2 блок вопросов

1 Решения для индивидуальной и коллективной работы пользователей корпоративных информационных систем. Назначение решений: интегрированные средства коммуникаций, рабочие области коллективной деятельности, мгновенный доступ к информации и людям, автоматизация бизнес-процессов.

В настоящее время требования, предъявляемые к корпоративным информационным системам, сводятся не только к обеспечению эффективной индивидуальной работы пользователей, но и к возможности коллективной работы при условии доступа к нужной информации в любом месте и в любое время.

Поддержка индивидуальной и коллективной работы пользователей корпоративных информационных систем может быть реализована на базе следующих решений:

* интегрированные средства коммуникаций;
* рабочие области коллективной деятельности;
* мгновенный доступ к информации и людям;
* автоматизация бизнес-процессов.

***Интегрированные средства коммуникаций.*** Сотрудники предприятий для доступа к информации используют городские и сотовые телефоны, смартфоны, КПК, персональные компьютеры, ноутбуки и Internet-киоски. ИТ-инфраструктура предприятия должна обеспечивать взаимодействие всех перечисленных устройств.

Решения Microsoft упрощают и интегрируют разнообразные средства коммуникаций, доступные группам и индивидуальным сотрудникам. Электронная почта, мгновенный обмен сообщениями, голосовая почта, телефоны, мобильные устройства и средства проведения конференций через Internet объединяются унифицированным программным обеспечением. Функции такого ПО должны быть доступны независимо от места нахождения пользователей или типа сетевого соединения. Microsoft предоставляет интеллектуальное ПО, которое управляет коммуникациями, с учетом возможностей линий связи, в реальном масштабе времени. Данное программное обеспечение способствует созданию эффективных коммуникаций как внутри предприятия, так и с партнерами, поставщиками и клиентами.

***Рабочие области коллективной деятельности.*** Для поддержки коллективной работы Microsoft предлагает использовать службу Windows SharePoint Services, которая устанавливается в Microsoft Windows Server 2003. Данная служба предоставляет надежные и простые в использовании рабочие области для групп, легко интегрируется с Microsoft Windows Server, позволяя ИТ-службе создавать рабочие области коллективной работы. Эти области облегчают проведение совещаний, управление проектами, создание документов и др. Windows SharePoint Services можно интегрировать с корпоративными бизнес-приложениями и, следовательно, получать к ним доступ посредством привычного пользователю интерфейса.

***Мгновенный доступ к информации и людям.*** Корпоративным пользователям требуются эффективные средства поиска информации во множестве источников. Для решения данной задачи Microsoft предлагает использовать портальные технологии и управление контентом. С помощью функциональности MySites в SharePoint пользователи могут создавать свои сайты под личные задачи. Такой сайт является единой точкой доступа к документам пользователя, новостям, электронной почте и другим приложениям.

***Автоматизация бизнес-процессов.*** При автоматизации внутренних бизнес-процессов предприятия появляется необходимость исключения бумажного документооборота из информационных потоков. Решения Microsoft позволяют использовать привычные программы, такие как Microsoft Windows Server, для обращения к корпоративной информации и приложениям. При интеграции ERP-систем с программами Microsoft Windows Server сотрудники предприятия могут обращаться к бизнес-приложениям прямо из Microsoft Windows Server. Поддержка XML в Microsoft Windows Server предоставляет большие возможности по формированию индивидуальных схем информационных потоков и позволяет применять гибкие средства управления процессами на основе документов.

2 Основные элементы ИТ-инфраструктуры, позволяющие реализовать эффективную поддержку коллективной работы. Решения Microsoft Windows.

Основные элементы ИТ-инфраструктуры, которые позволяют реализовать эффективную поддержку коллективной работы следующие:

* Exchange Server 2007 – поддержка доступа к электронной почте и информации практически из любого места, с любого устройства и в любое время;
* технологии Microsoft Windows Server – доступные, простые в эксплуатации и масштабируемые средства поддержки коллективной работы (от совместной деятельности в рамках отдела до взаимодействия между предприятиями). Эти технологии включают Microsoft Windows Server Portal Server (SPPS) 2003 и Windows SharePoint Services (SPS):
  + Microsoft Windows Server Portal Server 2007 – надежный, масштабируемый, простой в использовании и управлении портал для поддержки коллективной работы, который служит связующим звеном между людьми и информацией. SPPS 2003, построенный на платформе Microsoft Windows Server, позволяет организациям интегрировать бизнес-процессы и приложения, а также полный набор средств персонализации и коллективной работы пользователей;
  + Microsoft Windows Server Services 2.0 позволяет создавать Web –сайты, через которые члены группы могут обмениваться документами и совместно работать над проектами;
* InfoPath 2007 – гибкое и эффективное средство создания динамических форм и их заполнения в рамках группы или организации, которое способствует успешному ведению бизнеса, расширяя возможности коллективной работы и улучшая процесс принятия решений. Информацию, собираемую с помощью InfoPath 2007, можно передавать в Web-сервисы и бизнес-приложения, так как InfoPath 2007 поддерживает любые пользовательские XML-схемы;
* ISA Server 2004 – межсетевой экран и прокси-сервер, который обеспечивает безопасный доступ к данным и защищает конфиденциальную информацию, хранящуюся в корпоративной сети;
* Microsoft Windows Server – средства работы с документами, тесно интегрированные со средствами совместной работы SharePoint;
* служба управления правами Windows (Windows Rights Management Services, WRMS) – обеспечивает надежную защиту и контроль доступа на уровне отдельных документов;
* Microsoft Windows Server Communications Server 2007 в сочетании с Office Communicator 2007 – мощное, масштабируемое корпоративное решение для мгновенного обмена сообщениями, проведения аудио- и видеоконференций по IP-сетям в режиме реального времени с функциональностью определения присутствия. Live Meeting – отдельный Web-сервис, не требующий для установки в организации выделенного сервера и позволяющий проводить конференции через Internet;
* платформа Windows Server 2003 со службой каталогов Active Directory – основа ИТ-инфраструктуры, обеспечивающей максимальную эффективность работы сотрудников.

3 Платформы для построения корпоративных порталов. Расписать (Microsoft, IBM, Oracle).

1. ***Microsoft Share Point*** представляет собой рабочую платформу для создания сайтов и корпоративных порталов, интегрированные функции которой предоставляют широкие возможности коммуникации между людьми.

• Share Point Online — облачная служба, размещенная в Microsoft и предназначенная для предприятий любых размеров. Вместо локальной установки и развертывания Share Point Server любая организация может просто подписаться на план Office 365 или отдельную службу Share Point Online, чтобы сотрудники могли создавать сайты для доступа к документам и данным совместно с коллегами, партнерами и клиентами.

