С Ж Л

Д Т

2 = Л

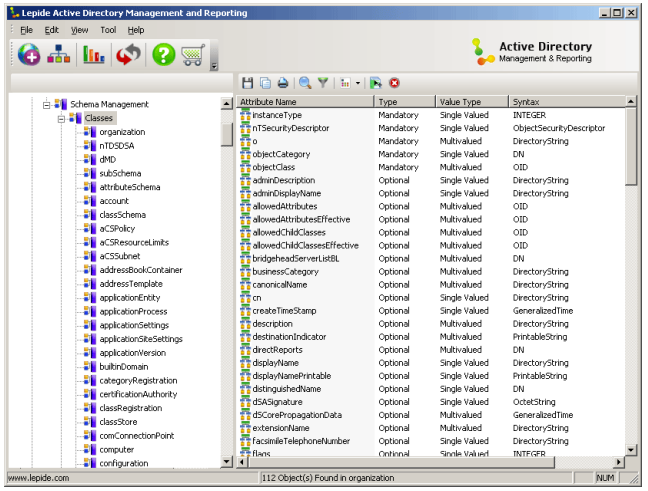
Active Directory Windows Server 2008 R2

- Предлагаемые Microsoft технологии Active Directory прошли длинный путь с того момента когда впервые появились в версии Windows 2000 Server. Из одного продукта, называвшегося просто Active Directory (AD), в Windows Server 2008 R2 они превратились в пять отдельных технологий.

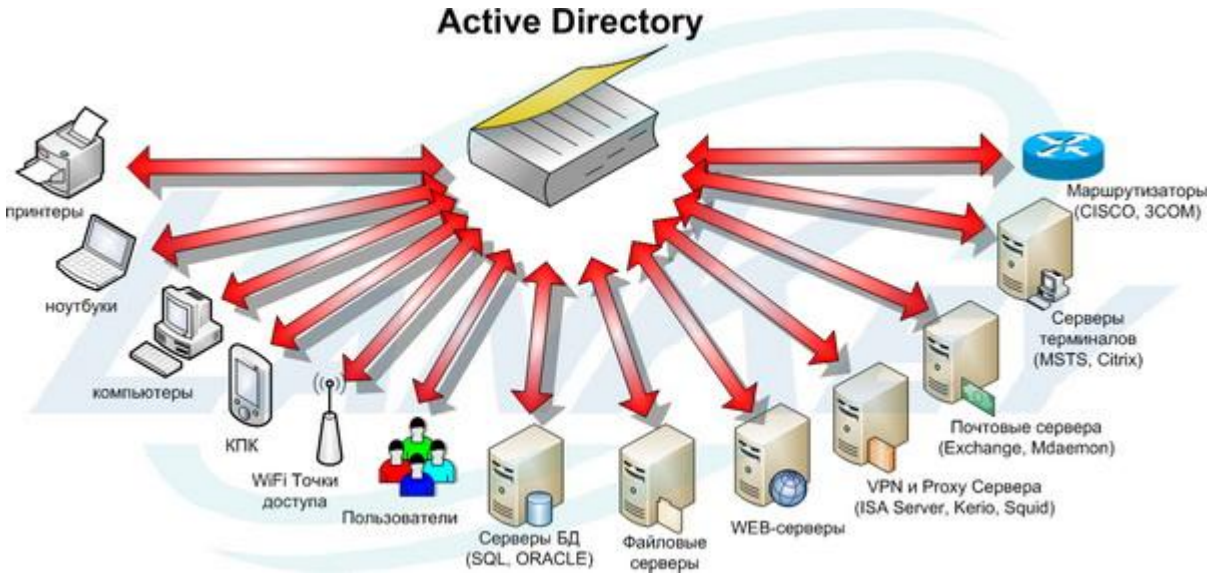
- **Active Directory Lightweight Directory Services — AD LDS** (Службы Active Directory облегченного доступа к каталогам)
- **Active Directory Federation Services — AD FS** (Службы федерации Active Directory)
- **Active Directory Certificate Services — AD CS** (Службы сертификатов Active Directory)
- **Active Directory Rights Management Services — AD RMS** (Службы управления правами Active Directory)

Эволюция служб каталогов

- Службы каталогов в той или иной форме существовали с самого начала эпохи компьютеров — они предназначались для обычного поиска файлов и для аутентификации в производственных сетевых реализациях.



- Служба каталогов **предоставляет подробную информацию о пользователях и об объектах сети**, примерно так же, как телефонная книга позволяет найти номер телефона по известной фамилии.



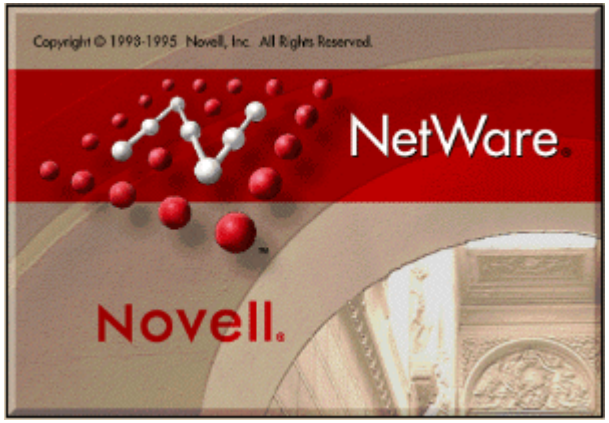
Службы каталогов обеспечивают определение и администрирование пользователей и объектов.

- Первые электронные каталоги были созданы вскоре после изобретения цифровых компьютеров и применялись для аутентификации пользователей и управления доступом к ресурсам.
- С расширением сети Интернет и увеличением совместного использования компьютеров в функции каталогов было включено хранение основной контактной информации о пользователях.

