Современные компьютерные сети крупных компаний все больше зависят от эффективной работы службы каталогов, которая является ядром этой сети, предоставляя хранилище для пользовательских и компьютерных объектов, инструменты для их централизованной настройки, а также множество возможностей для интеграции с другими корпоративными программными продуктами. Для того чтобы грамотно спланировать и развернуть службу каталогов в своей среде необходимо хорошо представлять себе, как она функционирует изнутри и какие механизмы и логика работы заложены в её основу. В связи с этим, в данной работе рассмотрена одна из наиболее популярных на сегодня служб каталогов - Microsoft Active Directory Service, который является качественным переходом в истории развития этого программного обеспечения. При переходе с Windows NT 4.0 на Windows 2000, служба каталогов Microsoft вплотную подобралась к тому, чтобы называться распределенной системой. Как известно, фундаментальный принцип распределенных систем гласит для пользователя распределённая система должна выглядеть так же, как нераспределённая система. Если в Windows NT 4.0 в распоряжении администратора была возможность создать лишь один Основной контроллер домена, для которого остальные выступали резервными, то в Windows 2000 появилась возможность создания любого количества контроллеров домена, каждый из которых может вносить изменения в базу данных Active Directory. И хотя некоторые специфические процессы, обеспечивающие работу службы каталогов, всё ещё требуют определения в сети мастера, отвечающего за конкретную операцию, мы уже можем, в некотором приближении, назвать службу каталогов Microsoft Active Directory распределенной системой.[1] При просмотре содержимого службы каталогов Active Directory мы видим (рис. 1) иерархическую структуру подобную той, что используется файловой системой - родительские и дочерние контейнеры, содержащие некоторый набор объектов. Физически же, на диске, база Active Directory хранится в виде файла. Рис. 1 - Оснастка Active Directory Users and Computers Рассмотрим, какие механизмы используются системой, для того чтобы получить такое представление данных. Логическая организация Технология хранения данных в Active Directory представлена несколькими компонентами, предоставляющими различные интерфейсы, используемые другими прикладными системами. Рассмотрим их по порядку Агент службы каталогов DSA. Это агент, работающий на всех контроллерах доменов представленный библиотекой ntdsa.dll, который предоставляет доступ к базе данных службы каталогов. Сам агент работает как часть системного процесса lsass.exe, который управляет аутентификацией пользователей и служб. Именно этот агент отвечает за такие процессы, как репликация, иерархическое представление информации хранимой в Active Directory, доступ к данным с использованием нескольких предлагаемых интерфейсов и протоколов. Служба каталогов Active

Directory даёт возможность получить доступ к данным в своем хранилище с использованием таких протоколов как LDAP, RPC и SMTP. Рассмотрим подробнее каждый из протоколов. LDAP - основной протокол для работы с Active Directory. Клиенты используют протокол LDAP v3 для подключения к агенту службы каталогов через интерфейс LDAP. Третья версия протокола обратно совместима со второй, которая широко применялась ранее. REPL - управляющий протокол, который используется для поиска информации о контроллерах доменов, преобразования имен сетевых объектов в разные форматы, работы с SPN и управления репликацией данных между серверами. MAPI - протокол для служб сообщений. Этот интерфейс используется для предоставления доступа к данных в Active Directory службам сообщений по стандартному для них протоколу. В связи с тем, что компания Microsoft прекратила дальнейшую разработку этого протокола, на данный момент он оставлен для обратной совместимости со старыми клиентами Microsoft Outlook. SAM - проприетарный протокол Microsoft для взаимодействия со старыми версиями Windows. Интерфейс SAM используется операционными системами Windows NT 4.0 и более ранними версиями, для взаимодействия с агентом DSA. Также этот интерфейс необходим для репликации данных Active Directory на резервные контроллеры домена, работающие под управлением Windows NT 4.0 LDAP выступает не только одним из протоколов службы каталогов. Операции над базой данных, также основаны на модели LDAP. Эта функциональная модель включает в себя такие стандартные операции, как подключение к базе, поиск данных и изменение данных. Таким образом, Active Directory поддерживает подключение к базе с помощью любых LDAP клиентов. Например, встроенной оснастки ADSI Edit (рис. 2). Рис. 2 - LDAP представление Active Directory Служба каталогов крупной компании может хранить сотни тысяч и даже миллионы объектов и включать в себя десятки контроллеров домена. Для того чтобы оптимизировать хранение таких объёмов данных в распределённой системе Active Directory использует множество различных механизмов. Прежде всего, данные в службе каталогов разбиты на разделы. Каждый контроллер хранит не все данные службы каталогов, а лишь те, что нужны ему для эффективного обслуживания своего сегмента сети. Для того чтобы распределить данные по разделам объекты категоризируются согласно схеме именования. Каждый контроллер хранит раздел, который содержит информацию об объектах его собственного домена - его пользователей, группы и организационные единицы. Кроме того, каждый контроллер домена хранит два служебных раздела общих для всех контроллеров в рамках одного «леса» - схему и раздел конфигурации. В качестве дополнительных разделов выступают, так называемые разделы приложений. В этих разделах могут хранить свои данные приложения, которые поддерживают интеграцию со службой каталогов, такие как, например, реализация службы DNS от Microsoft. Хранение всех дополнительных разделов

