

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Кафедра информационной безопасности

Составители
Е. В. Прокопенко
И. В. Чичерин

**АДМИНИСТРИРОВАНИЕ АВТОМАТИЗИРОВАННЫХ
РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ**

Методические материалы

Рекомендованы учебно-методической комиссией специальности
10.05.03 Информационная безопасность автоматизированных систем
в качестве электронного издания для использования
в образовательном процессе

Кемерово 2018

Рецензенты

Стенин Д. В. – кандидат технических наук, доцент, директор ИИТМА

Сыркин И. С. – кандидат технических наук, доцент кафедры информационных и автоматизированных производственных систем

Прокопенко Евгения Викторовна

Чичерин Иван Владимирович

Администрирование автоматизированных распределенных информационных систем: методические материалы [Электронный ресурс]: для обучающихся специальности 10.05.03 Информационная безопасность автоматизированных систем очной формы обучения / сост. Е. В. Прокопенко, И. В. Чичерин; КузГТУ. – Кемерово, 2018. – Систем. требования: Pentium IV; ОЗУ 8 Мб; Windows XP; мышь. – Загл. с экрана.

© КузГТУ, 2018

© Е. В. Прокопенко, И. В. Чичерин,
составление, 2018

1. Введение в администрирование автоматизированных распределенных информационных систем.

2. Общие сведения о сетевой инфраструктуре.

Понятие информационной системы

Информационная система (ИС) – совокупность внутренних и внешних информационных потоков объекта управления, методов, средств и специалистов, участвующих в процессе обработки информации и выработке управленческих решений.

ИС связывает объект и систему управления между собой и с внешней средой через информационные потоки.

Структура информационной системы

При рассмотрении информационных систем можно выделить несколько основных компонентов:

- информация, описывающая состояние системы или процесса;
- информационные технологии хранения, обработки, представления и передачи информации;
- организационная структура и связи между единицами управления, а также методы управления;
- функциональные компоненты информационной системы (отдельные подсистемы, решающие тот или иной набор задач реализующих обработку данных и модели принятия решений).

Составные части ИС

- информационное обеспечение – совокупность методов и средств по размещению и организации информации.
- программное обеспечение – совокупность программных средств необходимых для разработки и эксплуатации ИС средствами вычислительной техники.
- техническое обеспечение – комплекс технических средств, применяемых для функционирования ИС
- правовое обеспечение – совокупность правовых норм, регламентирующих создание и функционирование информационной системы.
- лингвистическое обеспечение – совокупность языковых средств, используемых на различных стадиях создания и эксплуатации ИС
- организационное обеспечение – совокупность методов и средств, позволяющих усовершенствовать организационную структуру объектов и управленческие функции.

Вычислительные сети

Современные информационные системы работают на основе применения вычислительных сетей.

Вычислительная сеть – совокупность компьютеров, связанных коммуникационной системой и снабженных необходимым программным обеспечением, позволяющим пользователям и приложениям получать доступ к ресурсам удаленных компьютеров и обеспечивающим обмен данными.

Распределенные информационные системы

Распределенная ИС обеспечивает высокую степень прозрачности сетевых ресурсов, т.е. распределенная ИС предоставляет пользователю и приложениям сетевые ресурсы в виде единой централизованной виртуальной машины.

Распределенная ИС позволяет распределить процессы по различным компьютерам для их хранения, обработки и представления.

Операционные системы

Операционная система – основа для функционирования прикладных программных продуктов, в том числе, программных компонентов любой информационной системы.

Сетевая операционная система обеспечивает функционирование распределенной информационной системы.

Функциональные компоненты сетевой ОС

Основные компоненты сетевой ОС:

- Средства управления локальными ресурсами компьютера реализует все функции ОС автономного компьютера (управление процессами, оперативной памятью, управление внешней памятью, пользователями и т.п.)
- Сетевые средства, разделяемые на три компонента:
 - Серверная часть ОС – средства предоставления локальных ресурсов и сервисов в общее пользование
 - Клиентская часть ОС – средства запроса на доступ к удаленным ресурсам и сервисам
 - Транспортные средства ОС, совместно с коммуникационной системой обеспечивающие передачу сообщений между компьютерами

Сетевые службы и сервисы

Сетевой службой называется совокупность серверной и клиентской частей ОС, предоставляющих доступ к конкретному типу ресурса компьютера через сеть.

Сервис – интерфейс между потребителем услуг (пользователем или приложением) и поставщиком услуг (службой)

Примеры служб:

- DHCP – служба автоматизации выдачи и учета IP-адресов
- DNS – служба преобразования ip-адресов в DNS имена компьютеров
- Server – служба предоставления доступа к файловым ресурсам компьютера
- Workstation – служба клиента, получения доступа к файловым ресурсам удаленного компьютера

Сетевые операционные системы

Компьютеры в сети, в зависимости от распределения функций, могут выступать в роли выделенного сервера или клиентского узла.

Сеть может быть построена по следующим схемам:

- на основе компьютеров, совмещающих функции клиента и сервера – одноранговая сеть
- на основе разделения функций клиентов и серверов – сеть с выделенными серверами
- сеть, включающая узлы разных типов – гибридная сеть

Модели сетевых служб и распределенных приложений

Выделяют три основных параметра организации работы приложений в сети:

- Способ разделения приложения на части, выполняющиеся на разных компьютерах сети;
- Выделение специализированных серверов в сети, на которых выполняются некоторые общие для всех приложений функции;
- Способ взаимодействия между частями приложений, работающих на разных компьютерах.

Способы разделения приложений на части

Приложения условно можно разделить на следующие функциональные части:

- Средства представления данных на экране;

- Логика представления данных на экране (описывает правила и сценарии взаимодействия пользователя с приложениями);
- Прикладная логика (правила для принятия решений, вычислительные процедуры и т.п.);
- Логика данных – операции с данными, хранящимися в некоторой базе;
- Внутренние операции БД – действия СУБД, вызываемые в ответ на выполнение запросов логики данных;
- Файловые операции – стандартные операции над файлами и файловой системой.

Двухзвенные схемы распределенных ИС

Двухзвенные схемы описывают разделение функций приложения между двумя компьютерами:

- Централизованная обработка данных;
- Схема «файл-сервер»;
- Схема «клиент-сервер»

Централизованная обработка данных



Достоинства схемы:

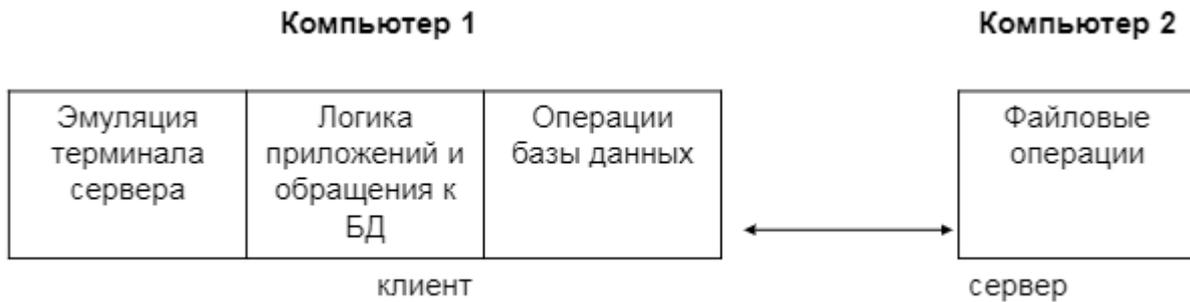
- Ресурсы клиентского компьютера используются в незначительной степени, загружаются только графические средства ввода-вывода;

- Простота организации программы;

Недостатки схемы:

- Недостаточная масштабируемость;
- Отсутствие отказоустойчивости.

Схема «файл-сервер»



Достоинства схемы:

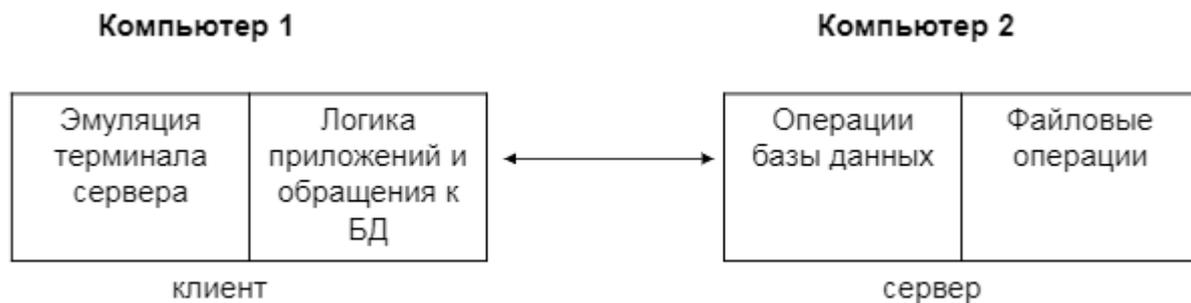
- Данная схема обладает хорошей масштабируемостью, поскольку дополнительные пользователи и приложения добавляют лишь незначительную нагрузку на центральный узел – файловый сервер.

Недостатки схемы:

- Во многих случаях возрастает нагрузка, что приводит к увеличению времени реакции на приложения;

- Клиентский компьютер должен обладать высокой вычислительной мощностью, чтобы справляться с представлением данных, логикой приложений, логикой данных и поддержкой операции БД.

Схема «клиент-сервер»



Достоинства схемы:

- Данная схема более равномерно распределяет функции между клиентской и серверной частями системы;

- Клиентский компьютер выполняет функции, специфические для данного приложения;

- Сервер-функции, реализация которых не зависит от специфики приложения, и данные функции могут быть оформлены в виде сетевых служб.

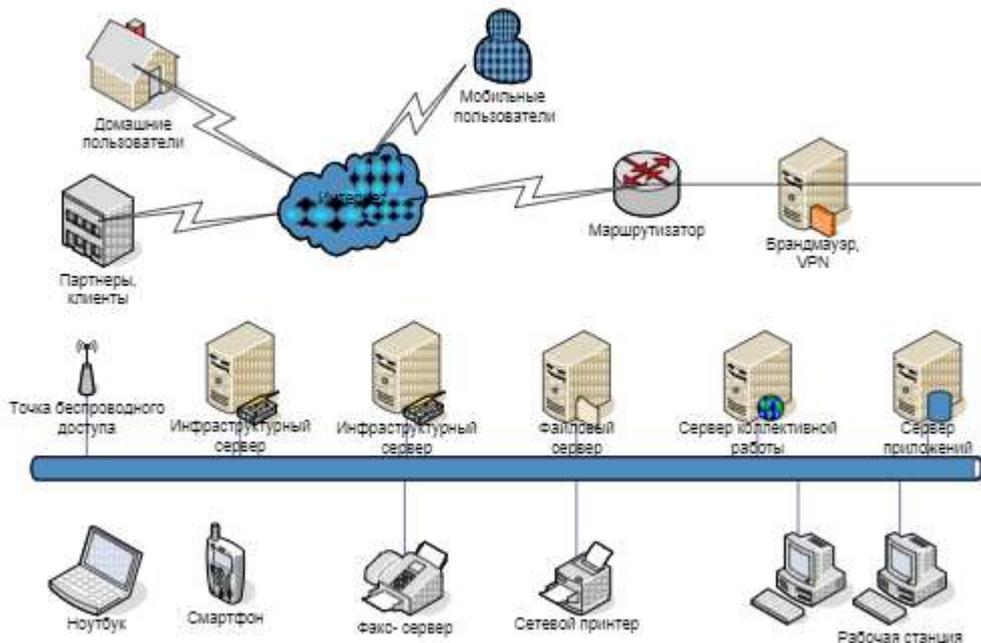
Трехзвенные схемы



Централизованная реализация логики приложения решает проблему недостаточной вычислительной мощности клиентских компьютеров для сложных приложений, упрощает администрирование и поддержку системы.

Упрощается разработка крупных приложений, поскольку четко разделены платформы и инструменты для реализации интерфейса и прикладной логики

Типовая сетевая инфраструктура современного предприятия



3. Хранение данных. Реализация хранилищ данных.

Варианты реализации хранилищ данных:

1. Виртуальное хранилище данных
2. Витрины данных
3. Глобальное хранилище данных

4. Многоуровневая архитектура хранилища данных

а. Хранение данных, на самом деле которых нет. В основе виртуального хранилища – слова или репозитории метаданных, OLTP, OLAP, БД транзакционных систем, все они присутствуют в репозитории. Репозиторий – (разделяемая (инструментальными средствами и системами) корпоративная база данных, содержащая информацию об артефактах проектирования, корпоративное надмножество словарей метаданных.

Реализована процедура sql-запросов, для считывания информации из источников и некоторые процедуры для обработки и формирования полученной информации.

Работают с транзакционными БД:

«+» для пользователя – каждый раз обращаясь получают самую последнюю информации.

«-» – значительное замедление объема данных, наблюдают замедление работы OLTP систем. Возникает реальная угроза целостности в случае неудачного использования пользователей аналитиков.

б. Набор тематически связанных БД, которые содержат в разрезе одной витрины, информации, относящиеся к какому-либо аспекту деятельности корпорации.

Каждая витрина – облегченный вариант хранилища данных. Они максимально приближены к тем пользователям, которым они нужны. Для реализации витрин данных не нужна сложная техника. «-» – избыточность, т.к. одни и те же данные могут быть выставлены в нескольких витринах. Данные часто не обновляются. Необходимость синхронизации данных.

с. Идея совмещения хранилища данных и витрины данных в месте, в одной реализации. Получается трехуровневая архитектура:

- Первый уровень – корпоративное хранилище интегрированных и в основном детализированных данных на основе одной из развитых современных реляционных СУБД.
- Второй уровень – витрины данных на основе многомерной системы управления базами данных, например Oracle Express Server.
- Третий уровень – клиентские рабочие места конечных пользователей.

Реляционные СУБД обеспечивают хранение и управление данных достаточно большого объема, но не слишком хорошо отвечают потребностям OLAP.

На втором уровне – такие СУБД лучше подходят для реализации OLAP. Но не позволяют хранить сверхбольшие объемы данных, размер не превышает десятков Гб, когда речь идет для витрины данных может содержать ссылки на хранилище и при необходимости получать информацию из хранилища, снимает ограничение на объем данных.

3 уровень. Установлены средства оперативного анализа данных.

Проектирование хранилищ – сложная задача:

- Менеджеру, принимающему решения, необходимы самые разнообразные отчеты, причем зачастую новые.
- Данные в хранилище должны регулярно пополняться (необходимо тщательно планировать обновления и резервное копирование).
- Поскольку отчет будет создавать конечный пользователь, должны быть упрощены требования к запросам (должны быть исключены запросы с множественными утверждениями (sql-запрос), с множественными обращениями к реляционным БД).
- Обработка запросов к хранилищу должна проводиться с высокой производительностью (максимально приближена к режиму реального времени)

Основные подходы к архитектуре Хранилищ данных:

- Корпоративная информационная фабрика (CIF) Билла Инмона
- Хранилище данных с архитектурой шины (BUS) Ральфа Кимболла

Архитектура CIF. Этот подход был известен под названием корпоративного ХД. Информация в БД хранится в виде двумерных таблиц. Получившиеся хранилища используются для того, чтобы наполнить информацией дополнительные репозитории. Данные в них относительно специализированы и предназначены для тех или иных видов анализа.

Конечные витрины данных создаются для обслуживания бизнес-отделов, для реализации бизнес-функций. И используют пространственную модель.

В отличие от исходной РБД данные организованы не в 3-й нормальной форме, хотя элементы реляционности здесь присутствуют. Источник данных для таблиц – множество репозиторияев.

Отличительные характеристики подхода Билла Инмона:

- Использование реляционной модели организации атомарных данных и пространственной – для организации суммарных данных.
- Использование итеративного или "спирального" подхода при создании больших Хранилищ данных (позволяет вносить изменения в относительно небольшие блоки данных, оформленные в витрины).
- Использование третьей нормальной формы для организации атомарных данных (высокая степень детальности интегрированных данных, которые позволяют широко манипулировать форматами и средствами, способами представления данных).
- Хранилище данных – это проект корпоративного масштаба (охватывает все отделы корпорации, обслуживает всех пользователей).
- Хранилище данных – это не механическая коллекция витрин данных, а физически целостный объект.

Архитектура шины BUS/ первичные данные преобразуются в информацию, используемую на этапе подготовки данных. Пространственная модель ХД содержит ту же атомарную информацию, что и нормализован-

ная модель. При этом запросы в процессе управления обращаются последовательно все к более низкому уровню детализации, как на уровне шины данных и шины витрин. На уровне шины данных пространственные модели служат не для бизнес-отделов, а для бизнес-процессов, которые в свою очередь связаны с отдельными бизнес-показателями или с бизнес-событиями.

Типичные черты подхода Ральфа Кимболла.

- Использование пространственной модели организации данных с архитектурой "звезда"

- Использование двухуровневой архитектуры

- BUS – хранилище обладает характеристиками:

- оно пространственное;

- оно включает как данные о транзакциях, так и суммарные данные;

- оно включает витрины данных, посвященные только одной предметной области или имеющие только одну таблицу фактов (fact table);

- оно может содержать множество витрин данных в пределах одной базы данных.

- Хранилище данных является «виртуальным» хранилищем. Это – коллекция витрин данных, каждая из которых имеет архитектуру типа "звезда".

Особенности Федерального Хранилища Данных

- Отсутствие необходимости стандартизации бизнес-структур и отчетности о бизнес-операциях;

- Ликвидация противоречий между центральным офисом и местными отделениями компании;

- Возможность постепенного, поэтапного построения Федерального ХД;

- Относительно высокая степень независимости локальных Хранилищ.

Необходимо иметь разнородную управленческую информацию, необходимо четко представлять, как на отрезок времени функционирует бизнес. Не многим компаниям удалось достичь информационного взаимопонимания. Обычный подход затруднял процедуру стандартизации по всем уровням модели. Не для всех процессов стандартизация важна, поэтому даже если бы удалось это сделать, то необходимость стандартизации отняла бы очень много времени у локального хранилища.

Экземпляры хранилищ функционируют на полуавтономной основе, они информационно и географически разнесены, тем не менее, в рамках одного ХД, они управляются как одно большое ХД. Такой подход существенно снижает риск неудачи. Каждые локальные ХД < по размеру, чем глобальные ХД.

Федеральные ХД могут предоставлять необходимую гибкость и обеспечить контроль, каждой из локальных ХД функционирует практиче-

ски независимо друг от друга. Данный подход выгоден не только с точки зрения ежедневных операций, он и при процессе внедрения существует возможность начать с реализации одного, может быть даже незначительного проекта в каком-нибудь подразделении, а затем стоит КИС, добавляя новые ХД. т.о. делает ненужным заранее строить архитектуру, и она заранее неизвестна. Региональные отделения несут затраты больше чем OLTP, но как показывает практика эти расходы быстро окупаются.

Наиболее интересный подход к интеграции БД считается виртуальное интегрирование данных. Для любой БД создается программа посредник, которая преобразует запросы из принятого в системе единого формата в запросы, которые адаптированы к контрольной базе и обратно. Таким образом, пользователь работает с единым форматом, который является глобальным.

Реализация таких требований в рамках одного сервера поражает либо дорогостоящие решения, либо трудная реализация.

Клиенты первой СУБД могут пользоваться сервером, который представляется средствами первой СУБД. Пользователи СУБД могут пользоваться как любыми возможностями СУБД 2, так и возможностями СУБД 1. При подключении к серверу СУБД 2, эти пользователи пользуются.

В то же время клиенты СУБД 2 могут в случае необходимости из мультимедийного приложения обратиться с запросами на поиски: СУБД 1 обрабатывает полученный запрос и результат отправляет обратно серверу 2. этот результат обрабатывается сервером 2, отправляется назад.

Многосерверная система требует разработки механизма межсерверных передач данных. Быстрая передача данных между разными СУБД может оказаться нерациональной и затруднительной. Может просто не найти ни одного протокола который поддерживается одной СУБД.

Современные принципы построения хранилищ данных

Проблемы формирования отчетов с использованием копий БД

1. Информации становится слишком много.
2. Как правило, разные процессы в организации обслуживаются разными программными продуктами.
3. Многие системы не могут хранить данные всей компании в целом.
4. В компании вырабатываются некие критерии эффективности, которые не хранятся в системе явно.

Ключевая фраза, описывающая работу Хранилища Данных:

«Данные забираются из источников, т.е. оперативных систем организации, перерабатываются, загружаются в БД хранилища, и затем на основе переработанных данных строятся отчёты».

Проблемы «данные забираются из источников»

Первая проблема – как выделить из базы данных источника только нужные записи.

Вторая проблема – это организация интерфейса между системой-источником и хранилищем (три подхода):

непосредственный доступ к БД источника;
 доступ к копии БД источника;
 выгрузка файлов.

Проблемы создания базы данных хранилища

Для отчётности требуются данные, изначально не предусмотренные моделью.

- С другой стороны, часть данных, которые предусмотрены, взять просто неоткуда.

- Все идентификаторы клиентов, документов и прочих объектов надо привести к единому формату.

- При этом должна остаться возможность по данным из хранилища найти объект в исходной системе.

- Взаимосвязи между объектами на источнике могут отличаться от связей, предусмотренных моделью.

Проблемы «преобразования»

Во-первых, администратор достаточно низкой квалификации должен увидеть проблему в тот момент, как она возникла.

Во-вторых, те люди, которые строили хранилище, с большой вероятностью уйдут,

а развитием и поддержкой будут заниматься другие.

В-третьих, SQL хорош для манипуляций данными, но совершенно не пригоден для выстраивания сложных потоков управления.

Реализация подходов к «построению отчетов»

Первый подход – online-отчётность.

Второй подход – ad hoc запросы.

Третий подход – интеллектуальный анализ данных, data mining.

Четвёртый подход – экспорт результатов анализа в другие системы.

Пятый подход – использование хранилища как ODS, operational data store.

Проблемы, связанные с эксплуатацией Хранилища

Первая проблема – данных и отчетов становится всё больше и больше с каждым днём.

Вторая проблема – некорректность исходных данных.

Третья проблема является логическим развитием первой и следствием решения второй: всё выше доверие к отчётам, всё больше пользователей получают доступ к данным.

Задачи СППР на основе технологии хранилищ данных

Анализ клиентской базы нацелен на измерение эффективности работы с клиентами и позволяет определить целевые сегменты клиентов для предложения им определенных продуктов и услуг.

Анализ продаж позволяет определять тенденции и зависимости в продажах, планировать продажи и проводить анализ выполнения плана по продажам.

Анализ доходов актуален для любого предприятия и позволяет формировать «уникальные» продукты для каждого «уникального» клиента исходя из максимизации прибыли в долгосрочной перспективе.

Перечень этапов по созданию хранилища данных

1. Предпроектное обследование организации (поиск приоритетных задач управления бизнесом, исследование информационных источников).

2. Логическое моделирование (построение логических моделей хранилищ и витрин данных).

3. Разработка архитектуры (выбор аппаратного и программного обеспечения, выбор способов взаимодействия компонентов архитектуры).

4. Физический дизайн баз данных хранилища и витрин данных (написание или автоматическая генерация программ для создания объектов баз данных: таблиц, представлений, учетных записей пользователей и др.).

5. Разработка процедур наполнения хранилища и витрин данных (настройка специализированных инструментов или разработка процедур с помощью традиционных средств разработки приложений).

6. Разработка пользовательских приложений (настройка специализированных инструментов или разработка приложений с использованием традиционных средств разработки приложений).

7. Поддержка и развитие системы (текущее администрирование, периодическая загрузка данных, регулирование прав доступа, итеративное расширение хранилища).

Модель снимков данных

Снимок данных – это представление данных в определенный момент времени. Данная модель характерна для оперативных систем (OLTP).

