейчас рассматриваются как стандарты Интернета.

Согласно RFC 2026, жизненный цикл стандарта выглядит следующим образом. Сначала рассматривается *Черновик* (Internet Draft). Он не имеет официального статуса и удаляется из базы через шесть месяцев после последнего изменения. Затем черновик получает статус *Предложенного стандарта* (Proposed Standard) и свой номер RFC. Наличие программной реализации стандарта желательно, но не обязательно. Следующая стадия — *Черновой стандарт* (Draft Standard). В этот документ могут вноситься незначительные поправки. Высший уровень — *Стандарт Интернета* (Internet Standard). Это спецификации с большим успешным опытом применения. Параллельно с нумерацией RFC такие документы имеют собственную нумерацию STD. Список стандартов имеется в документе STD 1 (RFC 3700). Из более чем трех тысяч RFC этого уровня достигли всего несколько десятков.

Многие старые документы RFC замещены более новыми версиями с измененными номерами или вышли из употребления. Такие документы получают статус *Исторических* (Historic).

RFC — это не только стандарты, но и концепции, введения в новые направления в исследованиях, исторические справки, результаты экспериментов, руководства по внедрению технологий, предложения и рекомендации по развитию существующих стандартов и другие новые идеи в информационных технологиях. Можно условно выделить следующие серии спецификаций:

- ❑ *экспериментальные* (Experimental) спецификации содержат информацию об исследованиях в ИТ-сфере, например, ими могут быть прототипы, реализующие новые концепции;
- ❑ *информационные* (Informational) RFC предназначены для ознакомления общественности. Они не являются ни стандартами, ни результатом консенсуса или рекомендациями. Некоторые черновики, не получившие статуса Предложенного стандарта, но представляющие интерес, могут быть опубликованы как Информационные RFC;
- ❑ серия *лучший современный опыт* (Best Current Practice) содержит рекомендации по реализации стандартов, в том числе от сторонних производителей ПО.

Почти все стандарты разрабатываются под эгидой каких-либо организаций, например, W3C, IETF, консорциума Юникода и др.

RFC по LDAP v2

- ❑ Lightweight Directory Access Protocol (RFC 1777)
- ❑ The String Representation of Standard Attribute Syntaxes (RFC 1778)
- ❑ A String Representation of Distinguished Names (RFC 1779)
- ❑ Using the OSI Directory to Achieve User Friendly Naming(RFC 1781)
- ❑ Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2 (RFC 2559)
- ❑ Lightweight Directory Access Protocol version 2 (LDAPv2) to Historic Status (RFC 3494)

RFC по LDAP v3

- ❑ LDAPv3 Protocol (RFC 2251)
- ❑ LDAPv3 Attribute Syntax Definitions (RFC 2252)
- ❑ LDAPv3 UTF-8 String Representation of Distinguished Names (RFC 2253)

- ❑ LDAPv3 String Representation of LDAP Search Filters (RFC 2254)
- ❑ LDAPv3 URL Format (RFC 2255)
- ❑ A Summary of the X.500(96) User Schema for use with LDAPv3 (RFC 2256)
- ❑ Authentication Methods for LDAP (RFC 2829)
- ❑ LDAPv3 Extension for Transport Layer Security (RFC 2830)
- ❑ LDAPv3 Technical Specification (RFC 3377)
- ❑ IANA Considerations for LDAP (RFC 3383)
- ❑ Lightweight Directory Access Protocol version 3 (LDAPv3): All Operational Attrib (RFC 3673)

Особенности и характеристики Active Directory

Active Directory (AD) — это служба каталогов, обеспечивающая централизованное управление сетью. Она содержит информацию о различных объектах в сети и обеспечивает доступ к ним.

Active Directory обладает следующими особенностями.

- ❑ *Масштабируемость.* В отличие от большинства других баз данных, которые являются реляционными, — Active Directory является иерархической. В реляционных базах данных взаимосвязи между записями формируются с помощью ключей, которые хранятся совместно с данными. В иерархической базе данных взаимосвязи между записями имеют характер "родитель-потомок": все записи, за исключением корневой, обладают родительской записью. У каждой родительской записи может быть один или несколько потомков. Иерархическая база данных позволяет хранить большое количество объектов, при этом обеспечивается быстрый доступ к необходимым объектам.
- ❑ *Поддержка открытых стандартов.* Active Directory включает в себя концепцию пространства имен Интернета со службой каталогов Windows NT, что позволяет объединять и управлять различными пространствами имен в разноразрядных аппаратных и программных средах. Для управления пространством имен Active Directory используется библиотека интерфейса службы активного каталога (Active Directory Service Interface — ADSI).

