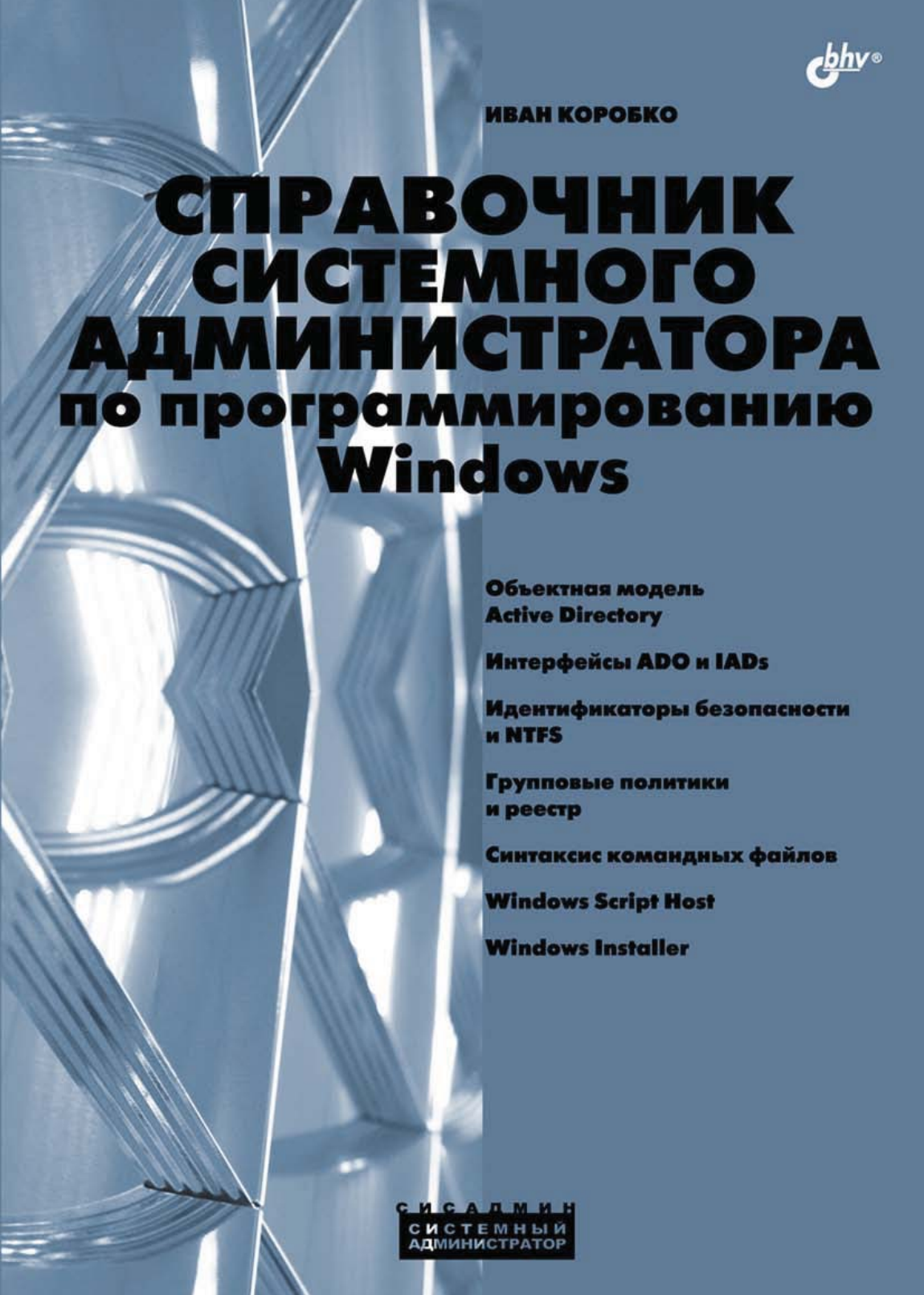

bhv

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

СИСАДМИН
СИСТЕМНЫЙ АДМИНИСТРАТОР

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	*Екатерина Кондукова*
Зам. главного редактора	*Игорь Шишигин*
Зав. редакцией	*Григорий Добин*
Редактор	*Юрий Якубович*
Компьютерная верстка	*Натальи Смирновой*
Корректор	*Наталия Першакова*
Дизайн серии	*Инны Тачиной*
Оформление обложки	*Елены Беляевой*
Зав. производством	*Николай Тверских*

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

Оглавление

ГЛАВА 1

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 бóльшим 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 Principial 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: • 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).