• Share Point Server — организации могут развернуть систему Share Point Server и управлять ею локально. В ее состав входят все функции SharePoint Foundation, а также дополнительные функции и возможности, такие как управление корпоративным контентом, бизнес-аналитика, поиск в корпоративной среде, личные сайты и канал новостей.

• Share Point Foundation — технология Share Point Foundation, которая использовалась в качестве основы для всех сайтов Share Point, больше не предоставляется отдельно для выпуска Share Point 2016. Share Point Foundation (прежнее название — Windows Share Point Services) предлагается бесплатно для локального развертывания. Share Point Foundation можно использовать для создания сайтов различного типа, совместной работы над веб-страницами, документами, списками, календарями и данными. Share Point Foundation используется для перечисленных ниже операций:

— координирование расписаний;

— организация документов;

— участие в обсуждениях с помощью рабочих областей группы, блогов, вики-сайтов и библиотек документов.

• Share Point Designer 2013 — бесплатная программа (последний выпуск в 2013 г.) для создания функциональных решений с поддержкой рабочих процессов и редактирования внешних типов контента для работы с внешними данными на основе служб Business Connectivity Services.

• Синхронизация One Drive для бизнеса — программа для настольных систем, с помощью которой можно синхронизировать документы с сайта группы или из One Drive для бизнеса с компьютером для работы в автономном режиме.

***2. IBM Web Sphere Portal.*** Передовые портальные решения IBM способствуют повышению удобства работы с веб-приложениями, позволяют защитить и сохранить инвестиции в существующие системы, повышают производительность и создают возможности для дальнейшего роста компании.

• Максимальное удобство веб-интерфейса — можно воспользоваться всеми достижениями технологии Web 2.0 для реализации современных бизнес-моделей.

• Расширение бизнес-активов — позволяет создавать и внедрять собственные, ориентированные на потребности рынка решения на основе новых и существующих бизнес-активов, используя их повторно и меняя их назначение при необходимости.

• Повышение эффективности работы — программное обеспечение Web Sphere является проверенным, надежным, масштабируемым и высокопроизводительным фундаментом для корпоративных приложений, процессов и транзакций.

• Обеспечение развития компании — позволяет «подключать» рассчитанные на конкретные бизнес-потребности инструменты, которые ускорят получение отдачи от решения и позволят использовать новые коммерческие возможности рынка, одновременно снижая затраты на развертывание порталов.

• Новая версия продукта Web Sphere Portlet Factory содержит еще более простые шаблоны, использует новые возможности технологии Web 2.0 и поддерживает средства визуальной разработки настольных веб-приложений.

***3. Oracle Portal.*** Эффективно решает все три основные задачи, предоставляя корпоративным пользователям интуитивный доступ к необходимым данным и сервисам, а также позволяет бесшовно интегрировать корпоративные приложения.

Перечислим основные составляющие Oracle Portal:

• средства построения порталов на основе портальных компонентов;

• библиотеки готовых компонентов;

• средства управления содержанием с поддержкой коллективной работы;

• средства для сквозного полнотекстового поиска информации на портале, в интернете (Интранете), в базах данных и в хранилищах неструктурированной информации;

• средства интеграции внешних систем, приложений, различных видов источников данных;

• средства для анализа бизнес-информации (Business Intelligence);

• средства однократной регистрации и управления информационной безопасностью;

• средства поддержки мобильного беспроводного доступа;

• интегрированное средство разработки веб-приложений. Архитектура Oracle Web Center Portal состоит из следующих ключевых компонентов:

• Application Development Framework (ADF) — технология разработки приложений;

• Web Center Portal: Framework — функциональное развитие технологии ADF для специфичных функциональных требований портала;

• Web Center Portal: Spaces — готовый к использованию, предна- строенный инструмент создания порталов совместной работы;

• Web Center Portal: Services — набор социальных инструментов портала;

• Composer — инструмент создания и модификации страниц, структуры портала без программирования;

• Discussion Server — реализация форумов;

• Analytics — механизм сбора статистики работы пользователей с объектами портала;

• Activity Graph — инструмент визуализации активностей пользователей;

• Personalization Server — набор функций для выполнения задач кастомизации портального интерфейса как пользователем, так и ГГ-специалистами;

• Portals — механизм создания отдельных порталов для пользователей и групп пользователей, «портал в портале»;

• Composite Applications — среда исполнения и интеграции композитных приложений.

4 Определение БД. Определение СУБД. Расписать два уровня администрирования в СУБД. Функции администратора СУБД.

**Базой данных (БД)** называется электронное хранилище информации, доступ к которому имеет один или несколько компьютеров

**Система управления базами данных (СУБД)** – это набор программ, которые управляют структурой БД и контролируют доступ к данным, хранящимся в БД. СУБД служит посредником между пользователем и БД. Сама структура БД хранится в виде набора файлов, и единственный способ получить доступ к данным в этих файлах – через СУБД.

**Два уровня администрирования в 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.

Разные БД могут быть связаны с разными проектами и даже с разными организациями, поэтому у каждой БД должен быть свой администратор. Функции системного администратора относятся ко всей системе в целом, его права и привилегии распространяются на все объекты и на всех субъектов в системе. Функции администратора БД относятся не только к подмножеству системных ресурсов, выделенных конкретной БД, его права и привилегии распространяются на объекты, относящиеся к данной БД, и на субъектов, имеющих к ним доступ.

**Функции администратора:**

• инсталляция СУБД - является функцией только системного администратора;

• управление памятью - 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;

• управление разделением данных между пользователями - 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 БД - Копирование и восстановление являются необходимыми для гарантирования сохранности данных даже при полном крахе системы;

• управление безопасностью в системе - Оно состоит в регистрации пользователей в системе, выделении пользователям привилегий и бюджетов;

• передача данных между СУБД и другими системами - .Данные, хранящиеся в БД, могут потребоваться для использования в других БД, работающих в другой инсталляции, или в приложениях, не зависящих от СУБД;

• управление производительностью - включает в себя три аспекта: настройку параметров функционирования самой СУБД, отдельных БД и отдельных приложений.

5 Какие группы пользователей СУБД выделяют? Дискреционное управление доступом. Средства дискреционной защиты в СУБД. Мандатное управление доступом. Средства мандатной защиты в СУБД.

Группы пользователей:

* Пользователи
* Администратор БД
* Разработчики и администраторы приложений

**Дискреционное управление доступом** – решение, позволяющее работать с конфиденциальными данными только лицам с определенным уровнем полномочий и закрывать доступ для остальных пользователей.