- *Поддержка стандартных форматов имен.* Active Directory поддерживает несколько форматов имен и позволяет приложениям и пользователям получать доступ к каталогу, применяя наиболее удобный для них формат (табл. 1.1).

Таблица 1.1. Форматы имен, используемые в Active Directory

Формат	RFC	Описание
UPN	RFC 822	Формат основного имени пользователя (User Principal Name, UPN). UPN-имена известны как адреса электронной почты. Active Directory обеспечивает "дружественные" имена в этом формате. В качестве имени для регистрации в сети пользователь может использовать как имя учетной записи SAM, так и имя в формате RFC 822. Пример: Pivanov@Island.ru
RDN (LDAP)	RFC 1779, RFC 2247	Имена в формате LDAP URL, также называемые RDN-именами (Relative Distinguished Name), имеют более сложную структуру по сравнению с UPN-именами. Имена LDAP в формате RDN состоят из нескольких частей: <ul style="list-style-type: none"> • CN расшифровывается как Common Name (общее имя); • OU означает организационную единицу (Organization Unit); • DC — класс объекта домена (Domain Object Class). Часть имени "DC=" обеспечивает подключение к виртуальному объекту RootDSE, с помощью которого осуществляется подключение к домену. Пример: LDAP://ISLAND.RU/CN=Pivanov,OU=WorkSpace или LDAP://CN=Pivanov,OU=WorkSpace,DC=Island,DC=ru
UNC	RFC 1123	UNC (Universal Naming Convention) имеет вид Hoda.Island.ru/WorkSpace/Pivanov. (Здесь Hoda — это имя контроллера домена.) В Active Directory данный формат является путем к объекту в иерархической структуре

Active Directory как часть файловой системы

База данных Active Directory по умолчанию хранится на контроллере домена (%WinDir%\System32) в файле Ntds.dit.

База данных имеет следующие особенности:

- ❑ размер файла Ntds.dit увеличивается фиксированными порциями, занимая отдельные страницы, что позволяет избежать их разбиения. Поэтому при добавлении объектов размер базы данных Active Directory кажется больше, чем он есть на самом деле;
- ❑ файлы базы данных Active Directory всегда открыты;
- ❑ размер открытого файла не обновляется. Фактический размер базы данных определяют по отображаемому свободному пространству на диске;
- ❑ в подключенном состоянии база данных не может быть дефрагментирована с помощью утилиты ntdsutil.exe.

Архитектура службы каталогов Active Directory

Чтобы понять, как хранятся и обрабатываются данные в Active Directory, необходимо знать порядок взаимодействия ее компонентов. Службу каталогов можно представить в виде многоуровневой структуры (рис. 1.1).

