1. Администрирование ИС. Вводные положения. Функции администратора системы.

Системный администратор - человек или группа людей которые создают а затем эксплуатируют информационную систему предприятия. Эксплуатация подразумевает обновление, сопровождение, обслуживание

Функции АС:

- Установка и сопровождение различного рода ИС
- Определение и согласование с поставщиками всей аппаратно - программной части
- Решение вопросов ведения проекта
- Обучение технического персонала и пользователей
- Консультирование персонала к компьютерным проблемам
- Решение проблем сбора статистики, мониторинга, диагностики, восстановления и сохранения системы.
- Разработка программных продуктов на языках управления заданиями
- Определение ошибок в работе информационной системы и их устранение

Часть этих функций может быть перенесена на соответствующие информационные службы предприятия, а именно:

- службами управления: конфигурацией, контролем характеристик, ошибочными ситуациями, безопасностью, производительностью;
- службами планирования и развития;
- службами эксплуатации и сопровождения;
- службами общего управления

Службы общего управления занимаются управлением работы всех информационных служб, согласованием их действий, выработкой корпоративных стандартов (например, на формат документов), разработкой инструкций для пользователей, их обучением и консультацией, ведением нормативно справочной документации необходимой в организации.

2. Администрирование ИС. Вводные положения. Состав служб администратора системы и их функции.

Системный администратор - человек или группа людей которые создают а затем эксплуатируют информационную систему предприятия. Эксплуатация подразумевает обновление, сопровождение, обслуживание

1. Службы управления: Служба управления: конфигурацией, по контролю ошибочных ситуаций, управления безопасностью, производительностью
2. Службы планирования и развития;
3. Службы эксплуатации и сопровождения;
4. Службы общего управления.

Службы управления конфигурацией занимаются вопросами зада-ния параметров запуска (инсталляции) операционных систем (ОС) и СУБД, заданием параметров запуска приложений

Службы управления безопасностью (иногда их называют службами защиты от несанкционированного доступа — НСД) осуществляют комплекс мероприятий по противодействию различным угрозам не-санкционированного доступа

Службы планирования и развития определяют техническую и экономическую эффективность от внедрения различного вида информационных услуг или сервисов компании, следят за появлением новых компьютерных технологий и оценивают целесообразность их использования

Службы эксплуатации и сопровождения осуществляют архивирование (копирование) и восстановление информационной системы. Эти службы определяют режимы копирования (копируется вся система или ее часть), расписание копирования (например, еженедельное с затиранием предыдущей копии), ведут базу данных копий

Службы общего управления занимаются управлением работы всех информационных служб, согласованием их действий, выработкой корпоративных стандартов (например, на формат документов), разработкой инструкций для пользователей, их обучением и консультацией, ведением нормативно справочной документации необходимой в организации.

3. Администрирование ИС. Вводные положения. Требования к специалистам служб администрирования ИС.

Системный администратор - человек или группа людей которые создают а затем эксплуатируют информационную систему предприятия. Эксплуатация подразумевает обновление, сопровождение, обслуживание

То что должен знать администратор :

1. Теория операционных систем
2. Теория БД и их администрирование
3. Сетевые технологии и вопросы диагностики сетевых проблем
4. Электротехника и реализация кабельных систем а также cable management
5. Реализация Веб приложений
6. Защита информации от несанкционированного доступа
7. Вычислительная техника
8. Проектирование информационных систем
9. Способы восстановления информации
10. Языки программирования (Bash, Perl, Python)
11. Методы управления в информационных системах (менеджеры управления доменами например)

Информационные системы:

1. Функциональные
2. Организационные - кадровый состав
3. Обеспечивающие - техническая часть, программная часть

4. Администрирование ИС. Вводные положения. Общие понятия об открытых и гетерогенных системах.

Системный администратор - человек или группа людей которые создают а затем эксплуатируют информационную систему предприятия. Эксплуатация подразумевает обновление, сопровождение, обслуживание

Гетерогенный = Разнородный

Корпоративной ИС называется информационная система, виртуально объединяющая (в информационном плане) все части одной организации, которые могут находиться в разных городах, частях страны или земного шара

Под открытыми спецификациями понимают опубликованные, общедоступные спецификации стандартизирующих организаций или компаний-разработчиков аппаратных и программных средств.

Использование при разработке систем открытых спецификаций позволяет третьим сторонам разрабатывать для этих систем различные аппаратные или программные средства расширения и модификации, а также создавать программно-аппаратные комплексы из продуктов разных производителей.

В современных ИС информация передается между компьютерами различных производителей. При этом используются различные интерфейсы и средства передачи данных, различное программное обеспечение и различная архитектура ЭВМ.

Таким образом, практически любая система является разнородной или гетерогенной, включающей в себя оборудование и программное обеспечение нескольких производителей, т. е. современные ИС в своем подавляющем большинстве являются открытыми гетерогенными системами

Гетерогенные пример: ноутбуки, компьютеры

Корпоративной информационной системой называют информационную систему, которая виртуально объединяет (в информационном плане) все части одной организации.

5. Администрирование ИС. Вводные положения. Стандарты работы ИС и стандартизирующие организации.

Системный администратор - человек или группа людей которые создают а затем эксплуатируют информационную систему предприятия. Эксплуатация подразумевает обновление, сопровождение, обслуживание

Стандарт — это вариант реализации протокола в аппаратуре или программном обеспечении, который отражается в документе, согласованном и принятом аккредитованной организацией, разрабатывающей стандарты. Стандарт содержит правила, руководства или характеристики для работ или их результатов в целях достижения оптимальной степени упорядочения и согласованности в заданном контексте

Юридические стандарты подтверждаются законами, которые приняты государством. Государственное управление деятельностью по стандартизации в Российской Федерации осуществляет Федеральное агентство по техническому регулированию и метрологии (Ростехрегулирование, www.gost.ru), на которое возложены функции Национального органа по стандартизации в соответствии с Федеральным законом «О техническом регулировании». Другие органы государственного управления организуют деятельность по стандартизации в пределах их компетенции.

Фактические стандарты существуют, но их использование не определено законами или нормативами.

С точки зрения авторства стандарт может быть частным (корпоративным) или созданным стандартизирующей организацией. Корпоративные стандарты разрабатываются и внедряются частными коммерческими компаниями для своих продуктов. Стандарты стандартизируемых организаций создаются специализированными организациями или самоорганизующимися комитетами и форумами.

TU (International Telecommunications Union) — Международный союз электросвязи; является структурным подразделением ООН.

ISO (The International Organization for Standardization, а так же International Standards Organization) — Международная организация по стандартизации.

IEEE (произносится «ай-трипл-и», Institute of Electrical and Electronics Engineers, Inc.) — Институт инженеров по электротехнике и электронике (США).

EIA (Electronics Industries Alliance) — Ассоциация предприятий электронной промышленности США, альянс EIA.

TIA (Telecommunication Industry Association) — Ассоциация телекоммуникационной промышленности США, ассоциация TIA. Ассоциация изготовителей средств связи, которая разрабатывает стандарты на кабельные системы

6. Объекты администрирования и модели управления. Объекты администрирования в информационных системах.

Объекты администрирования в ИС является ее подсистемы. Ими также могут быть системные процессы обработки данных

Задача Администрирования подсистем:

- администрирование кабельной системы;
- поддержка и сопровождение аппаратной части;
- администрирование сетевой системы;
- администрирование прикладной системы;
- администрирование операционной системы;
- Web-администрирование;
- управление информационными службами;
- администрирование СУБД.

Объектами администрирования также могут быть прикладные или системные процессы обработки данных, существующие в ИС и затрагивающие несколько подсистем (например, администрирование электронной почты или администрирование конфигурации ИС. Т. Е. объектами администрирования могут быть как отдельные подсистемы, так и информационные процессы, существующие в нескольких подсистемах.

7. Объекты администрирования и модели управления. Модель сетевого управления ISO OSI.

Модель сетевого управления ISO OSI Management Framework — определена в документе ISO/IEC 7498-4: Basic Reference Model, Part 4, Management Framework. Она является развитием общей семиуровневой модели взаимодействия открытых систем для случая, когда одна система управляет другой.
Документ ISO/IEC 7498-4 состоит из пяти основных разделов:

- термины и общие концепции;
- модель управления системами;
- информационная модель;
- функциональные области управления системами;
- структура стандартов управления системами.

Стандарты ISO в области управления используют специальную терминологию, которой в свою очередь воспользовались создатели Internet в протоколе SNMP (Simple Network Management Protocol — простой протокол управления сетью).

Протокол - SNetworkManagemntP - для удаленного управления оборудованием например
SMAE - для общения по модели OSI. Логическая связь. При это общение на уровне физическом.
Функционал SMAE реализуется уровнем представления.
Службы SMAE для обмена:

1. ASCE - служба установления ассоциаций, проверяет правильность команд, доступность агентов
2. RTSE - служба установления диалога для сеансового уровня
3. ROSE - выполняет выполнение команд

RPC (remote procedure call) - вызов удаленных процедур и функций.
С т.з. администрирования представлены 4-м уровнями: прикладной, сеансовый, транспортный, SMAE

8. Объекты администрирования и модели управления. Модель управления ITU TMN.

TMN (Telecommunication Management Network, TMN (Система управления сетями операторов электросвязи) предназначена для управления услугами сетей связи, для эксплуатации и технического обслуживания оборудования, для оперативно-технического контроля и администрирования сетевых устройств с целью обеспечить нормативное качество оказания услуг связи.

Объектами управления TMN являются телекоммуникационные ресурсы. Телекоммуникационные ресурсы управления физически представляют собой реальное оборудование связи — стойки, функциональные блоки, модули, на определенные свойства которых можно осуществлять целенаправленное управляющее воздействие.