В программах дискреционное управление доступом реализуется в виде матрицы. В столбцах указываются объекты, права доступа к которым регламентируются (АРМ, базы данных, программы и приложения, удаленные устройства, Интернет), а в строках – пользователи. Для каждого из них определяется список разрешенных действий для пользователей с определенным уровнем доступа с объектами:

* чтение;
* копирование и запись;
* внесение изменений;
* выполнение (для программ);
* передача прав другим пользователям.

**Мандатное управление доступом** (mandatory access control) — это разграничение доступа субъектов к объектам данных, основанное на характеризуемой меткой конфиденциальности информации, которая содержится в объектах, и на официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности.

При этом подходе с каждым зарегистрированным в системе пользователем (субъектом) и каждым защищаемым объектом системы связывается мандат, определяющий действия, которые может выполнять данный субъект над данным объектом

6 Определение транзакции. Суть механизма транзакций? Основные уровни восстановления БД.

**транзакции** – пакет запросов, который последовательно производит изменения БД и либо принимается, если все изменения записи подтверждены, либо отвергается, если хоть один запрос завершился неуспешно.

Транзакция, по сути, это механизм, который позволяет совершать различные действия над базой данных, как единый логический блок, и который переводит базу данных из одного целостного состояний в другое. Или не переводит, если транзакция была отвергнута.

**Основные уровни восстановления БД**

1. Оперативное восстановление. Характеризуется возможностью восстановления на уровне отдельного логического элемента работы при аномальном окончании управления данными (ошибка в программе, ошибка в аргументе и т.д.).

2. Промежуточное восстановление. Если возникают аномалии в системе (системно-программные ошибки, сбой аппаратного обеспечения, не связанный с разрушением базы данных), то требуется восстановить состояние всех выполняемых логических элементов работы на момент возникновения сбоя.

3. Длительное восстановление. При разрушении базы данных в результате дефекта на диске осуществляют восстановление с помощью копии базы данных. Затем воспроизводят результаты выполненных с момента снятия копии логических элементов работы и возвращают систему в состояние на момент разрушения.

7 Языковые средства разграничения доступа. Основные команды языка SQL. Концепция и реализация механизма ролей БД.

**Языковые средства разграничения доступа. Основные команды sql**

Раздаются права командой GRANT. Права можно не только дать, но и отнять. Делается это командой REVOKE, которая является копией GRANT, только с обратным действием.

Основные команды:

Команда SELECT является основой запроса. Большинство SQL-запросов начинаются с нее

Команда WHERE позволяет использовать условие, которые может быть верным или нет для каждой записи НД

Команда ORDER BY позволяет сортировать записи по определенному полю как в возрастающем, так и в убывающем порядке

Оператор IN позволяет определить набор значений

Оператор BEETWEEN работает примерно так же, как IN, но задает не список, а диапазон значений

Оператор LIKE работает только с символьными и строковыми полями

Агрегатные функции используются в запросах SQL, чтобы из группы записей сформировать одиночное значение одного поля. Имеются следующие агрегатные функции:

AVG – Функция возвращает среднее арифметическое значение из всех значений данного поля.

MIN – Функция возвращает минимальное значение указанного поля. Синтаксис аналогичен

функции AVG.

SUM – Функция возвращает максимальное значение указанного поля. Синтаксис аналогичен

функции AVG.

COUNT – Функция возвращает общее количество строк, сформированных запросом.

Команда GROUP BY позволяет группировать записи по какому-то определенному значению, и применяется совместно с агрегатными функциями

Команда DISTINCT (Отличие) предназначена для удаления избыточных (дублирующих) данных

Команда HAVING позволяет определить условия, чтобы удалить определенные группы из полученного набора данных, точно так же как команда WHERE делает это для отдельных записей.

**Концепция и реализация механизма ролей БД.**

Когда в организации работает множество пользователей, они, как правило, разбиваются на группы. Например, несколько бухгалтеров с одинаковыми правами. Чтобы не терять время на создание одинаковых прав для нескольких пользователей, для примера, в InterBase имеется механизм ролей. При пользовании этим механизмом, существует четыре последовательности действий:

1. Создать роль.

2. Присвоить этой роли необходимые права.

3. Назначить нужным пользователям эту роль.

4. При соединении с БД указать не только имя пользователя и пароль, но и его роль.

8 Преимущества СУБД InterBase. Назначение утилиты gbak, gfix, gsec в InterBase.

**Использование встроенных механизмов InterBase имеет следующие преимущества:**

InterBase позволяет осуществлять резервное копирование БД параллельно с работой других пользователей.

Во время резервного копирования InterBase считывает каждую запись из таблиц, параллельно занимаясь «сборкой мусора», поэтому в резервной копии не останется устаревших версий записей.

Оставшиеся данные переупаковываются, то есть, резервная копия не будет содержать тех «дырок», что были в базе данных. Можно сказать, что данные дефрагментируются.

Индексы пересчитываются, что приводит к оптимизации работы базы данных.

Созданная резервная копия может быть использована для миграции базы на другие серверы (InterBase новых версий, Firebird или Yaffil), а также при восстановлении позволяет исправить некоторые параметры БД, например, размер страниц.

**Для чего нужна утилита gbak?**

Как для создания резервной копии, так и для восстановления БД InterBase предлагает утилиту командной строки gbak

**Назначение утилиты gsec в InterBase**

GSEC – это утилита командной строки, обеспечивающая интерфейс к базе данных безопасности. Вы должны иметь права SYSDBA или суперпользователя (root для Unix), чтобы использовать GSEC. Данную утилиту можно использовать в интерактивном режиме или режиме командной строки.

di[splay] Показывает информацию обо всех пользователях из базы ISC4.GDB

di[splay] name Показывает информацию о пользователе name

a[dd] name -pw passwd [option argument option argument ...] Добавляет пользователя с именем name, паролем passwd и дополнительной информацией

mo[dify] name [options] Изменяет атрибуты пользователя

de[lete] name Удаляет информацию о пользователе с именем name из ISC4.GDB

h[elp] Показывает синтаксис команд GSEC

q[uit] Завершает сеанс

**Назначение утилиты gfix**

Эта утилита является одним из основных инструментов администратора БД. Утилита gfix позволяет:

 Выполнять принудительную чистку (sweep) базы данных;

 Изменять интервал автоматической чистки;

 Закрывать базу данных для получения монопольного доступа, и затем снова открывать ее;

 Переводить базу в режимы «чтение/запись» или «только чтение»;

 Переключаться между синхронным и асинхронным вводом (Forced Writes);

 Изменять диалект БД;

 Устанавливать размер кэша;

 Отыскивать повисшие транзакции и отменять или подтверждать их;

 Активировать или удалять теневые копии;

 Производить ремонт поврежденных баз данных.

