Задание

1. Изучить материал лекции, законспектировать.

2. Фотоотчет прислать на электронную почту

С уважением, Хвастова Светлана Ивановна

!!! Если возникнут вопросы обращаться по телефону 0721389311. Электронная почта: xvsviv@rambler.ru

Лекция на тему:

«Понятия администрирование, привилегия, доступ. Виды пользователей и группы привилегий, соответствующие виду пользователя. Возможности операционной системы для администрирования. Принцип и архитектура администрируемой базы данных»

План

1 Основные понятия и определения

В начале 1980-х годов персональные компьютеры стали объединять в сети для обмена данными и совместного использования файлов и ресурсов. К середине 1980-х годов эти сети становятся крупными и сложными. Для управления ими создаются отделы информационного обеспечения.

Управление сетью (Network management) – целенаправленное воздействие на сеть, осуществляемое для организации её функционирования по заданной программе. Оно включает следующие процедуры:

1. включение и отключение системы, каналов передачи данных, терминалов;

2. диагностика неисправностей;

3. сбор статистики;

4. подготовка отчётов и т.п.

С точки зрения модели OSI управление сетью подразделяется на управление:

1. конфигурацией;

2. отказами;

3. безопасностью;

4. трафиком;

5. учётом.

Традиционные методы управления основаны на использовании правил. Они предписывают системе управления в компьютерной сети предпринимать определённые действия (например, выдать предупреждающее сообщение на управляющую консоль) при наступлении определённых событий (превышение интенсивностью трафика заранее определённого порогового значения и др.).

Приемлемая в небольших сетях, методология управления на основе правил сталкивается с множеством препятствий в крупных сетях: сетях вычислительных центров и корпоративных информационных сетях (ИС). Основная трудность обусловлена тем, что функционирование мощной вычислительной среды может описываться многими тысячами параметров.

Корпоративная сеть (сеть масштаба предприятия, Enterprise network) – сеть смешанной топологии, в которую входят несколько локальных вычислительных сетей. Корпоративная сеть объединяет филиалы корпорации и является собственностью предприятия.

Сеть вычислительных центров – совокупность взаимодействующих вычислительных центров (узлов), объединённых каналами связи для наиболее полного обеспечения потребности пользователей (абонентов) в выполнении информационно-вычислительных работ.

Пользователь/Посетитель (User; Visitor):

1) абонент (клиент) сетевого ресурса;

2) посетитель сервера (сайта, портала) и пользователь доступного ему информационного ресурса в сети.

Сервер (Server) – компьютер, подключенный к сети, или выполняющаяся на нём программа, предоставляющие клиентам доступ к общим ресурсам и управляющие этими ресурсами.

Система управления сетью (Network management system) – аппаратные и (или) программные средства, применяемые для мониторинга и управления узлами сети. Программное обеспечение системы управления сетью состоит из агентов, локализующихся на сетевых устройствах и передающих информацию сетевой управляющей платформе.

Платформа управления сетью (Network management platform) – комплекс программ, предназначенных для управления сетью и входящими в неё системами. Для работы с платформой администратору предоставляется одна или несколько абонентских систем (консолей). Обычно платформа создаётся на базе протокола SNMP. Платформа обеспечивает:

1. контроль работы устройств и состояния кабелей;
2. контроль деловых процедур;
3. контроль других аспектов функционирования сети.

Чтобы компьютерная сеть могла эффективно выполнять свои функции, необходимо централизованно контролировать состояние основных её элементов, выявлять и разрешать возникающие проблемы, выполнять анализ производительности и планировать развитие сети и др. Эти виды работ являются основными задачами администрирования сетей.

Администрирование – процедуры управления, регламентирующие некоторые процессы или их часть. Как правило, оно фиксирует и руководит процессами и ситуациями, нуждающимися в ограничениях или целевом управлении.