Событийная модель

Событийная модель используется для моделирования данных о наступлении событий в определенные моменты времени

Статусная модель

Статусная модель используется для моделирования состояния объектов во времени:

непрерывная модель – для хранения промежутков времени используется одно поле даты,

при этом дата начала следующего периода совпадает с датой окончания предыдущего;

начало и окончание – для хранения промежутков времени используется два поля – дата начала и дата окончания периода действия статуса;

начало и длительность – для хранения промежутков времени используется одно поле даты (дата начала) и поле длительности периода.

Статусная модель «начало и окончание»

Необходимость обеспечения сохранности информации и классификация схем защиты ИС.

Причины необходимости обеспечения сохранности информации

- 1. Высокие темпы роста парка ЭВМ
- 2. Расширение областей использования ЭВМ
- 3. Высокая степень концентрации информации в центрах ее обработки
- 4. Совершенствование способов доступа пользователя к ресурсам ЭВМ
- 5. Усложнение вычислительного процесса на ЭВМ

4. Установка и настройка Windows Server. Роли сервера Windows Server.

Установка и настройка Windows Server

1. Устанавливаем Windows Server 2012R2 с графическим интерфейсом.

2. Настраиваем часовой пояс на Ekaterinburg Standard Time:
%windir%\system32\tzutil.exe /s "Ekaterinburg Standard Time"

После установки первым делом меняем IP-адрес на сетевой карте, можно через GUI, а можно из командной строки cmd так:

2.1 Смотрим имя интерфейса: netsh interface ip show config или ipconfig

2.2 Меняем IP-адрес:

```
netsh interface ipv4 set address name=Ethernet source=static address=192.168.100.2/24 gateway=192.168.100.1 store=persistent
```

```
netsh dns set dnsservers name=Ethernet source=static address=127.0.0.1
```

```
netsh interface ip delete arpcache
```

здесь указаны:

name=Ethernet – имя сетевого интерфейса на сервере, его мы узнали в пункте 2.1

192.168.100.2 – IP-адрес нашего сервера

255.255.255.0 – маска подсети нашего сервера

192.168.100.1 – шлюз по умолчанию в сети, у меня 192.168.100.1 это linux сервер с прозрачным прокси squid, у вас это может быть отдельный роутер

2.3 Если Вы не планируете использовать в своей сети IPv6, то я настоятельно рекомендую его отключить.

В отличие от других протоколов, IPv6 нельзя отключить просто убрав галку в свойствах сетевого интерфейса.

Если поступить таким образом, то можно получить определенные проблемы с приложениями, которые используют loopback и интерфейсное туннелирование. Правильным способом отключения протокола IPv6 является его деактивация через системный реестр или с помощью MicrosoftEasyFix.

Мы скачаем MicrosoftEasyFix с сайта Microsoft. Качаем файл «Отключение IPv6» (MicrosoftEasyFix20160.mini.diagcab) и запускаем на сервере.

Для любителей сделать все вручную через реестр, для отключения IPv6 в раздел реестра

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\TCP/IP6\Parameters

создаем параметр DWORD (32-бита) с именем DisabledComponents и значением FF в шестнадцатеричной системе (255 в десятичной) и перезагружаем сервер shutdown /r /t 00 или Запускаем PowerShell от имени Администратора и вводим:

```
Set-ItemProperty -Path
'HKLM:\System\CurrentControlSet\services\TCPIP6\Parameters' -name "DisabledComponents" -Value 255;
Restart-Computer -Force
```

2.4 Включаем RDP, т.к. по умолчанию он выключен на сервере.

Запускаем PowerShell от имени Администратора и вводим: Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server' -name "fDenyTSConnections" -Value 0;

Enable-NetFirewallRule -DisplayGroup "Дистанционное управление рабочим столом";

```
Set-ItemProperty -Path
'HKLM:\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp' -name "UserAuthentication" -Value 1;
```

3. Задаем имя нашего будущего контроллера домена. Запускаем PowerShell от имени Администратора и вводим: Rename-Computer -NewName DC1 -Restart -Force

4. Развертываем Active Directory. Традиционно для автоматической установки контроллера домена средствами командной строки использовалась команда Dcpromo, но в WindowsServer 2012 она признана устаревшей и рекомендуется использовать PowerShell, что мы и сделаем.

```
Как бы это выглядело через dcpromo: Dcpromo /unattend
/InstallDNS:Yes /dnsOnNetwork:No /ReplicaOrNewDomain:Domain
/NewDomain:Forest /NewDomainDNSName:corp.myorg.ru
/DomainNetBiosName:DC /DatabasePath:"C:\Windows\NTDS"
```

```
/LogPath:"C:\Windows\NTDS" /SysvolPath:"C:\Windows\SYSVOL"
/safeModeAdminPassword:P@ssw0rd /ForestLevel:4 /DomainLevel:4
/RebootOnCompletion:Yes
```

Но нас интересует PowerShell, поэтому открываем консоль PowerShell от имени Администратор и выполняем пункты 4.1 и 4.2

4.1 Для установки роли доменных служб введем команду: Import-Module ServerManager

```
Add-WindowsFeature -Name AD-Domain-Services -
IncludeAllSubFeature -IncludeManagementTools
```

Параметр `-IncludeAllSubFeature` задает установку всех зависимых служб и компонентов вместе с родительской ролью, службой роли или компонентом, заданным параметром `-Name`. Параметр `-IncludeManagementTools` задает установку средств администрирования и управления.

4.2 Для создания нового домена в новом лесу введите команду:

```
Import-Module ADDSDeployment
Install-ADDSForest -CreateDnsDelegation:$false -DatabasePath
"C:\Windows\NTDS" -DomainMode "Win2012" -DomainName
"corp.myorg.ru" -DomainNetbiosName "DC" -ForestMode "Win2012" -
InstallDns:$true -LogPath "C:\Windows\NTDS" -
NoRebootOnCompletion:$false -SysvolPath "C:\Windows\SYSVOL" -
Force:$true -SafeModeAdministratorPassword (convertto-securestring
"P@ssw0rd" -asplaintext -force)
```

После установки сервер будет автоматически перезагружен. В модуле ADDSDeployment есть еще несколько полезных командлетов, перечислю их:

Add-ADDSSReadonlyDomainControllerAccount – Установка контроллера только для чтения

Install-ADDSDomain – Установить первый контроллер домена в дочернем или дереве домена

Install-ADDSDomainController – Установить дополнительный контроллер домена

Install-ADDSForest – Установить первый контроллер в новом лесу

Test-ADDSDomainControllerInstallation Verify – необходимые условия для установки дополнительного контроллера домена (проверка)

Test-ADDSDomainControllerUninstallation – удаление сервиса AD с сервера (проверка)

Test-ADDSDomainInstallation – Проверка необходимых условий для установки первого контроллера домена в дочернем или дереве домена.

Test-ADDSForestInstallation – Установка первого контроллера в новом лесу (проверка)

Test-ADDSSReadonlyDomainControllerAccountCreation – Проверка необхо-

димых условий для установки контроллера только для чтения Uninstall-ADDSDomainController – Удаление контроллера домена с сервера

5. Приступить к дальнейшей настройке сервера, и первое, что нам нужно сделать – это создать обратную зону (reverse lookup zone) для нашей подсети 192.168.100.0/24 и добавить в неё PTR запись dc1.corp.myorg.ru с IP-адресом 192.168.100.2

Тут возможно 2 подхода: создать обратную зону из оболочки cmd с помощью dnscmd или на PowerShell.

5.1 Вариант с cmd

Запускаем командную строку cmd от имени Администратора и вводим:

```
dnscmd DC1 /zoneadd 100.168.192.in-addr.arpa /DSprimary
dnscmd DC1 /config 100.168.192.in-addr.arpa /allowupdate 1
dnscmd DC1 /recordadd 100.168.192.in-addr.arpa 2 PTR
```

dc1.corp.myorg.ru

5.2 Вариант с PowerShell

Запускаем PowerShell от имени Администратора и вводим: Add-DnsServerPrimaryZone -DynamicUpdate NonsecureAndSecure -NetworkId '192.168.100.0/24' -ReplicationScope Domain

```
Add-DnsServerResourceRecordPtr -Name "2" -ZoneName
"100.168.192.in-addr.arpa" -AgeRecord -PtrDomainName
"$env:COMPUTERNAME.corp.myorg.ru"
```

Теперь если мы сделаем: nslookup 192.168.100.2 то у нас произойдет нормальное обратное преобразование.

6. Теперь нам необходимо установить и настроить DHCP-сервер:

Запускаем PowerShell от имени Администратора и вводим:

```
Import-Module ServerManager
```

```
Add-WindowsFeature -Name DHCP -IncludeManagementTools
```

Добавим на сервер группы Пользователи DHCP и Администраторы DHCP:

```
Add-DHCPserverSecurityGroup -ComputerName $env:COMPUTERNAME
Restart-Service dhcpserver
```

Авторизируем наш новый DHCP сервера в домене Active Directory:

```
Add-DhcpServerInDC -DnsName $env:COMPUTERNAME -IPAddress
192.168.100.2
```

Зарегистрируем сервер DHCP для обновления зон в DNS:

```
$User = "$env:USERDOMAIN\$env:USERNAME"
```

```
$PWord = ConvertTo-SecureString -String "P@ssw0rd" -AsPlainText -Force
```

```
$Credential = New-Object -TypeName Sys-
```

```
tem.Management.Automation.PSCredential -ArgumentList $User, $PWord
```

```
Set-DHCPserverDnsCredential -ComputerName $env:COMPUTERNAME -
Credential $Credential
```

Теперь выведем список авторизованных DHCP серверов в Active Directory:

```
Get-DhcpServerInDC
```

Добавляем область и диапазон выдаваемых адресов для неё:

```
Add-DHCPservv4Scope -Name Office -StartRange 192.168.100.10 -EndRange 192.168.100.254 -SubnetMask 255.255.255.0 -State Active
```

Устанавливаем параметры DHCP-сервера:

```
Set-DHCPservv4OptionValue -ComputerName $env:COMPUTERNAME -DnsServer 192.168.100.2 -DnsDomain corp.myorg.ru -Router 192.168.100.1
```

Посмотрим результат конфигурации:

```
Get-DHCPservv4OptionValue -ComputerName $env:COMPUTERNAME | Format-
```

Установим параметры для области 192.168.100.0:

```
Set-DHCPservv4OptionValue -ComputerName $env:COMPUTERNAME -ScopeId 192.168.100.0 -DnsServer 192.168.100.2 -DnsDomain corp.myorg.ru -Router 192.168.100.1
```

На заметку: Если после конфигурации DHCP выходит сообщение, что конфигурация не настроена, то выполняем:

```
Set-ItemProperty -Path regis-try::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ServerManager\Roles\12 -Name ConfigurationState -Value 2
```

Теперь можно перезагрузить сервер:

```
Restart-Computer -Force
```

На этом настройка сервера завершена, после перезагрузки у нас будет работоспособный домен Active Directory со службами DNS и DHCP.

Роли сервера Windows Server

Роль сервера – это набор программ, которые при правильной установке и настройке позволяют компьютеру выполнять определенную функцию для нескольких пользователей или других компьютеров в сети. В общих случаях все роли имеют следующие характеристики.

- Они определяют основную функцию, назначение или цель использования компьютера. Можно назначить компьютер для выполнения одной роли, которая интенсивно используется на предприятии, или для выполнения нескольких ролей, если каждая из них применяется лишь изредка.

- Роли предоставляют пользователям во всей организации доступ к ресурсам, которые управляются другими компьютерами, таким как веб-сайты, принтеры или файлы, хранящиеся на разных компьютерах.

- Они обычно имеют собственные базы данных, в которых создаются очереди запросов пользователя или компьютера либо записываются сведения о сетевых пользователях и компьютерах, имеющих отношение к роли. Например, Службы домена Active Directory содержат базу данных для хранения имен и иерархических связей всех компьютеров в сети.

- После правильной установки и настройки роли функционируют автоматически. Это позволяет компьютерам, на которых они установлены, выполнять назначенные задачи при ограниченном участии пользователя.

Службы ролей – это программы, которые обеспечивают функциональные возможности роли. При установке роли можно выбрать, какие службы она предоставляет другим пользователям и компьютерам на предприятии. Некоторые роли, такие как DNS-сервер, выполняют только одну функцию, поэтому для них нет служб ролей. Другие роли, такие как службы удаленных рабочих столов, имеют несколько служб, которые можно установить в зависимости от потребностей предприятия в удаленном доступе. Роль можно рассматривать как совокупность тесно связанных, взаимодополняющих служб ролей. В большинстве случаев установка роли означает установку одной или нескольких ее служб.

Компоненты

Компоненты – это программы, которые не являются непосредственно частями ролей, но поддерживают или расширяют функции одной или нескольких ролей либо целого сервера независимо от того, какие роли установлены. Например, компонент «Средство отказоустойчивости кластеров» расширяет функции других ролей, таких как Файловые службы и DHCP-сервер, позволяя им присоединяться к серверным кластерам, что обеспечивает повышенную избыточность и производительность. Другой компонент – «Клиент Telnet» – обеспечивает удаленную связь с сервером Telnet через сетевое подключение. Эта функция расширяет возможности связи для сервера.

Когда Windows Server работает в режиме основных серверных компонентов, поддерживаются следующие роли сервера:

- службы сертификатов Active Directory;
- доменные службы Active Directory;
- DHCP-сервер;
- DNS-сервер;
- файловые службы (в том числе диспетчер ресурсов файлового сервера);
- службы Active Directory облегченного доступа к каталогам;
- Hyper-V;
- службы печати и документов;
- службы потокового мультимедиа;
- веб-сервер (в том числе подмножество ASP.NET);
- сервер обновления Windows Server;
- сервер управления правами Active Directory;
- сервер маршрутизации и удаленного доступа и следующие подчиненные роли:
 - посредник подключений служб удаленных рабочих столов;
 - лицензирование;

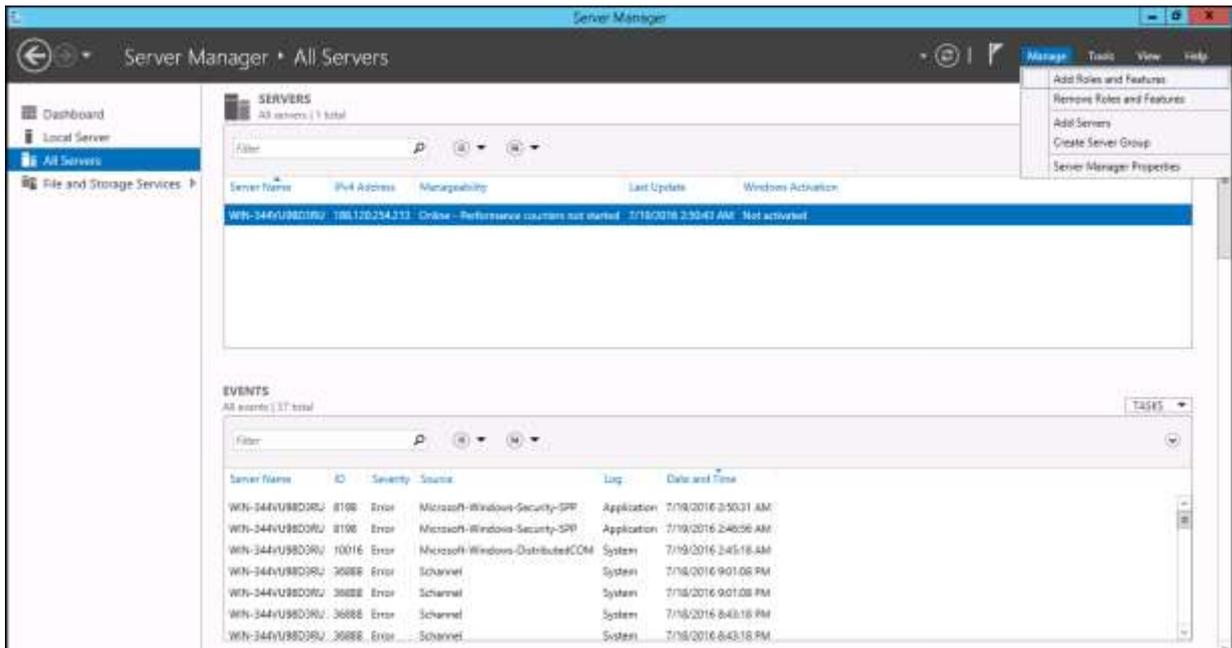
- виртуализация.

Когда Windows Server работает в режиме основных серверных компонентов, поддерживаются следующие компоненты сервера:

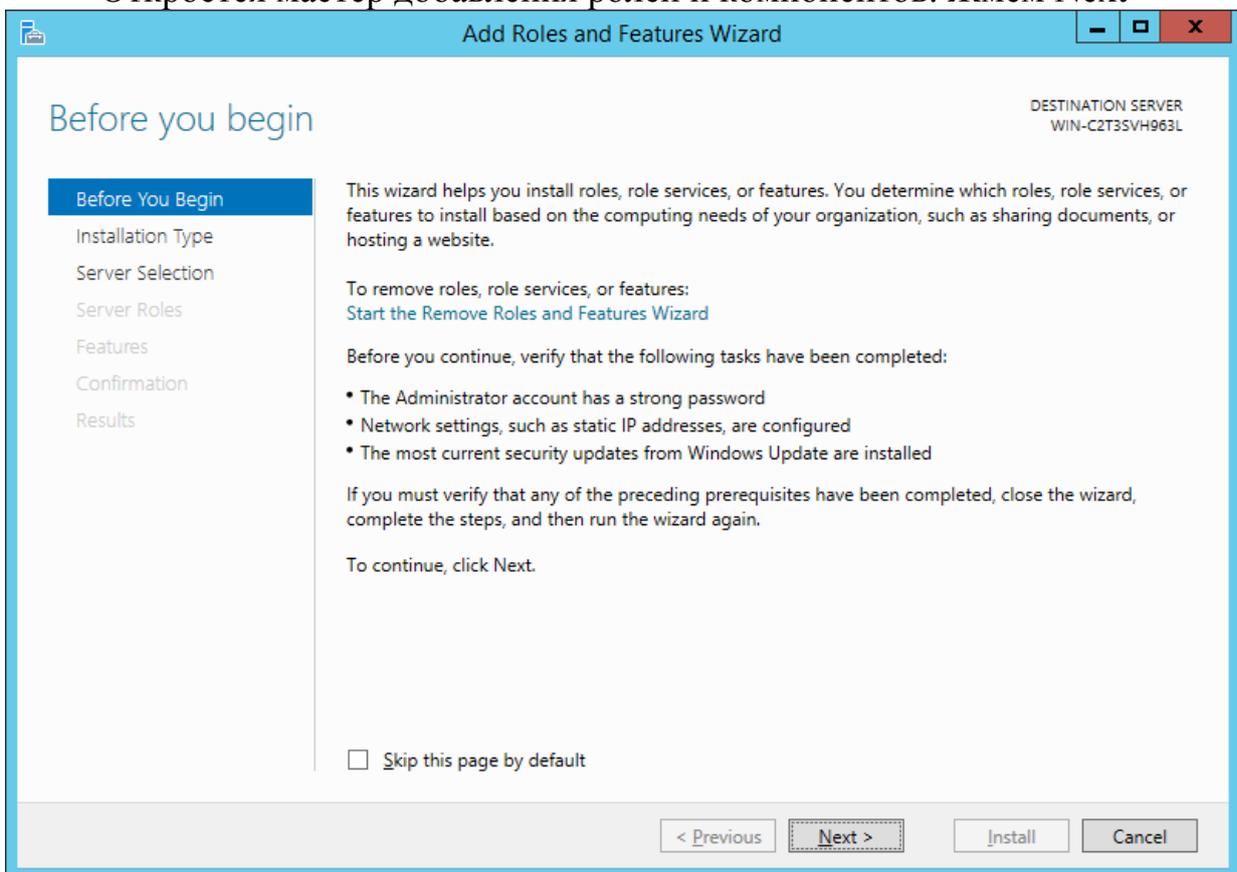
- Microsoft .NET Framework 3.5;
- Microsoft .NET Framework 4.5;
- Windows PowerShell;
- фоновая интеллектуальная служба передачи (BITS);
- шифрование диска BitLocker;
- сетевая разблокировка BitLocker;
- BranchCache
- мост для центра обработки данных;
- Enhanced Storage;
- отказоустойчивая кластеризация;
- Multipath I/O;
- балансировка сетевой нагрузки;
- протокол PNRP;
- qWave;
- удаленное разностное сжатие;
- простые службы TCP/IP;
- RPC через HTTP-прокси;
- сервер SMTP;
- служба SNMP;
- клиент Telnet;
- сервер Telnet;
- клиент TFTP;
- внутренняя база данных Windows;
- Windows PowerShell Web Access;
- служба активации Windows;
- стандартизированное управление хранилищами Windows;
- расширение IIS WinRM;
- WINS-сервер;
- поддержка WoW64.

Установка ролей сервера с помощью Server Manager

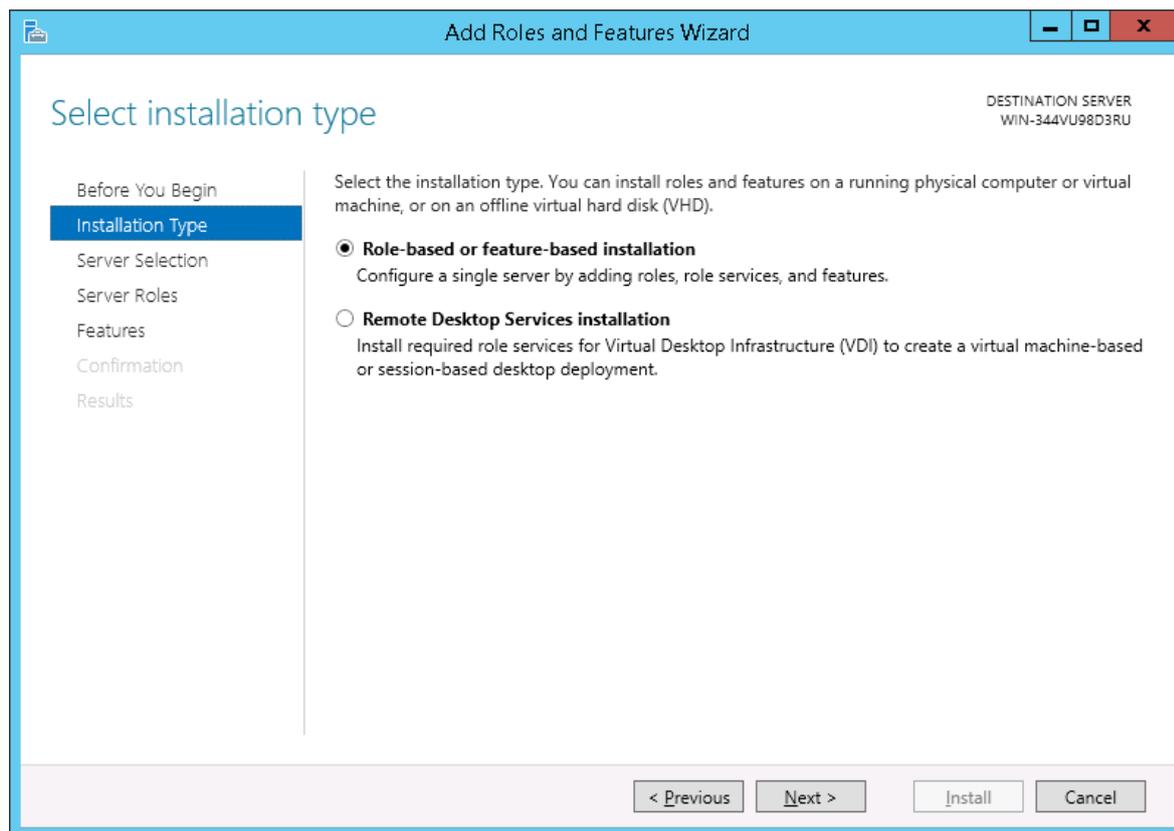
Для добавления открываем Server Manager и в меню Manage жмем Add Roles and features:



Откроется мастер добавления ролей и компонентов. Жмем Next



Installation Type, выбираем Role-based or feature-based installation.
Next:



Server Selection – выбираем наш сервер. Жмем Next Server Roles – Выберите роли, если необходимо, выберите службы ролей и нажмите кнопку Next, чтобы выбрать компоненты. В ходе этой процедуры Мастер добавления ролей и компонентов автоматически информирует о возникших конфликтах на конечном сервере, которые могут помешать установке или нормальной работе выбранных ролей или компонентов. Также появляется запрос на добавление ролей, служб ролей и компонентов, необходимых для выбранных ролей или компонентов.