9 Преимущества создания резервных копий БД встроенными средствами СУБД. Теневые копии (shadow) БД. Основные рекомендации по ремонту БД.

**Преимущества создания резервных копий БД встроенными средствами СУБД**

Использование встроенных механизмов InterBase имеет следующие преимущества:

• InterBase позволяет осуществлять резервное копирование БД параллельно с работой других пользователей.

• Во время резервного копирования InterBase считывает каждую запись из таблиц, параллельно занимаясь «сборкой мусора», поэтому в резервной копии не останется устаревших версий записей.

• Оставшиеся данные переупаковываются, то есть, резервная копия не будет содержать тех «дырок», что были в базе данных. Можно сказать, что данные дефрагментируются.

• Индексы пересчитываются, что приводит к оптимизации работы базы данных.

• Созданная резервная копия может быть использована для миграции базы на другие серверы (InterBase новых версий, Firebird или Yaffil), а также при восстановлении позволяет исправить некоторые параметры БД, например, размер страниц.

Сервер InterBase имеет механизм теневого (shadow) копирования базы данных. Такое копирование создает «зеркало» базы данных на случай какого-либо аппаратного или сетевого сбоя, или случайного удаления или повреждения базы данных операционной системой. В этом случае имеется возможность вручную или даже автоматически перейти с основной базы данных на теневую копию, и продолжить работу системы. Однако теневое копирование ни в коем случае не может заменить резервное копирование утилитой gbak, так как все ошибки и мусор, присутствующие в основной базе данных, будут присутствовать и в ее теневой копии. Shadow – файлы являются дополнительным средством безопасности данных, но никак не панацеей от всех возможных бед. Теневые копии можно создавать и в другой папке того диска, на котором находится основная база данных, однако при этом теряются все преимущества использования shadow копий. Обычно такие копии создают на другом жестком диске, физически подключенном к серверному ПК.

**Основные рекомендации по ремонту БД**

• Прежде всего, отключите от базы всех пользователей, не позволяйте им вносить изменения в БД

• Сделайте копию рабочей базы данных средствами файловой. Все попытки восстановления делайте с полученной копией, не трогая оригинал.

• Проведите полную проверку (gfix –v –full ). Если выводятся сообщения об ошибках контрольных сумм, можно добавить переключатель –i, чтобы игнорировать эти ошибки.

• Далее можно попытаться исправить разрушенные данные, помечая их как недоступные: gfix –mend –full –ignore

• После этого вновь выполните проверку на наличие разрушенных структур , как в № 3, но без –i.

• Затем попробуйте снова выполнить резервное копирование утилитой gbak, например: gbak –b –v –i

• Если это удалось, то все хорошо. Иначе попробуйте сделать еще одно резервное копирование, добавив параметр –g (не собирать мусор). Если разрушения связаны с повисшими limboтранзакциями, то –limbo.

• В большинстве случаев, такие меры позволяют сделать нормальную резервную копию. Попробуйте восстановить ее командой gbak –create –v

10 Определение каталога и службы каталогов. Назначение и функции служб каталога. Основные службы каталогов и стандарты, используемые в современных сетях.

**Каталог** представляет собой иерархическую структуру, в которой хранятся сведения об объектах в сети.

**Служба каталогов,** например доменные службы Active Directory (AD DS), предоставляет методы хранения данных каталога и предоставления этих данных сетевым пользователям и администраторам.

**Основные функции службы каталогов.**

Централизация. Смысл централизации - уменьшение количества каталогов в сети. Включение информации обо всех сетевых ресурсах в централизованный каталог создает единственную точку управления, что упрощает администрирование ресурсов и позволяет эффективнее делегировать административные задачи.

Масштабируемость. Служба каталогов должна допускать рост сети, не создавая при этом слишком больших издержек, - то есть она должна поддерживать какой-либо способ разбиения базы данных каталога на разделы, чтобы не утратить контроль над базой данных из-за ее чрезмерного разрастания и при этом сохранить преимущества централизации.

Стандартизация. Служба каталогов должна предоставлять доступ к своей информации по открытым стандартам.

Расширяемость. Служба каталогов должна тем или иным способом позволять администраторам и приложениям расширять в соответствии с потребностями организации набор информации, хранимой в каталоге.

Разделение физической сети. Благодаря службе каталогов топология физической сети должна быть прозрачной для пользователей и администраторов.

Безопасность. Служба каталогов должна поддерживать защищенные средства хранения, управления, выборки и публикации информации о сетевых ресурсах.

**Основные службы каталогов и стандарты, используемые в современных сетях.**

Active Directory (AD) - служба каталогов, поставляемая с Microsoft Windows, начиная с Windows 2000 Server. Active Directory содержит каталог, в котором хранится информация о сетевых ресурсах и службы, предоставляющие доступ к этой информации.

Х.500 и Directory Access Protocol (DAP). X.500 - спецификация International Organization for Standardization (ISO), определяющая, как должны быть структурированы глобальные каталоги. Х.500 также описывает применение DAP для обеспечения взаимодействия между клиентами и серверами каталогов;

Lightweight Directory Access Protocol (LDAP). Протокол LDAP был разработан в ответ на критические замечания по спецификации DAP, которая оказалась слишком сложной для применения в большинстве случаев.

Novell Directory Services (NDS). Служба каталогов для сетей Novell NetWare, совместимая со стандартом Х.500;

Windows NT и SAM. Ядром Windows NT NOS (Network Operating System - сетевая операционная система) является база данных SAM (Security Accounts Management - управление безопасными учетными записями). Она представляет центральную базу данных учетных записей, включающую все учетные записи пользователей и групп в домене. Эти учетные записи используются для управления доступом к совместным ресурсам, принадлежащим любому серверу в домене Windows NT.

11 Ключевые преимущества Active Directory. Область действия, пространство имен ActiveDirectory. Объект. Контейнер. Дерево.

**Ключевые преимущества Active Directory**

**Единая точка аутентификации.** Все учетные записи хранятся в общей базе данных, к которой при авторизации обращаются все ПК, включенные в сеть. Каждый пользователь домена включается в определенную группу. Последняя имеет свой уровень доступа к документам, приложениям, хранилищу данных и т. п. в зависимости от выполняемых ею обязанностей. Новый сотрудник, принятый на работу в компанию, получает учетную запись в соответствующей группе пользователей и тот же уровень доступа. При увольнении работника его исключают из списка и блокируют возможность доступа.