Построение компьютерных сетей вызвало необходимость управления (администрирования) ими и созданными на их основе компьютерными

вычислительными и информационными системами. В результате появилось системное администрирование.

Основной целью системного администрирования является приведение сети в соответствие с целями и задачами, для которых она предназначена. Достигается эта цель путём управления сетью, позволяющего минимизировать затраты времени и ресурсов, направляемых на управление системой, и в тоже время максимизировать доступность, производительность и продуктивность системы.

История системного администрирования насчитывает несколько десятилетий. Задачи управления вычислительными комплексами (системами) возникли сразу после появления самих этих комплексов. Доминировавшая до конца 1980-х годов централизованная вычислительная модель типа “мэйнфрейм–терминалы” непосредственно проецировалась на архитектуру средств администрирования, которую относят к категории системного. Такое решение означало существование единого образа вычислительной среды. В подобных средствах администрирования задачи управления сводились к контролю за функционированием отдельных компонентов, причём во многих случаях он заключался просто в сборе данных о ресурсах вместо действительного управления их работой. Такой тип управления нельзя отнести к сетевому администрированию в строгом смысле этого слова.

В начале 1990-х годов широкое распространение распределённых архитектур “клиент-сервер” вызвало перемены в управлении информационными системами, сменившими безраздельное господство хост-компьютеров. Вместо однородной среды администраторам пришлось иметь дело с многообразием ресурсов, включая компьютерные и программные платформы, а также сетевое оборудование. Такое положение потребовало решения новых административных задач: учёта распределённых ресурсов, электронного распространения ПО и контроля лицензий, анализа трафика и управления пропускной способностью сети, перераспределения серверной нагрузки, отслеживания состояния отдельных настольных систем и другое,

отсутствовавших в классической централизованной модели. В эту среду не переносились приложения администрирования, функционировавшие на мэйнфреймах, и производителям пришлось создавать новое управляющее ПО. Всё это способствовало появлению сетевого администрирования.

Сетевое администрирование (Network Management) возникает, когда у администратора сети появляется потребность и возможность оперировать единым представлением сети, как правило, это относится к сетям со сложной архитектурой. При этом осуществляется переход от управления функционированием отдельных устройств к анализу трафика в отдельных участках сети, управлению её логической конфигурацией и конкретными рабочими параметрами, причём все эти операции целесообразно выполнять с одной управляющей консоли. Задачи, решаемые в данной области, разбиваются на две группы:

1. Контроль за работой сетевого оборудования,
2. Управление функционированием сети в целом.

Конечной целью управления сетью является достижение параметров функционирования ИС, соответствующих потребностям пользователей. Пользователи оценивают работу ИС не по характеристикам сетевого трафика, применяемым протоколам, времени отклика серверов на запросы определённого типа и особенностям выполняемых сценариев управления, а по поведению приложений, ежедневно запускаемых на их настольных компьютерах.

Общая тенденция в мире сетевого и системного администрирования – перенос акцентов с контроля за отдельными ресурсами или их группами, с управления рабочими характеристиками ИС на максимальное удовлетворение запросов конечных потребителей информационных технологий способствовала появлению концепции динамического администрирования.

Такой подход предполагает, прежде всего, наличие средств анализа поведения пользователей, в ходе которого выявляют их предпочтения и проблемы, возникающие в повседневной работе. Результаты, полученные на

этом этапе, должны послужить отправной точкой для активного управления взаимодействием между основными объектами администрирования – пользователями, приложениями и сетью. Эти факторы дают основание полагать, что на смену сетевому и системному администрированию придёт управление приложениями и качеством сервиса, независящее от используемых вычислительных платформ или сетей.

Эволюция концепций администрирования коснулась не только архитектуры систем. Новые проблемы, возникшие в распределённых средах, привели к тому, что на некоторое время сетевое управление стали рассматривать как главную заботу администраторов ИС. Ситуация изменилась когда число распределённых приложений и баз данных, функционирующих в сети, превысило пороговое значение. При этом возросла роль системного администрирования, и неизбежным оказался процесс интеграции системного и сетевого администрирования.