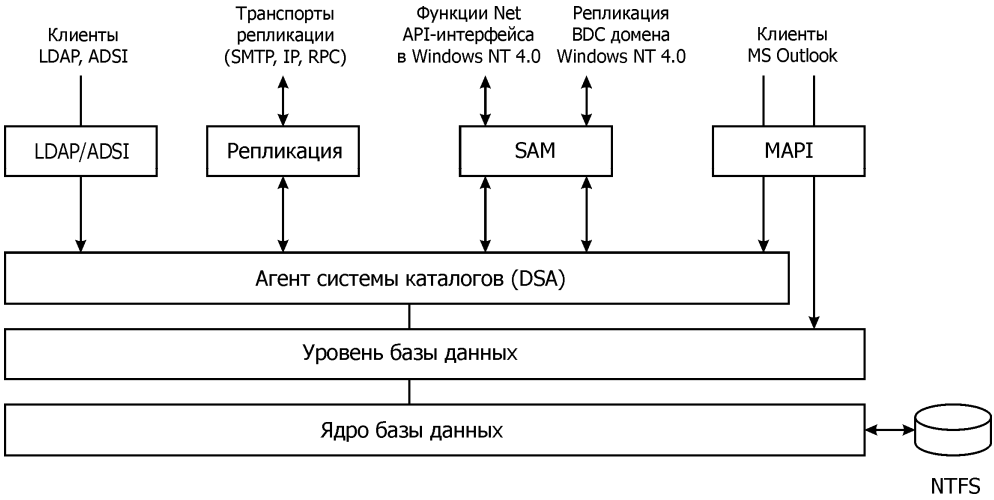

Рис. 1.1. Многоуровневая структура службы каталогов

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 9*x*.
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 Interfece, 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, поддерживающихся 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
```

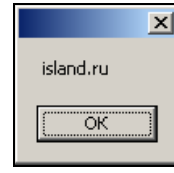

Рис. 1.3. Определение доступных имен глобального каталога

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.

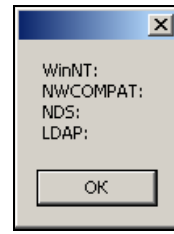

Рис. 1.4. Доступные в домене службы ADs

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

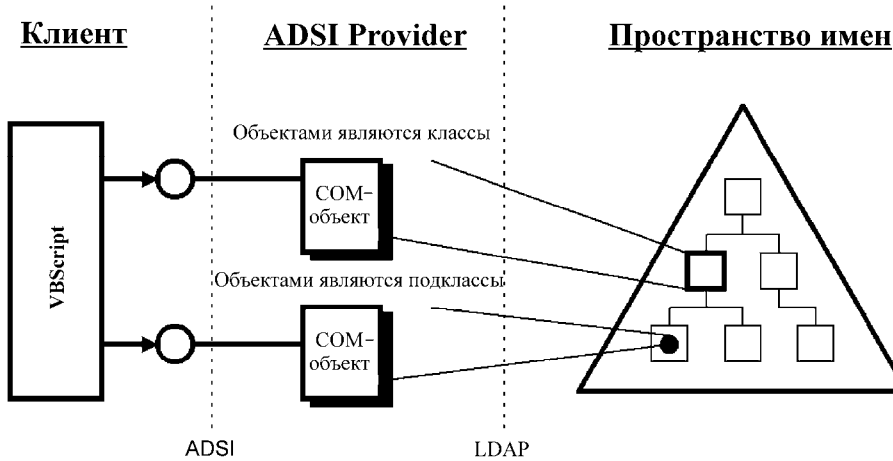

Рис. 1.5. Схема объектной модели ADSI

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
```