**Единая точка управления.** Каталог Active Directory позволяет распределить всех пользователей и ПК согласно имеющейся иерархии отделов и филиалов. К каждому из них применяются общие групповые политики. Они заключаются в одних и тех же настройках доступа и безопасности для каждого отдела. При добавлении нового ПК или пользователя его относят в одну из групп. При этом дополнительных настроек не требуется, они применяются автоматически. Групповые политики AD позволяют назначать сетевые принтеры, настраивать офисные приложения, устанавливать уровень безопасности браузера и т. п.

**Высокий уровень защиты данных.** Службы AD помогают значительно повысить безопасность хранения информации. Высокий уровень защищенности обеспечивается двумя направлениями:

* единым хранилищем учетных записей, которые располагаются на выделенных серверах домена;
* использованием для аутентификации в доменной среде протокола Kerberos, более безопасного, чем NTLM в рабочих группах.

**Высокие возможности интеграции**. Все службы Active Directory соответствуют стандарту LDAP – «легко расширяемому протоколу доступа к каталогам». Он позволяет осуществлять аутентификацию, поиск, сравнение, а также работу с учетными записями. LDAP поддерживается, например почтовыми и прокси-серверами, а также другими приложениями, не обязательно продуктами Microsoft®. К преимуществам такой интеграции относятся единые логин и пароль для всех приложений, с которыми работает пользователь. Это дает возможность подключаться и аутентифицироваться по корпоративным точкам доступа по Wi-Fi или внешнему VPN.

**Область действия, пространство имен Active Directory.**

Область действия (scope) Active Directory достаточно обширна. Она может включать отдельные сетевые объекты (принтеры, файлы, имена пользователей), серверы и домены в отдельной глобальной сети. Она может также охватывать несколько объединенных сетей. Active Directory может быть настроена на управление как отдельным компьютером, так и компьютерной сетью или группой сетей.

Пространство имен – это такая ограниченная область, в которой может быть распознано данное имя. Распознавание имени заключается в его сопоставлении с некоторым объектом или объемом информации, которому это имя соответствует. Active Directory образует пространство имен, в котором имя объекта в каталоге может быть поставлено в соответствие самому этому объекту.

**Объект. Контейнер. Дерево.**

**Объект** представляет собой уникальную сущность внутри Каталога и обычно обладает многими атрибутами, которые помогают описывать и распознавать его.

**Контейнер** – объект, содержащий другие объекты.

**Дерево** содержит один или несколько доменов, также связанных в иерархию транзитивными отношениями доверия.

12 Домен. Доменное дерево. Лес. Организационные единицы. Сайт, узел.

**Домен** формирует область административной ответственности. База данных домена содержит учетные записи пользователей, групп и компьютеров. Большая часть функций по управлению службой каталогов работает на уровне домена (аутентификация пользователей, управление доступом к ресурсам, управление службами, управление репликацией, политики безопасности).

**Дерево** является набором доменов, которые используют единое связанное пространство имен. В этом случае "дочерний" домен наследует свое имя от "родительского" домена. Дочерний домен автоматически устанавливает двухсторонние транзитивные доверительные отношения с родительским доменом. Доверительные отношения означают, что ресурсы одного из доменов могут быть доступны пользователям других доменов.

**Лес** объединяет деревья, которые поддерживают единую схему. В лесу между всеми доменами установлены двухсторонние транзитивные доверительные отношения, что позволяет пользователям любого домена получать доступ к ресурсам всех остальных доменов, если они имеют соответствующие разрешения на доступ. По умолчанию, первый домен, создаваемый в лесу, считается его корневым доменом, в корневом домене хранится схема AD.

**Организационные единицы OU** – это объекты в Active Directory, которые могут определяться пользователем и к которым может применяться групповая политика.

**Сайт** представляет область сети, где все контроллеры домена связаны быстрым, недорогим и надежным сетевым подключением.

**Узлом** (сайтом) называется такой элемент сети, который содержит серверы Active Directory. Узел обычно определяется как одна или несколько подсетей, поддерживающих протокол TCP/IP и характеризующихся хорошим качеством связи, которое подразумевает высокую надежность и скорость передачи данных.

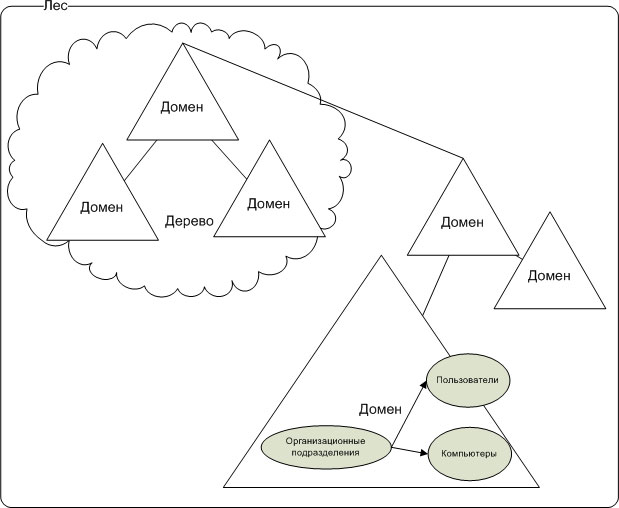
13 Функциональная структура Active Directory. Физическая структура Active Directory. Логическая структура Active Directory.

**Функциональная структура AD. Многоуровневая архитектура AD.**

Функциональную структуру Active Directory можно представить в виде многоуровневой архитектуры, в которой уровни являются процессами, предоставляющими клиентским приложениям доступ к службе каталога. Active Directory состоит из трех уровней служб и нескольких интерфейсов и протоколов, совместно работающих для предоставления доступа к службе каталога. Три уровня служб охватывают различные типы информации, необходимой для поиска записей в базе данных (БД) каталога. Выше уровней служб в этой архитектуре находятся протоколы и API интерфейсы, осуществляющие связь между клиентами и службой каталога.



**Логическая структура Active Directory** является моделью службы каталога, которая определяет каждого участника безопасности на предприятии, а также организацию этих участников.



**Физическое проявление службы Active Directory** состоит в наличии отдельного файла данных, расположенного на каждом контроллере домена. Физическая реализация службы Active Directory описывается местоположением контроллеров домена, на которых расположена служба. При реализации службы Active Directory можно добавлять столько контроллеров доменов, сколько необходимо для поддержания служб каталога в данной организации.

14 Какие сведения собираются на этапе предпроектного исследования для проектирования службы каталогов. Типовой план проектирования структуры ActiveDirectory. Какие объекты содержит БД ActiveDirectory.