Установка ролей с помощью PowerShell

Открываем Windows PowerShell Вводим команду Get-WindowsFeature, чтобы просмотреть список доступных и установленных ролей и компонентов на локальном сервере. Результаты выполнения этого командлета содержат имена команд для ролей и компонентов, установленных и доступных для установки.

```

Administrator: Windows PowerShell
[ ] Active Directory Certificate Services           AD-Certificate           Availab1e
[ ]   Certification Authority                     ADCS-Cert-Authority     Availab1e
[ ]   Certificate Enrollment Policy Web Service   ADCS-Enroll-Web-Pol    Availab1e
[ ]   Certificate Enrollment Web Service         ADCS-Enroll-Web-Svc    Availab1e
[ ]   Certification Authority Web Enrollment      ADCS-Web-Enrollment    Availab1e
[ ]   Network Device Enrollment Service         ADCS-Device-Enrollment Availab1e
[ ]   Online Responder                          ADCS-Online-Cert       Availab1e
[ ] Active Directory Domain Services             AD-Domain-Services     Availab1e
[ ] Active Directory Federation Services         ADFS-Federation        Availab1e
[ ] Active Directory Lightweight Directory Services ADLDS                   Availab1e
[ ] Active Directory Rights Management Services  AD RMS                  Availab1e
[ ]   Active Directory Rights Management Server  AD RMS-Server          Availab1e
[ ]   Identity Federation Support              AD RMS-Identity        Availab1e
[ ] Application Server                          Application-Server      Availab1e
[ ]   .NET Framework 4.5                      AS-NET-Framework      Availab1e
[ ]   COM+ Network Access                     AS-Ent-Services       Availab1e
[ ]   Distributed Transactions                 AS-Dist-Transaction   Availab1e
[ ]     WS-Atomic Transactions                 AS-WS-Atomic          Availab1e
[ ]     Incoming Network Transactions          AS-Incoming-Trans     Availab1e
[ ]     Outgoing Network Transactions          AS-Outgoing-Trans     Availab1e
[ ]   TCP Port Sharing                        AS-TCP-Port-Sharing   Availab1e
[ ]   Web Server (IIS) Support                 AS-Web-Support        Availab1e
[ ]   Windows Process Activation Service Support AS-WAS-Support        Availab1e
[ ]     HTTP Activation                       AS-HTTP-Activation    Availab1e
[ ]     Message Queuing Activation            AS-MSMQ-Activation    Availab1e
[ ]     Named Pipes Activation                AS-Named-Pipes        Availab1e
[ ]     TCP Activation                        AS-TCP-Activation     Availab1e
[ ] DHCP Server                               DHCP                   Availab1e
[ ] DNS Server                               DNS                    Availab1e
[ ] Fax Server                               Fax                    Availab1e
[X] File and Storage Services                 FileAndStorage-Services Installed
[ ] File and iSCSI Services                   File-Services          Availab1e
[ ]   File Server                             FS-FileServer          Availab1e
[ ]     BranchCache for Network Files          FS-BranchCache        Availab1e
[ ]     Data Deduplication                    FS-Data-Deduplication Availab1e
[ ]     DFS Namespaces                       FS-DFS-NameSpace     Availab1e
[ ]     DFS Replication                      FS-DFS-Replication   Availab1e
[ ]     File Server Resource Manager          FS-Resource-Manager  Availab1e
[ ]     File Server VSS Agent Service          FS-VSS-Agent          Availab1e
[ ]     iSCSI Target Server                   FS-iSCSITarget-Server Availab1e
[ ]     iSCSI Target Storage Provider (VDS and V... iSCSITarget-VSS-VDS  Availab1e
[ ]     Server for NFS                       FS-NFS-Service        Availab1e
[ ]     Work Folders                          FS-SyncShareService   Availab1e
[X] Storage Services                         Storage-Services       Installed
[ ] Hyper-V                                   Hyper-V                Availab1e
[ ] Network Policy and Access Services         NPAS                   Availab1e
[ ]   Network Policy Server                   NPAS-Policy-Server    Availab1e
[ ]   Health Registration Authority           NPAS-Health           Availab1e
[ ]   Host Credential Authorization Protocol   NPAS-Host-Cred        Availab1e

```

Введите `Get-Help Install-WindowsFeature` для просмотра синтаксиса и допустимых параметров командлета `Install-WindowsFeature` (MAN).

```

PS C:\Users\Administrator> Get-Help Install-WindowsFeature

Do you want to run Update-Help?
The Update-Help cmdlet downloads the most current Help files for Windows PowerShell modules, and installs them on your
computer. For more information about the Update-Help cmdlet, see http://go.microsoft.com/fwlink/?LinkId=210614.
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"):

NAME
    Install-WindowsFeature

SYNOPSIS
    Installs one or more roles, role services, or features on either the local or a specified remote server that is run
    ning Windows Server 2012 R2. This cmdlet is equivalent to and replaces Add-WindowsFeature, the cmdlet that was used
    to install roles, role services, and features in Windows Server 2008 R2.

SYNTAX
    Install-WindowsFeature [-Name] <Feature[]> [-ComputerName <String>] [-Credential <PSCredential>] [-IncludeAllSubFea
    ture] [-IncludeManagementTools] [-LogPath <String>] [-Restart] [-Source <String[]>] [-Confirm] [-WhatIf] [<CommonPa
    rameters>]

    Install-WindowsFeature [-ComputerName <String>] [-Credential <PSCredential>] [-LogPath <String>] [-Restart] [-Sourc
    e <String[]>] [-Vhd <String>] -ConfigurationFilePath <String> [-Confirm] [-WhatIf] [<CommonParameters>]

    Install-WindowsFeature [-Name] <Feature[]> [-ComputerName <String>] [-Credential <PSCredential>] [-IncludeAllSubFea
    ture] [-IncludeManagementTools] [-LogPath <String>] [-Source <String[]>] -Vhd <String> [-Confirm] [-WhatIf] [<Commo
    nParameters>]

DESCRIPTION
    The Install-WindowsFeature cmdlet installs the specified roles, role services, and features on a computer that is r
    unning Windows Server 2012 R2, or on an offline virtual hard disk (VHD) on which Windows Server 2012 R2 is installe
    d. This cmdlet works similarly to the Add Roles and Features Wizard in Server Manager, with an important exception:
    the cmdlet does not install management tools for roles, role services, and features by default. To install manage
    ment tools such as snap-ins on a target server, you must add the IncludeManagementTools parameter to your command.

    This cmdlet requires elevation; you must be running a Windows PowerShell session as an administrator to use this cm
    dlet.

RELATED LINKS
    Online Version: http://go.microsoft.com/fwlink/p/?linkid=287571
    Get-WindowsFeature
    Uninstall-WindowsFeature
    Enable-ServerManagerStandardUserRemoting
    Disable-ServerManagerStandardUserRemoting

REMARKS
    To see the examples, type: "get-help Install-WindowsFeature -examples".
    For more information, type: "get-help Install-WindowsFeature -detailed".
    For technical information, type: "get-help Install-WindowsFeature -full".
    For online help, type: "get-help Install-WindowsFeature -online"

PS C:\Users\Administrator>
  
```

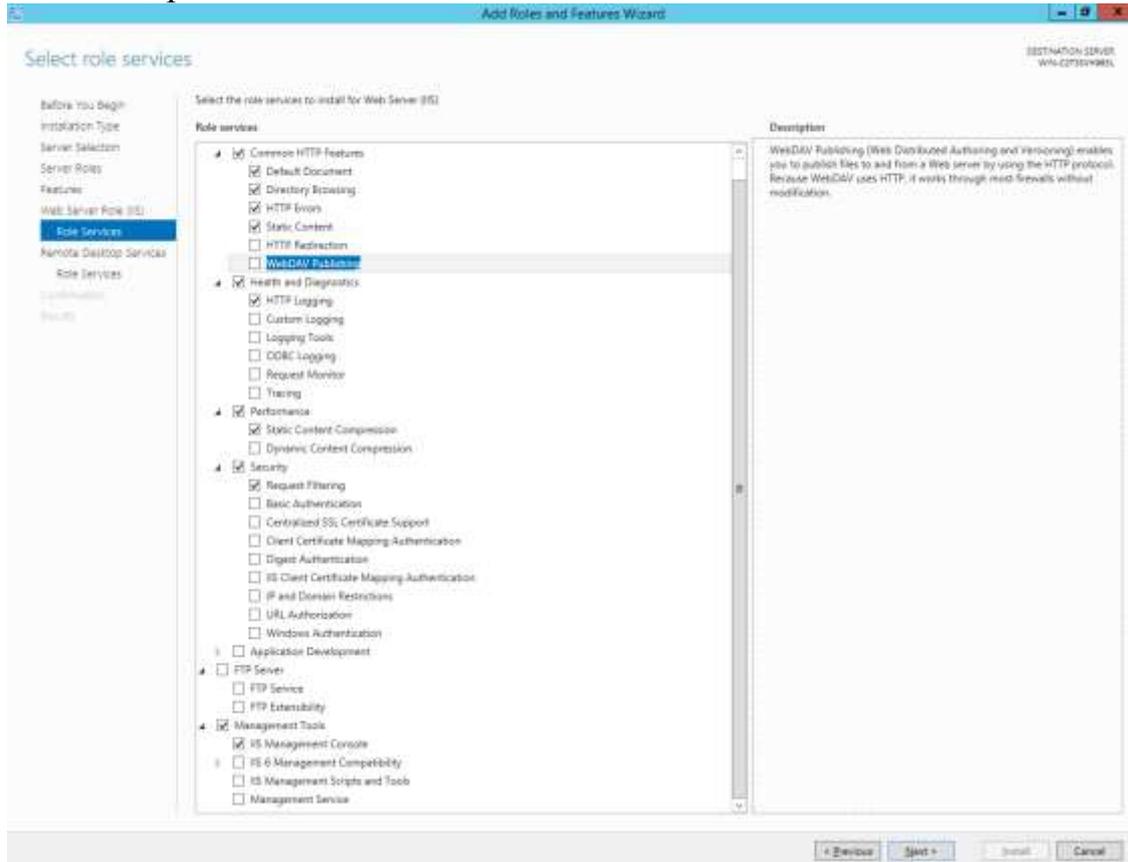
Вводим следующую команду (-Restart перезагрузит сервер, если при ус тановке роли требуется перезагрузка).

```
Install-WindowsFeature -Name <feature_name> -Restart
```

Описание ролей и служб ролей

Ниже описаны все роли и службы ролей. Расширенную настройку посмотрим для самых часто встречающихся в нашей практике Web Server Role и Remote Desktop Services

Подробное описание IIS

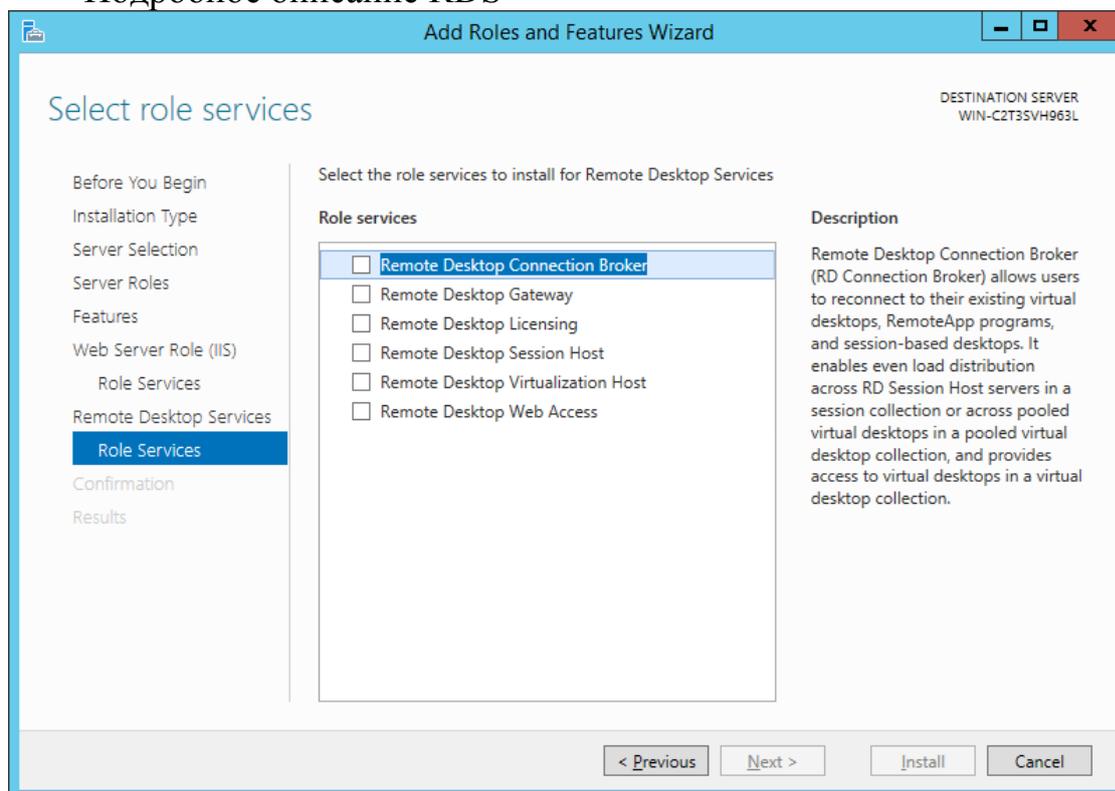


- Common HTTP Features – Основные HTTP компоненты
- Default Document – позволяет устанавливать индексную страницу у сайта.
 - Directory Browsing – позволяет пользователям видеть содержимое каталога на веб-сервере. Используйте Directory Browsing для того, чтобы автоматически сгенерировать список всех каталогов и файлов, имеющих в каталоге, когда пользователи не указывают файл в URL-адресе и индексная страница отключена или не настроена
 - HTTP Errors – позволяет настроить сообщения об ошибках, возвращаемых клиентам в браузере.
 - Static Content – позволяет размещать статический контент, например, картинки или html-файлы.
 - HTTP Redirection – обеспечивает поддержку перенаправления запросов пользователей.
 - WebDAV Publishing позволяет публиковать файлы с веб-сервера с помощью протокола HTTP.
 - Health and Diagnostics Features – Компоненты диагностики
 - HTTP Logging обеспечивает ведение журнала активности веб-сайта для данного сервера.
 - Custom Logging обеспечивает поддержку создания кастомных логов, которые отличаются от “традиционных” журналов.

- Logging Tools обеспечивает инфраструктуру для управления журналами веб-сервера и автоматизации общих задач ведения журнала.
- ODBC Logging обеспечивает инфраструктуру, которая поддерживает ведение журнала активности веб-сервера в ODBC-совместимой базе данных.
- Request Monitor предоставляет инфраструктуру для мониторинга состояния веб-приложений путем сбора информации о HTTP-запросах в рабочем процессе IIS.
- Tracing предоставляет инфраструктуру для диагностики и устранения неполадок веб-приложений. При использовании трассировки неудачных запросов, вы можете отследить трудно-фиксируемые события, такие как плохая производительность или сбои аутентификации.
- Performance компоненты увеличения производительности веб-сервера.
- Static Content Compression предоставляет инфраструктуру для настройки HTTP-сжатия статического содержимого
- Dynamic Content Compression предоставляет инфраструктуру для настройки HTTP-сжатия динамического содержимого.
- Security компоненты безопасности
- Request Filtering позволяет фиксировать все входящие запросы и фильтровать их на основании правил, установленных администратором.
- Basic Authentication позволяет установить дополнительную авторизацию
- Centralized SSL Certificate Support это функция, которая позволяет хранить сертификаты в централизованном месте, как общий файловый ресурс.
- Client Certificate Mapping Authentication использует клиентские сертификаты для аутентификации пользователей.
- Digest Authentication работает путем отправки хэша пароля в контроллер домена Windows, для аутентификации пользователей. Если вам необходимо более высокий уровень безопасности по сравнению с обычной проверкой подлинности, рассмотрите вопрос об использовании проверки подлинности Digest
 - IIS Client Certificate Mapping Authentication использует клиентские сертификаты для аутентификации пользователей. Сертификат клиента представляет собой цифровой ID, полученный из надежного источника.
 - IP and Domain Restrictions позволяет разрешать/запрещать доступ на основе запрашиваемого IP-адреса или доменного имени.
 - URL Authorization позволяет создавать правила, ограничивающие доступ к веб-контенту.
 - Windows Authentication Эта схема аутентификации позволяет администраторам домена Windows пользоваться преимуществами доменной инфраструктуры для аутентификации пользователей.

- Application Development Features компоненты разработки приложений
- FTP Server
- FTP Service Включает FTP публикации на веб-сервере.
- FTP Extensibility Включает поддержку FTP функций, расширяющих возможности
 - Management Tools инструменты управления
 - IIS Management Console устанавливает диспетчер IIS, который позволяет управлять Веб-сервером через графический интерфейс
 - IIS 6.0 Management Compatibility обеспечивает прямую совместимость для приложений и сценариев, которые используют Admin Base Object (ABO) и интерфейса службы каталогов (ADSI) API Active Directory. Это позволяет использовать существующие сценарии IIS 6.0 веб-сервером IIS 8.0
 - IIS Management Scripts and Tools предоставляют инфраструктуру для управления веб-сервером IIS программно, с помощью команд в окне командной строки или с помощью запуска сценариев.
 - Management Service предоставляет инфраструктуру для настройки интерфейса пользователя, диспетчера IIS.

Подробное описание RDS



- Remote Desktop Connection Broker – Обеспечивает повторное подключение клиентского устройства к программам, на основе сеансов настольных компьютеров и виртуальных рабочих столов.
- Remote Desktop Gateway – Позволяет авторизованным пользователям подключаться к виртуальным рабочим столам, программам

RemoteApp и основанных на сессиях рабочим столам в корпоративной сети или через Интернет.

- Remote Desktop Licensing – Средство управления лицензиями RDP

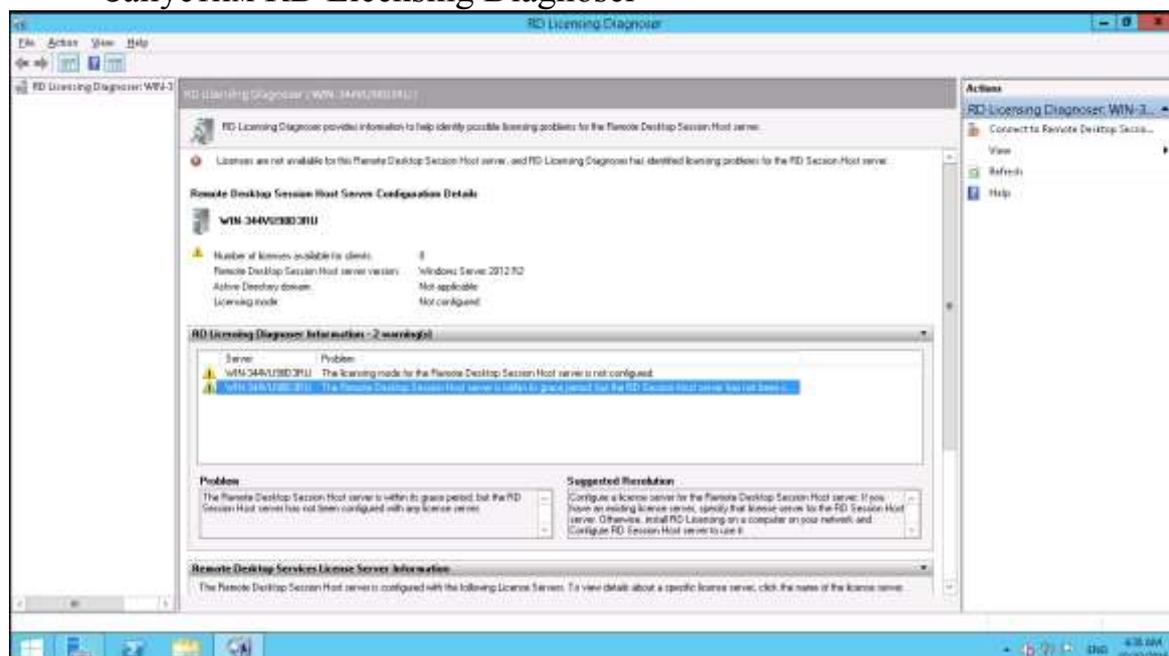
- Remote Desktop Session Host – Включает сервер для размещения программ RemoteApp или сеанса на основе рабочих столов.

- Remote Desktop Virtualization Host – позволяет настраивать RDP на виртуальных машинах

- Remote Desktop WebAccess – Позволяет пользователям подключаться к ресурсам рабочего стола с помощью меню Пуск или веб-браузера.

Рассмотрим установку и настройку сервера терминальных лицензий. Выше рассказано как устанавливаются роли, установка RDS не отличается от установки других ролей, в Role Services нам потребуется выбрать Remote Desktop Licensing и Remote Desktop Session Host. После установки в Server Manager-Tools появится пункт Terminal Services. В Terminal Services есть два пункта RD Licensing Diagonoser, это средство диагностики работы лицензирования удаленных рабочих столов, и Remote Desktop Licensing Manager, это средство управления лицензиями.