- Вскоре появились специализированные службы каталогов для приложений, **предназначенные для специальной адресации, поиска и ведения контактной информации для каждого программного продукта.** Доступ к таким каталогам был возможен только с помощью специальных методов, а область их применения была ограниченной.
- Приложениями, использующими эти типы каталогов, были такие программы, как **Novell GroupWise**, **Lotus Notes** и файл **/etc/aliases** утилиты **sendmail** в UNIX.

Дальнейшее развитие крупномасштабных служб каталогов для предприятий возглавила компания **Novell**, выпустив в начале девяностых годов прошлого века службу каталогов **Novell (Novell Directory Services — NDS)**

Она была принята организациями **NetWare**, а затем расширена за счет включения поддержки смешанных сред **NetWare/NT**.



Разработка облегченного протокола доступа к каталогам (**Lightweight Directory Access Protocol — LDAP**) была вызвана расширением Интернета и необходимостью более тесного взаимодействия и строгой стандартизации.

Этот общепринятый метод доступа к информации каталогов и ее модификации, **пользующийся всеми возможностями протокола TCP/IP, оказался надежным и функциональным,** и для его применения были разработаны новые реализации служб каталогов.

Сама служба AD DS разрабатывалась так, чтобы соответствовать стандарту LDAP.

Обзор первоначальных систем управления каталогами Microsoft

- В системе Exchange Server 5.5 существовала собственная служба каталогов, которая запускалась в виде части среды обмена электронными сообщениями.

Собственные службы каталогов существовали и в ряде других приложений Microsoft, например, в **Internet Information Server** (Сервер информации Интернета) и **Site Server** (Сервер сайтов).

Однако каждая из этих служб каталогов никак не соотносилась с другими, к тому же степень интеграции между различными реализациями была не очень высокой.

Ключевые функциональные возможности Active Directory Domain Services

- **Совместимость с TCP/IP.** В AD DS и Windows Server 2008 R2 в качестве главного метода для обмена данными используется именно стек протоколов TCP/IP.

Поддержка протокола LDAP (Lightweight Directory Access Protocol — облегченный протокол доступа к каталогам). Протокол LDAP был разработан в качестве стандартного Интернет-протокола для доступа к каталогам. Он применяется при обновлении и запросах данных, хранящихся в каталогах. В AD DS протокол LDAP поддерживается напрямую.

Поддержка системы доменных имен. Система доменных имен (Domain Name System — DNS) была создана для удовлетворения потребности в преобразовании упрощенных имен, понятных людям в IP-адреса, понятные компьютерам (вроде 12.155.166.151). В AD DS она не просто поддерживается, а даже требуется для нормальной работы.

Поддержка безопасности

- Поддержка безопасности в соответствии со стандартами Интернета чрезвычайно важна для бесперебойного функционирования среды, которая, по сути, подключается к миллионам компьютеров по всему миру. Нехватка надежных средств защиты служит своего рода приглашением для хакеров, поэтому в Windows Server 2008 R2 и AD DS возможности для обеспечения безопасности были значительно расширены.
- Так, в Windows Server 2008 R2 и AD DS была встроена непосредственная поддержка для IPSec, Kerberos, центров сертификации и шифрования с помощью протокола защищенных сокетов (Secure Sockets Layer — SSL).

- **Удобное администрирование.** Хотя при реализации мощных служб каталогов удобству администрирования и конфигурирования среды часто не уделяется должного внимания, этот аспект очень сильно влияет на общую стоимость эксплуатации сред.
- В **AD DS и Windows Server 2008 R2** было специально все продумано так, чтобы ими было удобно пользоваться, и чтобы на освоение новой среды тратилось как можно меньше усилий.
- В **Windows Server 2008 R2 улучшены** возможности для администрирования AD DS за счет добавления компонента Active Directory Administration Center (Центр администрирования Active Directory), компонента Active Directory Web Services (Веб-службы Active Directory) и модуля для администрирования Active Directory из оболочки Windows PowerShell.

Процесс развития AD DS

Впервые появившаяся в Windows 2000 Server как замена для доменов Windows NT 4.0 и (тогда называвшаяся просто AD), технология AD DS позже была значительно улучшена в Windows Server 2003 и Windows Server 2003 R2 Edition.

Она очень быстро получила широкое признание в промышленных кругах и зарекомендовала себя в качестве **надежной, масштабируемой и высокопроизводительной системы.**

- Появление AD DS позволило избавиться от некоторых ограничений, присущих схемам с доменами NT 4.0, а также обеспечить возможность интеграции будущих продуктов производства Microsoft и других производителей в один общий интерфейс.

Признание компанией Microsoft стандартов Интернета

- Разрабатывая Windows Server 2000/2003, а затем и Windows Server 2008 R2, в Microsoft всегда стремились к тому, чтобы все их программные продукты поддерживали стандарты Интернета.

С выходом Windows Server 2008 R2 готовность среды Microsoft к взаимодействию с Интернетом достигает новых уровней функциональности, благодаря **добавлению следующих улучшений**:

- восстановление удаленных объектов с помощью корзины Active Directory (Active Directory Recycle Bin);
- присоединение к домену в автономном режиме (Offline Domain Join);
- применение управляемых учетных записей служб (Managed Service Accounts);
- настройка множества политик паролей для каждого домена;
- создание контроллеров домена с доступом только для чтения (Read-Only Domain Controller — RODC);
- запуск и останов AD на контроллере домена (DC); ведение учета изменений, которые вносятся в объекты AD.

T,,

4 = О

3

b

2,

'Bdb

4 = Л

„ 

ЬТЁ

1 = С

З

3

1 = Н

Ч