**Какие сведения собираются на этапе предпроектного исследования для проектирования службы каталогов**

1. На данном этапе предпроектного исследования собираются основные сведения по существующей инфраструктуре в компании.
2. Для планирования структуры Active Directory - информация о доменной структуре и ее типе, структуре групп пользователей и распределении их по доменам, количестве существующих контроллеров доменов внутри каждого домена. Определение существующих доверительных отношений между доменами, односторонних и двухсторонних доверительных отношений и доменов, которые не должны включаться в леса Active Directory, пространства имен DNS, существующих в организации, и перечня существующих доменных имен организации, зарегистрированных в сети Интернет.
3. Для планирования сайтов Active Directory - информация о существующей структуре сайтов, о топологии сети, о каналах связи и их пропускной способности.
4. Для планирования переноса текущей структуры сетевых сервисов на платформу Active Directory - информация о топологии используемых сетевых сервисов DHCP, WINS, DNS.
5. Для обеспечения возможности резервного восстановления данных во время миграции - схема резервного копирования информации.
6. Для определения возможной расширяемости решения - исследование возможных вариантов изменения схемы при росте организации или ее реорганизации, определение области Active Directory (исследование подразделений, включая удаленные филиалы организации, необходимых для включения в Active Directory).
7. Для планирования миграции приложений, использующих Active Directory - список приложений, связанных с Active Directory, и возможных ограничений, накладываемых ими на структуру Active Directory, определение механизмов идентификации пользователей.

**Типовой план проектирования структуры Active Directory.**

Проектирование структуры Active Directory начинается с компонентов высшего уровня, а затем проектируются компоненты низших уровней. Это означает, что первый шаг состоит в создании проекта леса, затем следует проект доменов, проект DNS и, наконец, проект организационной единицы (OU)

Планирование структуры лесов

Планирование доменов для каждого леса

Планирование использования сайтов для каждого леса

Планирование структуры организационных единиц для каждого домена

Планирование реорганизации существующих доменов и их перевод на новую платформу Active Directory

Тестирование внедряемых решений и установка стенда

**Какие объекты содержит БД AD**

1. Разделы (сегменты). Разделы Active Directory называются контекстами именования (NC - Naming Contexts) и содержат следующие сегменты: раздел домена каталога, раздел конфигурации каталога, раздел схемы каталога, раздел глобального каталога, разделы приложений каталога.
2. Домены. Домен служит в качестве административной границы, он определяет и границу политик безопасности. Каждый домен имеет, по крайней мере, один контроллер домена (оптимально иметь два или более). Домены Active Directory организованы в иерархическом порядке. Первый домен на предприятии становится корневым доменом леса, обычно он называется корневым доменом или доменом леса.
3. Деревья доменов. Домены, которые создаются в инфраструктуре Active Directory после создания корневого домена, могут использовать существующее пространство имен Active Directory совместно или иметь отдельное пространство имен. Чтобы выделить отдельное пространство имен для нового домена, нужно создать новое дерево домена.
4. Леса. Лес определяет границу безопасности для предприятия, являясь общим для всех контроллеров домена в лесу. Все домены и доменные деревья существуют в пределах одного или несколько лесов Active Directory.
5. Сайты. Сайт представляет область сети, где все контроллеры домена связаны быстрым, недорогим и надежным сетевым подключением. Независимость логических компонентов от сетевой инфраструктуры возникает вследствие использования сайтов в Active Directory: они обеспечивают соединение между логическими компонентами Active Directory и физической сетевой инфраструктурой.
6. Организационные единицы. Организационные единицы предназначены для того, чтобы облегчить управление службой Active Directory. Они служат для создания иерархической структуры в пределах домена и используются, чтобы сделать более эффективным управление единственным доменом (вместо управления несколькими доменами Active Directory).

15 Доверительные отношения между доменами. Типы доверительных отношений. Контроллеры доменов, функции контроллера домена, их роли.

**Домен. Доверительные отношения. Типы доверительных отношений.**

Домен — это единая область, в пределах которой обеспечивается безопасность данных в компьютерной сети под управлением ОС Windows

Поскольку домены разграничивают зоны безопасности, специальный механизм, называемый доверительными отношениями (trust relationships), позволяет объектам в одном домене [доверяемом (trusted domain)] обращаться к ресурсам в другом [доверяющем (trusting domain)].

**Типы доверительных отношений:**

Доверие к родительскому и дочернему доменам

Доверие к корневому домену дерева

Доверие к внешнему домену

Доверие к сокращению

Доверие к сфере

Доверие к лесу

**Контроллеры доменов и их роли**

Контроллер домена — это компьютер-сервер, управляющий доменом и хранящий реплику каталога домена (локальную БД домена). Поскольку в домене может быть несколько контроллеров домена, все они хранят полную копию той части каталога, которая относится к их домену.

Каждый контроллер домена хранит полную копию всей информации Active Directory, относящейся к его домену, а также управляет изменениями этой информации и реплицирует их на остальные контроллеры того же домена.

Все контроллеры в домене автоматически реплицируют между собой все объекты в домене. Какие-либо изменения, вносимые в Active Directory, на самом деле производятся на одном из контроллеров домена. Затем этот контроллер домена реплицирует изменения на остальные контроллеры в пределах своего домена. Задавая частоту репликации и количество данных, которое Windows будет передавать при каждой репликации, можно регулировать сетевой трафик между контроллерами домена.

Важные обновления, например отключение учетной записи пользователя, контроллеры домена реплицируют немедленно.

Active Directory использует репликацию с несколькими хозяевами (multimaster replication), в котором ни один из контроллеров домена не является главным. Все контроллеры равноправны, и каждый из них содержит копию базы данных каталога, в которую разрешается вносить изменения. В короткие периоды времени информация в этих копиях может отличаться до тех пор, пока все контроллеры не синхронизируются друг с другом.

Наличие в домене нескольких контроллеров обеспечивает отказоустойчивость. Если один из контроллеров домена недоступен, другой будет выполнять все необходимые операции, например записывать изменения в Active Directory.

Контроллеры домена управляют взаимодействием пользователей и домена, например находят объекты Active Directory и распознают попытки входа в сеть.

Хозяин схемы (Schema Master). Первый контроллер домена в лесу принимает роль хозяина схемы и отвечает за поддержку и распространение схемы на остальную часть леса. Он поддерживает список всех возможных классов объектов и атрибутов, определяющих объекты, которые находятся в Active Directory. Если схему нужно обновлять или изменять, наличие Schema Master обязательно.