Интегрированная система управления сетью (Integrated network management system, INMS) – система управления, обеспечивающая объединение функций, связанных с анализом, диагностикой и управлением сетью.

Таким образом, эволюция средств и систем администрирования непосредственно связана с развитием основных информационных технологий.

Проекты развития административных механизмов обычно включают в себя задачи постановки стратегического управления, разработки политики информационного обеспечения и доступа к информационным ресурсам, а также программно-аппаратным устройствам, системам и комплексам, постановки и развития системы, совершенствование непрерывного управления.

Трудно говорить о том, по какому пути – интеграционному или дезинтеграционному – пойдёт развитие сетей. Ряд экспертов предполагает, что на смену сетевому и системному администрированию придёт управление приложениями и качеством сервиса, безотносительно к используемым

вычислительным платформам или сетям. В любом случае управление сетями осуществляют сетевые администраторы (администраторы сетей).

Администратор сети – специалист, отвечающий за нормальное функционирование и использование ресурсов автоматизированной системы и (или) вычислительной сети.

Администрирование информационных систем включает следующие цели:

1. Установка и настройка сети.
2. Поддержка её дальнейшей работоспособности.
3. Установка базового программного обеспечения.
4. Мониторинг сети.

В связи с этим администратор сети должен выполнять следующие задачи:

1. Планирование системы.
2. Установка и конфигурация аппаратных устройств.
3. Установка программного обеспечения.
4. Установка сети.
5. Архивирование (резервное копирование) информации.
6. Создание и управление пользователями.
7. Установка и контроль защиты.
8. Мониторинг производительности.

Обеспечение работоспособности системы требует и осуществления профилактических мероприятий. Администратор должен обеспечивать удовлетворение санкционированных запросов пользователей.

Очевидно, что эффективно выполнять все эти функции и задачи, особенно в сложных крупных компьютерных сетях, человеку весьма затруднительно, а порой и невозможно. Успешное администрирование, особенно сложными компьютерными сетями, реализуется путём применения новейших средств и систем автоматизации этих процессов.

2 Виды пользователей и группы привилегий

Пользователей СУБД можно разбить на три категории:

1. администратор сервера баз данных. Он ведает установкой, конфигурированием сервера, регистрацией пользователей, групп, ролей и т.п. Администратор сервера имеет имя ingres. Прямо или косвенно он обладает всеми привилегиями, которые имеют или могут иметь другие пользователи.

2. администраторы базы данных. К этой категории относится любой пользователь, создавший базу данных, и, следовательно, являющийся ее владельцем. Он может предоставлять другим пользователям доступ к базе и к содержащимся в ней объектам. Администратор базы отвечает за ее сохранение и восстановление. В принципе в организации может быть много администраторов баз данных. Чтобы пользователь мог создать базу и стать ее администратором, он должен получить (вероятно, от администратора сервера) привилегию creatdb.

3. прочие (конечные) пользователи. Они оперируют данными, хранящимися в базах, в рамках выделенных им привилегий.

Администратор сервера баз данных, как самый привилегированный пользователь, нуждается в особой защите. Компрометация его пароля фактически означает компрометацию сервера и всех хранящихся на нем баз данных.

Поручать администрирование различных баз данных разным людям имеет смысл только тогда, когда эти базы независимы и по отношению к ним не придется проводить согласованную политику выделения привилегий или резервного копирования. В таком случае каждый из администраторов будет знать ровно столько, сколько необходимо.

