

Удаленное администрирование

Для чего могут понадобиться такие программы? В большинстве случаев они используются для удаленного доступа к рабочему столу и действий для обслуживания компьютера системными администраторами и в сервисных целях.

Протокол удаленного рабочего стола, или RDP, позволяет получать удаленный доступ к компьютерам. На протяжении долгого времени RDP обеспечивает постоянно улучшающуюся поддержку удаленного доступа.

Впервые эта технология была представлена в 1998 для Windows NT 4.0 Terminal Server Edition (TSE) и с тех пор стала появляться практически в каждой новой версии Windows. Начиная с Windows 2000, практически любой мог легко получить удаленный доступ к серверной системе, поскольку службы терминалов были представлены в качестве дополнительного компонента Windows и могли настраиваться так, что систему можно было использовать либо как фактическую службу терминалов, либо как то, что мы сегодня называем удаленным рабочим столом.

В Windows Server 2003 и Windows XP была предоставлена собственная функция удаленного рабочего стола, позволяющая контролировать систему, как если бы вы сами находились в ней. В Windows XP и более поздних версиях Windows был добавлен удаленный помощник, работа которого схожа с функциями удаленного рабочего стола, но который разработан для локального пользователя, запрашивающего поддержку удаленного пользователя.

Active Directory- системные администраторы используют технологию Active Directory в Windows Server для хранения и организации объектов в сети в иерархическую защищенную логическую структуру, например пользователей, компьютеров или других физических ресурсов.

Лес и домен составляют основу логической структуры. Домены могут быть структурированы в лесу, чтобы обеспечить независимость данных и сервисов (но не изоляцию) и оптимизацию репликации. Разделение логических и физических структур улучшает управляемость системы и снижает административные затраты, потому что на логическую структуру не влияют изменения в физическом устройстве. Логическая структура позволяет контролировать доступ к данным, т.е. вы можете использовать логическую структуру для контроля доступа к различным блокам данных.

Данные, хранящиеся в Active Directory, могут поступать из разных источников. С большим количеством различных источников данных и множеством различных типов данных Active Directory должен использовать некоторый стандартизованный механизм хранения, чтобы поддерживать целостность хранящейся информации.

В Active Directory объекты используют каталоги для хранения информации, все объекты определены в схеме. Определения объектов содержат информацию, такую как тип данных и синтаксис, которую каталог использует, чтобы гарантировать достоверность хранения. Никакие данные не могут быть сохранены в каталоге, пока они не определены в схеме. Схема по умолчанию содержит все определения и описания объектов, которые необходимы для корректной работы Active Directory.

Когда вы имеете доступ к каталогу через логическую структуру, состоящую из таких элементов, как домены и леса, сам каталог реализуется через физическую структуру, состоящую из базы данных, которая хранится на всех контроллерах домена в лесу.

Хранилище Active Directory обрабатывает весь доступ к БД. Хранилище данных состоит из служб и физических файлов, которые управляют правами

доступа, процессами чтения и записи данных внутри базы данных на жестком диске каждого контроллера.

Структура и архитектура хранилища Active Directory состоит из четырех частей:

Домены и леса

Леса, домены и организационные единицы (OU) составляют основные элементы логической структуры Active Directory. Лес определяет единый каталог и представляет границу безопасности. Леса содержат домены.

Верхним уровнем структуры является лес — совокупность всех объектов, атрибутов и правил (синтаксиса атрибутов) в Active Directory. Лес содержит одно или несколько деревьев, связанных транзитивными отношениями доверия. Дерево содержит один или несколько доменов, также связанных в иерархию транзитивными отношениями доверия. Домены идентифицируются своими структурами имён DNS — пространствами имён[4].

Объекты в домене могут быть сгруппированы в контейнеры — подразделения. Подразделения позволяют создавать иерархию внутри домена, упрощают его администрирование и позволяют моделировать, например, организационную или географическую структуру организации в службе каталогов. Подразделения могут содержать другие подразделения. Microsoft рекомендует использовать как можно меньше доменов в службе каталогов, а для структурирования и политик использовать подразделения. Часто групповые политики применяются именно к подразделениям. Групповые политики сами являются объектами. Подразделение является самым низким уровнем, на котором могут делегироваться административные полномочия.

Другим способом деления являются сайты, которые являются способом физической (а не логической) группировки на основе сегментов сети. Сайты подразделяются на имеющие подключения по низко скоростным каналам (например, по каналам глобальных сетей, с помощью виртуальных частных сетей) и по высокоскоростным каналам (например, через локальную сеть). Сайт может содержать один или несколько доменов, а домен может содержать один или несколько сайтов. При проектировании службы каталогов важно учитывать сетевой трафик, создающийся при синхронизации данных между сайтами.

Ключевым решением при проектировании службы каталогов является решение о разделении информационной инфраструктуры на иерархические домены и подразделения верхнего уровня. Типичными моделями, используемыми для такого разделения, являются модели разделения по функциональным подразделениям компании, по географическому положению и по ролям в информационной инфраструктуре компании. Часто используются комбинации этих моделей.