Обмен командами управления и иной информацией между TMN и оборудованием связи осуществляется через опорные точки, которые реализуются в виде стандартизованных и нестандартизованных интерфейсов TMN. Функции прикладного уровня TMN реализуются с помощью одной или нескольких операционных систем

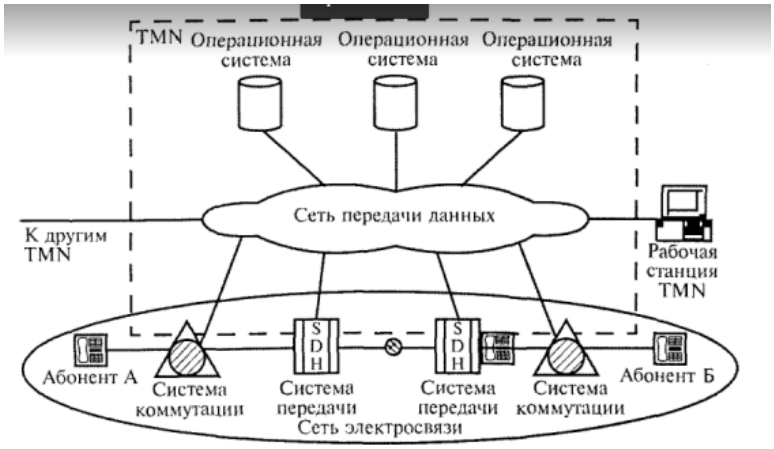


Рис. 4. TMN и сеть электросвязи

Задачи операционных систем:

- Обеспечение обработки данных (поступающих от управляемой сети электросвязи). В целях мониторинга и функционирования ГКО. Для работы TMN
- Поддержка информационной модели сети электросвязи - представлена как описание физических объектов электросвязи с использованием принятой инф.технологии
- Обеспечение работы прикладных программных средств управления, которые реализуют большинство услуг и функций управления системами

TMN должна обеспечивать

- Обмен информацией управления между сетями электросвязи и сетью TMN
- Анализ и соответствующая реакция на информацию управления
- Защищенный доступ к информации по управлению для пользователей TMN

Уровни управления TMN:

- Управления бизнесом (самый верхний уровнь)
- Управления услугами
- Управление сетью
- Управления элементом
- Элемент сети (NEL) самый нижний

9. Объекты администрирования и модели управления. Модель управления ISO FCAPS.

FCAPS (Fault Configuration Account Performance Security) – модель в которой отражены ключевые функции администрирования и управления сетями (обеспечивающей подсистемы ИС) и не рассматриваются вопросы администрирования функциональной или организационной подсистем Модель учитывает то, что современные ИС - это системы передачи цифровой информации и предназначены для описания функций администрирования только таких систем. Согласно модели FCAPS, все аспекты администрирования сети ИС можно описать при помощи пяти видов функций управления:

1. Упр. отказами (F) - обнаружение отказов от устройств сети, локализация, инициирование корректирующих действий
2. Упр. конфигурированием (C) - возможность отслеживания изменений, конфигурирования, передачи и установки ПО на всех устройствах связи. С помощью данной группы задач маршрутизаторам устанавливаются сетевые адреса. Схема сети корректируется автоматически при помощи опроса спец.программных средств. Используется протокол SNMP
3. Упр.учетом (A) - сбор и передача информации для генерации отчетов об использовании сетевых ресурсов
4. Упр. Производительностью (P) - непрерывный источник для мониторинга показателей работы сети и распределения сетевых ресурсов
5. Упр.безопасностью (S) - управление доступом к сетевым ресурсам и защитой от угроз

10.Active Directory Windows Server 2012. Общие положения. Эволюция службы каталогов.

Технологии Active Directory - пять отдельных технологий. Все они предназначены для обслуживания каталогов и в качестве платформы для интеграции технологий Microsoft.
Служба каталогов предоставляет подробную информацию о пользователях или объектах сети, примерно так же, как телефонная книга позволяет найти номер телефона по известной фамилии. Например, объект пользователя в службе каталогов может содержать номер телефона, адрес электронной почты, название подразделения и еще столько других атрибутов, сколько пожелает системный администратор. Службы каталогов часто называют "белыми страницами" сети. Они обеспечивают определение и администрирование пользователей и объектов.
Первые электронные каталоги были созданы вскоре после изобретения цифровых компьютеров и применялись для аутентификации пользователей и управления доступом к ресурсам. С расширением международной сети и ростом совместного использования компьютеров в функции каталогов было включено хранение основной контактной информации о пользователях. Примерами ранних каталогов могут служить MVS PROFS (IBM), база регистрационных данных Grapevine и WHOIS. Вскоре появились специализированные службы каталогов для специального поиска и ведения контактной информации для конкретных программных продуктов. Доступ к таким каталогам был возможен только с помощью специальных методов, а область их применения была ограниченной.
Разработка облегченного протокола доступа к каталогам (Lightweight Directory Access Protocol - LDAP) была вызвана ростом сети Интернета и необходимостью более тесного взаимодействия и строгой стандартизации. Этот общепринятый метод доступа к информации каталогов и ее модификации использовал все возможности протокола TCP /IP, оказался надежным и функциональным, и для его применения были разработаны новые реализации служб каталогов. Сама служба AD DS разрабатывалась так, чтобы соответствовать стандарту LDAP.

11.Active Directory Windows Server 2012. Основные характеристики доменной службы Active Directory.

Центральную роль в AD DS играют пять ключевых компонентов.

1. Совместимость с TCP /IP. В отличие от ряда специализированных протоколов вроде IPX/SPX и NetBEUI, протокол TCP /IP с самого начала создавался межплатформенным. Последующее принятие TCP /IP в качестве Интернет-стандарта для обмена данными сделало его одним из лидеров в мире протоколов и, по сути, превратило в обязательный протокол для операционных систем уровня предприятия. В AD DS и Windows Server 20 1 2 стек протоколов TCP /IP используется в качестве основного метода для обмена данными.
2. Поддержка протокола LDAP. Протокол LDAP (Lightweight Directory Access Protocol - облегченный протокол доступа к каталогам) 6ыл разработан в качестве стандартного Интернет-протокола для доступа к каталогам. Он применяется для обновления и запросов данных, хранящихся в каталогах. Служба AD DS непосредственно поддерживает LDAP.
3. Поддержка системы доменных имен. Система доменных имен (Domain Name System - DNS) была создана для преобразования упрощенных имен, понятных людям (таких как www.cco.com), в IP-адреса, понятные компьютерам (вроде 12.222.165.154). В AD DS она поддерживается и даже требуется для нормальной работы.
4. Поддержка безопасности. Поддержка безопасности в соответствии со стандартами Интернета чрезвычайно важна для бесперебойного функционирования среды, к которой подключены миллионы компьютеров по всему миру. Отсутствие надежных средств защиты привлекает хакеров, поэтому в Windows Server 201 2 и AD DS средства безопасности были значительно расширены. Так, в Windows Server 201 2 и AD DS была встроена непосредственная поддержка IPSec, Kerberos, центров сертификации и шифрования с помощью протокола защищенных сокетов (Secure Sockets Layer - SSL).
5. Легкость администрирования. При реализации мощных служб каталогов удобству администрирования и конфигурирования среды часто не уделяется должного внимания. А зря: этот аспект очень сильно влияет на общую стоимость эксплуатации. AD DS и Windows Server 2012 специально спроектированы так, чтобы ими было удобно пользоваться, и чтобы на освоение новой среды тратилось как можно меньше усилий.

12.Active Directory Windows Server 2012. Структура AD DS.

Домены в AD DS разграничиваются административную безопасность для объектов и содержат собственные политики безопасности. Домены - это логическая организация объектов, поэтому физических местоположений может быть много.

Домен AD DS, традиционно изображаемый в виде треугольника (рис. 11), является главной логической границей AD DS.

Рис. 11. Обозначение домена

Дерево AD DS состоит из нескольких доменов, соединенных двунаправленными транзитивными отношениями доверия. То есть если домен asia доверяет корневому домену companyabc, и домен europe также доверяет корневому домену, то домен asia доверяет europe. Доверительные отношения лишь обеспечивают путь от одного домена к другому. По умолчанию никакие права доступа от одного транзитивного домена к другому не передаются

Каждый домен в дереве AD DS использует общую схему и глобальный каталог. Корневым доменом дерева ADDS является companyabc.com, а asia.companyabc.com и europe.companyabc. com — его поддомены.

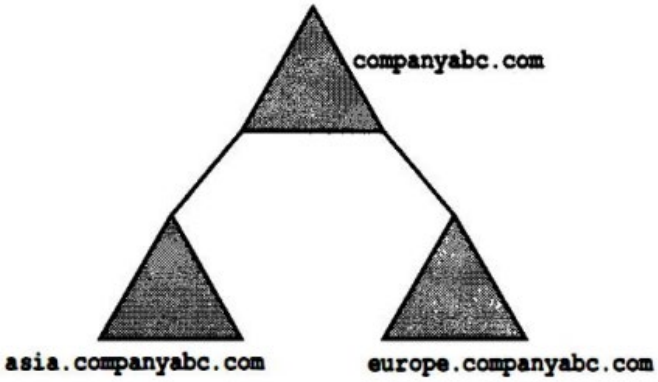


Рис. 12. Дерево ADDSc поддоменами

Лесами (forest) в AD DS называются группы связанных между собой деревьев доменов. Неявные отношения доверия объединяют корни всех деревьев в один общий лес.

Связями, объединяющими все домены и деревья доменов в общий лес, служит наличие общей схемы и общего глобального каталога. Хотя доменам и деревья доменов в этом лесу вовсе не обязательно использовать общее пространство имен. Например, домены microsoft. internal и msnbc. internal теоретически могут являться частями одного и того же леса, но при этом иметь собственные раздельные пространства имен. Леса служат основной границей организационной безопасности в AD DS, и потому предполагают наличие некоторой степени доверия к администраторам всех входящих в их состав доменов.

Все входящие в состав дерева домены используют общее пространство имен (в данном примере — companyabc. com), но содержат механизмы защиты для разграничения доступа из других доменов. То есть администратор домена europe может иметь относительный контроль над всем его доменом, а пользователи из домена asia или companyabc могут не располагать полномочиями на доступ к его ресурсам.

13.Проектирование структуры Active Directory. Общие положения. Структура доменов AD DS.