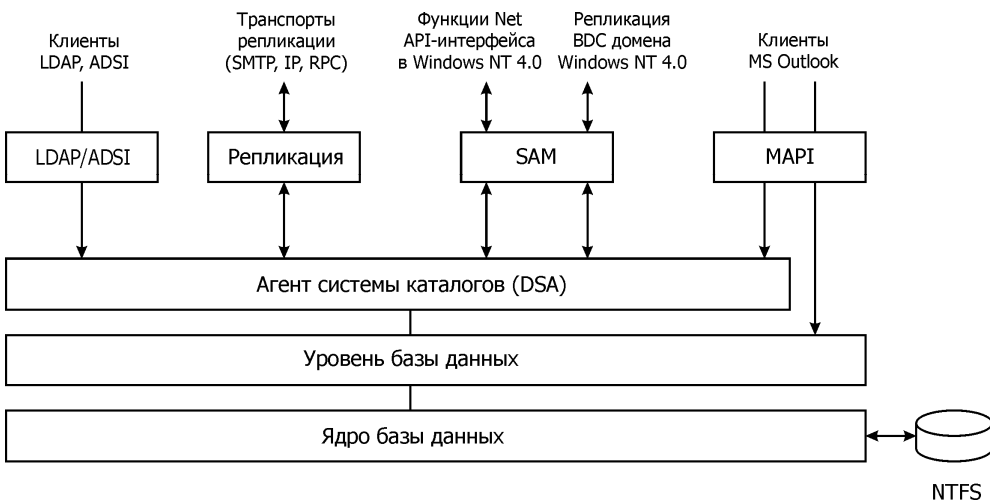


Рис. 1.1. Многоуровневая структура службы каталогов

DNS и Active Directory

Для иерархического именования доменов и компьютеров в Active Directory используется служба DNS (Domain Name System), поэтому объекты доменов и компьютеров являются частью иерархии доменов DNS и Active Directory. Несмотря на то, что имена в обеих системах идентичны, они относятся к разным пространствам имен. Взаимодействие DNS-имен доменов и их IP-адресов в Active Directory реализовано в соответствии с общепринятыми соглашениями об именовании в DNS.

Domain Name System — иерархическая система именования, которая используется для идентификации хостов. Основная функция DNS заключается в прямом и обратном разрешении имен компьютеров в IP-адреса.

База данных DNS представляет собой древовидную структуру, называемую пространством имен доменов (domain name space).

В Windows 2000 полное доменное имя (Fully Qualified Domain Name, FQDN) компьютера состоит из двух частей (рис. 1.2):

1. Имя DNS-узла. Крайняя левая часть FQDN — это полноценное имя DNS-узла, идентифицирующее учетную запись компьютера, хранящуюся в Active Directory. Кроме того, это имя локальной учетной записи компьютера в диспетчере безопасности учетных записей (Security Account Manager, SAM) на рабочей станции или рядовом сервере (не на контроллере домена). По умолчанию имя DNS-узла также используется в качестве NetBIOS-имени. Это делается для совместимости с доменами на основе Windows NT и с рабочими станциями под управлением Windows 9x.
2. Основной суффикс имени DNS домена. По умолчанию — это домен Windows, к которому относится данный компьютер.



Рис. 1.2. Схема образования полного доменного имени (FQDN)

Кроме DNS-имен компьютеров, контроллеры домена Active Directory идентифицируются по видам предоставляемых ими служб: серверы протокола

LDAP (Lightweight Directory Access Protocol); контроллеры доменов; сервер глобального каталога GC (Global Catalog). Получив указание на имя домена и службу, DNS-сервер ищет контроллер со службой нужного типа в данном домене.

Службы каталогов Active Directory

Существует несколько уровней служб, интерфейсов и протоколов, которые образуют полный спектр служб для управления каталогом. Три уровня служб содержат все данные для нахождения записей в базе данных каталога. Выше уровня служб находятся протоколы и API-интерфейсы, обеспечивающие взаимодействие при репликации или между клиентами и службами каталогов. Репликация выполняется между службами каталогов.

Основные службы-компоненты Active Directory (см. рис. 1.1):

- ❑ *агент системы каталогов* (Directory System Agent, DSA) формирует иерархию каталога на основе отношений "родитель-потомок" и обеспечивает интерфейс прикладного программирования (Application Programming Interface, API) для запросов на доступ к каталогу;
- ❑ *уровень базы данных* — промежуточный уровень абстракций между базой данных и приложениями;
- ❑ *ядро базы данных* (Extensible Storage Engine, ESE), работающее непосредственно с записями хранилища каталогов, различает объекты по атрибуту относительно составного каталога;
- ❑ *хранилище данных* — файл базы данных Ntds.dit. С этим файлом работает только ядро базы данных. Обращаться напрямую к нему можно с помощью программы ntdsutil.exe, которая находится в папке Support/Tools на диске с дистрибутивом операционной системы Windows 200x Server.