Можно провести аналогию между пользователем ingres и администраторами баз данных с одной стороны, и суперпользователем операционной системы (root в случае ОС UNIX) и служебными пользователями (в ОС UNIX это могут быть bin, lp, uucp и т.д.) с другой стороны. Введение служебных пользователей

позволяет администрировать функциональные подсистемы, не получая привилегий суперпользователя. Точно так же информацию, хранящуюся на сервере баз данных, можно разделить на отсеки, так что компрометация администратора одного отсека не означает обязательной компрометации другого. Привилегии в СУБД можно подразделить на две категории: привилегии безопасности и привилегии доступа. Привилегии безопасности позволяют выполнять административные действия. Привилегии доступа, в соответствии с названием, определяют права доступа субъектов к определенным объектам.

Привилегии безопасности всегда выделяются конкретному пользователю (а не группе, роли или всем) во время его создания (оператором CREATE USER) или изменения характеристик (оператором ALTER USER). Таких привилегий пять:

1. security - право управлять безопасностью СУБД и отслеживать действия пользователей. Пользователь с этой привилегией может подключаться к любой базе данных, создавать, удалять и изменять характеристики пользователей, групп и ролей, передавать права на доступ к базам данным другим пользователям, управлять записью регистрационной информации, отслеживать запросы других пользователей и, наконец, запускать INGRES-команды от имени других пользователей. Привилегия security необходима администратору сервера баз данных, а также лицу, персонально отвечающему за информационную безопасность. Передача этой привилегии другим пользователям (например, администраторам баз данных) увеличивает число потенциально слабых мест в защите сервера баз данных.

2. createdb - право на создание и удаление баз данных. Этой привилегией, помимо администратора сервера, должны обладать пользователи, которым отводится роль администраторов отдельных баз данных.

3. operator - право на выполнение действий, которые традиционно относят к компетенции оператора. Имеются в виду запуск и остановка сервера, сохранение и восстановление информации. Помимо администраторов сервера

и баз данных этой привилегией целесообразно наделить также администратора операционной системы.

4. maintain_locations - право на управление расположением баз администраторы сервера баз данных и операционной системы.

5. trace - право на изменение состояния флагов отладочной трассировки. Данная привилегия полезна администратору сервера баз данных и другим знающим пользователям при анализе сложных, непонятных ситуаций.

Привилегии доступа выделяются пользователям, группам, ролям или всем посредством оператора GRANT и изымаются с помощью оператора REVOKE. Эти привилегии, как правило, присваивает владелец соответствующих объектов (он же - администратор базы данных) или обладатель привилегии security (обычно администратор сервера баз данных). Прежде чем присваивать привилегии группам и ролям, их (группы и роли) необходимо создать с помощью операторов CREATE GROUP и CREATE ROLE.
Для изменения состава группы служит оператор ALTER GROUP.
Оператор DROP GROUP позволяет удалять группы, правда, только после того, как опустошен список членов группы.
Оператор ALTER ROLE служит для изменения паролей ролей, а DROP ROLE - для удаления ролей.

Создавать и удалять именованные носители привилегий, а также изменять их характеристики может лишь пользователь с привилегией security. При совершении подобных действий необходимо иметь подключение к базе данных iidbdb, в которой хранятся сведения о субъектах и их привилегиях. Привилегии доступа можно подразделить в соответствии с видами объектов, к которым они относятся. В СУБД INGRES таких видов пять:

1. таблицы и представления
2. процедуры
3. базы данных
4. сервер баз данных

5. события

3 Ресурсы администрирования

Автоматизированная информационная система (Automated information system, AIS) – совокупность программных и аппаратных средств, предназначенных для хранения и (или) управления данными и информацией и производства вычислений. Следовательно, автоматизированная информационная система (АИС) является частью любого административного механизма – платформой управления и сетевой службой.

Платформа управления сетью (Network management platform) – комплекс программ, предназначенных для управления сетью и входящими в неё системами.

Сетевая служба использует сервис, предоставляемый областью взаимодействия, и обеспечивает связь прикладных процессов, расположенных в различных абонентских системах сети.