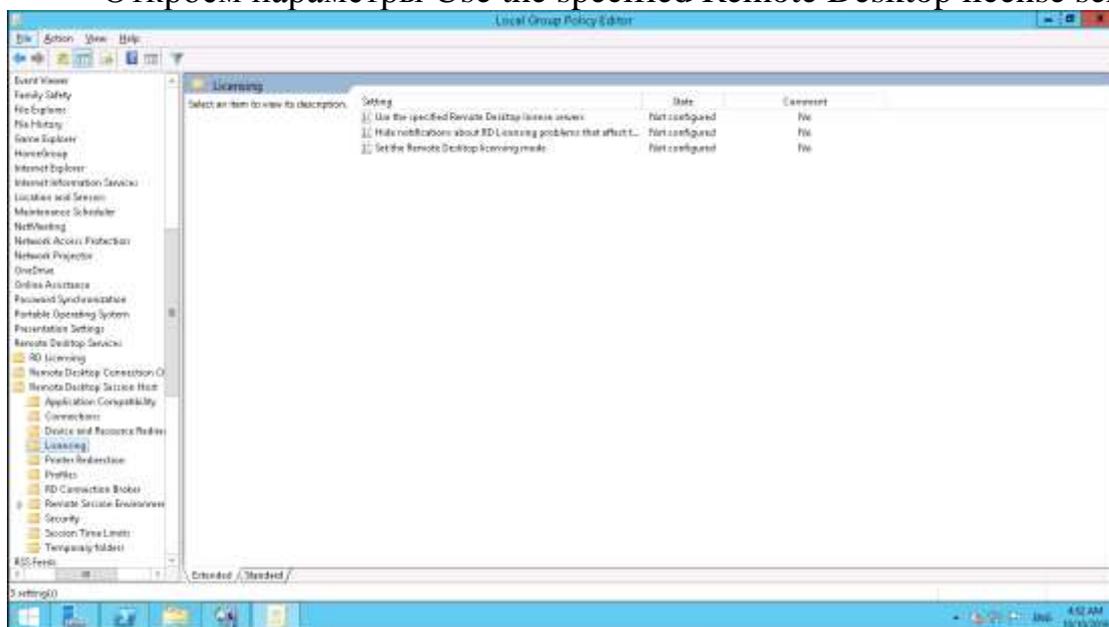
Запустим RD Licensing Diagonoser



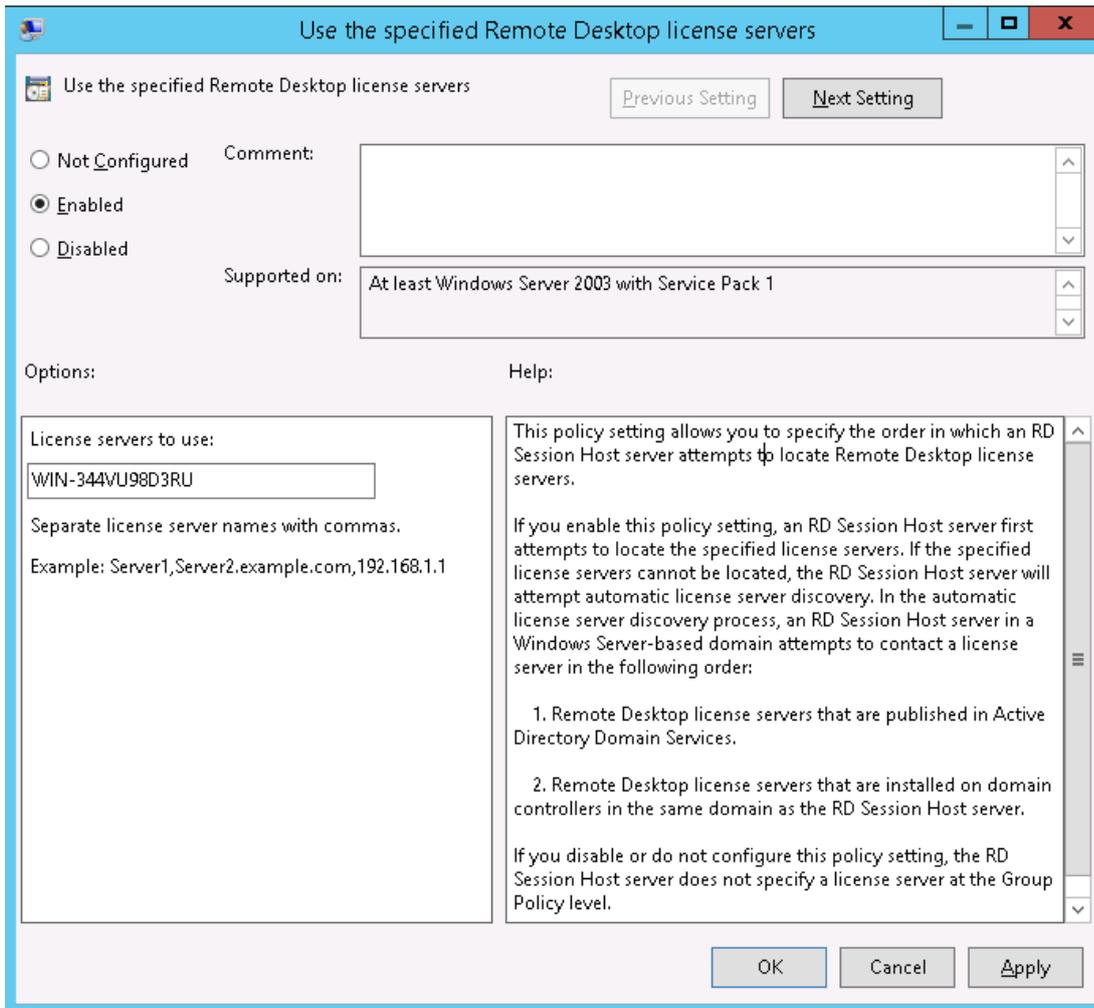
Здесь мы видим, что доступных лицензий пока нет, т. к. не задан режим лицензирования для сервера узла сеансов удаленных рабочих столов. Сервер лицензирования указывается в локальных групповых политиках. Для запуска редактора выполним команду gpedit.msc. Откроется редактор локальной групповой политики. В дереве слева раскроем вкладки:

- «Конфигурация компьютера» (Computer Configuration)
- «Административные шаблоны» (Administrative Templates)
- «Компоненты Windows» (Windows Components)
- «Службы удаленных рабочих столов» (Remote Desktop Services)

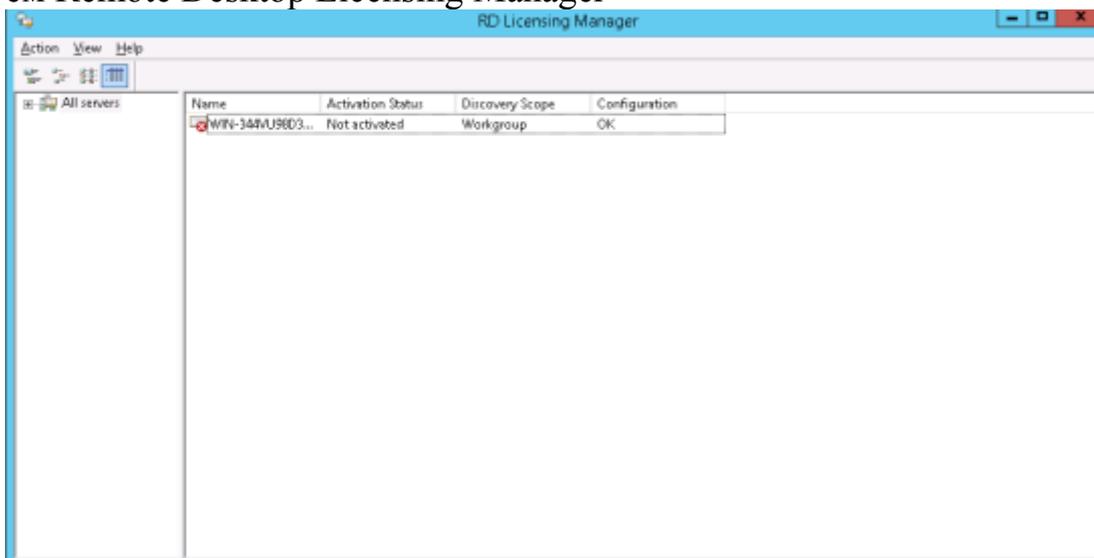
- «Узел сеансов удаленных рабочих столов» (Remote Desktop Session Host)
 - «Лицензирование» (Licensing)
- Откроем параметры Use the specified Remote Desktop license servers



В окне редактирования параметров политики включаем сервер лицензирования (Enabled) . Затем необходимо определить сервер лицензирования для службы удаленных рабочих столов. В моем примере сервер лицензирования находится на этом же физическом сервере. Указываем сетевое имя или IP-адрес сервера лицензий и нажимаем ОК. Если в дальнейшем будет изменяться имя сервера, сервер лицензий, то потребуются изменить в этом же разделе.



После этого в RD Licensing Diagonoser можно увидеть, что сервер терминальных лицензий настроен, но не включен. Для включения запускаем Remote Desktop Licensing Manager



Выбираем сервер лицензирования, со статусом Not Activated . Для активации кликаем по нему правой кнопкой мыши и выбираем Activate Server. Запустится Мастер активации сервера. На вкладке Connection

Method выбираем Automatic Connection. Далее заполняем информация об организации, после этого сервер лицензий активирован.

Active Directory Certificate Services

Службы AD CS предоставляют настраиваемые услуги по выдаче цифровых сертификатов, которые используются в системах безопасности ПО, применяющих технологии открытых ключей, и по управлению этими сертификатами. Цифровые сертификаты, предоставляемые AD CS, можно использовать для шифрования и цифрового подписывания электронных документов и сообщений. Эти цифровые сертификаты можно использовать для проверки в сети подлинности учетных записей компьютеров, пользователей и устройств. Цифровые сертификаты используются для обеспечения:

- конфиденциальности с помощью шифрования;
- целостности с помощью цифровых подписей;
- проверки подлинности с помощью привязывания ключей сертификата к учетным записям компьютеров, пользователей и устройств в сети.

AD CS можно использовать для повышения безопасности путем привязки удостоверения пользователя, устройства или службы к соответствующему закрытому ключу. В число применений, поддерживаемых AD CS, входят безопасные многоцелевые расширения стандарта почты Интернета (S/MIME), защищенные беспроводные сети, виртуальные частные сети (VPN), протокол IPsec, шифрованная файловая система (EFS), вход с помощью смарт-карт, протокол безопасности передачи данных и протокол безопасности транспортного уровня (SSL/TLS) и цифровые подписи.

Active Directory Domain Services

Используя роль сервера доменных служб Active Directory (AD DS), можно создать масштабируемую, безопасную и управляемую инфраструктуру для управления пользователями и ресурсами; кроме того, можно обеспечить работу приложений, поддерживающих каталоги, например Microsoft Exchange Server. Доменные службы Active Directory предоставляют распределенную базу данных, в которой хранятся сведения о сетевых ресурсах и данные приложений с поддержкой каталогов, а также осуществляется управление этой информацией. Сервер, на котором выполняются AD DS, называется контроллером домена. Администраторы могут использовать AD DS для упорядочения в иерархическую вложенную структуру таких элементов сети, как пользователи, компьютеры и другие устройства. Иерархическая вложенная структура включает лес Active Directory, домены в лесу и организационные подразделения в каждом домене. Средства безопасности интегрированы в AD DS в виде проверки подлинности и контроля доступа к ресурсам в каталоге. С помощью единого входа в сеть администраторы могут управлять по сети данными каталога и организацией. Авторизованные пользователи сети также могут ис-

пользовать единый вход в сеть для доступа к ресурсам, расположенным в любом месте сети. Доменные службы Active Directory предоставляют следующие дополнительные возможности.

- Набор правил – схема, определяющая классы объектов и атрибуты, которые содержатся в каталоге, ограничения и пределы для экземпляров этих объектов, а также формат их имен.
- Глобальный каталог, содержащий сведения о каждом объекте в каталоге. Пользователи и администраторы могут использовать глобальный каталог для поиска данных каталога независимо от того, какой домен в каталоге действительно содержит искомые данные.
- Механизм запросов и индексирования, благодаря которому объекты и их свойства могут публиковаться и находиться сетевыми пользователями и приложениями.
- Служба репликации, которая распределяет данные каталога по сети. Все контроллеры домена, доступные для записи в домене, участвуют в репликации и содержат полную копию всех данных каталога для своего домена. Любые изменения данных каталога реплицируются в домене на все контроллеры домена.
- Роли хозяев операций (известные также как гибкие операции с единым хозяином, или FSMO). Контроллеры доменов, исполняющие роли хозяев операций, предназначены для выполнения специальных задач по обеспечению согласованности данных и исключению конфликтующих записей в каталоге.

Active Directory Federation Services

AD FS предоставляют конечным пользователям, которым требуется доступ к приложениям на защищенном с помощью AD FS предприятии, в партнерских организациях федерации или в облаке, возможности упрощенной и безопасной федерации удостоверений и веб-службы единого входа (SSO) В Windows Server AD FS включают службу роли службы федерации, действующую в качестве поставщика удостоверений (выполняет проверку подлинности пользователей для предоставления маркеров безопасности для приложений, доверяющих AD FS) или в качестве поставщика федерации (применяет маркеры от других поставщиков удостоверений и затем предоставляет маркеры безопасности для приложений, доверяющих AD FS).

Active Directory Lightweight Directory Services

Службы Active Directory облегченного доступа к каталогам (AD LDS) – это протокол LDAP, который обеспечивает гибкую поддержку приложений, работающих с каталогами, без зависимостей и связанных с доменами ограничений доменных служб Active Directory. AD LDS можно запускать на рядовых или изолированных серверах. На одном сервере можно запустить несколько экземпляров AD LDS с независимо управляемыми схемами. С помощью роли службы AD LDS можно предоставить

службы каталогов для приложений с поддержкой каталогов, не используя служебные данные доменов и лесов и не требуя единой схемы для всего леса.

Active Directory Rights Management Services

Службы AD RMS можно использовать, чтобы расширить стратегию безопасности в организации, обеспечив защиту документов с помощью управления правами на доступ к данным (IRM). AD RMS позволяет пользователям и администраторам назначать разрешения доступа к документам, рабочим книгам и презентациям с помощью политик IRM. Это позволяет защитить конфиденциальную информацию от печати, пересылки или копирования пользователями, не имеющими на это прав. После того как разрешения для файла ограничены с помощью IRM, ограничения доступа и использования применяются независимо от местоположения информации, так как разрешение для файла хранится в самом файле документа. С помощью AD RMS и IRM отдельные пользователи могут применять свои личные настройки, касающиеся передачи личных и конфиденциальных сведений. Они также помогут организации применять корпоративную политику для управления использованием и распространением конфиденциальных и личных сведений. Решения IRM, поддерживаемые службами AD RMS, используются для обеспечения следующих возможностей.

- Постоянные политики использования, которые остаются с информацией независимо от ее перемещения, отправки или пересылки.
- Дополнительный уровень конфиденциальности для защиты конфиденциальных данных – например, отчетов, спецификаций продуктов, сведений о клиентах и сообщений электронной почты – от намеренного или случайного попадания в чужие руки.
- Предотвращение несанкционированной пересылки, копирования, изменения, печати, передачи по факсу или вставки ограничиваемого содержимого авторизованными получателями.
- Предотвращение копирования ограничиваемого содержимого с помощью функции PRINT SCREEN в Microsoft Windows.
- Поддержка срока действия файла, предотвращающего просмотр содержимого документов по истечении заданного периода времени.
- Внедрение корпоративных политик, управляющих использованием и распространением содержимого в организации

Application Server

Сервер приложений предоставляет интегрированную среду для развертывания и выполнения пользовательских бизнес-приложений на базе сервера.

DHCP Server

DHCP – это технология "клиент-сервер", с помощью которой DHCP-серверы могут назначать или сдавать в аренду IP-адреса компьютерам и другим устройствам, являющимся DHCP-клиентами. Развертывание в сети

DHCP-серверов обеспечивает автоматическое предоставление клиентским компьютерам и другим сетевым устройствам на базе IPv4 и IPv6 действительных IP-адресов и дополнительных конфигурационных параметров, необходимых данным клиентам и устройствам. Служба DHCP-сервера в Windows Server включает поддержку основанных на политике назначений и обработку отказов протокола DHCP.

DNS Server

Служба DNS – это иерархическая распределенная база данных, содержащая сопоставления доменных имен DNS с различными типами данных, таких как IP-адреса. Служба DNS позволяет использовать понятные имена, такие как `www.microsoft.com`, для облегчения нахождения компьютеров и других ресурсов в сетях, работающих на базе протокола TCP/IP. Служба DNS в Windows Server обеспечивает дополнительную улучшенную поддержку Модулей безопасности DNS (DNSSEC), включая регистрацию в сети и автоматизированное управление параметрами.

FAX Server

Факс-сервер отправляет и получает факсы, а также дает возможность управлять ресурсами факса, такими как задания, настройки, отчеты и факс-устройства на вашем факс-сервере.

File and Storage Services

Администраторы могут использовать роль "Файловые службы и службы хранилища" для настройки нескольких файловых серверов и их хранилищ, а также для управления этими серверами с помощью диспетчера серверов или Windows PowerShell. Некоторые конкретные приложения включают следующие функции.

- Рабочие папки. Использовать, чтобы разрешить пользователям хранение рабочих файлов и доступ к ним на личных компьютерах и устройствах помимо корпоративных ПК. Пользователи получают удобное место для хранения рабочих файлов и доступа к ним из любого места. Организации контролируют корпоративные данные, храня файлы на централизованно управляемых файловых серверах и при необходимости задавая политики устройств пользователей (такие как шифрование и пароли блокировки экрана).
- Дедупликация данных. Использовать для снижения требований к месту на диске для хранения файлов, экономя средства на хранилище.
- Сервер цели iSCSI. Использовать для создания централизованных, программных и аппаратно-независимых дисковых подсистем iSCSI в сетях хранения данных (SAN).
- Дисковые пространства. Использовать для развертывания хранилища с высоким уровнем доступности, отказоустойчивого и масштабируемого за счет применения экономичных стандартизованных в отрасли дисков.

- Диспетчер серверов. Использовать для удаленного управления несколькими файловыми серверами из одного окна.
- Windows PowerShell. Использовать для автоматизации управления большинством задач администрирования файловых серверов.

Hyper-V

Роль Hyper-V позволяет создавать виртуализованную вычислительную среду с помощью технологии виртуализации, встроенной в Windows Server, и управлять ею. При установке роли Hyper-V выполняется установка необходимых компонентов, а также необязательных средств управления. В число необходимых компонентов входят низкоуровневая оболочка Windows, служба управления виртуальными машинами Hyper-V, поставщик виртуализации WMI и компоненты виртуализации, такие как шина VMbus, поставщик службы виртуализации (VSP) и драйвер виртуальной инфраструктуры (VID).

Network Policy and Access Services

Службы сетевой политики и доступа предоставляют следующие решения для сетевых подключений:

- Защита доступа к сети – это технология создания, принудительного применения и исправления политик работоспособности клиента. С помощью защиты доступа к сети системные администраторы могут устанавливать и автоматически применять политики работоспособности, которые включают в себя требования к программному обеспечению, обновлениям для системы безопасности и другие параметры. Для клиентских компьютеров, не соответствующих требованиям политики работоспособности, можно ограничить доступ к сети до тех пор, пока их конфигурация не будет обновлена в соответствии с требованиями политики.

- Если развернуты точки беспроводного доступа с поддержкой 802.1X, вы можете использовать сервер политики сети (NPS) для развертывания методов аутентификации на основе сертификатов, которые более безопасны, чем аутентификация на основе паролей. Развертывание оборудования с поддержкой 802.1X с сервером NPS позволяет обеспечить аутентификацию пользователей интрасети до того, как они смогут подключиться к сети или получить IP-адрес от DHCP-сервера.

- Вместо того чтобы настраивать политику доступа к сети на каждом сервере доступа к сети, можно централизованно создать все политики, в которых будут определены все аспекты запросов на сетевое подключение (кто может подключаться, когда разрешено подключение, уровень безопасности, который необходимо использовать для подключения к сети).

Print and Document Services

Службы печати и документов позволяют централизовать задачи сервера печати и сетевого принтера. Эта роль также позволяет получать отсканированные документы с сетевых сканеров и передавать документы в

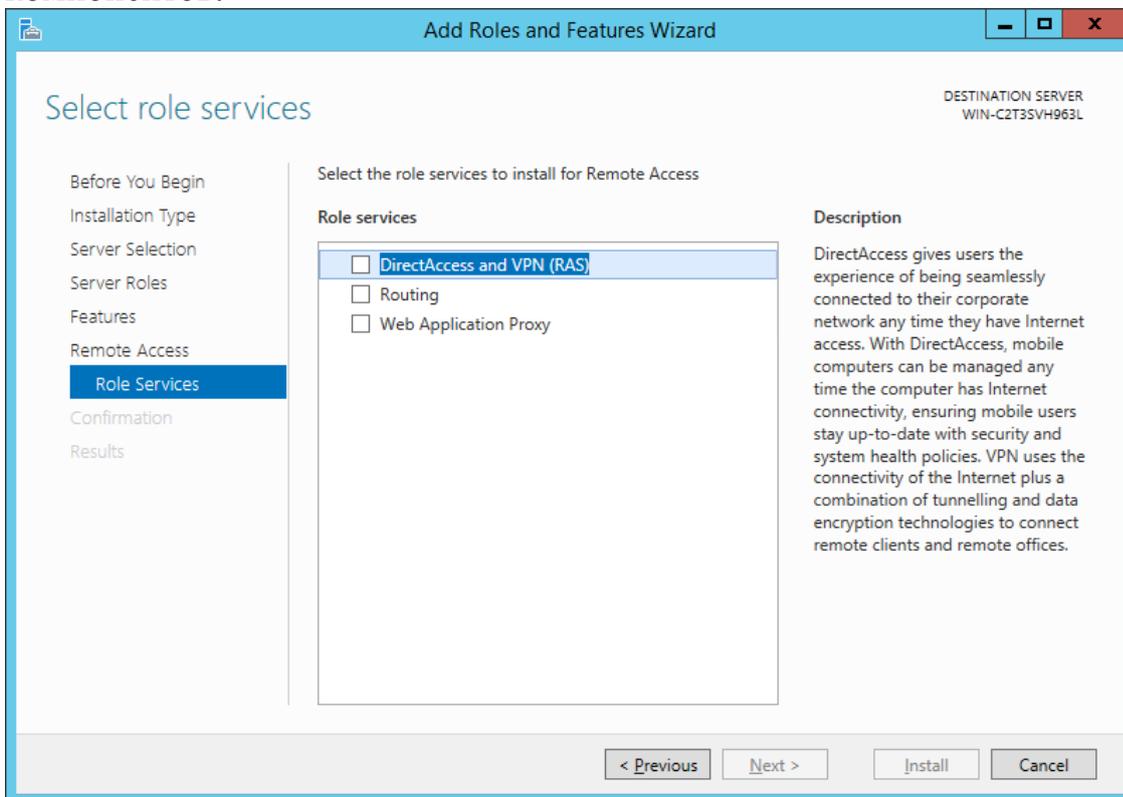
общие сетевые ресурсы – на сайт Windows SharePoint Services или по электронной почте.

Remote Access

Роль сервера удаленного доступа представляет собой логическую группу следующих технологий сетевого доступа.

- DirectAccess
- Маршрутизация и удаленный доступ
- Прокси-сервер веб-приложения

Эти технологии являются *службами ролей* роли сервера удаленного доступа. При установке роли сервера удаленного доступа можно установить одну или несколько служб ролей, запустив мастер добавления ролей и компонентов.



В Windows Server роль сервера удаленного доступа обеспечивает возможность централизованного администрирования, настройки и наблюдения за службами удаленного доступа DirectAccess и VPN со службой маршрутизации и удаленного доступа (RRAS). DirectAccess и RRAS можно развернуть на одном пограничном сервере и управлять ими с помощью команд Windows PowerShell и консоли управления (MMC) удаленного доступа.

Remote Desktop Services

Службы удаленных рабочих столов ускоряют и расширяют развертывание рабочих столов и приложений на любом устройстве, повышая эффективность удаленного работника, одновременно обеспечивая безопасность критически важной интеллектуальной собственности и упрощая со-

ответствие нормативным требованиям. Службы удаленных рабочих столов включают инфраструктуру виртуальных рабочих столов (VDI), рабочие столы на основе сеансов и приложения, предоставляя пользователям возможность работать в любом месте.

Volume Activation Services

Службы активации корпоративных лицензий – это роль сервера в Windows Server начиная с Windows Server 2012, которая позволяет автоматизировать и упростить выдачу корпоративных лицензий на программное обеспечение Microsoft, а также управление такими лицензиями в различных сценариях и средах. Вместе со службами активации корпоративных лицензий можно установить и настроить службу управления ключами (KMS) и активацию с помощью Active Directory.

Web Server (IIS)

Роль веб-сервера (IIS) в Windows Server обеспечивает платформу для размещения веб-узлов, служб и приложений. Использование веб-сервера обеспечивает доступ к информации пользователям в Интернете, интрасети и экстрасети. Администраторы могут использовать роль веб-сервера (IIS) для настройки и управления несколькими веб-сайтами, веб-приложениями и FTP-сайтами. В число специальных возможностей входят следующие.

- Использование диспетчера служб IIS для настройки компонентов IIS и администрирования веб-сайтов.
- Использование протокола FTP для разрешения владельцам веб-сайтов отправлять и загружать файлы.
- Использование изоляции веб-сайтов для предотвращения влияния одного веб-сайта на сервере на остальные.
- Настройка веб-приложений, разработанных с использованием различных технологий, таких как Classic ASP, ASP.NET и PHP.
- Использование Windows PowerShell для автоматического управления большей частью задач администрирования веб-сервера.
- Объединение нескольких веб-серверов в ферму серверов, которой можно управлять с помощью IIS.

Windows Deployment Services

Службы развертывания Windows позволяют развертывать операционные системы Windows по сети, что означает возможность не устанавливать каждую операционную систему непосредственно с компакт-диска или DVD-диска.