Клиенты могут получить доступ к Active Directory, используя один из следующих механизмов:

- ❑ LDAP/ADSI — клиенты, поддерживающие протокол LDAP (Lightweight Directory Access Protocol), используют его для доступа к агенту системы каталогов. Интерфейсы службы каталогов Active Directory (Active Directory Service Interface — ADSI) служат для абстрагирования от LDAP интерфейса прикладного программирования (API), представляя COM-

интерфейсы для взаимодействия с Active Directory. Однако нужно помнить, что в Active Directory используется только LDAP;

- ❑ MAPI — при обмене сообщениями и коллективной работе клиенты MS Outlook подключаются к агенту системы каталогов, используя механизм вызова удаленных процедур MAPI (Messaging Application Programming Interface) посредством интерфейса доступа к адресной книге;
- ❑ SAM — клиенты MS Windows NT 4.0 и более ранних версий, Windows 9x подключаются к агенту системы каталогов (DSA) через SAM (Security Account Manager);
- ❑ REPL — в процессе репликации каталогов агенты системы каталогов (DSA) Active Directory взаимодействуют через интерфейс RPC (Remote Procedure Call).

Существуют четыре способа доступа к Active Directory (см. рис. 1.1). С точки зрения программного управления Active Directory, системного администратора интересует только ADSI. ADSI поддерживает такие языки программирования, как C/C++, VB/VBScript, JScript, WSH. Он представляет объекты Active Directory в виде COM-объектов, а управление осуществляется с помощью COM-интерфейсов. Провайдеры ADSI отображают объекты ADSI в соответствующие пространства имен, то есть они преобразуют вызовы COM-интерфейсов к запросам API конкретной службы каталогов.

Глобальный каталог

Глобальный каталог (Global Catalog, GC) — это контроллер домена, в котором существуют три доступных для записи раздела: хранилища домена, схемы и конфигурации (листинг 1.1 и рис. 1.3). Каталог автоматически создается при репликации Active Directory. Все разделы каталогов на сервере глобального каталога хранятся в одной базе данных каталога Ntds.dit. Глобальный каталог хранит сведения обо всех лесах, поэтому его можно использовать для поиска любых объектов в лесу без переадресации на другие серверы. Если запрос осуществляется по порту 389 (стандартный порт протокола LDAP), то в случае неудачного поиска запрос будет последовательно передаваться другим контроллерам домена. Если обращение идет по стандартному порту глобального каталога (GC) 3268, то поиск осуществляется по всем разделам

леса. Для безопасного доступа к службам следует использовать порты, применяющие SSL (табл. 1.2).

Таблица 1.2. Описание портов, поддерживаемых ADSI

Порт	Описание
389	Порт для открытых запросов LDAP
636	Порт для запросов LDAP с использованием протокола SSL
3268	Порт для открытых запросов GC
3269	Порт для запросов GC с использованием протокола SSL

Листинг 1.1. Получение имени глобального каталога

```
temp = ""  
Set obj = GetObject("GC:")  
For Each el In obj  
    temp = temp & el.name  
Next  
MsgBox temp
```



Рис. 1.3. Определение доступных имен глобального каталога

Сценарий определения имени глобального каталога, приведенный в листинге 1.1, работает по следующему алгоритму: в первой строке неявно объявляется пустая переменная `temp`, в которую будут накапливаться доступные имена глобального каталога. Затем с помощью функции `GetObject()` получают доступ к глобальному каталогу с помощью провайдера GC. С третьей по пятую строку осуществляется считывание доступных пространств имен глобального каталога. На последней строке с помощью команды `MsgBox` осуществляется вывод информации на экран.

Провайдеры ADSI

Интерфейс ADSI поддерживает несколько провайдеров, позволяющих осуществлять программное администрирование. Их список приведен в табл. 1.3.

Таблица 1.3. Поддерживаемые ADSI-провайдеры

Название	Протокол	Описание
LDAP Provider	"LDAP:"	Администрирование Active Directory, Microsoft Exchange Server
WinNT Provider	"WinNT:"	Администрирование Windows NT, Windows 200x, Windows XP
NDS Provider	"NDS:"	Администрирование Novell NetWare Directory Service
NWCOMPAT	"NWCOMPAT:"	Администрирование Novell NetWare 3.1
IIS	"IIS:"	Протокол IIS предназначен для управления WWW- и FTP-узлами по протоколу HTTP

В зависимости от установленных на сервере компонентов список доступных провайдеров может отличаться от приведенного в табл. 1.3. Для определения всех доступных провайдеров в сети используют службу ADs. С помощью функции `GetObject()` получают доступ к коллекции провайдеров (листинг 1.2 и рис. 1.4).