Система административных регламентов и информационная система являются затратной частью системы управления, но их отсутствие не гарантирует качество, оперативность и эффективность управления. При этом технологии и инструменты являются более стабильной компонентой, чем системы управления. Изменения стратегии, политики, методики, исполнителей обычно приводят к изменению системы управления и информационной системы. При этом инструмент, например существующая АИС, может обеспечить решение новых задач, порой с минимальной дополнительной её настройкой. Смена инструмента обычно приводит к изменению работы системы управления. Поэтому при целостном, целенаправленном формировании и функционировании системы управления, следует осуществлять одновременное развитие АИС и административных механизмов управления ей.

Очевидно, что управление сетью, как правило, целесообразно осуществлять с одного рабочего места. Потребность в контроле за сетью с одной управляющей станции способствовала появлению различных архитектур платформ и приложений администрирования. Наибольшее распространение среди них получила двухуровневая распределённая архитектура “менеджер–агенты”. Программа-менеджер функционирует на управляющей консоли, постоянно взаимодействуя с модулями-агентами, запускаемыми в отдельных устройствах сети. На агенты в такой схеме возлагаются функции сбора локальных данных о параметрах работы контролируемого ресурса, внесение изменений в его конфигурацию по запросу от менеджера, предоставление последнему административной информации. Однако её применение в реальной сетевой среде приводит к возрастанию объёмов служебного трафика и, как следствие, снижению эффективной пропускной способности, доступной приложениям.

В качестве частичного решения проблемы исчерпания пропускной способности предлагается трёхуровневая схема, в которой часть управляющих функций делегируется важнейшим сетевым узлам. Инсталлированные в этих узлах программы-менеджеры через собственную сеть агентов управляют работой “подотчётных” им устройств и одновременно сами выступают в роли агентов по отношению к основной программе-менеджеру (менеджеру менеджеров), запущенной на управляющей станции. В результате основная часть служебного трафика оказывается локализованной в отдельных сетевых сегментах, поскольку “общение” локальных менеджеров с административной консолью осуществляется только тогда, когда в этом действительно возникает необходимость.

Одна из современных идей совершенствования технологий администрирования сетью заключается в сведении к минимуму роли человека в процессе администрирования ИС. Она подразумевает создание ПО, необходимого для администрирования ИС, например, совмещение контроля защиты, управления пользователями, маршрутизации, резервного

копирования информации в случае сбоев и т.д. Администрирование сети в этом случае осуществляет программа, настраиваемая администратором сети. Такое решение значительно облегчает процесс администрирования, поскольку настройка одной программы намного легче, чем настройка всей сети и всех приложений, связанных с работой в сети.

Другое предложение базируется на использовании беспроводных сетей с высокой скоростью передачи информации, например, на основе информации, передаваемой светом, что позволяет избежать проблем связанных с самим физическим строением сети и значительно увеличить скорость передачи информации, а также избежать ряда проблем имеющихся у проводных сетей.

Еще одна идея заключается в создании для администрирования информационных систем интеллектуального компьютера – нейрокомпьютера. Такое решение позволяет свести на нет роль человека в администрировании информационных систем, в то же время добиться максимального быстродействия сетей, и полного их соответствия заданным целям.

4 Принцип и архитектура администрируемой базы данных

Увеличение размеров сети приводит как к увеличению количества устройств, обеспечивающих её функционирование, так и к увеличению их сложности и числа пользователей сети. В различных сетях эта проблема может осложняться гетерогенностью программного и аппаратного обеспечения. При этом такие информационные системы и среды являются многопользовательскими.

Многопользовательская среда – компьютерная сетевая программа, создающая среду для реализации различных типов поведения различных пользователей.

Сложность организации гетерогенной компьютерной сети вынуждает администратора определять и использовать устройства для соединения двух

сетей. Всё шире для этих целей используют специальные устройства: повторители, мосты маршрутизаторы.

Повторители – самые простые устройства для соединения сетей (в т.ч. ЛВС), предназначенные для увеличение длины сегмента сети (сетевого кабеля). Так как повторители ретранслируют в другую сеть все принимаемые пакеты или кадры, то загрузка общей сети аддитивно возрастает.