Схемой в AD DS - набор определений для всех типов имеющихся в каталоге объектов и связанных с ними атрибутов. Задает способ хранения и представления в AD DS данных обо всех пользователях, компьютерах и других объектах, чтобы они имели стандартный вид по всей структуре AD DS. Защищается с помощью списков управления разграничением доступа (Discretionary Access Control List - DACL) и отвечает за предоставление возможных атрибутов для каждого объекта в AD DS. Представляет собой базовое определение самого каталога и является основой функционирования среды домена. Вносимые в схему изменения влияют на всю среду AD DS.

Active Directory объединяет: физическую и логическую структуру для компонентов сети. Логические структуры Active Directory помогают организовывать объекты каталога и управлять сетевыми учетными записями и общими ресурсами. К логической структуре относятся следующие элементы:

• организационное подразделение (organizational unit) — подгруппа компьютеров, как правило, отражающая структуру компании;

• домен (domain) — группа компьютеров, совместно использующих общую БД каталога;

• дерево доменов (domain tree) — один или несколько доменов, совместно использующих непрерывное пространство имен;

• лес доменов (domain forest) — одно или несколько деревьев, совместно использующих информацию каталога.

Физические элементы помогают планировать реальную структуру сети. На основании физических структур формируются сетевые связи и физические границы сетевых ресурсов. К физической структуре относятся следующие элементы:

• подсеть (subnet) — сетевая группа с заданной областью IP- адресов и сетевой маской;

• сайт (site) — одна или несколько подсетей. Сайт используется для настройки доступа к каталогу и для репликации.

Рис. 4.5. Явное доверие между двумя деревьями доменов

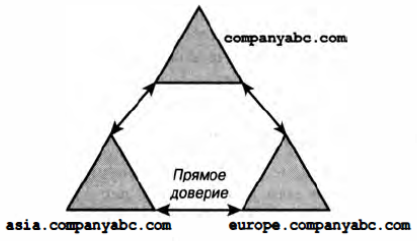


Рис. 4.6. Прямое доверие между двумя поддоменами леса

Доверительные отношения между доменами бывают:

1. Транзитивными - автоматически при создании домена. Двунаправленные. Права по умолчанию никакие не распределяются
2. Явные- устанавливаются вручную. Нужны для объединения двух несвязанных деревьев домена в один лес. Являются однонаправленными.
3. Прямые - когда явное отношение было установлено для направления потока доверительных отношений от одного поддомена к другому. Ускоряют аутентификацию, устраняя необходимость в перемещении по дереву вверх-вниз.

14.Проектирование структуры Active Directory. Выбор пространства имен для доменов.

Структуру AD DF легче всего реализовать в виде единого общего пространства имен DNS, отражающего имя компании и зарегистрированного в Интернете. Однако следует помнить, что публикация пространства имен AD DS открывает возможность взлома на основании полученных имен доменной системы. Настройка брандмауэра на блокирование внутренних запросов к DNS также затрудняется, если пространство имен организации совпадает с пространством имен, опубликованным в Интернете. Однако в этом случае достаточно создать простое правило, задающее блокировку любого трафика во внутреннюю структуру домена. Если организация использует несколько пространств имен, то их необходимо обеднить в лес.

Внутреннее пространство - не опубликовано в интернете. привносит в сеть дополнительный уровень сложности, поскольку в таком случае UPN-имена пользователей отличаются от их адресов электронной почты. Для данной структуры повышен уровень защиты. При этом такое пространство не должно быть зарегистрировано в интернете за пределами внутренней сети. Так как в этом случае могут возникнуть конфликты при выполнении DNS-запросов к лесу другой организации, которая опубликовало такое пространство имен.

15.Проектирование структуры Active Directory. Компоненты структуры доменов.

Компоненты Active Directory можно подразделить на две основные категории:

- Логические компоненты: Лес, Домены, Деревья доменов, Организационные подразделения
- Физические компоненты:
    - контроллеры домена - компьютер под управлением Windows Server. Может быть как физическим, так и виртуальным. На нем установлена роль служб домена Active Directory (AD DS),
    - сервер глобального каталога - нужен для того, чтобы пользователи из одного домена могли запрашивать интересующие их объекты из другого домена (в том же самом лесу). По сути частичная реплика доступных для записи объектов всего леса.
    - площадки Active Directory - определяют физическую топологию сетевой среды. Это могут быть например отдельные здания.

Объект- домен, папка, группа, пользователь, подразделение

Среди новых компонентов в Windows Server 2012:

- Поддержка виртуализации контроллеров доменов -
- Создание контроллера домена с носителя данных
- Транзитивные отношения доверия между лесами
- Функция переименования домена
- Корзина - возможность выполнять точное восстановление удаленных объектов в AD DS. То есть в лесе не придется создавать множество доменов для снижения риска связанного со случайным удалением объектов

Хорошо спроектированная Active Directory логическая структура предоставляет следующие преимущества:

- упрощенное управление сетями на основе Microsoft Windows, которые содержат большое количество объектов
- Объединенная структура домена и сокращение затрат на администрирование
- Возможность делегировать административный контроль над ресурсами соответствующим образом
- Снижение влияния пропускной способности сети
- Упрощенный общий доступ к ресурсам
- Оптимальная производительность поиска
- Низкая совокупная стоимость владения

16.Проектирование структуры Active Directory. Выбор доменной структуры. Модель с единственным доменом.

К числу главных моделей относятся:
• модель с единственным доменом;
• модель с несколькими доменами;
• модель с несколькими деревьями в одном лесе;
• модель с федеративными лесами;
• модель с выделенным корнем;
• модель с фиктивным доменом;
• модель специализированного домена.

Преимущества модели с единственным доменом:

- Простота
- Уменьшение расходов на администрирование, так как сложные структуры объединены в более простую

Недостатки:

- Не все структуры могут состоять из единственного домена
- Если контуры безопасности внутри организации должны иметь точные границы, то единый домен не подходит
- При наличии в лесу единственного домена компьютер с ролью эталона схемы должен находиться в этом же домене.

17.Проектирование структуры Active Directory. Выбор доменной структуры. Модель с несколькими доменами.

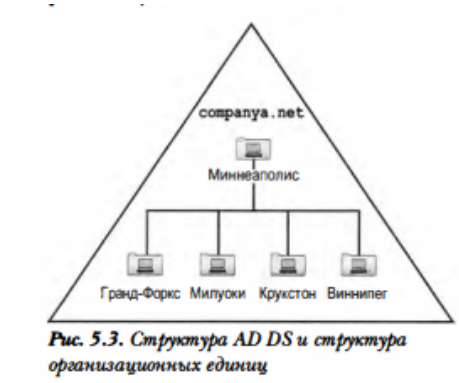


Рис. 5.3. Структура AD DS и структура организационных единиц

Рис. 5.4. Структура сайтов, созданная в соответствии с географическим расположением офисов

К числу главных моделей относятся:

- модель с единственным доменом;
- модель с несколькими доменами;
- модель с несколькими деревьями в одном лесе;
- модель с федеративными лесами;
- модель с выделенным корнем;
- модель с фиктивным доменом;
- модель специализированного домена.

Рекомендуется всегда сначала создать один домен и добавлять доп.домены только в случае крайней необходимости. По умолчанию всегда есть транзитивные отношения доверия, но они не позволяют делится ресурсами.

Причины такой необходимости:

1. Децентрализованное администрирование - если в различных филиалах применяются собственные структуры ИТ, и руководство не планирует объединять их в одну централизованную модель. Тогда добавляем. Каждый домен в таком случае будет играть роль границы безопасности для большинства видов деятельности и не позволять администрирование за своими пределами.
2. Географические ограничения - если различные филиалы соединяются очень медленными и ненадежными каналами связи или очень далеко друг от друга. Так повышается гибкость системы администрирования.
3. Уникальное пространство имен DNS - если какое-то подразделение использует для AD DS собственное зарегистрированное в Интернете пространство имен, но при этом использует общий лес, то добавляем как отдельный домен.
4. Необходимость в повышенной безопасности - потому что может понадобиться вынести роль эталона схемы в домен, отдельный от домена пользователей. Может потребоваться также использование модели с выделенным корнем или модель с фиктивным доменом.

18.Групповые политики Windows Server 2012 и управление политиками. Определение модели администрирования.

Групповые политики - это набор указаний для централизованной настройки и развертывания конфигураций компьютеров и пользователей. Групповая политика уже изначально содержит обширный набор параметров и может быть расширена с помощью сторонних поставщиков и собственной разработки параметров политик опытными администраторами групповых политик.

Начиная с Windows Server 2008, разработчики Microsoft определили два различных типа групповых политик: **локальные и доменные**.

Администраторы получили возможность создавать несколько локальных групповых политик, которые сейчас называются **локальными групповыми политиками**. Теперь на компьютерах можно создавать отдельные групповые политики пользователей для всех пользователей, для пользователей, которые не являются администраторами, и для пользователей-членов группы локальных администраторов. Эта возможность повышает безопасность и надежность компьютеров из состава рабочих групп или обособленных компьютеров.

Доменные групповые политики существенно отличаются от локальных групповых политик, поскольку для их создания и применения необходима среда Active Directory. Настройки в групповых политиках содержат узлы и политики, и предпочтений, что является еще одним значительным отличием, т.к. локальные групповые политики не содержат параметров предпочтений. Доменные групповые политики более удобны при указании, какие критерии используются для применении политики. Доменные политики можно фильтровать для применении к конкретным членам групп безопасности Active Directory, компьютеров или объектов в конкретной подсети или организационной единице (OU), либо их можно применять к компьютерам, работающим под конкретной версией ОС. Кроме того, при указании предпочтений в доменной групповой политике можно указывать применимость параметров на уровне отдельных элементов - на основании различных критериев.

Модель администрирования (управления) в ИС - это набор функций по управлению подсистемой или информационным процессом. Различные стандартизирующие организации предлагают разные наборы функций (различные модели) по управлению техническим обеспечением, организационной и функциональной подсистемами. Это модели ISO OSI, ISO FCAPS, OGC ITIL, ITU TMN, TMF eTOM.

При выборе модели администрирования учесть, что есть:

- модель с единственным доменом;
- модель с несколькими доменами;
- модель с несколькими деревьями в одном лесе;
- модель с федеративными лесами;
- модель с выделенным корнем;
- модель с фиктивным доменом;
- модель специализированного домена.