Листинг 1.2. Определение доступных в домене служб ADs

```
temp = ""
Set obj = GetObject("ADs:")
For Each el In obj
    temp = temp & el.name & vbNewLine
Next
MsgBox temp
```

Из всех перечисленных провайдеров мы рассмотрим только LDAP. Провайдер LDAP выполняется на клиенте ADSI и обеспечивает доступ к Active Di-

rectory. Кроме служб каталогов Active Directory Windows 2k, провайдер LDAP обеспечивает доступ к Microsoft Exchange Server, Microsoft Commercial Internet System (MCIS) Address Book Server и т. д.



Рис. 1.4. Доступные в домене службы ADs

Для программного управления Active Directory чаще всего используется именно LDAP. В качестве языка программирования обычно выбирают VBScript. Компания Microsoft специально для этих целей разработала язык программирования и интегрировала его во все современные версии Windows. В настоящее время появился альтернативный инструмент — командная оболочка PowerShell.

Схема объектной модели ADSI

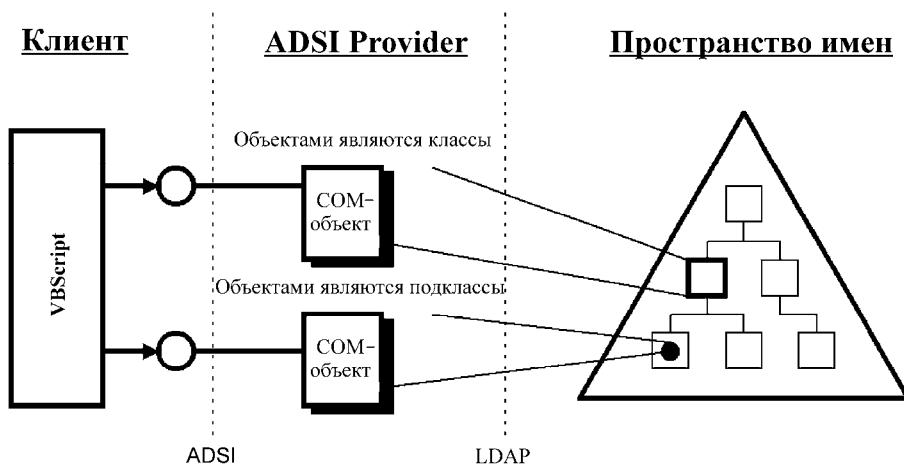


Рис. 1.5. Схема объектной модели ADSI

Схема объектной модели ADSI состоит из трех частей (рис. 1.5). Используя клиент — язык программирования, — сценарий получает доступ к COM-объектам. Объекты могут быть классами или подклассами. Взаимодействие между ними не показано, чтобы не загромождать рисунок. С помощью COM-объекта через протокол LDAP сценарий получает доступ к указанному объекту доступного пространства. Пространство имен условно обозначено треугольником; квадратами обозначены классы, а подклассы — кругами.

Объекты в Active Directory

Доступ к объектам Active Directory

Доступ к объектам Active Directory можно получить с помощью семейства интерфейсов IADs* (листинг 1.3а) или ADODB-соединения (листинг 1.3б). В зависимости от поставленных задач необходимо использовать тот или иной способ.

Листинг 1.3а. Шаблон использования функции GetObject ()

```
'Использование функции GetObejct ()
Set obj = GetObject ("LDAP://PATH_TO_OBJECT")
MsgBox obj.PROPERTY
```

Листинг 1.3б. Шаблон использования ADODB-соединения

```
'Создание ADODB-соединения
Set objConn = CreateObject ("ADODB.Connection")
Set objCom = CreateObject ("ADODB.Command")
objConn.Provider = "ADsDSOobject"
objConn.Open "Active Directory Provider"
Set objCom.ActiveConnection=objConn
'составление и обработка SQL-запроса
Query = "SELECT PROPERTY FROM 'LDAP://PATH_TO_OBJECT'"
Set st = objConn.Execute(Query)
'Вывод результата типа данных переменной
MsgBox = st.Fields ("PROPERTY").Value
```