Windows Server Essentials Experience

Данная роль позволяет решать следующие задачи:

- защищать данные сервера и клиентов, создавая резервные копии сервера и всех клиентских компьютеров в сети;
- управлять пользователями и группами пользователей через упрощенную панель мониторинга сервера. Кроме того, интеграция с Windows Azure Active Directory *обеспечивает пользователям простой до-

ступ к интернет-службам Microsoft Online Services (например, Office 365, Exchange Online и SharePoint Online) с помощью их учетных данных домена;

- хранить данные компании в централизованном месте;
- интегрировать сервер с интернет-службами Microsoft Online Services (например, Office 365, Exchange Online, SharePoint Online и Windows Intune):
 - использовать на сервере функции повсеместного доступа (например, удаленный веб-доступ и виртуальные частные сети) для доступа к серверу, компьютерам сети и данным из удаленных расположений с высокой степенью безопасности;
 - получать доступ к данным из любого места и с любого устройства с помощью собственного веб-портала организации (посредством удаленного веб-доступа);
 - управлять мобильными устройствами, с которых осуществляется доступ к электронной почте организации с помощью Office 365 посредством протокола Active Sync, из панели мониторинга;
 - отслеживать работоспособность сети и получать настраиваемые отчеты о работоспособности; отчеты можно создавать по требованию, настраивать и отправлять по электронной почте определенным получателям.

Windows Server Update Services

Сервер WSUS предоставляет компоненты, которые необходимы администраторам для управления обновлениями и их распространения через консоль управления. Кроме того, сервер WSUS может быть источником обновлений для других серверов WSUS в организации. При реализации служб WSUS хотя бы один сервер служб WSUS в сети должен быть подключен к Центру обновления Майкрософт для получения информации о доступных обновлениях. В зависимости от безопасности сети и ее конфигурации администратор может определить, сколько других серверов напрямую подключено к Центру обновления Майкрософт.

5. Основы виртуализации.

Само по себе понятие виртуализации существует уже 50-60 лет. Еще в 60-х годах прошлого столетия этим вопросом занималась компания IBM. Однако, на тот момент виртуализация не нашла достаточного использования в существующих технологиях, поскольку компьютеров было немного и они всегда использовались под завязку. После появления персональных компьютеров в 80-х годах ситуация в корне не изменилась, поскольку идея заключалась в запуске всего лишь одной программы на одном устройстве, и поэтому использование ресурсов было очень низким. Всех это долгое время устраивало вплоть до наступления энергетического кризиса, когда

цена на электроэнергию возросла по всему миру. Как следствие, возник вопрос экономии ресурсов.

В 1999 году компания VMware впервые виртуализировала компьютер на базе Intel: на одном аппарате было запущено несколько операционных систем и, соответственно, несколько приложений. При этом затраты электроэнергии распределялись на несколько операционных систем уже на одном комплекте аппаратного обеспечения, что позволило рационализировать нагрузку.

Как всё это работает? Между сервером и операционными системами есть тонкий слой программного обеспечения для виртуализации или же на сервере устанавливается ОС, на которую накладывается уровень виртуализации.

Задачей виртуализации является введение в заблуждение ОС, чтобы она идентифицировала её как собственное аппаратное обеспечение. Подобные хитрости необходимы из-за слишком большого количества приложений, созданных под конкретную ОС. Таким образом виртуальная машина имеет ряд преимуществ, таких как *инкапсуляция*, *изоляция* отдельного приложения, *совмещение* его с ОС и другими программами, и при этом создаётся некая *независимость* аппаратного обеспечения. Рассмотрим эти компоненты по-отдельности.

Инкапсуляция – это сбор данных или функций в единый компонент. Создаётся программа, которая маскируется под отдельную физическую машину, выполняющую все свои функции. И ОС вместо того, чтобы идентифицировать набор различных устройств, на самом деле видит набор разных файлов.

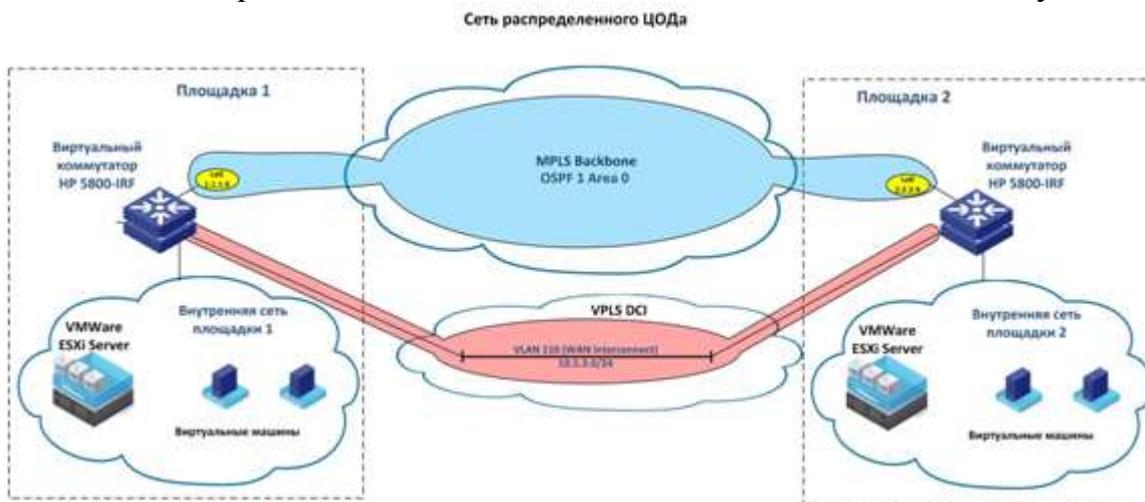
Изоляция означает, что все приложения, работая на одном устройстве, работают независимо друг от друга, идентифицируя себя, как разные устройства. В результате, если зависает или падает одна ОС, это никак не влияет на работу других ОС и приложений.

Совмещение означает создание отдельного кластера, где ОС и все системы, которые с ней работают имеют все функции отдельного компьютера. Но, хотя машина является виртуальной, а не реальной, она в любом случае взаимодействует со всеми ОС и приложениями, которые работают на базе Intel x86.

Независимость аппаратного обеспечения означает, что виртуальную машину можно перенести с реального аппаратного обеспечения на одной системе в другое без особых проблем. К примеру, рассмотри два сервера: HP и Cisco. Для переноса запущенной программы на ОС и обеспечении HP на Cisco в обычных условиях была бы необходима повторная инсталляция этой программе на новой ОС. В итоге, много работы по инсталляции и тестированию всей системы. Виртуальная же машина позволяет произвести беспрепятственный перенос с одной системы на другую. Причём большинство систем виртуальных машин позволяют переносить конкретную вир-

туальную машину с одной системы на другую в рабочем режиме серверов. Это также позволяет делиться ресурсами, дисковым пространством и процессорной мощностью. Так, для приложения, которому требуется большое количество дискового пространства, нет необходимости добавлять диски к физическому серверу – их можно реконфигурировать в процессе работы. Таким образом системные администраторы получают куда больший простор для творчества.

В современных условиях при установке в дата-центре нового обеспечения все машины виртуализируются. Виртуальными становятся сети, системы хранения и сами дата-центры. Сегодня при желании занять свой собственный центр обработки данных достаточно определиться с конфигурацией оборудования, обратиться в хостинговую компанию, где будет создан персональный ЦОД. Естественно, что физически всё заявленное оборудование должно где-то находиться. Основной дата-центр (производственный) – это часть видимая пользователем. Но есть еще один ЦОД (резервный), который имеет двойную роль: он функционирует как резервная копия реального ЦОД и как участок для разработчиков. Основной ЦОД предназначен для пользователя, а место для разработчиков – резервный ЦОД, где есть почва для тестирования приложений. После тестирования виртуальные машины переносятся из резервного ЦОД на основной, где непосредственно используются. В случае нештатных ситуаций в основном дата-центре виртуальные машины могут также перетаскиваться на резервный. Таким образом вся система становится намного более доступной.



Каковы же основные причины популярности виртуализации в наше время? Во-первых, это снижение затрат на физическую инфраструктуру, что означает меньшее количество серверов, шкафов, комнат. Во-вторых, снижение оперативных затрат, таких как электричество и охлаждение. В-третьих, увеличивается операционная гибкость и производительность системных администраторов.

Как яркий пример физической экономии можно привести модель, где 4 сервера, оснащённых системой VMware заменяет собой 50 физических

серверов. При этом производительность возросла с 5–10% до 80%, а вместо 10 шкафов требуется всего один. Касаемо операционных затрат, расход энергии снижается на 80%, при этом ещё 25% энергии снижается за счёт оптимизации нагрузки. Продуктивность работы системных администраторов увеличивается элементарно за счёт снижения количества выполняемых задач и большей доступности оборудования.

На данный момент половина серверов во всём мире виртуальны. Именно виртуализация является направляющей всей IT-индустрии, поэтому всё новейшее обеспечение готовится уже под задачи виртуализации.

6. Архитектура стека протоколов TCP/IP.

7. IP-адресация и маршрутизация.

Набор многоуровневых протоколов, или как называют стек TCP/IP (таблица), предназначен для использования в различных вариантах сетевого окружения. Стек TCP/IP с точки зрения системной архитектуры соответствует эталонной модели OSI (Open Systems Interconnection – взаимодействие открытых систем) и позволяет обмениваться данными по сети приложениям и службам, работающим практически на любой платформе, включая Unix, Windows, Macintosh и другие.

Семейство протоколов TCP/IP

Название протокола	Описание протокола
1	2
WinSock	Сетевой программный интерфейс
NetBIOS	Связь с приложениями ОС Windows
TDI	Интерфейс транспортного драйвера (Transport Driver Interface) позволяет создавать компоненты сеансового уровня.
TCP	Протокол управления передачей (Transmission Control Protocol)
UDP	Протокол пользовательских дейтаграмм (User Datagram Protocol)
ARP	Протокол разрешения адресов (Address Resolution Protocol)
RARP	Протокол обратного разрешения адресов (Reverse Address Resolution Protocol)
IP	Протокол Internet (Internet Protocol)
ICMP	Протокол управляющих сообщений Internet (Internet Control Message Protocol)

Название протокола	Описание протокола
IGMP	Протокол управления группами Интернета (Internet Group Management Protocol),
NDIS	Интерфейс взаимодействия между драйверами транспортных протоколов
FTP	Протокол пересылки файлов (File Transfer Protocol)
TFTP	Простой протокол пересылки файлов (Trivial File Transfer Protocol)

Реализация TCP/IP фирмы Microsoft соответствует четырехуровневой модели вместо семиуровневой модели, как показано на рис. 2.2. Модель TCP/IP включает большее число функций на один уровень, что приводит к уменьшению числа уровней. В модели используются следующие уровни:

- уровень Приложения модели TCP/IP соответствует уровням Приложения, Представления и Сеанса модели OSI;
- уровень Транспорта модели TCP/IP соответствует аналогичному уровню Транспорта модели OSI;

Модель OSI		Модель TCP/IP									
Уровень приложения	<table border="1" style="width: 100%; text-align: center;"> <tr> <td style="width: 50%;">Сокеты Windows</td> <td style="width: 50%;">NetBIOS</td> </tr> <tr> <td colspan="2">Интерфейс TDI</td> </tr> <tr> <td>TCP</td> <td>UDP</td> </tr> </table>	Сокеты Windows	NetBIOS	Интерфейс TDI		TCP	UDP	Уровень приложения			
Сокеты Windows		NetBIOS									
Интерфейс TDI											
TCP	UDP										
Уровень представления											
Уровень сеанса											
Уровень транспорта	<table border="1" style="width: 100%; text-align: center;"> <tr> <td colspan="3">Интерфейс NDIS</td> </tr> <tr> <td>ICMP</td> <td>IP</td> <td>ARP</td> </tr> <tr> <td>IGMP</td> <td></td> <td>RARP</td> </tr> </table>	Интерфейс NDIS			ICMP	IP	ARP	IGMP		RARP	Уровень транспорта
Интерфейс NDIS											
ICMP	IP	ARP									
IGMP		RARP									
Уровень сети		Межсетевой уровень									
Канальный уровень	<table border="1" style="width: 100%; text-align: center;"> <tr> <td style="width: 33%;">Ethernet</td> <td style="width: 33%;">Драйверы сетевых карт</td> <td style="width: 33%;">PPP</td> </tr> <tr> <td>FDDI</td> <td>Сетевые адаптеры</td> <td>Трансляция кадров</td> </tr> </table>	Ethernet	Драйверы сетевых карт	PPP	FDDI	Сетевые адаптеры	Трансляция кадров	Уровень сетевого интерфейса			
Ethernet		Драйверы сетевых карт	PPP								
FDDI	Сетевые адаптеры	Трансляция кадров									
Физический уровень											

Соответствие семиуровневой модели OSI и четырехуровневой модели TCP/IP

- межсетевой уровень модели TCP/IP выполняет те же функции, что и уровень Сети модели OSI;
- уровень сетевого интерфейса модели TCP/IP соответствует Канальному и Физическому уровням модели OSI.

Уровень Приложения

Через уровень Приложения модели TCP/IP приложения и службы получают доступ к сети. Доступ к протоколам TCP/IP осуществляется посредством двух программных интерфейсов (API – Application Programming Interface):

- Сокеты Windows;
- NetBIOS.

Интерфейс сокетов Windows, или как его называют WinSock, является сетевым программным интерфейсом, предназначенным для облегчения взаимодействия между различными TCP/IP – приложениями и семействами протоколов.

Интерфейс NetBIOS используется для связи между процессами (IPC – Interposes Communications) служб и приложений ОС Windows. NetBIOS выполняет три основных функции: определение имен NetBIOS; служба дейтаграмм NetBIOS; служба сеанса NetBIOS.

Уровень транспорта

Уровень транспорта TCP/IP отвечает за установления и поддержания соединения между двумя узлами. Основные функции уровня:

- подтверждение получения информации;
- управление потоком данных;
- упорядочение и ретрансляция пакетов.

В зависимости от типа службы могут быть использованы два протокола:

- TCP (Transmission Control Protocol – протокол управления передачей);
- UDP (User Datagram Protocol – пользовательский протокол дейтаграмм).

TCP обычно используют в тех случаях, когда приложению требуется передать большой объем информации и убедиться, что данные своевременно получены адресатом. Приложения и службы, отправляющие небольшие объемы данных и не нуждающиеся в получении подтверждения, используют протокол UDP, который является протоколом без установления соединения.

Протокол управления передачей (TCP)

Протокол управления передачей данных – TCP (Transmission Control Protocol) – обеспечивает надежную передачу сообщений между удаленными прикладными процессами за счет образования виртуальных соединений. Появился в начальный период создания сетей, когда глобальные сети не отличались особой надежностью.

Надежность протокола TCP заключается в следующем:

- он диагностирует ошибки,

- при необходимости посылает данные повторно,
- если не может самостоятельно исправить ошибку, сообщает о ней на другие уровни.

Перед отправкой сегментов информации вниз по модели отправляющий протокол TCP контактирует с принимающим протоколом TCP с целью установления связи. В результате создается виртуальный канал. Такой тип коммуникации называется ориентированным на соединение.

Установление соединения происходит в три шага:

1. Клиент, запрашивающий соединение, отправляет серверу пакет, указывающий номер порта, который клиент желает использовать, а также код (определенное число) ISN (Initial Sequence number).

2. Сервер отвечает пакетом, содержащий ISN сервера, а также ISN клиента, увеличенный на 1.

3. Клиент должен подтвердить установление соединения, вернув ISN сервера, увеличенный на 1.

Принцип работы TCP:

- берет из приложения большие блоки информации, разбивает их на сегменты,

- нумерует и упорядочивает каждый сегмент так, чтобы протокол TCP на принимающей стороне мог правильно соединить все сегменты в исходный большой блок;

- согласовывает с протоколом принимающей стороны количество информации, которое должно быть отправлено до получения подтверждения от принимающего TCP;

- после отправки сегментов TCP ждет подтверждения от целевого TCP о получении каждого из них;

- заново отправляет те сегменты, получение которых не было подтверждено.

Трехступенчатое открытие соединения устанавливает номер порта, а также ISN клиента и сервера. Каждый, отправляемый TCP-пакет содержит номера TCP-портов отправителя и получателя, номер фрагмента для сообщений, разбитых на меньшие части, а также контрольную сумму, позволяющую убедиться, что при передаче не произошло ошибок. Протокол TCP отвечает за надежную передачу данных от одного узла сети к другому. Он создает сеанс с установлением соединения, иначе говоря, виртуальный канал между машинами.

Пользовательский протокол дейтаграмм (UDP)

Протокол UDP предназначен для отправки небольших объемов данных (дейтаграмм) без установки соединения и используется приложениями, которые не нуждаются в подтверждении адресатом их получения [6]. UDP считается более простым протоколом, так как не загромождает сеть служебной информацией и выполняет не все функции TCP. Однако он

успешно справляется с передачей информации, не требующей гарантированной доставки, и при этом использует намного меньше сетевых ресурсов. UDP не создает виртуальных каналов и не контактирует с целевым устройством перед отправкой информации. Поэтому он считается протоколом без постоянного соединения, или не ориентированным на соединение [3].

Принцип работы UDP:

- получает с верхних уровней блоки информации, разбивает их на сегменты;
- нумерует каждый из сегментов, чтобы все сегменты можно было воссоединить в требуемый блок в пункте назначения, но не упорядочивает сегменты и не заботится о том, в каком порядке они поступят в место назначения,
- отправляет сегменты и «забывает» о них;
- не ждет подтверждений о получении и даже не допускает таких подтверждений и потому считается ненадежным протоколом. Но это не значит, что UDP неэффективен – просто он не относится к надежным протоколам.

UDP также использует номера портов для определения конкретного процесса по указанному IP-адресу. Однако UDP-порты отличаются от TCP-портов и, следовательно, могут использовать те же номера портов, что и TCP, без конфликта между службами.

Межсетевой уровень

Межсетевой уровень отвечает за маршрутизацию данных внутри сети и между различными сетями. На этом уровне работают маршрутизаторы, которые зависят от используемого протокола и используются для отправки пакетов из одной сети (или ее сегмента) в другую (или другой сегмент сети). В стеке TCP/IP на этом уровне используется протокол IP.

Протокол Интернета IP

Протокол IP обеспечивает обмен дейтаграммами между узлами сети и является протоколом, не устанавливающим соединения и использующим дейтаграммы для отправки данных из одной сети в другую. Данный протокол не ожидает получение подтверждения (ASK, Acknowledgment) отправленных пакетов от узла адресата. Подтверждения, а также повторные отправки пакетов осуществляется протоколами и процессами, работающими на верхних уровнях модели.

К его функциям относится фрагментация дейтаграмм и межсетевая адресация. Протокол IP предоставляет управляющую информацию для сборки фрагментированных дейтаграмм. Главной функцией протокола является межсетевая и глобальная адресация. В зависимости от размера сети, по которой будет маршрутизироваться дейтаграмма или пакет, применяется одна из трех схем адресации.

Адресация в IP-сетях

Каждый компьютер в сетях TCP/IP имеет адреса трех уровней: физический (MAC-адрес), сетевой (IP-адрес) и символьный (DNS-имя) [3].

Физический, или локальный адрес узла, определяемый технологией, с помощью которой построена сеть, в которую входит узел. Для узлов, входящих в локальные сети – это MAC-адрес сетевого адаптера или порта маршрутизатора, например, 11-A0-17-3D-BC-01. Эти адреса назначаются производителями оборудования и являются уникальными адресами, так как управляются централизованно. Для всех существующих технологий локальных сетей MAC-адрес имеет формат 6 байтов: старшие 3 байта – идентификатор фирмы производителя, а младшие 3 байта назначаются уникальным образом самим производителем.

Сетевой, или IP-адрес, состоящий из 4 байт, например, 109.26.17.100. Этот адрес используется на сетевом уровне. Он назначается администратором во время конфигурирования компьютеров и маршрутизаторов. IP-адрес состоит из двух частей: номера сети и номера узла. Номер сети может быть выбран администратором произвольно, либо назначен по рекомендации специального подразделения Internet (Network Information Center, NIC), если сеть должна работать как составная часть Internet. Обычно провайдеры услуг Internet получают диапазоны адресов у подразделений NIC, а затем распределяют их между своими абонентами. Номер узла в протоколе IP назначается независимо от локального адреса узла. Деление IP-адреса на поле номера сети и номера узла гибкое, и граница между этими полями может устанавливаться произвольно. Узел может входить в несколько IP-сетей. В этом случае узел должен иметь несколько IP-адресов, по числу сетевых связей. IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

При разработке протокола IP на основе размера сетей были выделены их классы (см. таблицу):

Класс а – немногочисленные сети с очень большим количеством узлов; номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети.

Класс В – сети средних размеров; под адрес сети и под адрес узла отводится по 16 битов (по 2 байта).

Класс С – сети с малым числом узлов; под адрес сети отводится 24 бита (3 байта), а под адрес узла – 8 битов (1 байт).

Классы сетей

Класс	Формат	Диапазон адресов	Максимальное количество сетей	Максимальное количество узлов в одной сети
А	0Сеть.узел.узел.узел	0.0.0.0 – 0.255.255.255	зарезервировано	
		1.0.0.0 – 126.255.255.255	126	16 777 216
		127.0.0.0 – 127.255.255.255	зарезервировано	
В	10Сеть.сеть.узел.узел	128.XXX.0.0 – 191.XXX.255.255	16 384	65 534
С	110Сеть.сеть.сеть.узел	192.XXX.XXX.0 – 223.XXX.255.255	2 097 152	254
Д	1110Группа.группа. группа.группа	224.0.0.0 – 239.255.255.255	–	268 435 454
Е	1111Резерв.резерв. ре- зерв.резерв	240.0.0.0 – 255.255.255.255	зарезервировано	

Адреса класса D – особые, групповые адреса – multicast; могут использоваться для рассылки сообщений определенной группе узлов. Если в пакете указан адрес назначения, принадлежащий классу D, то такой пакет должны получить все узлы, которым присвоен данный адрес.

Адреса класса E зарезервированы для будущих применений.

Помимо вышеописанных адресов существуют зарезервированные адреса, которые используются особым образом.

- если в поле номера сети стоят 0

0 0 0 0.....0 Номер узла,

то по умолчанию считается, что этот узел принадлежит той же самой сети, что и узел, который отправил пакет: если адрес компьютера 128.187.0.0, то указанный в сообщении адрес 0.0.25.31 неявно преобразуется в адрес 128.187.25.31;

- адрес 127.0.0.X зарезервирован для организации обратной связи при тестировании работы программного обеспечения узла без реальной отправки пакета по сети. Этот адрес имеет название loopback или localhost. Если программа отправит пакет с таким адресом, то этот пакет, не выйдя за пределы компьютера, пройдет по всем уровням сетевой подсистемы и вернется к этой программе. Позволяет разрабатывать и тестировать сетевое программное обеспечение на локальном компьютере, в т. ч. и вообще не имеющем сетевого адаптера.

- если все двоичные разряды IP-адреса равны 1

1 1 1 1.....1 1,

то пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и отправитель. Такая рассылка называется ограниченным широковещательным сообщением (limited broadcast);

- если в поле адреса узла назначения стоят сплошные 1

Адрес сети 1111.....11,

то пакет, имеющий такой адрес, рассылается всем узлам сети с заданным адресом. Такая рассылка называется широковещательным сообщением (broadcast);

- адреса класса D – форма группового IP-адреса – multicast. Пакет должен быть доставлен сразу нескольким узлам, которые образуют группу с номером, указанным в поле адреса. Узлы сами идентифицируют себя, то есть определяют, к какой из групп они относятся. Один и тот же узел может входить в несколько групп. Такие сообщения, в отличие от широковещательных, называются мультивещательными. Групповой адрес не делится на поля номера сети и узла и обрабатывается маршрутизатором особым образом.

