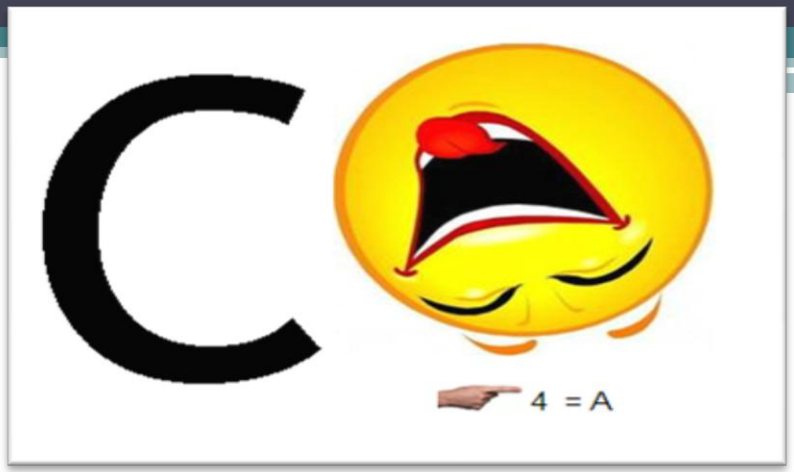
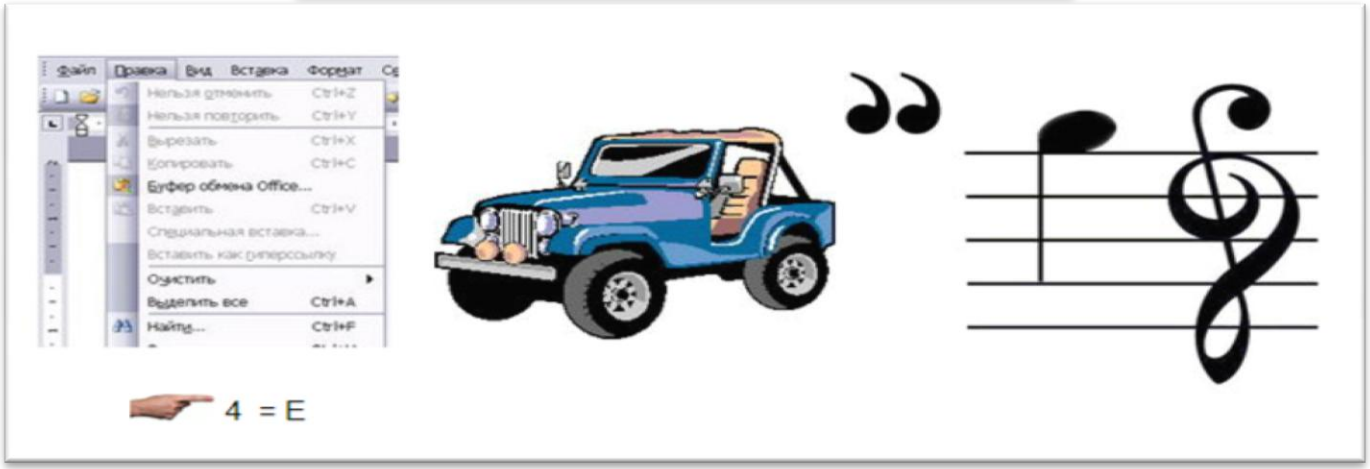

С
4 = А


Файл
Правка
Вид
Вставка
Формат
Нельзя отменить Ctrl+Z
Нельзя повторить Ctrl+Y
Вырезать Ctrl+X
Копировать Ctrl+C
Буфер обмена Office...
Вставить Ctrl+V
Специальная вставка...
Вставить как гиперссылку
Очистить
Выделить все Ctrl+A
Найти... Ctrl+F
4 = Е


Д
1 = Г

Р 

+ С

ЧЬЕ

1 = С

Е

РА

СВЕТА

2

Управление производительностью, безопасностью сети

Задачи управления конфигурацией сети

- отслеживание оборудования и программного обеспечения
- управление файловыми архивами
- учет сетевых услуг

Устранение возникающих неисправностей

Для выявления и устранения неисправностей в компьютерной сети используются аппаратные, программные и административные средства.

Цель использования этих средств – быстрое выявление и устранение неисправного компонента (или потенциально неисправного компонента) в компьютерной сети.

Задачи, решаемые аппаратными, программными и административными средствами

- быстрое нахождение и устранение неисправностей (по мере возможности предупреждение неисправностей);
- установка приоритета в предупреждении и устранении неисправностей;
- своевременное решение проблем пользователей и удовлетворение их запросов.

Управление производительностью сети

Управление производительностью сети заключается в:

- периодическом отслеживании различных характеристик
- поиск «узких мест» (bottlenecks)
- просчитывание возможного развития событий и выработку рекомендаций по дальнейшему улучшению сети.