Хозяин именования доменов (Domain Naming Master). Протоколирует добавление и удаление доменов в лесу и жизненно необходим для поддержания целостности доменов. Domain Naming Master запрашивается при добавлении к лесу новых доменов. Если Domain Naming Master недоступен, то добавление новых доменов невозможно; однако при необходимости эта роль может быть передана другому контроллеру.

Хозяин RID (Relative Identifier (RID) Master). Отвечает за выделение диапазонов относительных идентификаторов (RID) всем контроллерам в домене. SID в Windows Server 2003 состоит из двух частей. Первая часть - общая для всех объектов в домене; для создания уникального SID к этой части добавляется уникальный RID. Вместе они уникально идентифицируют объект и указывают, где он был создан.

Эмулятор основного контроллера домена (Primary Domain Controller (PDC) Emulator). Отвечает за эмуляцию Windows NT 4.0 PDC для клиентских машин, которые еще не переведены на Windows 2000, Windows Server 2003 или Windows XP и на которых не установлен клиент службы каталогов. Одна из основных задач эмулятора PDC - регистрировать устаревшие клиенты. Кроме того, к эмулятору PDC происходит обращение, если аутентификация клиента оказалась неудачной. Это дает возможность эмулятору PDC проверять недавно измененные пароли для устаревших клиентов в домене, прежде чем отклонять запрос на вход.

Хозяин инфраструктуры (Infrastructure Master). Регистрирует изменения, вносимые в контролируемые объекты в домене. Обо всех изменениях сначала сообщается Infrastructure Master, и лишь потом они реплицируются на другие контроллеры домена. Infrastructure Master обрабатывает информацию о группах и членстве в них для всех объектов в домене. Еще одна задача Infrastructure Master - передавать информацию об изменениях, внесенных в объекты, в другие домены.

**функции контроллеров доменов:**

Каждый контроллер домена хранит полную копию всей информации Active Directory, относящейся к его домену, а также управляет изменениями этой информации и реплицирует их на остальные контроллеры того же домена.

Все контроллеры в домене автоматически реплицируют между собой все объекты в домене.

Важные обновления, например отключение учетной записи пользователя, контроллеры домена реплицируют немедленно.

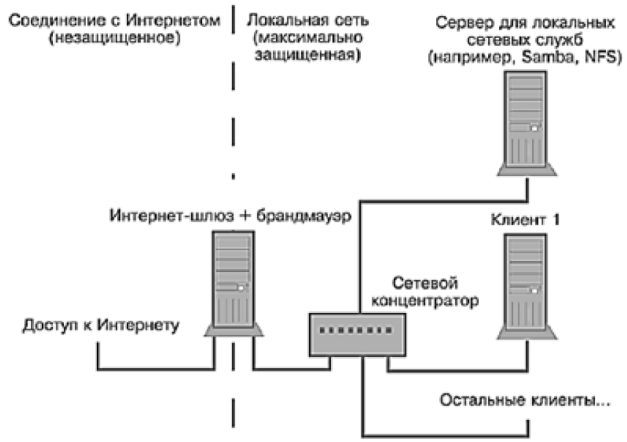
Active Directory использует репликацию с несколькими хозяевами (multimaster replication), в котором ни один из контроллеров домена не является главным.

Наличие в домене нескольких контроллеров обеспечивает отказоустойчивость.

Контроллеры домена управляют взаимодействием пользователей и домена, например находят объекты Active Directory и распознают попытки входа в сеть.

16 Брандмауэры. Определение, общая информация, схема работы, Demilitarized Zone.

Под брандмауэром будем понимать совокупность методов, повышающих надежность обмена информацией, проходящей по TCP/IP через фильтр пакетов. Такой фильтр анализирует все сетевые пакеты, приходящие на компьютер, а также пакеты, которые уходят с компьютера в сеть. В зависимости оттого, все ли правила соблюдаются, пакеты могут быть пропущены или заблокированы.



Demilitarized Zone – сегмент сети, содержащий общедоступные сервисы и отделяющий их от частных. В качестве общедоступного может выступать, например, веб-сервис: обеспечивающий его сервер, который физически размещён в локальной сети (Интранет), должен отвечать на любые запросы из внешней сети (Интернет), при этом другие локальные ресурсы (например, файловые серверы, рабочие станции) необходимо изолировать от внешнего доступа.

Цель ДМЗ – добавить дополнительный уровень безопасности в локальной сети, позволяющий минимизировать ущерб в случае атаки на один из общедоступных сервисов: внешний злоумышленник имеет прямой доступ только к оборудованию в ДМЗ.

17 Методы виртуализации операционных системы. Характеристика метода, примеры фирм и программ.

Виртуализация — это общий термин, охватывающий абстракцию ресурсов для многих аспектов вычислений. Некоторые наиболее характерные примеры виртуализации приведены ниже.

***Паравиртуализация***

Паравиртуализация — техника виртуализации, при которой гостевые операционные системы подготавливаются для исполнения в виртуализированной среде, для чего их ядро незначительно модифицируется. Операционная система взаимодействует с программой гипервизора, который предоставляет ей гостевой API, вместо использования напрямую таких ресурсов, как таблица страниц памяти. Код, касающийся виртуализации, локализуется непосредственно в операционную систему. Паравиртуализация требует, чтобы гостевая операционная система была изменена для гипервизора, и это является недостатком этого метода, так как подобное изменение возможно лишь в случае, если гостевые ОС имеют открытые исходные коды, которые можно модифицировать согласно лицензии. �В то же время паравиртуализация предлагает производительность почти как у реальной невиртуализированной системы, а также возможность одновременной поддержки различных операционных систем, как и при полной виртуализации.

***Виртуализация инфраструктуры***

В данном случае, будем понимать под этим термином создание ИТ-инфраструктуры, не зависимой от аппаратной части. Например, когда нужный нам сервис находится на гостевой виртуальной машине и нам в принципе не особо важно, на каком физическом сервере он располагается.

Виртуализация серверов, десктопов, приложений – существует множество методов для создания подобной независимой инфраструктуры. В этом случае на одном физическом или хост-сервере посредством специального ПО, именуемого "гипервизор", размещается несколько виртуальных или "гостевых" машин.

Современные системы виртуализации, в частности, VMware и Citrix XenServer в большинстве своем работают по принципу bare metal, то есть ставятся прямо на "голое железо".

Виртуальная система, построена не на bare metal гипервизоре, а на сочетании операционной системы Linux CentOS 5.2 и VMware Server на базе серверной платформы Intel SR1500PAL, 2 процессора Intel Xeon 3.2/1/800, 4Gb RAM, 2xHDD 36Gb RAID1 и 4xHDD 146Gb в RAID10 общим объемом 292Gb. На хост-машине размещены четыре виртуальные машины:

* почтовый сервер Postfix на базе операционной системы FreeBSD (Unix). Для доставки почты конечному пользователю использовался протокол POP3.
* прокси-сервер Squid на базе все той же системы FreeBSD.
* выделенный контроллер домена, DNS, DHCP на базе Windows 2003 Server Standard Edition.
* управляющая рабочая станция на базе Windows XP для служебных целей.