19. Групповые политики Windows Server 2012 и управление политиками. Знакомство с администрированием сайтов Active Directory.

Групповые политики - это набор указаний для централизованной настройки и развертывания конфигураций компьютеров и пользователей. Групповая политика уже изначально содержит обширный набор параметров и может быть расширена с помощью сторонних поставщиков и собственной разработки параметров политик опытными администраторами групповых политик.

Сайт — это группа компьютеров в одной или нескольких IP-подсетях, используемая для планирования физической структуры сети. Планирование сайта происходит независимо от логической структуры домена. Active Directory позволяет создать множество сайтов в одном домене или один сайт, охватывающий множество доменов.

В рамках Active Directory сайт определяет внешние и внутренние границы репликации и помогает пользователям найти ближайшие серверы для аутентификации и доступа к сетевым ресурсам. Он может также исполнять роль границы административного управления - например, при делегировании локальному администратору ответственности за сайт AD.

Сайты AD обычно содержат ресурсы, соединенные каналами с высокой пропускной способностью, и могут состоять из одной или нескольких компьютерных площадок, в зависимости от сетевой архитектуры.

После определения сайта AD серверы и клиентские рабочие станции используют информацию, хранимую в конфигурации сайта, для нахождения ближайших контроллеров домена, серверов глобальных каталогов и распределенных общих файловых ресурсов.

Конфигурирование сайта требует немного времени, поскольку требуется манипуляция очень немногими компонентами. В большинстве случаев определение и настройка конфигурации сайта в Active Directory требует лишь нескольких часов работы. После начальной установки сайты AD обычно не требуют изменений - разве что если существенно изменится сетевая топология, в том числе IP-адреса, будут добавлены или удалены контроллеры домена или будут добавлены новые сайты и удалены старые.

20.Средства администрирования ОС. Администрирование файловых систем.

Основной функцией операционной системы (ОС) является функция управления ресурсами компьютера, включая управление оперативной и дисковой памятью, управление периферийными устройствами и процессором.

Параметры ядра ОС задаются администратором системы (АС) при инсталляции ОС. После установки ОС администратор системы задает атрибуты пользователей в системе и осуществляет оперативное управление ОС.

В процессе авторизации пользователей АС может задать ряд параметров их работы: права доступа, максимальный объем дискового пространства, пароль пользователя и т.д. Средства учета ресурсов ОС позволяют администратору системы накапливать для дальнейшего анализа информацию об использовании отдельными пользователями таких ресурсов, как число блоков, считанных/записанных с диска сервера, число блоков, записанных за день, продолжительность работы приложения и т.д.

Утилиты работы с консолью сервера позволяют администратору системы контролировать функционирование рабочих станций, останавливать или запускать принтер, управлять очередями заданий к принтерам, посылать сообщения пользователям ИС. Операционные системы имеют похожие, но все же отличающиеся средства оперативного управления, которые описываются в технической документации по конкретной ОС.

Файл — это объект, представляющий собой данные и их атрибуты поименования и доступа. ОС организует доступ к данным не по их именам, а по адресам и соответственно должна поддерживать: таблицы преобразования имен в адреса (директории), информацию об атрибутах доступа и размерах данных, способы поиска записей в файлах (методы доступа к данным, например, по индексам). Совокупность директорий (каталогов) и других метаданных, т. е. структур данных, отслеживающих размещение файлов на диске и свободное дисковое пространство, называется файловой системой.

В различных файловых системах принят различный формат имен файлов и типы атрибутов доступа. Кроме того, каждая ОС поддерживает определенные и различные в разных файловых системах операции над файлами (открытия, закрытия, чтения/записи, поиска, обновления данных, обработки блоков переполнения).

АС должен помнить, что сложные и развитые методы доступа обычно используются при реализации не универсальных ОС, а СУБД, как специализированных ОС для работы с данными. Поэтому при реализации ИС следует обратить внимание на методы доступа к данным, которые применяются в используемой СУБД и, по возможности, выбрать метод, наиболее адекватный задаче ИС.

Любая ОС имеет набор утилит для работы с файловой системой для реализации задач дефрагментации файлового пространства, шифрования данных, поддержки транзакций ОС, восстановления после сбоев. При этом АС должен учесть, что транзакции СУБД и транзакции ОС могут не соответствовать друг другу, а методы восстановления данных СУБД превосходить существующие в ОС. Кроме того, ОС, поддерживая файловые системы, не занимаются вопросами целостности данных. Это реализуется только СУБД. Задача АС правильно комбинировать имеющиеся системные средства и избегать их противоречий.

21. Средства администрирования ОС. Параметры ядра ОС. Инсталляция ОС.

Инсталляция (установка) ОС включает в себя подготовку площадки и оборудования, инсталляцию файл-сервера и инсталляцию программного обеспечения рабочих станций, планирование структур каталогов (директорий), планирование пользователей и групп пользователей, планирование защиты, планирование процедур регистрации, настройку параметров. Поэтому администратор должен:

1. Проверить условия эксплуатации и выполнение требований по электропитанию оборудования. В «Руководстве по эксплуатации ОС» или в документации с аналогичным названием определены конкретные требования по следующим вопросам: температура/влажность; максимальная высота, глубина, ширина оборудования; требования электропитания - частота тока, потребляемая мощность, рассеиваемая мощность.
2. Аппаратные средства следует подключить к специализированным линиям питания, выделенным только для работы компьютерного оборудования.
3. Создать рабочие копии дистрибутива (поставляемой производителем ОС копии продукта). Оригинальный дистрибутив должен храниться в сейфе. При инсталляции АС должен использовать рабочие копии. АС должен решить, делает ли он обновление существующей версии ОС (upgrade) или первичную инсталляцию. Следует внимательно просмотреть инструкции по ОС для каждой из этих операций, так как действия при их осуществлении обычно различны, зависят от конкретной ОС и может существовать не один метод обновления
4. Записать в рабочую таблицу (worksheet) информацию по устанавливаемому серверу.

Таблица содержит следующую информацию: имя, марку, модель файл-сервера; размер памяти; несетевые платы - тип и настройка; сетевые платы - соответствующие драйверы, адрес сети, номер сети, адрес памяти, прерывание; плата процессора - модель, скорость работы; дисковые подсистемы - тип контроллера, драйверы, емкость, модель, производитель, число каналов ввода-вывода.

5. Подготовить для работы ОС подсистемы ввода-вывода на жесткие диски. После всех предварительных мероприятий осуществляется непосредственно процесс инсталляции с помощью утилит, предлагаемых производителем ОС (например, командой Install или Setup).

Процесс инсталляции ОС состоит в следующем: системные файлы помещаются на диск в специальную область. Загружаются дисковые, сетевые драйверы и драйверы периферийных устройств. Задаются параметры их работы. Это может выполняться либо администратором системы, например, отдельной командой Load, либо автоматически самой ОС. После этого администратор системы загружает ядро ОС с помощью вызова команды, предлагаемой производителем, например, Server.exe, и задает основные параметры работы ядра. К этим параметрам относятся: имя сервера; имя администратора и его пароль; список сетевых протоколов и их настройки (например, TCP/IP); параметр блокирования консоли сервера; опция шифрования паролей в системе; номера очередей печати; команды трассировки действий ядра (например, Track On) и т. д. Конкретный список таких параметров приводится в документации

по конкретной операционной системе. Затем администратору системы следует установить ОС на рабочих станциях ИС аналогично установке сервера. Далее АС должен сконфигурировать (иногда и установить) сетевые платы и загрузить драйвер сетевого адаптера с указанием параметров реса памяти и прерывания, по которым он работает и специальную оболочку (Shell), определяющую, является обращение прикладной программы обращением к локальной ОС или к сетевой.

Далее АС должен спланировать процедуру регистрации пользователя на сервере. Фактически выполняются всегда две процедуры - сначала системная (для настройки рабочей среды всех пользователей), а затем пользовательская (для настройки среды конкретного пользователя). В системную процедуру могут входить общие приветствия всех пользователей, назначения имен (буквы английского алфавита) сетевым дискам (tap), подключение групп пользователей к различным серверам (attach). В процедурах пользовательской регистрации инициализируются параметры среды каждого пользователя, например, доступ к данному серверу только данного пользователя. Конкретные возможности процедур регистрации зависят от реализации ОС.

22.Средства администрирования ОС. Подсистема ввода-вывода (дисковая подсистема) и способы организации дискового пространства. IDE, SATA, SCSI.

Современная дисковая подсистема ввода-вывода состоит из адаптеров на материнской плате HBA (Host Bus Adapter), шины (интерфейс), дискового контроллера и непосредственно жестких дисков.

Так как обычно операционная система может поддерживать более одного канала ввода-вывода, АС должен изучить особенности работы конкретной ОС. С увеличением числа каналов ввода-вывода обычно резко растет производительность системы. Кроме того, производительность дисковой подсистемы зависит от типа интерфейса.

Распространенные типы интерфейсов.

- IDE: контроллер располагается непосредственно на диске, благодаря чему скорость возрастает до 12 Мбит/с. Используется RLL-кодирование и сняты ограничения на объем дисковой памяти.
- EIDE - Enhanced (расширенный) IDE: добавляет специальную систему адресации для дисков системы адресации AT Attachment (ATA). Система адресации ATA - это промышленный стандарт, который описывает способ адресации диска емкостью свыше 528 Мбайт с помощью BIOS компьютера. Скорость интерфейса составляет до 13,3 Мбит/с, а адаптеры на материнской плате компьютера для подключения контроллеров дисков Host Bus Adapters (HBA) позволяют подключать до 4 дисков и различные периферийные устройства.
- SCSI (Small Computer Systems Interface) - это высокоскоростной параллельный интерфейс, стандартизированный ANSI. Он позволяет подключать к одной шине множество устройств, вытягивая их в цепочку. К каждому дисковому контроллеру SCSI можно присоединить до семи устройств. В настоящее время SCSI широко применяется на серверах, высокопроизводительных рабочих станциях. Скорость записи на диск достигает 600 Мбит/с.
- SATA - Serial ATA - высокоскоростной последовательный интерфейс обмена данными с накопителями информации (как правило, с жесткими дисками). Является развитием интерфейса ATA (переименован в PATA (Parallel ATA)). Обеспечивает скорость до 600 Мбит/с. Предполагает отказ от плоских параллельных кабелей с разъемами для двух дисков и переход к последовательной передаче данных по витой паре. Но к каждому контроллеру подключается только один диск одним кабелем. Особенностью стандарта по является использование встроенной очереди команд NCQ (Native Command Queuing), которое позволяет устройству накапливать запросы и оптимизировать порядок их выполнения с учетом внутренней архитектуры устройства (минимизация количества перемещений головок, простоя в ожидании нужного сектора на треке). Повышается производительность решения задач, связанных с произвольным чтением, обработкой данных от двух и более источников, одновременную работу нескольких программ. Горячая замена устройств.