Характеристики производительности сети

- *Количество байт, полученных с сервера и записанных на него* позволяет получать информацию о загрузке сервера.

- *Количество команд в очереди на исполнение* также является показателем загрузки сервера. Это число не должно быть большим.

- *Количество коллизий в секунду* (в сетях Ethernet).

- *Количество ошибок системы безопасности*. Высокий уровень неудачных входов в сеть, неудачных доступов к объектам и неудачных изменений настроек безопасности могут указывать на попытки взлома сети.

- *Сеансы соединений с сервером.* Если сеанс завершается в результате ошибки или из-за истечения периода ожидания сервера (time-out), то возможно сервер перегружен и отказывает в соединении, либо не может их быстро обслуживать.

Инструменты отслеживания характеристик производительности сети

- **Event viewer** - поддерживает три регистрационных списка:
  - один для регистрации событий системы безопасности (security log)
  - второй для системной информации (system log)
  - третий для сообщений приложений (application log).

User Manager for Domains- записывает сообщения событий системы безопасности на основе фильтров

Performance monitor - регистрирует отдельные события (записывает и отслеживает тенденции изменения параметров системы).

Network monitor. - отслеживает поток сетевых данных, записывает адреса отправителя и получателя, заголовки и данные для каждого пакета.

Общесистемное управление

На производительность сети влияет не только сеть, но и другое оборудование.

Кроме отслеживания работы самой сети, следует большое внимание уделять жестким дискам и оперативной памяти на серверах.

Жесткий диск- отслеживаются следующие характеристики:

- оставшееся дисковое пространство
- скорость обработки запросов (это и средняя пропускная способность, и количество переданных данных)
- частота занятости диска (как частота его работы, так и среднее количество запросов в очереди диска).

Оперативная память

Оперативная память сервера требуется для обслуживания входящих запросов.

Windows Server спроектирована так, чтобы сбрасывать из памяти на диск (в swap file) не используемые в данный момент данные.

Управление безопасностью сети

Управление безопасностью сети направлено на защиту данных и оборудования в сети.

Оно включает в себя аппаратные, программные и административные средства для уменьшения опасности изнутри или снаружи организации.

Управление безопасностью сети решает следующие задачи:

- определение возможных опасностей и их последствий;
- разработка и внедрение политики защиты компьютерной сети;
- администрирование учетных записей пользователей;
- использование различных средств для слежения за деятельностью пользователей и оповещения о сомнительных действиях пользователей.

Для реализации политики защиты необходимо идентифицировать пользователей и ресурсы сети с помощью различных схем сетевого наименования.

Схемы сетевого наименования

Каждому компьютеру в сети должно быть **присвоено имя**, чтобы он мог взаимодействовать с другими компьютерами в сети.

Кроме того, имена нужны пользователям сети для работы с разделенными (shared) ресурсами.

Сетевые имена могут быть разделены на следующие категории: учетные записи, компьютеры, ресурсы.

Учетные записи

Учетная запись представляет собой объединение всей информации, относящейся к пользователю или группе пользователей в сети.

Имена компьютеров

Каждый компьютер в сети может иметь много имен в зависимости от того, какой процесс, протокол или устройство взаимодействует с ним в данный момент.

Имена ресурсов

Каждый ресурс можно идентифицировать по имени.

Разработка и внедрение политики защиты компьютерной сети

Разработка политики защиты состоит из трех этапов.

- Выяснение потребности компании.
- Разработка политики защиты (безопасности), соответствующей этим потребностям.
- Реализация политики защиты.

Дополнительные средства защиты

Аудит (auditing) – это способ отслеживания событий и действий пользователей.

Аудит формирует список событий (audit log), в котором хранится информация кто, когда и что делал в сети.

Windows Server имеет мощные средства аудита и позволяет аудит удачного и неудачного выполнения следующих событий:

- Вход в сеть (logon) и выход из сети (logoff). Пользователь вошел в сеть или вышел из нее, создал или оборвал сетевое соединение с сервером.

- Доступ к файлам и объектам (file and object access). Пользователь получил доступ к каталогу, файлу или принтеру, который настроен на проведение аудита (файлы и каталоги – только в NTFS

- Использование прав пользователя (Use of user rights). Пользователь использовал свое право (за исключением входа в сеть и выхода из нее).
- Управление группами и пользователями (User and group management). Учетная запись пользователя или группы было создана, изменена или удалена. Или учетная запись пользователя была переименована, заблокирована или разблокирована, или пароль был установлен или изменен.
- Изменение политики защиты (Security policy changes). Было произведено изменение прав пользователя, политики аудита или доверительных отношений.

- Перезапуск (restart), выключение (shutdown) и системные события (system). Пользователь перезагрузил или выключил компьютер, или произошло событие, влияющее на безопасность системы.
- Отслеживание процессов (process tracking). Отслеживание детальной информации о различных событиях, например активизации программ, появление повторяющихся дескрипторов, косвенный доступ к объектам и завершение процесса.