Тема. Изучить консоль ММС

Задание

1. Открыть консоль ММС
2. Изучить для чего она используется? Что можно настроить с её помощью?
3. Изучить каждый элемент консоли по следующему плану:
   - Для чего служить этот элемент
   - Какие настройки у него существуют и что они позволяют делать
   - Изменить ряд настроек/показателей – отследить изменения системы.
4. Создайте собственную консоль ММС.
5. Научиться назначать задания по расписанию:
   a. Назначить старт блокнота при старте Windows. Проверить работоспособность;
   b. Назначить старт калькулятора в 10:00 каждый день. Проверить работоспособность;
   c. Назначить старт программы Paint в 10:00 в понедельник и пятницу. Проверить работоспособность;
   d. Удалить все назначенные задания.
6. Добавить элемент «Создание и управление учетными записями». Создать несколько учетных записей и групп. Научиться менять принадлежность учетной записи к группе. На что это будет влиять у учетной записи?
7. Настроить Мониторинг системы. Посмотреть как отслеживать кеш, оперативную память, процессы. Как добавлять и удалять показатели, по которым производиться отслеживание?
8. Настроить аудит. Отследить вход-выход в систему. Какие состояния есть у адуита?
9. Подключить журналирование.
10. Научиться отслеживать события:
    a. По времени:
       i. За весь период;
       ii. За месяц;
       iii. За неделю;
       iv. За выбранный пользователем период;
    b. По коду
    c. По пользователю
    d. По источнику.

Контрольное демонстрационное задание по Групповой политике:

1. Локально добавьте на открытую консоль администрирования системную оснастку «Групповая политика».
2. В дереве консоли «Политика «Локальный компьютер» щелкните манипулятором мышь по папке «Конфигурация компьютера | Конфигурация Windows | Параметры безопасности | Локальные политики | Политика аудита» для настройки локальных политик аудита.
3. Настройте политики аудита. Для этого в области сведений дважды щелкните на политике аудита, для которой необходимо изменить параметры аудита и установите один или оба флажка («успех» или «отказ») для успешных или неуспешных системных событий, которые необходимо регистрировать. Повторите действия указанные в текущем пункте секции для других политик аудита в случае необходимости.
4. Настройте аудит файлов и папок. Для этого измените параметры «успех» или «отказ» категории событий «Аудит доступа к объектам». Укажите файлы или папки для аудита, выполнив следующие действия:
   a. · на вкладке «Безопасность» команды «Свойства» файла или папки нажмите кнопку «Дополнительно»,
   b. · на вкладке «Аудит» нажмите кнопку «Добавить»,
   c. · в диалоговом окне «Выбор: пользователь, компьютер или группа» выберите имя пользователя или группы, для действий которых требуется производить аудит файлов и папок, и нажмите кнопку OK для подтверждения выбора;

d. · в появившемся диалоговом окне «Элемент аудита» в группе «Доступ» установите флажки «успех», «отказ» или оба эти флажка одновременно напротив действий, для которых требуется провести аудит,
e. · выберите из выпадающего меню «Применить:» опцию «Для этой папки и ее подпапок» (или любую другую опцию на Ваш выбор), а затем нажмите кнопку OK и Примерить для подтверждения ввода.
f. Если указанные выше действия выполнить не удалось по причине отсутствия вкладки «Безопасность» в «Свойствах» объекта, выполните следующее:
g. · в дереве консоли «Политика «Локальный компьютер» щелкните манипулятором мышь по папке «Конфигурация пользователя | Административные шаблоны | Компоненты Windows | Проводник»;
h. · в области сведений дважды щелкните на «Удалить вкладку «Безопасность», измените системный параметр на «Отключено» на одноименной вкладке и подтвердите выбор, кликнув OK;
i. · выберите команду Панель управления в меню Пуск, откройте компонент «Свойства папки» на панели управления, дважды щелкнув по нему мышью, и на вкладке «Вид» в группе «Дополнительные параметры | Файлы и папки» снимите флажок «Использовать простой общий доступ к файлам (рекомендуется)».

5. Не закрывая консоль администрирования MMC, сохраните ее.
6. При выполнении заданий секции используйте следующие инструкции:
   a. · перенесите последовательность выполняемых действий по каждому из пунктов 1-5 в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),
   b. · сделайте вывод о проделанной работе и запишите его в отчет.

Контрольное демонстрационное задание по Аудиту:

1. Локально добавьте на открытую консоль администрирования новую системную оснастку «Просмотр событий».

2. В дереве консоли щелкните манипулятором мышь по оснастке «Просмотр событий» и обратите внимание на появившиеся три журнала и их текущие размеры в области сведений справа. Последовательно перебирая журналы приложений, безопасности и системы, отметьте в них наличие всех указанных выше типов системных событий (табл. 20). При этом обратите внимание на то, что такие типы событий как аудиты отказов и успехов присущи только журналу безопасности, который был Вами настроен в предыдущей секции. Остальные типы событий встречаются как в журнале приложений, так и в журнале системы.

3. Воспользовавшись меню «Вид» изучаемой оснастки, отфильтруйте:

· в журнале приложений событие «Уведомление» за прошедшее время,

· в журнале безопасность событие «Аудит отказов» за __ квартал,

· в журнале система событие «Ошибка» за последнюю неделю, с сортировкой по дате «от старых к новым».

4. В окне журнала событий системы удалите столбцы «Пользователь», «Компьютер» и «Категория», оставив остальные.

5. Воспользовавшись системой поиска, найдите событие типа «Предупреждение» с кодом 1003 от источника DHCP в журнале событий системы.

6. Создайте собственный журнал событий, содержащий только сведения об ошибках приложений и программ. Установите максимальный размер этого журнала в 128 Кб и возможность затирания старых событий по необходимости. Сохраните созданный журнал в двоичном виде с расширением .evt.

7. Создайте инструмент для регистрации событий аудита любого компьютера рабочей группы или домена и осуществите просмотр системных событий другого узла локальной сети с его помощью.

8. Не закрывая консоль администрирования MMC, сохраните ее.

При выполнении заданий секции используйте следующие инструкции:

· перенесите последовательность выполняемых действий по каждому из пунктов 1-6 в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),

· сделайте вывод о проделанной работе и запишите его в отчет.