23.Средства администрирования ОС. Подготовка дисковой подсистемы для ее использования ОС.

Любая дисковая подсистема требует подготовки для работы с ней конкретной ОС. Часто часть этой подготовки производится на заводах производителях или компаниями-поставщиками оборудования.

Подготовка дисковой подсистемы содержит три этапа: форматирование низкого уровня, организация разделов, форматирование высокого уровня.

- Форматирование низкого уровня (Low level format) - необходимо контроллеру диска, чтобы читать его по секторам. Выполняется на заводе-производителе дисков, и соответствующая утилита прилагается к дисковой подсистеме. Действия: проводится анализ дискового пространства на наличие ошибок; сектора диска разбиваются на треки (дорожки) и присваиваются идентификаторы секторов; помечаются испорченные сектора (bad-сектора); устанавливается чередование секторов (interleave), когда номера секторов не совпадают с их физической последовательностью. Чередование секторов необходимо, чтобы синхронизировать работу процессора (обработку данных) и контроллера (считывание с диска). От этого зависит скорость работы подсистемы ввода-вывода. Необходимо если :
    - ставятся новые дисковые подсистемы (если это не сделано производителем); обнаружено большое число дисковых ошибок (если средства ОС не помогают их устранить);
    - необходимо поменять параметр interleave (ОПАСНО, следует понимать, как именно обрабатываются данные контроллером и ОС и зачем нужно что-то менять);
    - возникает необходимость переразметить bad-сектора.

  ПОСЛЕ НЕГО ВОССТАНОВИТЬ ИНФОРМАЦИЮ НЕЛЬЗЯ
- Организация разделов - это процесс разбиения жесткого диска на логические части - партиции (partitions). Необходимо так как на одном компьютере может работать несколько ОС. Для каждой из них нужно свое дополнительное форматирование.
    - Первичная партиция (primary partition) для ОС загруженной первой
    - В начале каждого диска на нулевом треке располагается специальная таблица (partition table). В ней находится информация о том, как будет использоваться дисковое пространство согласно различным партициям. Ее потеря означает для администратора системы потерю всей информации в системе.
- Форматирование высокого уровня (High level format) осуществляется средствами той ОС, которая работает в этой партиции. Во время этого форматирования создается оглавление диска и его подготовка для конкретной ОС. В различных ОС при этом выполняются различные функции.

Разбиение на тома, чтобы выделить логически единые части информации. Том может быть частью партиции, состоять из одной целой партиции или из нескольких партиций. В начале каждого тома хранится специальная таблица VDT (Volume Definition Table). Обычно она дублируется, располагаясь в нескольких местах. В VDT находится информация о том, какие треки используются для этого тома в партиции.

24.Средства администрирования ОС. Технология RAID. RAID 0, RAID 1, RAID 5.

Термин RAID (Redundant Array of Independent/Inexpensive Disks) определяет любую дисковую подсистему, которая объединяет два или более стандартных физических диска в единый логический диск (дисковый массив). Такие дисковые массивы служат для повышения надежности хранения данных и для повышения скорости чтения/записи информации. Они также упрощают сопровождение дисковой подсистемы, так как АС вместо нескольких дисков обслуживает как бы один. Обычно объединение в логический диск осуществляется программно средствами ОС на базе подсистемы ввода-вывода SCSI (для небольших систем на базе SATA).

RAID 0 - разделение данных между дисками и чередование блоков. Система пишет блоки данных на каждый диск массива подряд. Преимущества: улучшенная производительность и увеличение объема логических томов; разделение данных между дисками позволяет предотвратить ситуации, в которых происходит постоянное обращение к одному диску, в то время как другие диски простаивают. Недостатки: отсутствие избыточности; поскольку весь массив дисков представляет собой один логический том, то при выходе из строя любого диска из строя выходит весь массив.

RAID 1 - зеркальное отображение/дуплекс. Диски зеркалируются или дублируются. Каждый байт записывается на два идентичных диска. Преимущества: если один диск выходит из строя, другой продолжает работать. Повышается скорость чтения данных, поскольку можно начать поиск данных на одном диске, в то время как другой диск обрабатывает предыдущий запрос. Однако скорость записи в этом случае замедляется, поскольку данные необходимо записать сразу на два диска. Влияние этой стратегии на производительность зависит от соотношения операций чтения/записи в используемых приложениях. Недостатки: дороговизна, поскольку для функционирования системы требуется в 2 раз больше дискового пространства, чем это действительно необходимо. Кроме того, необходимо дополнительное место в сервере и дополнительное электропитание.

RAID 5 - разделение данных с чередованием блоков и распределенным контролем четности; разделение блоков данных между всеми дисками. Данные для контроля целостности хранятся на всех дисках (см. рис. 9). Преимущества: операции чтения и записи могут осуществляться параллельно, что повышает скорость передачи данных. Этот тип массива высокоэффективен при работе с малыми блоками данных. Предоставляет избыточность с небольшими расходами. Эффективность пятого уровня растет в зависимости от числа дисков, используемых в массиве, поскольку объем данных для контроля целостности обычно занимает один диск, хотя хранятся эти данные на нескольких дисках одновременно. Иногда в массивах пятого уровня используются смонтированные, но бездействующие диски. В случае возникновения неисправности у одного из дисков, входящих в массив, свободный диск может быть автоматически использован для замены поврежденного диска и восстановления данных. Недостатки: менее производителен из-за необходимости рассчитывать данные для коррекции ошибок.

25.Средства администрирования ОС. Вопросы администрирования файловых систем.

Файл — это объект, представляющий собой данные и их атрибуты поименования и доступа. ОС организует доступ к данным не по их именам, а по адресам и соответственно должна поддерживать: таблицы преобразования имен в адреса (директории), информацию об атрибутах доступа и размерах данных, способы поиска записей в файлах (методы доступа к данным, например, по индексам). Совокупность директорий (каталогов) и других метаданных, т. е. структур данных, отслеживающих размещение файлов на диске и свободное дисковое пространство, называется **файловой системой.**

В различных файловых системах принят различный формат имен файлов и типы атрибутов доступа. Кроме того, каждая ОС поддерживает определенные и различные в разных файловых системах операции над файлами (открытия, закрытия, чтения/записи, поиска, обновления данных, обработки блоков переполнения).

АС должен помнить, что перед обращением к файловой системе надо смонтировать том, на котором она будет располагаться. При этой операции проводят проверку типа файловой системы тома и ее целостности, считывания системных структур данных (оглавления тома), инициализация соответствующего модуля ОС, включение файловой системы в общее пространство имен.

26.Администрирование процесса поиска и диагностики ошибок. Общие положения.

Процесс поиска и диагностики ошибок в ИС может быть чрезвычайно сложным и многосторонним. В данном случае он будет рассматриваться на основе поиска и диагностики ошибок сетевых систем. Но поскольку практически любой специалист по информационным технологиям сталкивается в настоящее время со средой протоколов TCP/IP, особое внимание и место в этой главе уделено практическому решению проблем, возникающих при их использовании. Как уже отмечалось, администрирование систем осуществляется на основе различных моделей управления, а администрирование сетевых систем - на основе модели FCAPS, согласно которой, все аспекты управления сетью могут быть описаны с помощью пяти областей управления.

Как уже отмечалось, рекомендации ITU-T X.700 и близкий к ним стандарт ISO 7498-4 делят задачи системы управления на пять функциональных групп:

(F) Fault Management (управление отказами) - обнаружение отказов в устройствах сети, сопоставление аварийной информации от различных устройств, локализация отказов и инициирование корректирующих действий.

(C) Configuration Management (управление конфигурированием) - возможность отслеживания изменений, конфигурирования, передачи и установки программного обеспечения на всех устройствах сети.

(A) Accounting Management (управление учетом) - возможность сбора и передачи учетной информации для генерации отчетов об использовании сетевых ресурсов.

(P) Performance Management (управление производительностью) - непрерывный источник информации для мониторинга показателей работы сети (QoS, ToS) и распределения сетевых ресурсов.

(S) Security Management (управление безопасностью) - возможность управления доступом к сетевым ресурсам.

27.Администрирование процесса поиска и диагностики ошибок. Задачи функциональной группы F. Двенадцать задач управления при обнаружении ошибки.

Эта группа задач включает выявление, определение и устранение последствий сбоев и отказов в работе сети. На этом уровне выполняется не только регистрация сообщений об ошибках, но и их фильтрация, маршрутизация и анализ на основе знаний и опыта администратора системы. Фильтрация позволяет выделить только важные сообщения из весьма интенсивного потока сообщений об ошибках, который обычно наблюдается в большой сети. Маршрутизация обеспечивает их доставку нужному элементу системы управления, а корреляционный анализ позволяет найти причину, породившую поток взаимосвязанных сообщений.

Устранение ошибок в системе может быть автоматическим и полуавтоматическим. При автоматическом устранении ошибок ИС непосредственно управляет оборудованием или программными комплексами и обходит отказавший элемент за счет резервных каналов или специальных технологий, например, протоколов. В полуавтоматическом режиме основные решения и действия по устранению неисправности выполняют службы администратора системы, а специализированная система управления MS (Management System) только помогает в организации этого процесса, например, оформляет квитанции на выполнение работ и отслеживает их поэтапное выполнение.