Символьный адрес, или DNS-имя, например, SERV1.IBM.COM. Этот адрес назначается администратором и состоит из нескольких частей, например, имени машины, имени организации, имени домена. Такой адрес используется на прикладном уровне, например, в протоколах FTP или telnet.

Числовая адресация удобна для машинной обработки таблиц маршрутов. Для использования человеком она представляет определенные трудности. Для облегчения взаимодействия вначале применялись таблицы соответствия числовых адресов именам машин. Например, в ОС UNIX в каталоге /etc находится файл с именем hosts, который может иметь следующий вид:

```
IP-адрес  Имя машины
127.0.0.1 localhost
144.206.160.32 Polyn
144.206.160.40 Apollo
```

По мере роста сети была разработана система доменных имен – DNS (Domain Name System), которая позволяет присваивать компьютерам легко запоминаемые имена, например yahoo.com, и отвечает за перевод этих имен обратно в IP-адреса. DNS строится по иерархическому принципу, однако эта иерархия не является строгой. Фактически нет единого корня всех доменов Internet.

Компьютерное имя имеет по меньшей мере два уровня доменов, отделяемых друг от друга точкой (.). Идущие после доменов верхнего уровня домены обычно определяют либо регионы (msk), либо организации (ulstu). Следующие уровни иерархии могут быть закреплены за небольшими организациями, либо за подразделениями больших организаций или частными лицами (например, alvinsoft.h11.ru).

Все, что находится слева, является поддоменом для общего домена. Таким образом, в имени somesite.uln.ru, somesite является поддоменом uln, который в свою очередь является поддоменом ru.

Наиболее популярной программой поддержки DNS является BIND, или Berkeley Internet Name Domain, – сервер доменных имен, который широко применяется в Internet. Он обеспечивает поиск доменных имен и IP-адресов для любого узла сети. BIND обеспечивает также рассылку сообщений электронной почты через узлы Internet.

BIND реализован по схеме «клиент-сервер». Различают четыре вида серверов:

- primary master-сервер поддерживает свою базу данных имен и обслуживает местный домен;

- secondary master-сервер обслуживает свой домен, но данные об адресах части своих машин получает по сети с другого сервера;

- caching-сервер не имеет своего домена. Он получает данные либо с одного из master-серверов, либо из буфера;

- удаленный сервер обычный master-сервер, установленный на удаленной машине, к которому обращаются программы по сети.

Primary или secondary master-серверы устанавливаются обычно на машинах, которые являются шлюзами для локальных сетей.

Шлюз (Gateway) – система, выполняющая преобразование из одного формата в другой.

Сервер имен может быть установлен на любой компьютер локальной сети. При этом необходимо учитывать его производительность, так как многие реализации серверов держат базы данных имен в оперативной памяти. При этом часто подгружается информация и с других серверов. Поэтому это может быть причиной задержек при разрешении запроса на адрес по имени машины.

Протоколы сопоставления адреса ARP и RARP

Для определения локального адреса по IP-адресу используется протокол разрешения адреса Address Resolution Protocol (ARP) [3]. ARP работает различным образом в зависимости от того, какой протокол канального уровня работает в данной сети – протокол локальной сети (Ethernet, Token Ring, FDDI) с возможностью широковещательного доступа одновременно ко всем узлам сети, или же протокол глобальной сети (X.25, frame relay), как правило, не поддерживающий широковещательный доступ. Существует также протокол, решающий обратную задачу – нахождение IP-адреса по известному локальному адресу. Он называется реверсивный ARP – RARP (Reverse Address Resolution Protocol) и используется при старте бездисковых станций, не знающих в начальный момент своего IP-адреса, но знающих адрес своего сетевого адаптера.

В локальных сетях ARP использует широковещательные кадры протокола канального уровня для поиска в сети узла с заданным IP-адресом.

Узел, которому нужно выполнить отображение IP-адреса на локальный адрес, формирует ARP-запрос, вкладывает его в кадр протокола канального уровня, указывая в нем известный IP-адрес, и рассылает запрос широковещательно. Все узлы локальной сети получают ARP-запрос и сравнивают указанный там IP-адрес с собственным адресом. В случае их совпадения узел формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес и отправляет его уже направленно, так как в ARP-запросе отправитель указывает свой локальный адрес. ARP-запросы и ответы используют один и тот же формат пакета.

Протокол ICMP

Протокол управления сообщениями Интернета (ICMP – Internet Control Message Protocol) используется IP и другими протоколами высокого уровня для отправки и получения отчетов о состоянии переданной информации. Этот протокол используется для контроля скорости передачи информации между двумя системами. Если маршрутизатор, соединяющий две системы, перегружен трафиком, он может отправить специальное сообщение ICMP-ошибку для уменьшения скорости отправления сообщений. Является частью сетевого уровня набора протоколов TCP/IP.

Протокол ICMP для своих целей использует сообщения, два из которых называются эхо-запрос ICMP и эхо-ответ ICMP:

Эхо-запрос подразумевает, что компьютер, которому он был отправлен, должен ответить на этот пакет.

Эхо-ответ – это тип ICMP-сообщения, которое используется для ответа на такой запрос.

Эти сообщения отправляются и принимаются с помощью команды **ping** (Packet Internet Groper).

С помощью специальных пакетов ICMP можно получить информацию:

- о невозможности доставки пакета,
- о превышении времени жизни пакета,
- о превышении продолжительности сборки пакета из фрагментов,
- об аномальных величинах параметров,
- об изменении маршрута пересылки и типа обслуживания,
- о состоянии системы и т. п.

Протокол IGMP

Узлы локальной сети используют протокол управления группами Интернета (IGMP – Internet Group Management Protocol), чтобы зарегистрировать себя в группе. Информация о группах содержится на маршру-

тизаторах локальной сети. Маршрутизаторы используют эту информацию для передачи групповых сообщений.

Групповое сообщение, как и широковещательное, используется для отправки данных сразу нескольким узлам.

NDIS

Network Device Interface Specification (NDIS) – спецификация интерфейса сетевого устройства, программный интерфейс, обеспечивающий взаимодействие между драйверами транспортных протоколов, и соответствующими драйверами сетевых интерфейсов. Позволяет использовать несколько протоколов, даже если установлена только одна сетевая карта.

Уровень сетевого интерфейса

Этот уровень модели TCP/IP отвечает за распределение IP-дейтаграмм. Он работает с ARP для определения информации, которая должна быть помещена в заголовок каждого кадра. Затем на этом уровне создается кадр, подходящий для используемого типа сети, такого как Ethernet, Token Ring или ATM, затем IP-дейтаграмма помещается в область данных этого кадра, и он отправляется в сеть.

8. Имена в TCP/IP и протокол DHCP.

Стеком протоколов TCP/IP называют набор сетевых протоколов, используемых в интернете.

В этом стеке различают несколько уровней, и протоколы высокого уровня всегда базируются на протоколах более низких уровней.

В самом низу находятся *физический уровень* и *канальный уровень*. Пример – интерфейс Ethernet, описывающий передачу данных по коаксиальному кабелю или витой паре. Протоколы этих уровней обычно реализуются на уровне железа, например в сетевой карте компьютера.

Выше идёт *сетевой уровень*, где находится протокол IP, описывающий структуру сети и доставку пакетов.

Ещё выше – *транспортный уровень*, где находится протокол TCP, использующийся для передачи данных. Эти протоколы обычно реализуются на уровне операционной системы.

На самом верху находится множество протоколов *прикладного уровня*, выполняющих конкретные прикладные задачи. Обычно они программируются в отдельных приложениях.

IP – протокол, лежащий в основе Интернета, его название так и расшифровывается: Internet Protocol.

В настоящее время используются следующие две версии протокола IP:

- **IPv6** – сравнительно новая (текущая версия спецификации опубликована в декабре 1998^[11]); IP-адрес имеет разрядность 128 бит и записывается в виде восьми 16-битных полей, с использованием шестнадцатеричной системы счисления и с возможностью сокращения двух и более последовательных нулевых полей до `::`; пример: `2001:db8:42::1337:cafe`;

- **IPv4** – «классическая» (1981 г.^[21]); IP-адрес имеет разрядность 32 бита и записывается в виде четырех десятичных чисел в диапазоне 0 ... 255 через точку; пример: `192.0.2.34`.

Каждый узел может напрямую связаться только с узлами своей *сети* (например: подключенными к тому же сегменту Ethernet), для определения которых используется *адрес сети* – часть IP-адреса, определяемая маской сети). Связь с узлами других сетей осуществляется через промежуточные узлы – маршрутизаторы.

Посмотреть, как выглядит маршрут пакета от вашего компьютера к другим узлам, можно с помощью команды tracert (в Linux) или tracert (в Windows).

TCP протокол базируется на IP для доставки пакетов, но добавляет две важные вещи:

- *установление соединения* – это позволяет ему, в отличие от IP, гарантировать доставку пакетов
- *порты* – для обмена пакетами между приложениями, а не просто узлами

Протокол TCP предназначен для обмена данными – это «надежный» протокол, потому что:

1. Обеспечивает надежную доставку данных, так как предусматривает установления логического соединения;
2. Нумерует пакеты и подтверждает их прием квитанцией, а в случае потери организует повторную передачу;
3. Делит передаваемый поток байтов на части – сегменты – и передает их нижнему уровню, на приемной стороне снова собирает их в непрерывный поток байтов.

TCP-соединение

Соединение двух узлов начинается с *handshake* (рукопожатия):

1. Узел А посылает узлу В специальный пакет SYN – приглашение к соединению
2. В отвечает пакетом SYN-ACK – согласием об установлении соединения
3. А посылает пакет ACK – подтверждение, что согласие получено

После этого TCP-соединение считается установленным, и приложения, работающие в этих узлах, могут посылать друг другу пакеты с данными.

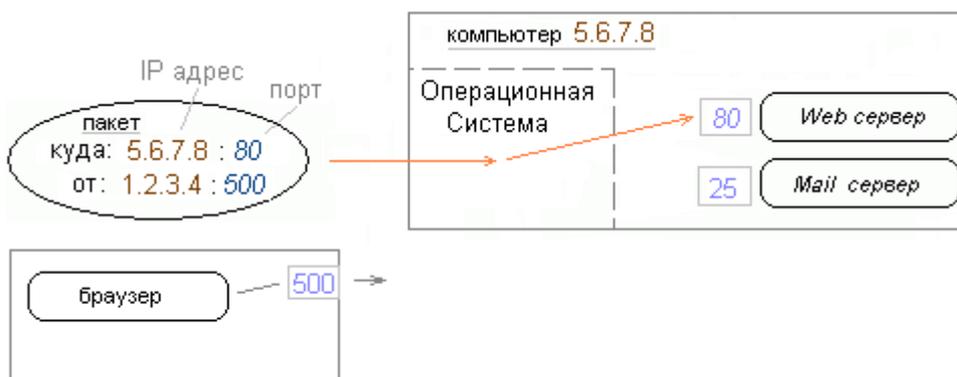
«Соединение» означает, что узлы помнят друг о друге, нумеруют все пакеты, идущие в обе стороны, посылают подтверждения о получении каждого пакета и перепосылают потерявшиеся по дороге пакеты.

Для узла А это соединение называется **исходящим**, а для узла В – **входящим**.

Отметим, что эти термины не имеют никакого отношения к входящему или исходящему трафику. Они показывают только инициатора соединения, то есть направление самого первого пакета (SYN). Любое установленное TCP-соединение симметрично, и пакеты с данными по нему всегда идут в обе стороны.

Когда один из узлов решает, что пора заканчивать соединение, он посылает специальный пакет FIN, после этого узлы прощаются и разрывают соединение.

Порт



Сетевой порт – это сетевой ресурс, отображаемый в виде числа (1-65535), которое определяет назначение входящих или исходящих сетевых потоков данных на заданном устройстве.

Если прибегнуть к аналогии, IP адрес – это адрес общежития с вахтёром, а порт – номер комнаты в этом общежитии или фамилия ее жильца.

Согласно IP, в каждом пакете присутствуют IP-адрес узла-источника и IP-адрес узла-назначения. В TCP-пакетах дополнительно указываются *порт источника* и *порт назначения*.

Например, почтовое письмо (пакет данных) имеет информацию об отправителе (порт) и информацию о получателе (фамилия или номер комнаты по конкретному адресу).

Узел назначения ("вахтер"), получив пакет ("письмо"), смотрит на порт назначения ("фамилию или номер комнаты") и передает пакет соответствующему у себя приложению ("конкретному жильцу").

Использование портов позволяет независимо использовать TCP протокол ("почтовые услуги") сразу многим приложениям на одном и том же компьютере (общежитии).

Клиентом называют приложение, которое пользуется каким-то сервисом, предоставляемым другим приложением – Сервером, обычно на

удаленном компьютере. Практически всегда клиент начинает исходящие соединения, а сервер ожидает входящих соединений (от клиентов), хотя бывают и исключения.

Сервер при запуске сообщает Операционной Системе, что хотел бы «занять» определенный порт (или несколько портов). После этого все пакеты, приходящие на компьютер к этому порту, ОС будет передавать этому серверу. Говорят, что сервер «слушает» этот порт.

Клиент, начиная соединение, запрашивает у своей ОС какой-нибудь незанятый порт во временное пользование, и указывает его в посланных пакетах как порт источника. Затем на этот порт он получит ответные пакеты от сервера.

Таким образом, сервер:

- слушает на определённом порту, заранее известном клиенту
- занимает этот порт всё время, пока не завершит работу
- об IP-адресе и номере порта клиента узнаёт из приглашения, посланного клиентом

Клиент:

- заранее знает IP-адрес и порт сервера
- выбирает у себя произвольный порт, который освобождает после окончания соединения
- посылает приглашение к соединению

UDP

UDP – это ещё один протокол транспортного уровня. Он тоже базируется на IP и тоже использует порты, но в отличие от TCP он не устанавливает соединений и не требует подтверждения получения каждого пакета.

Поэтому пакеты могут теряться или приходить в неправильном порядке. Зато этот протокол быстрее и использует меньше ресурсов.

На UDP обычно базируют прикладные протоколы, которым скорость доставки данных важнее надежности, например для передачи потокового видео, общения голосом или онлайн-игр.

Прикладные протоколы

Большинство прикладных протоколов базируется на TCP.

У многих протоколов прикладного уровня для серверов определены **стандартные порты**, используемые по умолчанию. Самые известные прикладные протоколы и их стандартные порты:

- **HTTP** – основной протокол всемирной паутины (TCP-порт 80)
- **SMTP** – протокол пересылки почты (TCP-порт 25)
- **FTP** – протокол передачи файлов (TCP-порт 21)
- **DNS** – протокол сопоставления доменных имен IP-адресам (UDP-порт 53)

Благодаря использованию стандартных портов мы можем набирать в браузере адреса веб серверов и не указывать порт – наши браузеры сами добавляют стандартный номер порта. Например, ад-

рес <http://www.example.com/> на самом деле полностью выглядит так: <http://www.example.com:80/>

Разумеется, стандартный – не значит обязательный. Практически во всех прикладных протоколах можно указать серверу слушать произвольный номер порта. Правда, тогда этот номер уже указывать обязательно, например <http://www.example.com:8080/>

Порты в диапазоне от 1 до 1023 называются *хорошо известными*. Службы, которыми используются эти порты, должны быть описаны как RFC и одобрены IESG. Далее идут *зарегистрированные порты* (1024 – 49151). Вы можете зарегистрировать в IANA (эта организация как раз занимается всем этим) один или несколько из этих портов под свою программу. Оставшиеся порты с 49152 по 65535 можно использовать без какой-либо регистрации.

- Номера портов (IANA)

URI

Чтобы указать на документ, расположенный в сети, используется *унифицированный идентификатор ресурса*, или URI (англ. Unified Resource Identifier), например: <https://ru.wikibooks.org/wiki/TCP/IP>. Первая часть адреса (от начала до двоеточия) называется *схемой* (в данном случае – https). Дальше идёт часть, зависящая от схемы.

Идентификаторы ресурсов (URI) в свою очередь делят на включающие информацию о размещении ресурса в сети URL (англ. Unified Resource Locator), и лишённые таковой URN (англ. Unified Resource Name.) Приведенный выше URI является примером URL; примеры URN: news:m5jgdq\$7ig\$1@reader1.panix.com, urn:ietf:rfc:2648, urn:isbn:0-13-066102-3, geo:48.2010,16.3695,183.

Ясно, что для получения ресурса по его URN, программное обеспечение должно вначале каким-либо образом определить (или предположить) его наличие на некотором сетевом ресурсе. Так, NNTP-сервер для URN-схемы news: может быть задан переменной окружения NNTPSERVER. Относящиеся к пространству urn:ietf: URN можно преобразовать по образцу: urn:ietf:rfc:2648 → <https://tools.ietf.org/html/rfc2648>, или же <https://www.rfc-editor.org/rfc/rfc2648.txt>.

DHCP – это протокол динамической настройки узла.

Как можно понять из названия, DHCP предназначен для настройки хоста через удаленный сервер. DHCP поддерживается по умолчанию большинством современных операционных систем, и этот протокол выступает в качестве отличной альтернативы рутинной ручной настройке параметров сети для сервера или подключаемого устройства.

Данный протокол работает на основе модели "Клиент-сервер". Являясь протоколом, DHCP имеет свой собственный метод обмена сообщения-

ми между клиентом и сервером. Ниже представлен состав сообщения DHCP:

Поле	Длина (байты)	Описание
op	1	Тип сообщения
htype	1	Тип адреса аппаратной части
hlen	1	Длина адреса аппаратной части
hops	1	Используемое количество агентов ретрансляции. Клиенты устанавливают значение на 0.
xid	4	ID (уникальный идентификационный номер) транзакции используемой клиентом и серверов во время сессии
secs	2	Прошедшее время (в секундах) с момента запроса клиентом начала процесса
flags	2	Значение флагов
ciaddr	<i>Также интересно:</i> 4	IP-адрес клиента (если имелся ранее).
yiaddr	4	IP-адрес, предложенный сервером клиенту
siaddr	4	IP-адрес сервера
giaddr	4	IP-адрес relay-агента (агента ретрансляции)
chaddr	16	Адрес аппаратной части клиента (в основном MAC).
sname	64	Имя сервера.
file	128	Название загрузочного файла.
options	изменяемая	Дополнительные опции

Знание основ DHCP помогает в устранении различных проблем с сетью. В следующей части статьи мы затронем принципы работы протокола.

Как работает DHCP?

Перед изучением самого процесса, с помощью которого достигается поставленная цель, необходимо понять различные принципы обмена информацией, которые используются в данном процессе.

DHCPDISCOVER

Это сообщение обозначает начало DHCP взаимодействия между клиентом и сервером. Данное сообщение отправляется клиентом (компьютером или устройством), подключенным к сети. В этом сообщении используется 255.255.255.255 как IP-адрес доставки, тогда как исходным адресом является 0.0.0.0

DHCPOFFER

Это сообщение отправляется в ответ на DHCPDISCOVER от сервера DHCP для подключенных клиентов. В этом сообщении содержатся необходимые сетевые настройки.

DHCPREQUEST

Данное сообщение является ответом на DHCP OFFER, и обозначает, что клиент принял отправленные настройки.

DHCPACK

Данное сообщение отправляется на сервер протокола DHCP в ответ на DHCPREQUEST от клиента. Сообщение обозначает конец процесса, начатого с сообщения DHCPDISCOVER. Т.е. DHCPACK – это не что иное, как подтверждение от сервера начала авторизации клиента и принятие параметров конфигурации, полученных в самом начале от сервера.

DHCPNAK

Данное сообщение является противоположностью DHCPACK, описанного выше. Оно отправляется на сервер в случае, если невозможно удовлетворить параметры DHCPREQUEST клиента.

DHCPDECLINE

Сообщение отправляется клиентом на сервер в случае, если IP-адрес, присваиваемый в DHCP уже используется.

DHCPINFORM

Сообщение отправляется серверу в том случае, если клиенту DHCP присвоен статический IP-адрес, а по настройкам конфигурации необходим динамический адрес.

DHCPRELEASE

Сообщение отправляется клиентом в том случае, если он завершает процесс использования сетевого адреса.

Теперь, когда мы познакомились с различными сообщениями в DHCP, можно изучить весь процесс работы, чтобы получить более полное представление. Шаги ниже описываются исходя из того, что все настройки установлены по умолчанию.

Шаг 1.

Когда клиент (компьютер или устройство) загружается или подключается к сети, серверу отправляется сообщение DHCPDISCOVER. Если нет никаких дополнительных данных о конфигурации, то сообщение отправляется с адреса 0.0.0.0 к 255.255.255.255. Если сервер DHCP находится в локальной подсети, то она напрямую получает сообщение, если он находится в другой подсети, то используется агент ретрансляции для передачи запроса к серверу DHCP. Используется протокол передачи UDP через порт 67. Клиент на данном этапе начинает стадию авторизации.

Шаг 2.

В тот момент как сервер получил запрос DHCPDISCOVER, то он отправляет в ответ сообщение DHCP OFFER. Как говорилось ранее, в этом сообщении содержатся все необходимые параметры конфигурации, запрашиваемые клиентом. Например, IP-адрес, необходимый клиенту, а также значение маски подсети и информация о шлюзе. Также сервер сразу заполняет значения MAC-адреса в поле CHADDR. Сообщение отправляется клиенту от адреса 255.255.255.255 напрямую, а если сервер находится в

другой подсети, то используются агенты ретрансляции, который отвечает за то, чтобы сообщение было доставлено. В этом случае для передачи применяется протокол UDP через порт 68. На этом этапе клиент начинает подбирать параметры.

Шаг 3.

Клиент формирует сообщение DHCPREQUEST, которое служит ответом на DHCPOFFER от сервера, указав, что он принимает параметры конфигурации, отправленные ему. Если бы было несколько серверов DHCP, то клиент бы получил также несколько сообщений DHCPOFFER, но клиент отвечает только одному серверу, заполняя параметры конфигурации для настройки. Таким образом, он проходит авторизацию с получением IP-адреса от одного конкретного сервера DHCP. Все сообщения от других серверов блокируются. Сообщение DHCPREQUEST по-прежнему будет содержать адрес источника 0.0.0.0, если клиенту все еще нельзя использовать IP-адреса, полученные в сообщении DHCPOFFER. В течение этого этапа клиент получает ответы на свои запросы.

Шаг 4.

Как только сервер получает DHCPREQUEST от клиента, он посылает DHCPACK сообщение о том, что теперь клиент может использовать IP-адрес, назначенный к нему. Клиент окончательно подключается к сети и с настроенными параметрами.

Концепция аренды

В дополнении к остальной необходимой информации о том, как работает DHCP, следует также знать IP-адрес, назначенный в DHCP сервером в аренду клиенту. После истечения срока аренды сервер DHCP может свободно присвоить этот IP-адрес другому компьютеру или устройству, запрашивающему то же самое. Например, сохранение срока аренды 8-10 часов полезно для компьютеров, которые обычно выключают в конце дня. Поэтому аренда должна продлеваться время от времени. После истечения половины срока аренды, DHCP клиент обычно пытается автоматически продлить данный срок. Это делается путем обмена DHCPREQUEST и DHCPACK сообщениями. Благодаря этому начинается стадия обновления данных для клиента.

9. Планирование и управление Active Directory.

Что необходимо понимать под таким мудреным определением как «Планирование ActiveDirectory»? А если по простому – нельзя просто так установить Windows Server, а потом поднять Active Directory и все, а потом «как карта ляжет», так как часто неопытные сетевые администраторы так и делают, а потом пожизненно имеют проблемы по данному направлению.

Вообще проектирование систем на базе Windows Server требует больших ресурсов, как временных, так и людских. Успех проекта зависит во многом от того, насколько корректно управляется проект, как распределены ресурсы, от подготовленности специалистов и персонала. Довольно много работы, перед тем как начать самое простое в данном вопросе, установку Windows Server. Самое главное это правильно сформулировать и определить цели и задачи, «зачем» и «для чего» мы это делаем.

