ПРАКТИЧЕСКАЯ РАБОТА №4

Работа со средствами мониторинга и диагностики в Windows

Цель работы: Ознакомиться со встроенными средствами технического мониторинга, назначением и принципами работы Prefomance Monitor. Получить навыки сбора и анализа данных, позволяющих оценивать производительность системы. Получить практические навыки поиска "узких мест" в производительности системы. Получить дополнительные навыки по управлению Windows Server, управлению процессами и журналами работы.

Необходимо:

- Установленная на компьютере среда виртуализации **ORACLE Virtual Box**
- Образы виртуальных жёстких дисков операционных систем **Windows Server 2012/2016.**
- Доступ к Microsoft Evaluation Center (https://www.microsoft.com/ru-ru/evalcenter)

Краткие теоретические сведения

Одной из важнейших составляющих обеспечения функциональности системы является ее мониторинг. Современные ОС содержат средства для осуществления технического мониторинга. К целям технического мониторинга относятся:

1) наблюдение за текущими параметрами системы;

2) сбор статистики для ретроспективного анализа, построения профилей загрузки системы, отладки и настройки приложений, прогностического анализа;
3) автоматизации реакции системы на определенные ее состояния.

В системе ОС Windows содержится компонент Performance Monitor, реализующий технический мониторинг.

Performance Monitor позволяет создавать:

1) Группу Сборщиков Данных – набор единообразно управляемых журналов сбора данных. В ней создавать:
2) Счетчик Производительности - журнал, в который с определенной периодичностью заносятся значения Счетчиков – атрибутов программных объектов, представляющих или аппаратные или программные подсистемы (Процессор, UDP, Файл Подкачки и т.п.).
3) Сборщик данных отслеживания событий - куда заносятся все события, происходящие в подсистеме, которая выбрана в виде провайдера при создании сборщика.
4) Оповещение счетчика производительности – специального журнала, позволяющего автоматически реагировать на определённое состояние счетчика.

В Performance Monitor содержит раздел Отчетов, через который доступны обработанные сводные данные журналов.

Если журнал Счетчик Производительности ведется в бинарном формате, то конвертировать его в текстовый формат позволяет утилита **relog.exe**

Для конвертации журнала Сборщик данных отслеживания событий используется утилита **tracerpt.exe**

Как любая зрелая операционная система Windows содержит подсистему видения системных журналов. Доступны системные журналы (Приложения, Безопасность, Система, Установка, Перенаправленные события) и журналы приложений и служб.

Для работы с журналами служат оснастка Просмотр событий (eventvwr.msc), консольная утилита Wevtutil и PowerShell.

Windows содержит механизм запуска процессов по расписанию или событиям - Планировщик Заданий. Для работы с ним служат консоль taskschd.msc, утилиты schtasks.exe и at (устарела), а также PowerShell.

Порядок выполнения работы:

Часть 1. Работа с процессами. Разработка скриптов.

1. Напишите скрипт, который создает Журнал Работы с именем «ProcessMonitoringLog». Если журнал существует, то выводится сообщение об этом.
2. Напишите скрипт на PowerShell, который:
    a. при запуске выводит список запущенных процессов (PID, Имя процесса, Путь к исполняемому файлу, Пользователь процесса, Утилизация CPU, Занимаемая память, Время Получения данных).
    b. Записывает эти данные в CSV файл.
    c. При успешном сохранении данных пишет в журнал ProcessMonitoringLog сообщение об успехе, при ошибках сохранения – сообщение об ошибке.

Часть 2. Планирование периодического выполнения.

1. С помощью PowerShell добавьте автоматический запуск скрипта из Части 1. п.2 в планировщике заданий Windows (Task Scheduler), так чтобы, но запускался каждые 3 минуты, даже тогда, когда питание идет не от батареи или ИБП.
2. Убедитесь в работоспособности решения.

Часть 3. Работа с журналом событий.

1. Ознакомитесь с журналом событий.
2. Создайте настраиваемое представление журнала, позволяющее увидеть все неудачные попытки входа в ОС под именем Администратора.
3. С помощью PowerShell напишите скрипт, который выводит в текстовый файл:
   a. время последних 10 включений компьютера,
   b. время 5 последних установок пакетов обновлений с указанием названий обновлений (например KB1299393),
   c. количество ошибок и количество предупреждений за последние 24 часа.

Часть 4. Сбор и анализ данных

1) создать в программе Performance Monitor Группу Сборщиков Данных, которая будет содержать:
   a. Счетчик Производительности записи которого позволят сравнить загрузку аппаратного обеспечения платформы. Счетчики для этого следует выбрать самостоятельно, но они должны отражать использование памяти, дисковой подсистемы, процессора и сети.
   b. Периодичность журнала установить в 5 секунд.

c. Сборщик данных отслеживания событий, фиксирующий события ядра Windows.

2) С помощью Группы Сборщиков Данных сравните загрузку системы в двух разных ситуациях. Это может быть загрузка при использовании разных приложений одного типа (2 антивируса, 2 браузера, 2 СУБД, 2 кодека и т. п.), наборы разных программ (MS Word + MS Excel и MS Excel + MS Access и т.п.) или одно и тоже приложение при разной его конфигурации.
3) С помощью механизма отчетов дайте первичный анализ загрузки в обоих случаях.
4) С помощью электронных таблиц или других средств анализа данных представите данные о загрузке в виде графиков.

Часть 5. Автоматизация реакции системы на ее состояние

1) Добавьте в виртуальную машину еще один жесткий диск объемом 200 Мб. Включите виртуальную машину и создайте на новом диске раздел.
2) Создайте скрипит, который постепенно заполняет новый логический диск файлами размером до 1 Мб.
3) Создайте скрипит, очищающий новый диск.
4) В Performance Monitor создайте новую Группу Сборщиков Данных с Оповещением счетчика производительности, который, срабатывает в случае, если осталось менее 20% свободного места на новом разделе и выводящее предупреждение в журнал событий и запускающее сприт из п.3.

   Разработчики Performance Monitor предполагают, что нужно в Планировщике заданий создать задание, выполняющее скрипт из

п. 3 и указать имя этого задания в настройках Сборщика данных отслеживания событий.

5) Проверьте срабатывание оповещений. Вероятно, вы обнаружите неожиданное поведение системы. Попробуйте выяснить причину, заменяя используемые счетчики.

Содержание отчета

Требуется подготовить отчеты в формате DOC\DOCX или PDF. Отчет содержит титульный лист, артефакты выполнения и ответы на вопросы.

Артефакты:

1) Скрипты из Части 1
2) Скрипты из Части 2
3) Параметры Представления из Части 3, п.2
4) Скрипт из части 3. п. 3
5) Материалы и результаты анализа из Части 4 п. 3-4
6) Скрипты из части 5.

Вопросы:

1) В чем назначение каждого из разделов журнала событий?
2) Зачем нужен раздел Перенаправленные события?
3) Где находится журналы событий Windows в виде файлов?
4) Как с помощью графической оснастки журнала событий установить по известному VID коду, когда было подключено и настроено устройство?
5) Почему были выбраны конкретные счетчики в Части 4 п.1? Обоснуйте выбор.

6) Как получить на консоль подробные параметры запланированного задания с помощью утилиты schtasks.exe? Проиллюстрируйте ответ на примере задания из части 5.
7) Опишите ваши выводы по пункту 5. Части 5.

Отчет выслать на адрес edu-net@yandex.ru.

В теме письма: №группы ФИО (латинскими буквами) №работы (например: 5555 Fedor Sumkin 4)