В модели FCAPS идентифицировано 12 задач управления администратора системы как необходимых для успешной работы по управлению отказами и поиску ошибок. К ним относятся:

1) определение ошибки;
2) коррекция ошибки;
3) изоляция ошибки;
4) восстановление после ошибки;
5) поддержка тревожных сигналов (alarms);
6) фильтрация тревожных сигналов;
7) генерация тревожных сигналов;
8) проблема объяснения ошибки (корреляция);
9) проведение диагностических тестов;
10) ведение журнала ошибок;
11) сбор статистики ошибок;
12) сопровождение ошибок.

Эти задачи обычно в том или ином объеме решаются системой управления, используемой администратором системы. Однако АС должен понимать, что управляющая система помогает ему, а не думает за него. Помимо управляющей системы, а также в ситуации, когда она не используется вовсе, АС должен пользоваться моделью поиска ошибок, которую рекомендуют обычно разработчики операционных систем.

28.Администрирование процесса поиска и диагностики ошибок. Базовая модель поиска ошибок.

Базовая модель поиска ошибок предусматривает последовательное выполнение администратором системы следующих действий:

1. Убедиться в том, что ошибки действительно есть. Другими словами, после сообщения пользователя о некорректной работе ИС надо убедиться в том, что этот пользователь выполняет все процедуры корректно и правильно оценивает работу ИС.
2. Провести инвентаризацию. Это означает, что необходимо выяснить, все ли части ИС на месте: все кабели существуют, все части ИС взаимодействуют и правильно соединены. При этом NMS может помочь провести автоматический опрос параметров работы оборудования и программного обеспечения, дать план системы. У администратора системы должна быть исполнительная документация по ИС с картой сети и списками всех параметров загрузки серверов, рабочих станций, коммутационного оборудования (worksheet). Нужно убедиться в том, что «все на месте» и соответствует документации.
3. Сделать копии ИС (backup). Причем желательно это делать «быстрыми средствами» (например, не утилитой копирования СУБД, а утилитами ОС «том в том» или «диск в диск»).
4. Сделать перезагрузку всех компонент ИС (restart). Есть два режима перезагрузки: холодный режим (с отключением питания) и горячий режим (без отключения питания). При холодном рестарте заново загружается все ПО оборудования, все драйверы, все процессы ОС и СУБД, заново инициализируется память серверов. Поэтому при ошибочных ситуациях надо использовать холодный рестарт. Однако если есть ошибки оборудования, то оно после этого может вообще не загрузиться. Перед перезагрузкой нужна не забыть завершить работу всех процессов различных ОС и СУБД (обычно команды типа Down или Shutdown).
5. После перезагрузки необходимо упростить работу ИС, например, завершить работу всех резидентных программ, не обязательных для работы в простейшем варианте ИС.
6. Если система загрузилась, нужно проверить права и привилегии работающих пользователей (например, одно приложение запускается и работает нормально с данными правами пользователя, а другое нет).
7. Надо убедиться, что версии программного обеспечения являются текущими. Следует работать не на последней версии продуктов, а на стабильной, хорошо отлаженной. Нужно убедиться в том, что никто из пользователей не поставил себе никаких обновлений программного обеспечения. Хотя при правильных действиях АС и NMS такой возможности у пользователя не должно быть.
8. Только после всех перечисленных действий надо собирать информацию об ошибке. Для этого следует проанализировать журналы ИС (логи). Выявить симптомы проблемы, а также тех, кто был ею затронут, проанализировать использование процессов во время возникновения ошибки, изменения, произошедшие в системе, после которых появились сообщения об ошибке в журналах.
9. Необходимо разработать план по изоляции ошибки. Для этого строятся гипотезы о причинах ошибки в ИС. Это могут быть ошибки каналов связи (80% всех ошибок), аппаратные ошибки, ошибки системного программного обеспечения, прикладного программного обеспечения. Всегда следует учитывать, что тираж аппаратных средств больше, чем тираж программных продуктов.

Например, процессоров Intel выпускается больше, чем установок какой-либо одной ОС, поэтому аппаратных ошибок будет меньше, чем программных. Аналогично тираж системного программного обеспечения больше, чем тираж прикладного ПО, поэтому в первом меньше ошибок, чем в последнем. Просто чем больше тираж продукта, тем лучше он отлажен.

10. После разработки плана по изоляции ошибки следует ранжировать гипотезы по вероятности их подтверждения. Начинать проверку целесообразно не с самой вероятной гипотезы, а с той, которую можно быстрее всего проверить. Тем самым можно быстро отсечь часть гипотез и сузить процесс проверки.

11. Затем гипотезы проверяются по очереди (строго по одной в единицу времени), в определенной последовательности. В восходящем направлении — от рабочей станции к коммутационной аппаратуре или серверу либо в нисходящем направлении — от сервера или коммутационной аппаратуры к рабочей станции. Для проверки используются только специальные проверенные версии программных продуктов, специальные тестовые кабели и проверенные надежные тестовые диагностические средства.

12. Наконец, последним действием является документирование проблемы и способа ее решения в специальном журнале. Обязательно должны быть созданы инструкции службам администратора системы по действиям, предотвращающим повторное появление проблемы.

29.Администрирование процесса поиска и диагностики ошибок. Стратегии определения ошибок.

Существуют два подхода к поиску неисправностей:

1. Практический - опыт специалиста-практика подсказывает, что при возникновении неисправности целесообразно начинать менять сетевые платы, кабели, аппаратные средства и программное обеспечение до тех пор, пока система не начнет работать
2. При теоретическом подходе специалист-теоретик анализирует ситуацию до тех пор, пока не будет найдена точная причина ошибки. При таком решении, например, сетевой проблемы требуется современный высокопроизводительный протокольный анализатор для набора и анализа огромного количества сетевого трафика в течение значительного времени. Затем сетевому специалисту необходим длительный теоретический анализ данных. Этот процесс надежен, однако не многие компании могут себе позволить, чтобы их ИС или сеть не функционировала в течение нескольких часов или даже дней

Действия администратора системы должны базироваться на стратегии управления ошибками. Стратегия управления ошибками может быть:

1. Проактивная - с ростом объема ИС возрастает потребность в ее надежности и, соответственно, возрастает потребность в предварительном мониторинге производительности системы, предупреждениях пользователям о возможных проблемах, постоянной бдительности администратора системы.
2. Реактивная - стратегия, при которой АС не предупреждает появление ошибок, а разбирается с ошибками по мере их возникновения

Обычно системы управления отказами (ошибками) - NMS разбивают сложную задачу идентификации и диагностики ошибки на четыре подзадачи: определение ошибки; генерация тревожного сигнала; изоляция ошибки; коррекция ошибки.

При этом возможны две технологии работы NMS:

1. Пассивная технология. С помощью протокола SNMP устройства оповещают управляющую систему о выполнении заранее предусмотренного и заданного параметрами системы условия, например, отличие какого-либо параметра от номинального значения. Эта технология должна применяться администратором системы при идентификации проблем, не связанных с аппаратными сбоями, например, при изменении производительности, проблемах интерфейсов и т. д.
2. Активная технология. Система NMS тестирует ИС (например, с помощью утилиты PING) и опрашивает каждое из устройств на регулярной основе. Если какое-либо устройство не реагирует в заданный администратором системы интервал времени или его параметры отличаются от желаемых, посылается сообщение администратору системы о сбое устройства. АС должен выбрать систему управления, позволяющую использовать обе стратегии. Кроме того, правильно спроектированная система управления дает возможность администратору системы выполнять далее перечисленные логические действия по управлению ошибками. Выбрать время, когда управление ошибками осуществляется полностью, не осуществляется вовсе или осуществляется частично. Время работы ИС определяется в специальном документе - соглашении об уровне сервиса SLA

(Service Level Agreement). И это время может отличаться от часов работы данного предприятия. Например, предприятие работает с 9.00 до 18.00, а ИС работает 24 часа, 7 дней в неделю и 365 дней в году. Часть времени ИС может быть занято под специальные действия, не требующие контроля над возможными ошибками. Это можно указать в параметрах настройки MS. Например, мониторинг ошибок проводится в течение 20 из 24 часов. Если это требование выполняется, считается, что ошибок нет. При настройке MS создать специальные триггеры, определяющие, какую ситуацию в данной системе следует рассматривать как ошибочную. В некоторых случаях надо подавлять сообщения об ошибках. Например, сообщение о том, что производительность упала на 0,5%, что не существенно для большинства систем. Настроить параметры автоматической перезагрузки системы и переустановки параметров (reset). Можно настроить параметры MS так, чтобы в определенных случаях система сама перезагружалась и устанавливала определенные параметры в номинальные значения. Установить подавление предупреждений об ошибках в некоторых случаях. Например, если известен дефект работы устройства, но он не влияет на работу ИС.

30.Администрирование процесса поиска и диагностики ошибок. Средства администратора системы по сбору и поиску ошибок.

Средства ОС и СУБД. В составе любой ОС и СУБД всегда есть специализированные утилиты (возможно, модули ядра) или утилита «Монитор». Это программные продукты, запускаемые на файл-сервере либо на сервере БД, либо на специализированных выделенных серверах под управлением ОС. Монитор или мониторы позволяют собирать статистику ошибок, анализировать их, выдавать предупреждения администратору системы о сбоях и т.д. Эти утилиты частично выполняют функции MS или NMS. Загружаются они при загрузке ОС либо при запуске приложения (сессии приложения), либо при запуске ядра СУБД. Средства эмуляции предназначены для эмуляции системной консоли оборудования в удаленном варианте. Они обычно входят в состав любой операционной системы и используются, например, для управления консолью любого сетевого оборудования с персонального компьютера администратора системы. Существует промышленный стандарт на такую эмуляцию, реализованный в программах Telnet и SSH. Программное обеспечение Telnet первоначально использовалось на UNIXсерверах и предназначено для конфигурации и администрирования сетевых устройств с машины администратора системы. Работает продукт на третьем и четвертом уровнях модели OSI. Его можно применять в целях удаленного управления только в том случае, если АС уверен в отсутствии сетевых ошибок или в отсутствии необходимости обновления параметров. SSH используется в тех же целях, но в продукте реализована часть функций защиты от несанкционированного доступа при его применении. Они используют в своей работе только возможности серийного порта и кабеля, запускаются на станции администратора системы, присоединяемой непосредственно по интерфейсу физического уровня модели OSI к сетевому устройству. В этом случае нет вероятности сетевой ошибки, которая в свою очередь помешала бы исправлению ошибки, обнаруженной администратором системы. Дополнительные продукты используются для активного поиска ошибок в быстром режиме, например: анализаторы протоколов для сетевых систем, эмуляторы трафика (для эмуляции загрузки ИС), симуляторы атак (для проверки защиты от НСД), симуляторы ошибок (для проверки защищенности ИС от ошибок). Специализированные утилиты используются для тестирования ИС с помощью средств ОС или СУБД, например, утилиты Ping или Traceroot.

