Функции, процедуры и службы администрирования

- Поскольку информационные системы могут иметь много пользователей, должно существовать лицо или группа лиц, управляющих этой системой. Такое лицо называется администратором информационных систем. В любой организации должен быть хотя бы один человек, выполняющий административные обязанности; если информационная система большая, эти обязанности могут быть распределены между несколькими администраторами.

Функции администрирования

К функциям администрирования относятся:

- - инсталляция и обновление версий сервера и прикладных инструментов;
- - распределение дисковой памяти и планирование будущих требований системы к памяти;
- - создание первичных структур памяти;
- - создание первичных объектов по мере проектирования приложений разработчиками;
- - модификация структуры данных в соответствии с потребностями;
- - зачисление пользователей и поддержание защиты системы;

Функции администрирования

- - соблюдение лицензионного соглашения;
- - управление и отслеживание доступа пользователей к информационным системам;
- - отслеживание и оптимизация производительности программ;
- - планирование резервного копирования и восстановления;
- - поддержание архивных данных на устройствах хранения информации;
- - осуществление резервного копирования и восстановления;
- - обращение в корпорации разработчиков или дилеров за техническим сопровождением.

Процедуры администрирования

- *Исследование активности системы*
- *Очистка аудиторских записей из аудиторского журнала*
- *Защита журнала проверки*

Исследование активности системы

- *Исследование активности системы* с целью генерирования следующей общей информации:
- - имя пользователя, выполнявшего отслеживаемое предложение;
- - код действия, указывающий выполненное предложение;
- - объекты, адресуемые в отслеживаемом предложении;
- - дату и время выполнения отслеживаемого предложения.

Администратор обязан контролировать рост журнала и его размер. Когда генерируются записи использования системы, журнал системного администратора растет за счет двух факторов:

- - числа включенных опций проверки;
- - частоты выполнения отслеживаемых операций.

Исследование активности системы

Для контроля за ростом журнала проверки надо использовать следующие методы:

- 1. Включать и выключать проверку информационной системы. Когда проверка включена, записи генерируются и поступают в журнал; когда проверка выключена, записи не генерируются.
- 2. Жестко контролировать возможности осуществлять проверку объектов. Это можно делать двумя различными способами:
- 3. Всеми объектами владеет администратор,
- 4. Все объекты содержатся в схемах, которые не соответствуют реальным пользователям информационной системы.

Очистка аудиторских записей из аудиторского журнала

- После того, как проверка включена в течение некоторого времени, администратор может удалить записи из журнала, - как для того, чтобы освободить память, так и для облегчения управления этим журналом. Если информация журнала должна архивироваться для целей накопления истории, администратор может скопировать соответствующие записи.

Защита журнала проверки

- Осуществляя отслеживание подозрительной деятельности в информационной системе, следует защищать целостность записей журнала проверки, чтобы гарантировать точность и полноту информации

Службы администрирования

- *Служба соблюдения правил эксплуатации*
- *Службы проектирования и приемки информационных систем*
- *Служба защиты от вредоносного программного обеспечения*
- *Служба обслуживания систем*
- *Сетевая служба*
- *Служба защиты носителей информации*
- *Служба обмена данными и программным обеспечением*

Служба соблюдения правил эксплуатации

- Обязанности администратора: обеспечить правильную и надежную работу информационной системы.
- Администратор должен определить обязанности и процедуры по администрированию и обеспечению функционирования компьютеров и сетей. Они должны быть зафиксированы в инструкциях и процедурах реагирования на инциденты. Для уменьшения риска некорректных или несанкционированных действий администратору следует применять принцип разделения обязанностей.

Службы проектирования и приемки информационных систем

- Обязанности администратора: свести риск отказов информационных систем к минимуму.
- Администратор обязан учитывать, что для обеспечения доступности ресурсов и необходимой производительности информационных систем требуется предварительное планирование и подготовка. Для уменьшения риска перегрузки систем необходимо учитывать будущие потребности и необходимую производительность. Эксплуатационные требования к новым системам следует определять, документировать и проверять до их приемки. Должны быть выработаны требования к переходу на аварийный режим для сервисов, поддерживающих несколько приложений.

Служба защиты от вредоносного программного обеспечения

- Обязанности администратора: обеспечить целостность данных и программ.
- Для предотвращения и выявления случаев внедрения вредоносного программного обеспечения администратору требуется принятие соответствующих мер предосторожности. В настоящее время существует целый ряд вредоносных программ («компьютерные вирусы», «сетевые черви», «троянские кони» и «логические бомбы»), которые используют уязвимость программного обеспечения по отношению к несанкционированной модификации. Администраторы информационных систем должны быть всегда готовы к проникновению вредоносного программного обеспечения в информационные системы и принимать специальные меры по предотвращению или обнаружению его внедрения. В частности, важно принять меры предосторожности для предотвращения и обнаружения компьютерных вирусов на персональных компьютерах.

Служба обслуживания систем

- Обязанности администратора: обеспечить целостность и доступность информационных сервисов.
- Для поддержания целостности и доступности сервисов администратору требуется выполнение некоторых служебных процедур: должны быть сформированы стандартные процедуры резервного копирования, регистрации событий и сбоев, а также контроля условий функционирования оборудования.

Сетевая служба

- Обязанности администратора: обеспечить защиту информации в сетях.
- Управление безопасностью сетей, отдельные сегменты которых находятся за пределами организации, требует особого внимания. Для защиты конфиденциальных данных, передаваемых по открытым сетям, могут потребоваться специальные меры.

Служба защиты носителей информации

- Обязанности администратора: предотвратить повреждение информационных ресурсов и перебои в работе организации.
- Необходимо контролировать носители информации и обеспечивать их физическую защиту. Следует определять процедуры для защиты носителей информации (магнитные ленты, диски, кассеты), входных/выходных данных и системной документации от повреждения, хищения и несанкционированного доступа.

Служба обмена данными и программным обеспечением

- Обязанности администратора: предотвратить потери, модификацию и несанкционированное использование данных.
- Администратору следует контролировать, чтобы обмены данными и программами между организациями осуществлялись на основе формальных соглашений. Должны быть установлены процедуры и стандарты для защиты носителей информации во время их транспортировки. Необходимо уделять внимание обеспечению безопасности при использовании электронного обмена данными и сообщениями электронной почты.

Контрольные вопросы

- 1. Обозначьте основные функции администрирования
- 2. Приведите основные процедуры администрирования
- 3. Расскажите об исследовании активности
- 4. Очистка аудиторских записей из аудиторского журнала
- 5. Защита журнала проверки
- 6. Перечислите основные службы администрирования