Процесс проектирования инфраструктуры Active Directory состоит из четырех этапов, а именно:

- Создание плана лесов.
- Создание плана доменов.
- Создание плана подразделений.
- Создание топологического плана сайтов.

Вроде бы с первого раза все просто. Но конкретных советов в развертывании быть не могут, потому как каждый проект индивидуален, и имеет свои, только ему присущие особенности, так что советы могут быть только общего плана. Поэтому в проектировании Active Directory необходимо объединить усилия большего количества людей для реализации этого проекта.

Исполнители проекта, их количество и их роли зависят от масштаба проекта, но их роли остаются неизменными, даже когда всем этим занимается один системный администратор, просто он совмещает по очереди все эти роли.

Под понятием «проектным решением инфраструктуры Active Directory» мы будем понимать план, отражающий сетевую структуру нашего предприятия.

Руководитель службы ИТ. В их обязанностях входит определение и установка новых приоритетов планируемой инфраструктуры. Помогает определить цель проекта. Выступает посредником между исполнителями проекта и вышестоящими. Решает возникшие конфликты. Понимает проблемы организации. Ясно представляет, какие проблемы можно решить средствами Windows Server и Active Directory на данном предприятии.

Руководитель проекта. Принимает решения по разворачиванию новой инфраструктуры в заданное время и в рамках, определенных в проекте. С членами команды определяет задачи проекта, спецификации новой инфраструктуры. Вырабатывает график работ.

Глубоко знает свойства Windows XP Professional (Windows 7) и Windows Server. Увязывает цели руководства с целями команды.

Разработчик и тестировщик. Рассматривает технические решения, планируемые к использованию в новой инфраструктуре. Помогают разрабатывать начальное решение. Определяют потенциальные проблемы и способы их разрешения до разворачивания. Играет активную роль в разработке инфраструктуры. Знания в области разработки сложных служб опе-

рационной системы. Понимание технических требований. Отвечают за разработку отдельных звеньев, например, Active Directory, системы безопасности, почтовой системы и т. п. Высокий уровень знаний в своих областях и глубокое знание Windows 2003. Имеет навыки управления проектом. Выполняют анализ производительности и масштабируемости. Знание требований к совместимому оборудованию. Имеет опыт в отладке и тестировании систем и приложений.

Это не универсальная схема. Так как задачу разработчиков и тестировщиков можно разграничить отдельно. Так же здесь не указан персонал, который будет ответственен за обучение пользователей, а так же специалистов которые будут все эти процессы документировать, что является так же очень важной стороной процесса проектирования.

В зависимости от целей и задач проекта можно сформировать группы, ответственные за ключевые направления:

- Active Directory;
- службу имен (DNS, WINS, DHCP);
- безопасность;
- администрирование;
- работу приложений в среде Windows Server (различных необходимых производственных программ и баз данных)
- почту;
- конфигурирование клиентов;
- управление удаленными пользователями;

**При планировании руководствуйтесь основным правилом:
Чем проще, тем лучше.**

Чем больше звеньев, лесов, доменов, тем сложнее управление. Постарайтесь воспроизводить сложную структуру организации только в крайних случаях. Скажем, стремясь снизить трафик репликации, вы создадите сложную структуру сайтов и связей между ними. Но помните, что при этом вы усложните процесс управления этими сайтами ну и так далее.

Но и при использовании, данного правила не старайтесь есть борщ вилкой. Структура каталога должна отражать структуру организации, быть удобна, проста в управлении, легко изменяема если в этом возникнет необходимость и всегда доступна. При правильно спроектированным Active Directory, есть гарантия, что вы избавитесь от различного «геморроя», но не забывайте что Active Directory универсальное лекарство, способная решить абсолютно все проблемы организации.

Итак, сперва вам как допустим руководителю службы ИТ и с вашей командой, нужно произвести ревизию сети, и всех имеющихся в сети ресурсов, программного обеспечения. Это обязательное начало, и при этом необходимо все это задокументировать. Так же нужно произвести анализ коммерческого контекста, бизнес процессов, направление имеющегося

потока данных. И это также надо задокументировать. О составлении и согласовании технического задания и прочего говорить не буду, хотя иногда это спасает от многих конфликтов, так как некоторые пользователи "просыпаются" тогда когда уже поздно менять что либо, поэтому вовлечение в проект всех будущих пользователей системой, и учет всех их требований (задокументированных) абсолютно необходимый процесс. Перейдем непосредственно к проектированию Active Directory.

Примечание: Это непосредственно к теме не относится, но в дальнейшем если вы будете составлять такой документ как "Политика безопасности предприятия", то данные задокументированные процессы очень будут кстати, так как стандарт в области безопасности строго требует документирование всех процессов и изменений связанных с IT технологиями.

Первый этап. Создание плана лесов.

Лес Active Directory предназначен для того, чтобы быть отдельным самостоятельным модулем. Внутри леса легко совместно использовать информацию и сотрудничать с другими пользователями из того же самого подразделения. Проектируя самый высокий уровень инфраструктуры Active Directory, вы должны решить, нужно ли вам развертывать один лес или несколько.

Давайте вспомним, чем характеризуется лес доменов:

- наличием общей схемы,
- общего контейнера конфигурации,
- единого Глобального каталога (GC),
- полных транзитивных доверительных отношений между доменами.

Это позволяет пользователям регистрироваться в пределах леса применяя свое основное имя (UPN), выполнять поиск ресурсов в ГК и осуществлять к ним доступ в пределах всего леса. Администраторы же могут не заботиться о доверительных отношениях и легко управлять конфигурацией, что очень немаловажно.

Примечание: UPN (user principal name) – основное имя пользователя. У каждой учетной записи есть «удобное» имя и называется она основным именем пользователя –UPN и это и есть учетная запись пользователя и еще в купе с именем домена естественно, где эта учетная запись зарегистрирована и имеет смысл. Иногда UPN называют регистрационным именем пользователя или именем входа или логином от userlogin name.

Так сколько лесов создавать? Исходя из основного правила (смотри выше), слышу крики – Only One! (только один). И вы правы! Именно в одном лесу пользователи работают с единым каталогом, задействуют все преимущества транзитивных доверительных отношений, а администраторы легко управляют всеми доменами. Однако, существуют ситуации, когда необходимо и мы вынуждены использовать несколько лесов. Примером может служить объединение нескольких предприятий партнеров, или при-

каз министра производить обмен информацией между самостоятельными предприятиями по горизонтали, но подчиняющимися по вертикали одному министерству, или покупка нашей фирмы другой фирмы с уже существующим лесом, ну не ломать же его. Да, их связывают тесные партнерские отношения, им часто надо обмениваться информацией. Но это еще не повод для того, чтобы предоставлять пользователям разных предприятий или партнерских фирм прозрачный доступ к своим ресурсам. Администраторы разных организаций могут не доверять друг другу, они могут не прийти к согласию в том, как лес может изменяться. В такой ситуации не обойтись без нескольких лесов.

Если быть более строгим в изложении, то перечислим ситуации, в которых введение нескольких лесов оправдано.

- Задачи сетевого администрирования выполняются несколькими самостоятельными группами, между которых нет абсолютного доверия.

- Организационные единицы в силу «политических» причин разделены на самостоятельные группы.

- Существует необходимость в разделенном ведении организационных единиц.

- Леса содержат различные схемы каталога, контейнеров конфигурации и глобального каталога (GC). В этом случае требуется через создание лесов изолировать их друг от друга.

- Требуется в целях безопасности ограничить область доверительных отношений между доменами и деревьями доменов.

Конечно в идеале один лес – это хорошо, так как при создании лесов вы сознательно идете на дополнительные издержки. Во-первых, новый лес – это минимум еще один домен, и управление им так же ляжет на ваши плечи; во-вторых, это новая схема и конфигурация, которыми надо управлять. В-третьих, чтобы пользователь из одного леса осуществил доступ к ресурсам в другом лесу, нужны явные нетранзитивные доверительные отношения (Настраиваю внешние нетранзитивные доверительные отношения между доменами в разных лесах. При подготовке возник вопрос, а именно: Есть Лес А, домен domain1.local и два DNS сервера dc.domain1.local и bdc.domain1.local Лес В, домен domain2.local и два DNS сервера dc1.domain2.local и dc2.domain2.local На данный момент разрешил передачу зон с DNS сервера dc.domain1.local на DNS сервер dc1.domain2.local, и на dc1.domain2.local добавил дополнительную зону domain1.local. С сервера dc2.domain2.local домен domain1.local нормально резолвится, а с сервера dc1.domain2.local – НЕТ. Причина понятна, так как в настройках DNS сетевого интерфейса они стоят перекрестом друг к другу, а на сервере dc2.domain2.local дополнительной зоны domain1.local – НЕТ. Скажите, по BEST PRACTICES (или я пока не правильно настроил) лучше сделать передачу зон с 1. Зону domain1.local с DNS сервера dc.domain1.local разрешить на два DNS сервера dc1.domain2.local и dc2.domain2.local и указать в

этой зоне основные сервера `dc.domain1.local` и `bdc.domain1.local` 2. Зону `domain1.local` с DNS сервера `bdc.domain1.local` разрешить на два DNS сервера `dc1.domain2.local` и `dc2.domain2.local` и указать в этой зоне основные сервера `dc.domain1.local` и `bdc.domain1.local` и 3. Зону `domain2.local` с DNS сервера `dc1.domain2.local` разрешить на два DNS сервера `dc.domain1.local` и `bdc.domain1.local` и указать в этой зоне основные сервера `dc1.domain2.local` и `dc2.domain2.local` 4. Зону `domain2.local` с DNS сервера `dc2.domain2.local` разрешить на два DNS сервера `dc.domain1.local` и `bdc.domain1.local` и указать в этой зоне основные сервера `dc1.domain2.local` и `dc2.domain2.local` Или оставить только так как я сделал и этого будет достаточно???)

Администраторы должны сконфигурировать доверительные отношения вместо использования встроженных. Наконец, чтобы пользователи одного леса увидели в GC объекты другого леса, Вы должны либо импортировать эти объекты и постоянно поддерживать их свежую версию, либо пользователи должны уметь искать объекты в другом лесу. Если какая-либо информация должна быть синхронизована между лесами, то это также надо сконфигурировать.

В заключение по планированию лесов стоит упоминать о том, что, создав два или больше леса, Вы не сможете объединить их в один. Можно клонировать лишь отдельные объекты, но перенос доменов и слияние лесов невозможны. Поэтому, планируя структуру леса, надо очень хорошо подумать. Вот так.

Кроме того на этом этапе определяется владелец леса и создается так называемая «политика изменений леса» – документ который определяет круг лиц обладающих полномочиями управлением схемой и регулируют механизмы администрирования изменений, воздействующие на лес в целом.

В технических терминах просто определить, кто является владельцем леса. Группы `Schema Admins` (Администраторы схемы), `Enterprise Admins` (Администраторы предприятия) и `Domain Admins` (Администраторы домена) в корневом домене могут быть определены как владельцы леса, потому что они управляют теми изменениями, которые могут быть сделаны в лесу. Это роли чисто технические, и люди в этих группах почти не имеют окончательных полномочий на то, будут ли на самом деле сделаны модификации к лесу. Например, группа `Schema Admins` может изменять схему, но член группы `Schema Admins` обычно не имеет полномочий для принятия заключительного решения относительно того, будет ли запрос на изменение схемы одобрен.

Владельцы леса должны обладать комбинацией технической компетенции и понимания модели бизнеса. Они должны быть людьми, которые знают общие деловые требования организации и в то же время понимают техническое значение выполнения всех этих требований. Владельцы леса могут решить, что будет развернуто приложение, изменяющее схему, по-

тому что оно принесет значительную деловую пользу компании, а затем администратору схемы дают задание изменить схему так, как это требуется.

Это политика определяет то, какие изменения могут быть сделаны к конфигурации уровня леса и при каких обстоятельствах. Существует два типа изменений леса:

- изменения схемы и
- изменения раздела конфигурации каталога (например, добавление или удаление доменов и разделов приложений каталога, изменение конфигурации сайта).

Политика управления изменениями леса также определяет процедуры тестирования, одобрения и реализации любых изменений леса. Это важно для изменений схемы, поскольку их нелегко восстановить, поэтому любое изменение схемы должно быть совместимо со всеми другими изменениями. Политика управления изменениями леса должна определить процедуру тестирования изменений схемы, и владельцы леса должны поддерживать испытательную лабораторию для тестирования этих изменений. Политика управления изменениями леса должна требовать полного испытания всех изменений уровня леса и гарантировать, что тестирование закончится быстро. Если каждый запрос на изменение будет занимать много времени на обработку, то уровень расстройств пользователей будет постоянно возрастать.

Документ «политика управления изменениями леса» должна быть сформирована прежде, чем вы начнете развертывать Active Directory. Она так же должна быть прописана в документе более высокого ранга такой как «Политика IT безопасности предприятия» в целом. На предприятиях с разнообразными и обособленными деловыми подразделениями пояснение этой политики может быть трудным делом и занять много времени, но и после развертывания Active Directory делать это совсем не легче. Если деловые подразделения не смогут договориться о политике управления изменениями леса перед развертыванием, вы должны принять решение о развертывании нескольких лесов, что весьма «не очень»

И это правда, так как знаю по собственному опыту какие стрессы и скандалы вызывают изменения, внесенные в лес или даже в отдельном домене, если нет хорошо проработанного документа такой как «Политика IT безопасности предприятия» и все вытекающие из него документов.

Второй, третий и четвертый этап планирования.

Планирование ActiveDirectory. Создание плана доменов.

Продолжим нашу тему о проектированию и развертыванию Active Directory. Из предыдущей темы мы ознакомились с основными принципами и рекомендациями по построению плана лесов.

Процесс планирования доменов, как и при планировании леса, начинается так же с анализа нашей компании, фирмы или предприятия, называйте, как хотите, и выявления или скажем формулирования требований целесообразности именно построения такого плана доменов а не «как бог на душу положит». При этом желательно не забыть все это в какой либо форме задокументировать. Но и при планировании плана доменов не забывайте о правиле которая облегчит вашу сисадминовскую и так не легкую жизнь, а именно «чем проще тем лучше». Но и здесь не доходите до примитивизма.

Конечно идеальная модель это один маленький «лесок» в котором один маленький «доменок». Не надо иметь «seven пядей во лбу» что бы понять, что введение в составе леса новых доменов, неизбежно повлечет за собой увеличение издержек на администрировании этими доменами а так же материальные затраты на аппаратное обеспечение. Поэтому всегда стремитесь свести количество доменов к минимуму насколько это возможно.

Тут может возникнуть такой вопрос – допустим, вы установили Windows Server, подняли на нем Active Directory с одним доменом, и как вы не смотрите на него, даже вооруженным глазом, не видно никакого леса. Так вот – этот ваш первый, может быть и единственный домен, и есть и «лес» и «домен» и по совместительству и «корневой домен» и все остальное, как говорится – «все в одном флаконе».

Чем хорош один домен? Перечислим преимущества:

- Отпадает необходимость планирования доверительных отношений (о доверительных отношениях смотрите здесь).
- Становится проще управлять пользователями и группами.
- При необходимости предоставления прав на администрировании или как говорится при делегировании прав, это делается на уровне организационных подразделений (OU).
- Единая политика безопасности.

Хочу заметить, что даже в случае с единственным доменом, перед тем как его создать, хорошо подумайте, как он будет функционировать и о его внутренней структуре, так как однажды созданный домен довольно сложно перенести или переименовать.

Однако жизнь не всегда «мармеладная» и нам предстоит встретиться и с ситуацией когда сама жизнь или скажем условия предприятия заставит создавать и администрировать несколько доменов.

Давайте рассмотрим данную ситуацию более детально.

Как мы уже знаем, домены применяются в случаях, когда необходимо по тем или иным причинам, которые диктуются требованиями предприятия или фирмы, для разделения большого леса на более мелкие компоненты для целей репликации или администрирования.

Также хочу напомнить важные характеристики домена, которые следует учитывать при проектировании и развертыванию Active Directory :

Граница репликации. Как мы знаем, в границах домена реплицируется каталог домена хранящейся в папке Sysvol (общий системный том, создается при установке Active Directory). Данные, хранящиеся в Sysvol, – это общедоступные файлы, реплицируемые между всеми контролерами данного домена. В частности, в нем хранятся сценарии регистрации и некоторые объекты групповой политики (об этом поговорим позже). В то время как другие разделы каталога Active Directory, такие как «раздел схемы», «раздел конфигурации и GC», хранящиеся в папке Ntds, реплицируются по всему лесу, но не полностью, но та часть каталога Active Directory, а именно «раздел домена» которая относится к домену реплицируется только в пределах домена. Еще хочу сказать, что график репликации системного тома или Sysvol совпадает с графиком Active Directory или Ntds.

Граница доступа к ресурсам. Именно границы домена определяют границы доступа к ресурсам нашей сети. Границы домена являются также границами для доступа к ресурсам. По умолчанию пользователи одного домена не могут обращаться к ресурсам, расположенным в другом домене, если только им не будут явно даны соответствующие разрешения.

Граница политики безопасности. Если говорить о групповых политиках безопасности то хочу просто пока написать, чтобы вы запомнили, что эти политики в общем могут быть переменены на трех уровнях, а именно:

- на уровне домена,
- на уровне сайта,
- на уровне подразделений.

Более детально о них мы поговорим в процессе. Но некоторые политики безопасности могут быть установлены только на уровне домена. Эти политики, такие как политика паролей, политика блокировки учетных записей и политика билетов Kerberos, применяются ко всем учетным записям домена.

Перечислим ситуации, когда создание нескольких доменов необходимо и оправдано:

- В случае когда необходимо привязать к различные политики безопасности. Так как политики безопасности могут содержать различные требования то мы вынуждены создать дополнительные домены и к каждому из них привязать необходимую политику, или более жесткую или скажем более либеральную.

- Обеспечение соответствия административным требованиям, связанным с правовыми соображениями или конфиденциальностью. Одним словом, когда не надо всех админов пускать или админы не доверяют друг другу по той или иной причине.

- При большом трафике репликации в целях его оптимизации проводят деление доменов или добавление доменов или, изначально зная, что трафик будет большим, и сразу создают больше доменов в зависимости от реальной ситуации.

- При наличии в сети старых доменов которых нужно сохранить под управлением Windows NT.

- Необходимость создания отдельного пространства имен.

Если из всех перечисленных ситуаций ни одна к вам он не относится, то вам повезло и у вас будет один домен.

Давайте рассмотрим некий алгоритм деления вашей сети на домены. Допустим, вы новый админ и вы решили установить Windows Server и поднять Active Directory. Какие шаги вы должны при этом сделать, чтобы принять решение о необходимости деления на домены, их количество и прочие необходимые работы.

Количество доменов.

Шаг номер один.

Вы проводите ревизию своей сети (пусть сеть Ethernet). Составляете физическую и логическую топологию сети. Под физической топологией имеется в виду сами провода и скорость передачи линий, тип связи. Под логической топологией – деление физической сети на подсети (сегменты) и прочие. Хорошо бы сделать мониторинг сети и посмотреть на загруженность сети, объем трафика в зависимости от протоколов и сетевых программных приложений.

Вы создаете план сети, на бумаге указывая на каждом сегменте сети:

- количество пользователей,
- скорость передачи линии,
- надежность связи,
- все основные используемые протоколы,
- программные приложения производящий обмен данными по сети,
- тип связи (выделенные, коммутируемые),
- загрузку каждого сегмента.

Примечание. Если вы не знаете, как делать мониторинг сети, или просто такой возможности нет по той или иной причине, пока на «глаз», исходя из имеющейся информации, такой как количество пользователей данного сегмента сети, работающие сетевые приложения и сервисы производящий трафик, вы можете примерно определить загруженность сети пока на уровне типа большой, средний, малый трафик. Также это необходимо сделать, если даже сети нет и она только собирается быть созданной.

На основе этих данных на плане обозначьте сегменты с хорошей пропускной способностью сети и надежной связью. Объедините близко расположенные сегменты в участки.

Шаг второй.

После того как участки обозначены, посмотрите на ваш план и соедините или разграничьте эти участки на области, разместите в каждой области по одному контролеру домена. На этом этапе о количестве контролеров пока не задумываемся. К примеру, берем область на плане с высокой скоростью и хорошей надежностью. Туда и добавляем один контроллер на плане (допустим это наш главный офис). А на участке, где и канал хороший по скорости, надежность связи неплохая, но трафик большой, то может, стоит поделить сеть на логические подсети (сегменты), чтобы снизить служебный трафик; в любом случае выделяем эти участки в отдельную область или области (если таких участков много) и ставим туда же по контроллеру. Если у нас, например, филиал, и канал связи слабый, ненадежный или перегружен, то эти области также отмечаем на плане и туда также добавляем по контроллеру. Но не отмечайте филиалы, в которых, к примеру, два компьютера, так как тогда вам нужно будет туда поставить контроллер домена, а это дополнительные затраты. Следует исходить из того что, если связь хорошая и сеть не перегружена, то это одна область и туда помещаем контроллер домена (к примеру это наш центральный офис). Если больше никаких проблемных участков нет и один участок помещается в одну область, то вам повезло. Если между участками плохая связь или канал ненадежный или перегружен, то эти участки группируем (или делим) отдельно в области (допустим связь между филиалами). Если вы изучили все предыдущие темы на сайте, а особенно статьи, описывающие сайты, то вам на ум должно прийти, что данные области есть и будущие прототипы или претенденты на наши сайты. То есть, проводя по плану то, что у нас нарисовано на бумаге, такие разбиения, которые мы описали, мы создаем и план сайтов. Но к плану сайтов вернемся ниже.

Шаг третий.

Теперь после того, как мы определили, где у нас будут размещаться контроллеры доменов в нашей сети, привяжем их к домену. Первое, что надо сделать, это проследить путь регистрации пользователя в сети. Обязательно учтите тот факт, что при регистрации пользователя в сети контроллер домена обращается к глобальному каталогу (GC), если глобальный каталог расположен далеко и на медленном или ненадежном или перегруженном сегменте, это плохо. Учтите это. На основе этих данных вы и будете принимать решение, сколько контролеров домена у вас будут в домене. Также необходимо посмотреть в сети путь прохождения репликации между контроллерами. Если, допустим, мы решили, что у нас будет один домен, а он получается очень большим, то тогда и трафик репликации, не считая весь сетевой трафик, будет большим. В таком случае следует подумать может быть стоит поделить данный домен на два домена поменьше и тогда мы как бы локализуем репликацию в пределах домена а не пускаем ее в всю сеть. От этого выигрывает весь сетевой трафик.

Шаг четвертый.

Продиктован обстоятельствами, которые описаны выше, при описании, когда необходимо поделить один домен на большее количество, чем один.

Не забывайте, что с увеличением количества доменов увеличиваются издержки на администрирование и также на необходимость покупки железа.

Далее необходимо проделать одну операцию, а именно выбор корневого контроллера домена.

Выбор корневого домена.

В этой роли по сути может выступить любой из существующих доменов в нашем лесу доменов. Однако мы можем создать и специальный домен. Второй вариант предпочтительный. Почему? Создавая как бы специализированный корневой домен, мы в конечном итоге получим некоторые преимущества по части администрирования системы защиты, оптимизации трафика репликации и еще этим специализированным корневым доменом мы получим возможность более гибкого управления или лучше сказать масштабируемости нашего леса.

К определению основного контроллера домена леса надо подходить со всей возможной внимательностью. Дело в том, что переназначение другого домена на эту роль – довольно неблагоприятная задача. То же самое относится и к нашему специализированному домену. То есть мы берем и создаем такой специальный корневой домен. В этом специальном корневом домене мы храним только учетные записи администраторов разного уровня, то есть учетные записи администраторов предприятия, администраторов схемы, администраторов домена и какие там еще есть по умолчанию при создании домена или скажем при поднятии Active Directory. Об этих учетных записях поговорим далее более детально. К корневому домену мы не привязываем никакие подразделения. Это делается из-за того, что подразделения могут меняться или вообще могут быть удалены, а вот корневой домен леса всегда необходим, то есть "живее всех живых" с его учетными административными записями, созданными по умолчанию. Лучше всего размещать такой корневой домен там, где находится руководство или поближе к нему. Дело в том, что такой корневой специализированный домен позволяет жестко ограничивать круг лиц, а также контролировать их, администрирующих (управляющих, разрешающих) правами на остальные административные группы, которые у нас есть. Еще одно преимущество – в его доступности, так как он не связан жестко со структурой предприятия или фирмы, а также генерирует малый объем трафика репликации.