31.Администрирование сетевых систем. Вопросы внедрения мостов и коммутаторов. Управление коммутаторами.

Для учета конфигураций, слежения за производительностью сетевой системы, защиты от несанкционированного доступа администратор системы использует специальные программные продукты - NMS (Network Management System).

Информационные системы администрирования - это программные или программно-аппаратные продукты, предназначенные для решения комплекса задач централизованного управления распределенными ИТ ресурсами, обеспечения их гарантированной доступности для пользователей в соответствии с заданными эксплуатационными требованиями. Они позволяют обеспечить управление всеми составляющими технологического, прикладного и организационно-технологического уровней информационной инфраструктуры предприятия

Системы сетевого администрирования выполняют управление только сетевой подсистемой ИС, т. е. коммутаторами, маршрутизато-рами, шлюзами и другими сетевыми устройствами, обычно на базе протокола SNMP. Но поскольку основной проблемой сетевого управления стала проблема управления производительностью, то современные системы сетевого администрирования часто базируются на протоколе управления NetFlow.

Сетевые средства развиваются чрезвычайно быстро. Так при необ-ходимости перехода на новый протокол маршрутизации в корпоративной сети передачи данных следует рассматривать в первую очередь переход именно на протокол OSPF.

В настоящее время протокол OSPF считается более перспективным решением для использования в средних и крупных корпоративных сетях передачи данных. У него множество положительных отличий по сравнению с другими распространенными в настоящее время внутренними протоколами маршрутизации, главные из них: открытая спецификация, иерархическая архитектура, а также значительно лучшие времен-ные параметры обнаружения и обработки изменений в топологии сети передачи.

32.Администрирование сетевых систем. Задача проектирования сети.

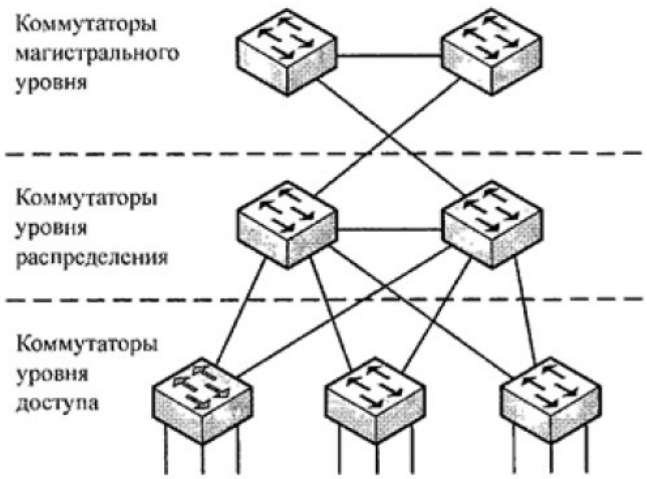


Рис. 10. Трехуровневая модель сети

Тщательное проектирование сети является важнейшей задачей служб администратора системы. Если при проектировании сети допущены ошибки, то может возникнуть множество непредвиденных проблем в приложениях ИС.

Для решения задачи проектирования сетей принят трехуровневый подход

На **уровне доступа** происходит передача данных в сеть и осуществляется входной контроль. Через этот уровень конечные пользователи получают доступ к сети. Коммутатор уровня доступа обеспечивает физический канал от интерфейса конечного пользователя до устройств, расположенных на уровне распределения. Уровень доступа использует списки доступа, которые предназначены для предотвращения несанкционированного доступа пользователей к сети. На этом уровне принимаются решения политик безопасности. Уровень доступа также предоставляет доступ к узлам удаленных сетей.

Уровень распределения определяет границы сети и обеспечивает манипуляцию пакетами в сети. Его назначение состоит в отделении процес-сов магистрального уровня от остальной части сети. Этот уровень определяет политику (стратегию) доступа к сети. Для обеспечения безопасности сети и экономии ресурсов путем предотвращения передачи нежелательных данных могут быть использованы различные политики.

Магистральный уровень предназначен для создания оптимизированной и надежной транспортной структуры для передачи данных с большими скоростями. Иными словами, базовый уровень должен передавать данные максимально быстро, а само устройство должно быть очень надежным и содержать самые быстрые процессоры в сети. Администратор системы должен учесть, что устройства этого уровня не должны быть загружены выполнением таких операций, как проверка списков доступа, шифрование данных, трансляция адресов и других функций, которые препятствуют коммутации пакетов с максимально возможной скоростью. Устройства магистрального уровня должны иметь доступ к любому узлу сети.

33.Администрирование сетевых систем. Вопросы внедрения маршрутизаторов. Протоколы маршрутизации. Маршрутизаторы, протоколы маршрутизации.

Маршрутизатор (router) — устройство, работающее на третьем сетевом уровне модели OSI. Маршрутизатор принимает решения о пересылке пакетов сетевого уровня модели OSI их получателю на основании информации об устройствах в сети (таблицы маршрутизации) и определенных правил. При этом в пределах сегмента он работает на канальном уровне модели OSI, а между сегментами — на сетевом. На сетевом уровне создается логический адрес сети. Этот адрес присваивается операционной системой или администратором системы для идентификации группы компьютеров. Такую группу иначе называют subnet (подсеть)

Маршрутизация — это процесс поддержания таблицы маршрутизации и обмена информацией об изменениях в топологии сети с другими маршрутизаторами. Эта функция реализуется с помощью одного или нескольких протоколов маршрутизации либо с помощью статически настроенных таблиц маршрутизации

Протокол маршрутизации — сетевой протокол, используемый маршрутизаторами для определения возможных маршрутов следования данных в составной компьютерной сети. Применение протокола маршрутизации позволяет избежать ручного ввода всех допустимых маршрутов, что, в свою очередь, снижает количество ошибок, обеспечивает согласованность действий всех маршрутизаторов в сети и облегчает труд администраторов.

В зависимости от алгоритма маршрутизации протоколы делятся на два вида:

- дистанционно-векторные протоколы (основаны на алгоритме DVA — англ. distance vector algorithm) - RIP;
- протоколы состояния каналов связи (основаны на алгоритме LSA — англ. link state algorithm) - OSPF.

OSPF (англ. Open Shortest Path First) — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути алгоритм Дейкстры.

Принцип работы заключается в следующем:

1. После включения маршрутизаторов протокол ищет непосредственно подключенных соседей и устанавливает с ними «дружеские» отношения.
2. Затем они обмениваются друг с другом информацией о подключенных и доступных им сетях. То есть они строят карту сети (топологию сети). Данная карта одинакова на всех маршрутизаторах.
3. На основе полученной информации запускается алгоритм SPF (Shortest Path First, «выбор наилучшего пути»), который рассчитывает оптимальный маршрут к каждой сети. Данный процесс похож на построение дерева, корнем которого является сам маршрутизатор, а ветвями — пути к доступным сетям. Данный процесс, то есть конвергенция, происходит очень быстро.

34.Администрирование сетевых систем. Конфигурирование протокола маршрутизации.

В маршрутизаторах различных производителей все протоколы маршрутизации имеют общие аспекты конфигурирования.

Для запуска протокола маршрутизации используется определенная команда (например, router).

После запуска процесса маршрутизации необходимо в режиме конфигурирования выбранного протокола маршрутизации задать номера сетей, которые будут участвовать в выбранном процессе маршрутизации. Это делается при помощи специальной команды (например, network), а также дополнительными командами конфигурирования конкретных протоколов маршрутизации.

Количество одновременно используемых маршрутов может быть указано с помощью специальной команды (например, maximum-paths). Число маршрутов для перераспределения нагрузки в большинстве протоколов маршрутизации не должно превышать четырех. Маршрутизатор осуществляет балансировку нагрузки по циклическому принципу, который предполагает, что по очереди используется сначала первый, потом второй и так далее параллельный канал. По достижении последнего канала процедура повторяется.

35.Администрирование баз данных. СУБД. Администрирование баз данных и администрирование данных.

Во всех СУБД различаются (хотя и называются по-разному) два уровня администрирования: системный администратор (администратор СУБД) и администраторы базы данных (БД). Одна копия программного продукта СУБД может поддерживать одновременное существование многих БД - коллекций данных и прикладных средств их обработки. Разные БД могут быть связаны с разными проектами и даже с разными организациями, поэтому у каждой БД должен быть свой администратор.

Функции администратора сводятся к следующим:

- инсталляция СУБД;
- управление памятью;
- управление разделением данных между пользователями;
- копирование и восстановление БД;
- управление безопасностью в системе;
- передача данных между СУБД и другими системами;
- управление производительностью.

Инсталляция СУБД является функцией только системного администратора.

Данные в СУБД хранятся на внешней памяти. Администратор должен обеспечить такое выделение памяти, чтобы с одной стороны, ее было достаточно для хранения и эффективного доступа к данным, а с другой - минимальное количество выделенной памяти оставалось неиспользованным.

Разделение данных между пользователями при их параллельной работе обеспечивается автоматически средствами СУБД и поддерживается средствами языка SQL. Однако при одновременной работе независимых приложений (иногда - и в рамках одного приложения) могут возникать конфликты одновременного доступа. Администратор, имея исчерпывающее представление о дисциплинах разделения, применяемых СУБД, выступает в роли консультанта прикладных программистов, сводя к минимуму взаимное блокирование приложениями друг друга.

Копирование и восстановление являются необходимыми для гарантирования сохранности данных даже при полном крахе системы. Эта часть функций администратора включает в себя работу с соответствующими утилитами СУБД и с протоколами транзакций.

Управление безопасностью данных защищает их от несанкционированных пользователей. Оно состоит в регистрации пользователей в системе, выделении пользователям привилегий и бюджетов.