***Виртуализация серверов***

Виртуальная машина — это окружение, которое представляется для «гостевой» операционной системы, как аппаратное. Однако на самом деле это программное окружение, которое симулируется программным обеспечением хостовой системы. Эта симуляция должна быть достаточно надёжной, чтобы драйверы гостевой системы могли стабильно работать. При использовании паравиртуализации, виртуальная машина не симулирует аппаратное обеспечение, а, вместо этого, предлагает использовать специальное Application Programming Interface (API).

Bochs

FAUmachine

KVM

Parallels (Параллелз Софтвер)

Qemu

SVISTA

twoOStwo

VirtualBox

Virtual Iron

Microsoft Virtual PC

Microsoft Virtual Server

VMware (VMware ESX Server)

Xen

Аналитики Gartner отмечают: «Виртуализация х86 серверной инфраструктуры выступает отправной точкой для двух важнейших современных отраслевых тенденций – модернизации инфраструктуры и облачных вычислений». Более того, «она коренным образом меняет подход предприятий к развертыванию, управлению и предоставлению IT». Исследователи убеждены, что «виртуализация х86 серверной инфраструктуры является сейчас ключевым направлением развития информационных технологий, делая стратегическое развитие серверной виртуализации в сторону облачных вычислений более очевидным для IT-директоров крупных предприятий».

***Виртуализация уровня ОС***

Виртуализация на уровне операционной системы — виртуализирует физический сервер на уровне ОС, позволяя запускать изолированные и безопасные виртуальные серверы на одном физическом сервере.

Solaris Containers/Zones

FreeBSD Jail

Linux-VServer

FreeVPS

OpenVZ

Virtuozzo (Parallels) Виртуоззо Рисерч

VDSmanager

***Виртуализация ресурсов***

Разделение ресурсов (partitioning) — это разделение единого, обычно достаточно большого для этого, ресурса (например дисковое пространство или пропускной канал сети) на некоторое количество меньших, легче используемых ресурсов того же типа.

Например, к реализации разделения ресурсов можно отнести Проект Crossbow, позволяющий создавать несколько виртуальных сетевых интерфейсов на основе одного физического.

Агрегация, распределение или добавление множества ресурсов в большие ресурсы или объединение ресурсов. Например, симметричные мультипроцессорные системы объединяют множество процессоров; RAID и дисковые менеджеры объединяют множество дисков в один большой логический диск; RAID и сетевое оборудование использует множество каналов, объединённых так, чтобы они представлялись, как единый широкополосный канал. На мета-уровне компьютерные кластеры делают все вышеперечисленное. Иногда сюда же относят сетевые файловые системы абстрагированные от хранилищ данных на которых они построены, например, Vmware VMFS, Solaris ZFS, NetApp WAFL

***Виртуализация приложений***

Виртуализация прикладных приложений — включает в себя рабочую среду для локально выполняемого приложения, использующего локальные ресурсы. Виртуализируемое приложение запускается в небольшом виртуальном окружении, которое включает в себя ключи реестра, файлы и другие компоненты, необходимые для запуска и работы приложения. Такая виртуальная среда работает как прослойка между приложением и операционной системой, что позволяет избежать конфликтов между приложениями. К виртуализации прикладных приложений можно отнести такие системы как Softgrid и Thinstall.

18 Модель управления для администрирования сетевых систем FCAPS.

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

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

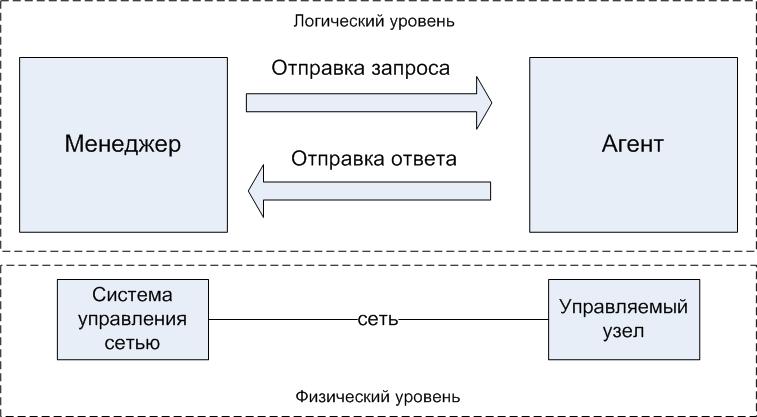
(A) Accounting Management (управление учетом) - возможность сбора и передачи учетной информации для генерации отчетов об использовании сетевых ресурсов.

(Р) 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.

19 Системы управления MS (Management System), NMS (Network Management System). Схема работы NMS.

Системы управления сетью - Network Management System (NMS) являются системами, реализующими уровень NML модели TMN. Физически NMS представляет собой комбинацию программного обеспечения с аппаратной частью, на которой это программное обеспечение имеет серверную часть.



20 Базовая модель поиска ошибок при администрировании ИС.

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. Например, некая операция действительно занимает много времени, а пользователь считает, что ИС медленно работает.
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 программныхпродуктов, 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.

21 Стратегии определения ошибок при администрировании ИС. Два подхода к поиску неисправностей. Типы стратегий. Технологии работы NMS.

***Существуют два подхода к поиску неисправностей - теоретический и практический.***

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.

При ***практическом*** подходе 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. Это вовсе не означает, что все компоненты системы функционируют должным образом, главное, что они вообще функционируют. К сожалению, во многих руководствах по эксплуатации в разделе поиска неисправностей фактически рекомендуется прибегнуть к стилю специалиста-практика, вместо предоставления подробной инструкции по устранению технических неисправностей. Этот подход быстрее предыдущего. Однако он очень ненадежен и первопричина неработоспособности системы может быть так и не устранена.

Стратегия управления ошибками может быть ***проактивной*** либо ***реактивной***. 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. Такая стратегия предупреждения ошибок называется ***проактивной***. Стратегия, при которой АС не предупреждает появление ошибок, а разбирается с ошибками по мере их возникновения, называется ***реактивной***. АС должен приложить усилия и воспользоваться средствами MS или NMS для перехода от реактивной стратегии к проактивной.

***При этом возможны две технологии работы NMS - пассивная и активная.***

***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.

***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.