Мосты – достаточно эффективное средство объединения разных сетей в простой сетевой структуре.

Они позволяют локализовать нагрузку в отдельных сегментах сети, не пропуская пакеты или кадры, адресованные станциям данного сегмента, в другие сегменты, что приводит к значительному повышению эффективности использования всей сети за счёт снижения общего трафика. В сетях с относительно простой топологией достаточно легко гарантировать существование одного пути между любыми двумя устройствами. Когда количество соединений велико или сетевые связи становятся более сложными, увеличивается вероятность возникновения дублирующих маршрутов (маршрутизация) между устройствами, которые могут приводить к возникновению паразитных циклов (active loops). Хотя администраторам с целью создания избыточных связей может потребоваться формировать и дублирующие маршруты.

Маршрутизатор – специальный компьютер, распознающий различные протоколы и способный правильно направлять пакеты информации из одной сети в другую.

Маршрутизаторы более гибкие устройства, чем мосты. Они могут различать пути в зависимости от цены, скорости и задержки в сети; использовать все активные пути, имеющиеся в сети, а также обеспечивать разграничение потоков данных между разными подсетями. Маршрутизаторы облегчают управление большими сетями; поддерживают любую топологию и обеспечивают простой процесс настройки при увеличении размеров и сложности сети.

В отличие от мостов маршрутизаторы работают с логическими идентификаторами каждого сегмента сети. В связи с этим межсетевое взаимодействие, основанное на маршрутизаторах, позволяет объединить множество логически различных подсетей, в принципе являющихся независимыми административными доменами. Маршрутизаторы являются многопротокольными. В отличие от мостов, они имеют ПО, позволяющее реализацию соответствующего протокола и работающее с более полной информацией, сохраняемой в БД маршрутизатора. БД маршрутизатора называется таблицей маршрутизации и отличается от БД моста. Принципиальное различие состоит в том, что таблица маршрутизации включает информацию о путях (маршрутах), пройденных каждым пакетом по сети от отправителя до получателя.

Существуют устройства, совмещающие функции мостов и маршрутизаторов.

Мосты-маршрутизаторы (bridge/router) – устройства, позволяющие совместить преимущества мостов и маршрутизаторов. Как правило, мост-маршрутизатор реализует полные функции маршрутизации согласно одному или нескольким протоколам и действует как мост для всех других протоколов. Для повышения скорости передачи информации по межсетевому соединению многие мосты и маршрутизаторы используют алгоритмы сжатия данных, дающие выигрыш в случае использования низкоскоростных или сильно загруженных линий связи. При этом скорость передачи данных в межсетевом соединении более 64 Кбит/с не приносит выгод от сжатия данных, так как в этом случае может потребовать больше времени, чем простая передача данных без сжатия.

Многопользовательские объектно-ориентированные среды

Многопользовательские объектно-ориентированные среды (MOOs) – это основанные на тексте среды, установленные на персональных компьютерах для осуществления коммуникации в реальном режиме времени

между двумя и более удалёнными друг от друга участниками. Пользователи общаются между собой через Интернет, применяя доступное в сети специальное программно-инструментальное обеспечение, включая осуществляемую в реальном режиме времени аудиосвязь или текстовый чат. Изначально MOOs использовались для неформального общения и профессионального обучения на расстоянии. Работа в многопользовательской среде в первую очередь связана с присутствием в ней большого количества различных пользователей.

Пользователь информационной системы (Information system user) – лицо, группа лиц или организация, пользующиеся услугами информационной системы для получения информации или решения других задач.

Пользователей можно разделить на две категории:

Администраторы – пользователи, совершающие программные настройки и установки сети и устройств в ней, просматривающие все сообщения системы, изменяющие её свойства и др.

Обычные пользователи – пользователи, которые имеют доступ к сетевым ресурсам и устройствам, определяемым администраторами.