В составе любой ОС и СУБД всегда есть специализированные утилиты (возможно, модули ядра) или утилита «Монитор». Это программные продукты, запускаемые на файл-сервере либо на сервере БД, либо на специализированных выделенных серверах под управлением ОС. Монитор или мониторы позволяют собирать статистику ошибок, анализировать их, выдавать предупреждения администратору системы о сбоях и т.д. Эти утилиты частично выполняют функции MS или NMS. Загружаются они при загрузке ОС либо при запуске приложения (сессии приложения), либо при запуске ядра СУБД.

36.Администрирование баз данных. СУБД. Инсталляция СУБД.

Во всех СУБД различаются (хотя и называются по-разному) два уровня администрирования: системный администратор (администратор СУБД) и администраторы базы данных (БД). Одна копия программного продукта СУБД может поддерживать одновременное существование многих БД - коллекций данных и прикладных средств их обработки. Разные БД могут быть связаны с разными проектами и даже с разными организациями, поэтому у каждой БД должен быть свой администратор.

Инсталляция СУБД является функцией только системного администратора

37.Администрирование процесса конфигурации. Необходимость администрирования процесса конфигурации. Последовательность процесса конфигурации.

Под конфигурацией ИС будем понимать разработку и реализацию концепции, позволяющей администратору системы быть уверенным в непротиворечивости, целостности, проверяемости и повторяемости параметров системы.

Сначала следует установить базовую конфигурацию и задокументировать ее. Затем нужно определить механизм изменения и модификации базовой конфигурации. После этого внедрить процесс проверки текущей конфигурации на соответствие заданным базовым параметрам (аудит конфигурации).

Для первого шага следует установить некоторую текущую конфигурацию как базовую и соответствующую ей связь между устройствами и программными продуктами. Это не столько техническая, сколько организационная процедура по фиксированию текущих параметров и функциональных схем взаимодействия устройств и программ в некотором журнале. Время проведения этой процедуры и дата ее окончания определяются администратором системы. После этой даты все изменения параметров должны проводиться по новым процедурам, установленным администратором системы.

Вторым шагом является организация централизованной БД, хранящей параметры устройств и программных продуктов. Обычно такие централизованные БД поддерживаются управляющими системами. Управляющая система создает схемы взаимодействия устройств (например, карты сети) и программных продуктов. Но для небольшой ИС администратор системы может использовать средства любой СУБД для организации такого хранилища данных Обычно процесс документирования конфигураций частично выполняется MS, частично вручную администратором системы.

Третьим шагом в администрировании конфигураций является выработка механизма опроса конфигураций, подтверждения их и документирования изменений. Этот механизм должен дать администратору системы уверенность в том, что изменения конфигураций прошли корректно, и о модификации параметров извещены соответствующие службы администратора системы, разработчики прикладных систем и (при необходимости) производственные структуры организации. АС должен быть уверен, что проинформированные службы обоснованно приняли (либо отвергли) эти изменения.

Четвертым шагом является реализация процесса аудита параметров относительно базовых, поскольку, вне зависимости от способа изменения параметров (автоматически или вручную) существует вероятность того, что внесены некорректные обновления или изменения параметров, не синхронизированные между собой. Процесс аудита похож на процесс документирования, но с обнаружением ситуаций и оповещением о них администратора системы (если процесс управляется, например, NMS). Аудит может производиться автоматически через регулярные интервалы времени или инициироваться администратором системы.

38.Администрирование процесса конфигурации. Задачи и проблемы конфигурации.

Под конфигурацией ИС будем понимать разработку и реализацию концепции, позволяющей администратору системы быть уверенным в непротиворечивости, целостности, проверяемости и повторяемости параметров системы.

Задачи:

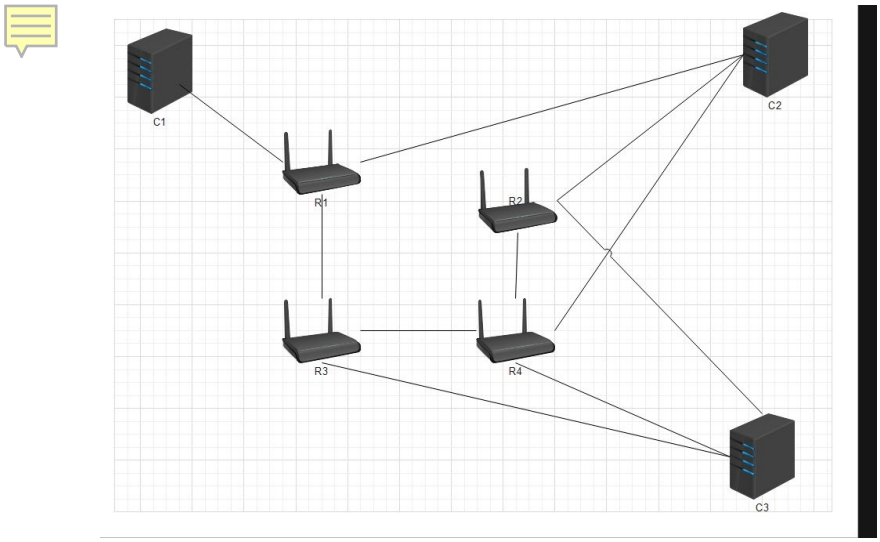
- **Стандартизация параметров**. АС должен создать стандарт на задание параметров для каждого вида коммуникационных устройств, серверов, ОС, СУБД и модулей прикладных систем. Такой стандарт должен стать стандартом организации, где функционирует ИС. При этом необ-ходимо учитывать, что стандарты данной организации не должны противоречить отраслевым стандартам.
- **Задание параметров при инициализации ресурсов**. Задание параметров работы оборудования, ОС, СУБД или ИС при установке продукта администратором системы практически определяет дальнейшую эффективность, а часто и работоспособность системы. АС в процессе первоначальной загрузки модулей ИС должен внимательно относиться к умолчаниям (default), которые рекомендовали разработчики компо-нент ИС. Умолчания следует обязательно документировать (отражать в документации базовой конфигурации) и менять только в случае необ-ходимости при понимании сути производимых компонентами ИС дей-ствий.
- **Обеспечение загрузки компонент** (provision/deprovision). Новые устройства или программные компоненты ИС должны легко загружаться или удаляться вместе с их параметрами.
- **Восстановление параметров**
- **Инвентаризация параметров и документирование функциональных схем работы компонент системы**. при ее решении проверять версии установленных компонент ИС, иметь графическое представление о взаимодействии всех аппаратных и программных компонент, производить аудит работы всех сетевых протоколов. Следует также отметить, что инвентаризация системы входит в регламентные работы администратора системы и должна выполняться регулярно по выработанному им расписанию регламентных работ.
- **Конфигурация параметров согласно политике организации**. В процессе стандартизации параметров АС должен учитывать и отражать в конфигурации корпоративные технологические стандарты, сетевые стандарты, стандарты безопасности, отраслевые стандарты. В этом случае при изменениях в этих стандартах все конфигурации различных компонент ИС меняются одинаково и одновременно по единым правилам (политике).

Практическая задача

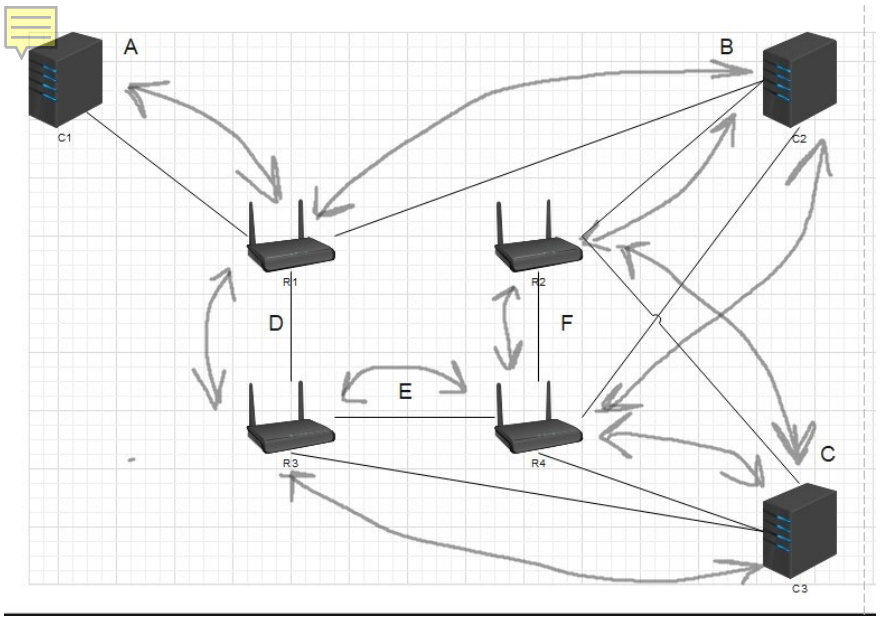
Практическое задание (пример)

1. Даны метрики сети:
   C1-C2 => 3, 1, 4
   C1-C3 => 2, 4, 3
   C2-C3 => 1, 2, 3
   Построить мнемосхему сети, которая содержит:
   клиентские узлы: C1, C2, C3.
   маршрутизаторы: R1, R2, R3, R4. На каждом из маршрутизаторов установлен файервол (Shorewall).
2. Дано исходное адресное пространство: 172.18.27.0/27.
   Разбить адресное пространство на необходимое количество подсетей согласно построенной схеме (методом пересчета маски). Для каждой из подсетей:
   а) рассчитать диапазон адресов;
   б) назначить адреса каждому из интерфейсов.
3. От C1 к C2:
   а) запретить SFTP, IMAP;
   б) разрешить MANET, LDP.
   От C1 к R3:
   а) разрешить LDAP, Kerberos.
   б) запретить RAdmin.

1. Даны метрики сети:



2. Разделение:



3. Запреты

#ACTION	SOURCE	DEST	PROTO	DPORT
Reject	C1	C2	tcp	115
Reject	C1	C2	tcp	143
Reject	C1	R3	tcp	3899 (RADMIN)
Accept	C1	C2	tcp	269
Accept	C1	C2	tcp	646
Accept	C1	R3	tcp	389
Accept	C1	R3	tcp	88