После того как мы определились с корневым доменом, следует операция определения доменной иерархии (или объединение доменов в деревья).

Определение иерархии доменов (или объединение доменов в деревья).

Если у нас один домен, то и объединять нечего и никакой иерархии доменов или дерева у нас не будет. Этот единственный домен у нас будет и нашим лесом и нашим корневым доменом, если мы не создали специальный корневой домен, и этот процесс абсолютно не обязательный.

Если мы планируем дальше развиваться и создать лес с деревьями, то имя единственного пока (или первого созданного) домена и будет основой для всех дочерних доменов в дереве.

Имена доменов в дереве смежные, то есть если у нас домен родитель `rk.com`, то дочерний домен – домен первого уровня по отношению к родителю будет к примеру `antarctida.rk.com` или еще один домен того же уровня по отношению у родителю `africa.rk.com`. Дочерний домен от `antarctida.rk.com` будет, к примеру, `kontora.antarctida.rk.com`, а также в иерархии будет на уровень ниже, чем его родитель по отношению к пра-родителю (или скажем дедушке, под этим я имею ввиду основной домен родитель иерархии доменов `rk.com`).

Если в лесу несколько деревьев, то их корни связаны напрямую с корневым доменом леса.

Естественно, что имена доменов разных деревьев являются не смежными. Если у нас родитель иерархии первого домена в лесу, допустим, домен `rk.com`, то все имена иерархии доменов будут иметь в имени атрибуты родителей, то иерархия второго, допустим, дерева `hi.com` будет иметь в имени атрибуты этого родителя и всех остальных родителей по иерархии вниз.

Главное, что нужно учитывать при строении дерева, это то, что если вы потом захотите удалить или переместить в другое дерево промежуточный иерархический домен, сделать это можно, только если мы удалим домен и все нижележащие дочерние домены. Следовательно, если вы это предполагаете это сделать в последующем, поместите такой домен в отдельное дерево.

Сделаем некоторый общий алгоритм того, что нужно сделать, чтобы задать иерархию доменов.

1. Определить количество деревьев в лесу.
2. Назначить каждому дереву свой корневой домен.
3. Расположить оставшиеся дочерние домены на более низких чем корневые домены уровнях иерархии.

Еще нам предстоит дать наименование нашим доменам.

Процесс именования доменов.

Данный процесс строится по следующему алгоритму.

1. Присваивание имен DNS корневым доменам во всех наших лесах.
2. Присваивание имен DNS корневым доменам всем деревьям нашей фирмы.

3. Присваивание имен DNS всем оставшимся дочерним доменам, в строгой соответствии с их положением в иерархии.

Третий этап. Создание плана подразделений (OU).

На этом этапе, как и на предыдущих, проводится анализ выставляемых предприятием или фирмой требований или требований, вами разработанных. Затем определяется структура подразделений. Некоторые системные администраторы на этом этапе при создании подразделений полностью копируют структуру организации со всеми ее отделами и производствами. Насколько это правильно – сразу ответить сложно. Ответ на этот вопрос можно дать, только проанализировав все аспекты взаимодействия отделов или структурных подразделений на конкретной фирме. Но как показывает практика, это иногда нецелесообразно. Для того что бы это выяснить в общих чертах, стоит задать вопрос – совпадает ли структура управления со структурой компании. Вполне вероятно, что все управление централизовано (из единого центра), и тогда создание копии структуры предприятия через создание в Active Directory подразделения только усложнит администрирование этими подразделениями. В этом случае достаточно создать одно подразделение (OU), а внутри этого подразделения создать и группировать в зависимости от требований посредством групп. Когда пользователи в вашей фирме обращаются и работают с ресурсами только своего отдела, то в этом случае можно создать полную копию структуры предприятия. Тем не менее не стоит забывать, что у подразделений (OU) нет собственных границ безопасности, но групповые политики применительны и к ним. И если даже политика у нас по отношению к подразделениям одинакова, тем не менее нам потребуется указать ее для каждого подразделения в отдельности.

Три основных цели, побуждающие к созданию подразделений, заключаются в следующем:

- делегирование административных полномочий,
- сокрытие объектов,
- администрирование групповой политики.

Делегирование полномочий позволяет, с одной стороны, избавиться от присутствия и вмешательства "противных" администраторов, а с другой – уменьшить их объем работы, передав отдельные административные функции в подразделения.

Сокрытие объектов применяется при необходимости скрыть некоторые объекты в сети от некоторых пользователей. Для этого можно создать отдельное подразделение и ограничить круг лиц с правом List Contents для этого OU.

Под администрированием групповой политики надо понимать применение групповых политик на данное OU. Если вы не собираетесь применять различные групповые политики к отдельным OU, то надобность в таких подразделениях отпадает.

Четвертый этап. Создание топологического плана сайтов.

Если говорить о сайтах, то основное значение сайтов по сути – это физическая группировка компьютеров с целью оптимизации сетевого трафика.

Структура сайтов Active Directory показывает нам размещение пользовательских сообществ, что видно из нашего плана, который мы составили.

Отдельный сайт нужно создать для следующих объектов:

- для каждой локальной сети или набора локальных сетей, подключенных к высокоскоростным линиям связи;
- для каждой области, которая не связана с остальными нашими сайтами напрямую, и обмен информации доступен только по протоколу SMTP.

После анализа нашего составленного на бумаге плана выявление отдельных областей, то есть сайтов, мы поставили по одному контроллеру домена в сайтах. Хотя в том алгоритме говорится о том, что количество контроллеров вы принимаете исходя из требования того, что контроллер домена всегда доступен и время его реагирования на наши запросы быстрое. Это мы определяем, проследив путь регистрации пользователей, трафика репликации, размещение GC и общий анализ загрузки сети. На основе этой информации мы принимаем решение о количестве контроллеров домена.

Тем не менее, что бы добиться оптимальных показателей быстродействия нашей сети и готовность приложений, по правилам нужно разместить по меньшей мере:

- по одному контроллеру домена на каждом сайте,
- по два контроллера доменов в каждом домене.

То есть, как мы видим из этих требований, могут быть сайты без контроллеров домена, но это не желательно, так как одна их причин разделения на сайты и есть скорость обмена между ними. И тогда подумайте о тех пользователях, которые окажутся в сайтах, которые по той или иной причине не имеют свой контроллер домена.

Необходимость в размещение дополнительных контроллеров домена возникает в следующих ситуациях, когда при многочисленности зарегистрированных на сайте пользователей:

- канал связи медленный,
- канал ненадежный,
- канал перегружен.

Тут же на этом этапе определяемся со стратегией репликации. Правильный выбор стратегии репликации повышает отказоустойчивость и эффективность репликации. Тут нам предстоит, как сетевым администраторам, создать конфигурацию межсайтовых ссылок, назначить транспорт репликации, установить частоту репликации и готовность репликации.

Кроме того, мы можем указать предпочтительные серверы-плацдармы (bridgehead servers) между сайтами.

И в завершении этого этапа мы определяемся с размещением в лесу серверов глобального каталога (также прослеживаем путь пользователей и контролеров до этих серверов) и назначение главных операционных ролей.

Все это мы будем делать непосредственно в Active Directory. Но главное не в умении ставить фишки в настройке, а понимать, что ты делаешь, поэтому сперва столько теории.

Управление Active Directory через командную строку весьма мощный инструмент в руках профессионала. Представьте себе, что управление ресурсами целого предприятия сосредоточено в одном окне командной оболочки. Создание, удаление, модификация объектов Active Directory возможны и с применением сценариев автоматизации командной строки.

Служба каталогов Active Directory

Active Directory – одна из самых важных областей управления сетями в Windows. Active Directory – расширяемая и масштабируемая служба каталогов, которая поддерживает охватывающую всю сеть базу данных для хранения учетных записей и информации о ресурсах. При работе с Active Directory вы имеете дело с целостной системой именования, описания, поиска, изменения и защиты информации о ресурсах. Поэтому Active Directory отлично подходит как для управления учетными записями пользователей, групп и компьютеров, так и для работы с приложениями, файлами, принтерами и другими типами ресурсов. Active Directory применяется для управления сетевой инфраструктурой, системного администрирования и управления пользовательскими средами.

Active Directory доступна только в доменах Windows с контроллерами домена под управлением Windows 2000 или более поздней версии. Контроллер домена (domain controller) – это сервер под управлением серверной версии операционной системы Windows. Active Directory, можно рассматривать как усовершенствование доменной архитектуры Windows NT, в которой на смену базе данных SAM (Security Accounts Manager) пришла более гибкая, расширяемая и масштабируемая база данных. Как и SAM, Active Directory используется в качестве централизованного хранилища информации защиты; однако в отличие от SAM служба Active Directory является еще и средством интеграции гетерогенных систем. Она позволяет выполнять все операции управления ресурсами с помощью единого набора GUI-средств администрирования, работающих в Windows. В этой главе рассматриваются эквивалентные средства командной строки, управляющие службой каталогов.

Управление Active Directory из командной строки

Чтобы использовать многочисленные средства командной строки, управляющие Active Directory, нужны базовые знания об Active Directory и

ее структурах. В соответствии с замыслом Microsoft эта служба использует в качестве системы именования DNS (Domain Name System). В DNS информация о сетевых ресурсах хранится в виде иерархической структуры, соответствующей схеме управления ресурсами. Эта иерархия доменов, или дерево доменов, лежит в основе среды Active Directory и во многом аналогична структуре каталогов файловой системы. Еще одно название этой иерархии – пространство имен (namespace). В каждой организации, использующей домены Active Directory, существует своя иерархия (или пространство имен) Active Directory.

Домены, контейнеры и объекты

Для представления сетевых ресурсов, таких как пользователи, группы и компьютеры, в Active Directory используются объекты. Кроме того, специализированные объекты, называемые контейнерами, служат для упорядочения сетевых ресурсов по территориальным, функциональным или бизнес-признакам. Обычно контейнеры используются для группирования объектов, имеющих одинаковые атрибуты. Например, если требуется применить определенный набор разрешений ко всем инженерам, это проще сделать, поместив всех этих пользователей в один контейнер.

Каждый контейнер отражает группу объектов, а каждый ресурс представляется уникальным объектом Active Directory. Самый общий тип контейнера Active Directory – организационная единица, или OU (organizational unit). Объекты, помещаемые в OU, принадлежат только домену, к которому она относится.

Домены, поддомены и OU в Active Directory никак не связаны с реальным миром, даже если вы используете территориальное группирование доменов и OU. Это просто области каталога, где хранятся соответствующие данные. В Active Directory они физически находятся в одном месте, пока вы не укажете, какие физические структуры сопоставляются вашим логическим структурам доменов, поддоменов и OU.

На практике каждая из этих логических структур может охватывать более одного участка. И не важно, что представляют собой эти участки, – разные этажи одного здания, разные здания или даже города. Главное, что это различные физические участки. Чтобы сообщить Active Directory об этих участках, вы должны определить подсети и сайты. Подсеть (subnet) – часть сети со специфическим диапазоном IP-адресов и сетевой маской. Сайт (site) – группа, содержащая одну или несколько подсетей и сопоставленная физической структуре вашей сети. Поскольку сопоставления сайтов не зависят от логической структуры доменов, физическая структура сети и логическая структура доменов не обязательно должны быть связаны между собой.

Средства командной строки для управления Active Directory

Чтобы использовать многочисленные средства командной строки, управляющие Active Directory, нужны базовые знания об Active Directory и

ее структурах, В соответствии с замыслом Microsoft эта служба использует в качестве системы именования DNS (Domain Name System). В DNS информация о сетевых ресурсах хранится в виде иерархической структуры, соответствующей схеме управления ресурсами. Эта иерархия доменов, или дерево доменов, лежит в основе среды Active Directory и во многом аналогична структуре каталогов файловой системы. Еще одно название этой иерархии – пространство имен (namespace). В каждой организации, использующей домены Active Directory, существует своя иерархия (или пространство имен) Active Directory.

Гибкость управления Active Directory из командной строки

Освоив базовые структуры Active Directory и научившись идентифицировать используемые объекты по DN, вы готовы управлять Active Directory из командной строки. Применение командной строки дает важное преимущество – дополнительную гибкость. Из командной строки легко выполняются многие операции, осуществить которые GUI-средствами гораздо сложнее или просто невозможно. Например, вы можете найти все учетные записи компьютеров, неактивные более недели, и отключить эти записи. Или одной командой изменить свойства нескольких учетных записей пользователей.

Для работы с Windows-доменами Windows Server 2003 и Windows XP предоставляют набор средств командной строки, управляющих Active Directory. К ним относятся:

1. DSADD – добавляет объекты в Active Directory;
2. DSGET – показывает свойства объектов, зарегистрированных в Active Directory;
3. DSMOD.– изменяет свойства объектов, существующих в Active Directory;
4. DSMOVE – перемещает один объект в новое место в том же домене или переименовывает объект, не перемещая его;
5. DSQUERY – ищет объекты Active Directory по определенному критерию;
6. DSRM – удаляет объекты из Active Directory.

Каждая из утилит командной строки предназначена для работы с определенным набором объектов Active Directory (AD).

Вопросы для самостоятельного изучения:

1. Ищем объекты командой DSQUERY
2. Перемещение объектов Active Directory
3. Удаление объектов Active Directory
4. Управление учетными записями компьютеров
5. Создание учетных записей компьютеров
6. Свойства учетных записей компьютеров
7. Расположение учетной записи компьютера

8. Перемещение учетных записей компьютеров
9. Работа с контроллером домена
10. Серверы глобального каталога
11. Проверка настроек глобального каталога
12. Назначение ролей в каталоге
13. Настройка ролей координаторов
14. Управление пользователями в Active Directory
15. Добавление учетных записей пользователей
16. Настройка атрибутов доменных учетных записей
17. Управление учетными записями пользователей
18. Поиск учетных записей пользователей
19. Включение и отключение учетных записей
20. Обзор управления учетными записями групп
21. Добавление учетных записей групп
22. Создание локальных групп
23. Просмотр и поиск учетных записей групп
24. Изменение типа или области групп
25. Добавление, удаление или замена членов групп
26. Администрирование служб печати
27. Информация о спулере печати
28. Управление принтерами
29. Установка принтеров
30. Использование принтеров
31. Управление очередями печати
32. Возобновление и перезапуск печати

10. Средства обеспечения безопасности автоматизированных распределенных информационных систем.

Информационная безопасность – неперемное условие нормального функционирования любой компании, так или иначе связанной с внешним миром. Все большее число компаний используют Интернет как одну из составляющих своего бизнеса, вследствие чего постоянно возрастает роль аппаратных и программных средств как для обеспечения безопасного функционирования внутренних приложений компании в ее IT-инфраструктуре, так и для общей политики компаний в области безопасности. При этом нередко бывает весьма сложно оценить экономический эффект от внедрения подобных средств, по крайней мере в сравнении с оцен-

кой эффективности офисных приложений или систем управления предприятием.

Согласно классификации аналитической компании Butler Group (<http://www.butlergroup.com/>), средства обеспечения информационной безопасности предприятий можно разделить на три большие группы: средства антивирусной защиты, брандмауэры и средства обнаружения атак. Если первые две категории средств применяются довольно широко, то последняя группа является относительно новой, хотя некоторые продукты, относящиеся к классу брандмауэров, содержат и средства обнаружения атак. Ниже мы подробнее остановимся на каждой из этих категорий, но прежде перечислим возможные виды нарушений информационной безопасности.

Наиболее распространенные виды атак

Как правило, атаки направлены на получение административных привилегий с целью запуска определенных процессов и неправомерного использования корпоративных ресурсов¹. Атака может исходить как извне, так и изнутри, но независимо от ее источника первым шагом должен стать поиск уязвимых мест, позволяющих получить административные права. К сожалению, подобные уязвимые места существуют во многих программных продуктах и нередко хорошо документированы.

Список возможных видов атак, которые могут использовать в своих целях «слабое звено» программного продукта, довольно широк – начиная с угадывания паролей и заканчивая атаками на Web-серверы и внедрением в Web-страницы объектов, содержащих исполняемый код (таких, как элементы управления ActiveX). К самым распространенным из них относятся:

- переполнение буфера – неавторизованный пользователь направляет большое число запросов приложению, на которое производится атака, вследствие чего становится недоступной функциональность данного приложения, связанная с реакцией на запланированную одновременно с этим атаку. Хотя такой вид атаки известен очень давно, приложения, обладающие подобной уязвимостью, по-прежнему создаются;
- использование стандартных паролей – этот вид рассчитан на то, что администратор сети или базы данных не изменил административных паролей, значение которых по умолчанию документировано и, следовательно, известно;
- malware (malicious software) – использует специальное программное обеспечение, предназначенное для несанкционированного мониторинга сети, поиска уязвимых мест и выявления паролей;
- вирусы – разновидность malware; это ПО, служащее, как правило, для разрушения данных либо для нарушения в работе сети и отличающееся способностью к саморазмножению. Нередко вирусы используются и для получения контроля над сетью или для несанкционированного доступа к ресурсам;

- отказ в обслуживании (Denial of Service, DoS) – один из наиболее распространенных видов сетевых атак. Простейшая форма проявления подобной атаки – отказ от выполнения вполне легитимного запроса в связи с тем, что все ресурсы сети (либо функционирующего в ней программного обеспечения) заняты обслуживанием большого количества запросов, поступающих из других источников. Отметим, что следует не только защищать свою сеть от подобных атак, но и предотвращать возможность использования ее в качестве источника атаки на сети других компаний.

Обычно средства обеспечения информационной безопасности применяются в комплексе, поэтому во многих источниках нередко говорят не о конкретных продуктах, а о платформах безопасности – security platforms. Далее мы рассмотрим наиболее распространенные составные части таких платформ.

Антивирусное программное обеспечение

Антивирусное программное обеспечение предназначено для защиты предприятия от различных типов вирусных атак. Поскольку сегодня передача вирусов происходит в основном посредством сообщений электронной почты, наиболее распространенной категорией корпоративного антивирусного ПО являются антивирусы для почтовых серверов, распознающие сигнатуры вирусов внутри сообщений. Наряду с этим многие компании выпускают антивирусное ПО для файловых серверов, а также специализированное ПО, используемое Интернет-провайдерами.

Антивирусное ПО обязательно содержит следующие компоненты:

- приложение для управления настройками;
- средства сканирования файлов и поиска сигнатур вирусов;
- база данных или библиотека, содержащая определения известных вирусов (заметим, что успешность функционирования антивирусного ПО зависит от регулярности обновления баз данных, содержащих определения вирусов).

По сведениям аналитической компании Gartner Group, лидерами рынка антивирусного программного обеспечения являются Network Associates, Symantec, TrendMicro. Значительную роль на рынке играют и компании Sophos, Computer Associates, F-Secure. Все указанные фирмы производят продукты для настольных систем, файловых серверов, SMTP-шлюзов, Web- и FTP-серверов, а также позволяют поддерживать распределенные системы.

На российском рынке, помимо перечисленных выше продуктов, широко распространены корпоративные антивирусы «Лаборатории Касперского» и ЗАО «ДиалогНаука».

Корпоративные брандмауэры

Корпоративные брандмауэры контролируют трафик, поступающий в локальную корпоративную сеть и выходящий из нее, и могут представлять собой как чисто программные средства, так и аппаратно-программные

комплексы. Каждый пакет данных, проходящий через брандмауэр, анализируется им (например, на предмет происхождения или соответствия иным правилам пропускания пакетов), после чего пакет либо пропускается, либо нет. Обычно брандмауэры могут выполнять роль фильтра пакетов или роль прокси-сервера, в последнем случае брандмауэр выступает в качестве посредника в выполнении запросов, иницилируя собственный запрос к ресурсу и тем самым не допуская непосредственного соединения между локальной и внешней сетями.

При выборе брандмауэра компании обычно руководствуются результатами независимого тестирования. Наиболее распространенными стандартами, на соответствие которым тестируются брандмауэры, являются ITSEC (Information Technology Security Evaluation and Certification Scheme) и IASC (Information Assurance and Certification Services), также носящий название Common Criteria Standard.

Самыми популярными производителями корпоративных брандмауэров, с точки зрения Gartner Group, являются CheckPoint Software, Cisco Systems, Microsoft, NetScreen Technologies и Symantec Corporation.

Отметим, что продукты Check Point Software Technologies, Cisco Systems и NetScreen Technologies представляют собой аппаратно-программные комплексы, тогда как продукты Microsoft и Symantec – это программные средства, функционирующие на обычных компьютерах под управлением стандартных серверных операционных систем.

Средства обнаружения атак

Средства обнаружения атак предназначены для определения событий, которые могут быть интерпретированы как попытка атаки, и для уведомления об этом IT-администратора. Данные средства можно разделить на две категории по принципу их функционирования: средства, анализирующие трафик всей сети (в этом случае на рабочих станциях сети нередко устанавливается часть соответствующего программного обеспечения, называемая агентом), и средства, анализирующие трафик конкретного компьютера (например, корпоративного Web-сервера). Средства обнаружения атак, как и брандмауэры, могут быть реализованы и в виде программного обеспечения, и в виде аппаратно-программного комплекса. Очевидно, что подобные средства требуют тщательной настройки, чтобы, с одной стороны, были обнаружены истинные попытки атак, а с другой – чтобы по возможности были исключены ложные срабатывания.

Лидерами рынка средств обнаружения атак, по мнению Gartner Group, являются Cisco Systems, Internet Security Systems, Enterasys Networks и Symantec. По данным Butler Group, весьма популярными производителями этой категории средств обеспечения безопасности являются также Computer Associates и Enterscept Security Technology.

Средства, анализирующие трафик конкретного компьютера, производятся компаниями Symantec и Enterscept Security Technology. Продукт

Cisco IDS 4210 является аппаратно-программным комплексом, остальные вышеперечисленные продукты – программными средствами, которые выполняются под управлением стандартных операционных систем на обычных компьютерах.

О политике и стандартах безопасности

Рассмотренное в этой статье программное обеспечение может оказаться совершенно бесполезным при отсутствии надлежащей политики безопасности, определяющей правила применения компьютеров, сети и данных, а также процедуры, предназначенные для предотвращения нарушения этих правил и для реакции на подобные нарушения, если таковые возникнут. Отметим также, что при выработке подобной политики требуется оценка рисков, связанных с той или иной деятельностью, например в случае предоставления бизнес-партнерам данных из корпоративной информационной системы. Полезные рекомендации на этот счет содержатся в международных стандартах, в частности в международном стандарте безопасности информационных систем ISO 17799. Выбор аппаратных и программных средств обеспечения безопасности во многом определяется политикой, выработанной конкретной компанией.

Прогнозы аналитиков

Рассмотрев современное состояние рынка корпоративных средств обеспечения информационной безопасности, в заключение приведем некоторые прогнозы аналитиков по поводу того, в каком направлении будут развиваться указанные категории продуктов.

Согласно прогнозам Gartner Group, одним из ключевых направлений развития рынка корпоративных средств обеспечения информационной безопасности будет дальнейшее развитие так называемых платформ безопасности (security platforms), комбинирующих аппаратные и программные брандмауэры, средства обнаружения атак, средства поиска уязвимостей, антивирусное программное обеспечение и, возможно, средства сканирования электронной почты и антиспамовые средства.

Еще одним фактором, влияющим на развитие технологий обеспечения корпоративной безопасности, по мнению Gartner Group, станет рост применения Web-сервисов. Поэтому от производителей брандмауэров и средств обнаружения атак следует ожидать выпуска дополнительных инструментов защиты сетей от атак, использующих в качестве средств проникновения SOAP-сообщения и XML-данные.