может быть настроено администратором сети в зависимости от потребностей в конкретном сегменте сети и от её пропускной способности. В отличие от реализаций служб каталогов других разработчиков, Microsoft Active Directory является плоской базой, и администратор не может создавать разделы для частичного хранения данных одного домена. В качестве инструмента масштабирования Microsoft предлагает использовать домен, как наименьшую структуру хранения данных. Физическая организация На физическом уровне хранилище данных Active Directory представлено в виде файла (Ntds.dit), содержащего саму таблицу данных и таблицу ссылок и файлов логов (EDB.log, RES1.LOG, RES2.LOG). Файлы логов используются для того, чтобы реализовать принцип атомарности транзакций. Каждая транзакция либо выполняется целиком, либо не выполняется вообще. Для того чтобы достичь этого, во-первых, операция всегда выполняется только над одним объектом, а во- вторых, транзакция сначала выполняется над копией объекта в памяти, затем записывается в лог откуда потом будет обработана внутренними механизмами базы данных. Файл Ntds.dit содержит все разделы службы каталогов. Строками в этой таблице являются объекты, а столбцами - атрибуты в соответствии со схемой. Для оптимизации размера базы, служба каталогов выделит под хранение каждого объекта лишь тот объём памяти, который он уже использует (например, для пользователя, чьё поле описание содержит на 10 символов меньше, чем у остальных, объем выделенной памяти также будет меньше). Все объекты хранятся в страницах памяти размером 8 Кб. Данные в этих страницах упорядочены. То есть, при добавлении объекта, который должен храниться на определенной странице, система не может поместить его на другую страницу в случае нехватки свободного объема памяти. Вместо этого будет выделена новая страница, в которую и будет помещен объект. При удалении объектов данные не вычищаются из таблицы сразу, а лишь помечаются системой для последующего удаления. Такой подход к хранению обеспечивает максимальные скорости поиска и добавления данных, однако он не очень эффективно использует свободное место. Для решения этой проблемы существуют процессы онлайн и оффлайн дефрагментации базы данных. Эти процессы реорганизуют расположение данных в таблице для корректного использования дискового пространства. Заключение Подобный подход к хранению данных службой каталогов не является единственным. Другие производители программного обеспечения используют иные технологии в своих продуктах. В качестве вывода можно отметить, что способ реализации хранения данных выбранный Microsoft для службы каталогов Active Directory обеспечивает высокую эффективность при выполнении стандартных операций, а также позволяет осуществлять ее ежедневную поддержку инженерам без большого опыта работы или высокой квалификации. Однако подобное решение имеет и свои минусы. Возможность масштабирования и разделения данных должна быть предусмотрена на этапе

планирования доменной инфраструктуры. Если есть возможность разрастания определенной части базы данных, имеет смысл предусмотреть выделение её в отдельный домен, для эффективности хранения. Если это не было сделано на этапе планирования, то единственным выходом остается реструктуризация службы каталогов с выделением новых доменов. Таким образом, возникает потребность в высококвалифицированном персонале на этапе планирования внедрения службы, либо при необходимости её реструктуризации.