ТЕМА 9. МОНИТОРИНГ И УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

В данной теме рассматриваются следующие вопросы:

- мониторинг производительности;
- журналы событий;
- методика устранения неисправностей;
- обзор продуктов: SC OM, OMS, Zabbix.

Лекции – 2 часа, лабораторные занятия – 2 часа, самостоятельная работа – 6 часов.

Минимальный набор знаний:

Четыре вида ресурсов для мониторинга

Понятие базовой линии производительности

Встроенные инструменты мониторинга

Журналы событий Windows

9.1. Мониторинг производительности

Для поиска источника неисправностей, а также для заблаговременного получения информации о возможных проблемах используются средства измерения производительности и других показателей работы компьютера.

> Существует четыре вида ресурсов: CPU, Memory, Disk, Network.
>
> После установки и настройки сервера имеет смысл создать для него базовую линию производительности, а затем по мере возрастания нагрузки сравнивать с ней текущую степень нагрузки и определять изменения. Для этого нужно в течение недели взять образцы значений за 30-45 минут в пиковые часы (утром или после обеда), во время простоя и во время нормального рабочего состояния.

9.1.1. Обзор инструментов измерения производительности

Для проведения анализа мощности и производительности системы нужны специальные средства и знание того, как правильно их использовать, что даст возможность получить ценные данные. Некоторые из этих средств позволяют даже предсказать мощность системы, в зависимости от количества предоставленной им информации.

Компания Microsoft предлагает несколько удобных утилит, либо встроенных в Windows Server 2012, либо продаваемых в виде отдельных продуктов. Утилиты, включенные в операционную систему: диспетчер задач, сетевой монитор, монитор надежности и производительности Windows, а также улучшенное средство просмотра событий — предоставляют только базовые функции сбора данных и их отображения. Для глубокого анализа и построения информативных отчетов, следует экспортировать данные, собранные этими утилитами, в другие приложения, подобные Microsoft Excel или Access. Могут применяться и другие утилиты Microsoft, продаваемые отдельно: диспетчер конфигурации системного центра (System Center Configuration Manager — SCCM) и диспетчер операций системного центра (System Center Operations Manager — OpsMgr).

Существует также множество других программ, например, Nagios, Pandora FMS, Zabbix и другие.

Диспетчер задач

Диспетчер задач (Task Manager) предоставляет множество возможностей. С его помощью можно просматривать и наблюдать в реальном времени информацию, связанную с процессором, памятью, приложениями, сетью, службами, пользователями и процессами данной системы. Эта утилита очень популярна среди IT-специалистов и удобна для быстрого просмотра основных индикаторов работоспособности системы с минимальным влиянием на производительность.

Для запуска диспетчера задач воспользуйтесь одним из следующих способов.

- Нажмите комбинацию клавиш <Ctrl+Shift+Esc> или <Ctrl+Shift+End> в случае подключения через службу удаленных рабочих столов.
- Щелкните правой кнопкой мыши в панели задач и выберите в контекстном меню пункт **Task Manager** (Диспетчер задач).

• Нажмите комбинацию клавиш <Ctrl+Alt+Delete>, а затем выберите в открывшемся меню пункт Task Manager.

Диспетчер задач в Windows Server 2012 по умолчанию открывается в компактном представлении (Summary), которое содержит список выполняющихся приложений. Из этого представления можно завершить работу приложения.

Кнопка **More Details** (Подробно) открывает более привычное окно диспетчера задач, содержащее следующие пять вкладок.

• **Processes** (Процессы). Эта вкладка содержит основную информацию о процессах, выполняющихся в системе в текущий момент. Можно упорядочить процессы по приложениям или фоновым процессам, использованию ресурсов процессора или памяти, состоянию процессов и т.д.

• **Performance** (Производительность). Эта вкладка содержит обширную информацию о потреблении и параметрах процессора, использовании и выделении памяти и использовании и конфигурации сети. На ней имеется также ссылка на монитор ресурсов из состава Windows Server 2012.

• **Users** (Пользователи). На этой вкладке отображаются пользователи, находящиеся в данный момент в системе, и на ней можно отключать таких пользователей.

• **Details** (Сведения). Эта вкладка содержит обширную информацию о выполняющихся процессах в привычном по предыдущим версиям виде. Более подробная информация содержит сведения о вводе-выводе, идентификаторах сеансов, пуле памяти и сходстве и приоритетах процессов.

• **Services** (Службы). Эта вкладка появилась в диспетчере задач относительно недавно. Она позволяет видеть все выполняющиеся службы и запускать и останавливать их без загрузки специальной консоли.

Монитор производительности Windows

Монитор производительности (Performance Monitor) позволяет собирать информацию со счетчиков производительности системы и различных приложений, сохранять ее на диске или в базе SQL Server и отображать в виде графика, столбчатой диаграммы или отчета.. В комплект поставки входит несколько готовых наборов сборщиков данных для некоторых типовых случаев, например, Active Directory Diagnostics и System Diagnostics. Монитор производительности можно запустить из диспетчера серверов Windows Server 2012 Server Manager либо из стартового окна.

Диспетчер операций System Center Operations Manager

Диспетчер операций (System Center Operations Manager 2012 — OpsMgr) стал заменой своего популярного предшественника, диспетчера операций SCOM 2007 R2. Он содержит значительные усовершенствования по сравнению с предыдущими версиями в отношении доступности, масштабируемости и мониторинга гетерогенных систем. Это всестороннее решение мониторинга и отчетности, которое составляет отчет о состояниях, связанных с производительностью служб, системы и сети, и в случае возникновения проблем отправляет администраторам уведомления — например, когда важные службы не могут начать свою работу, когда процент использования процессора постоянно находится выше

обозначенного порогового значения, или, когда агент OpsMgr считает, что используется слишком много страниц. OpsMgr интегрируется непосредственно с Active Directory, Windows Server 2012 и большинством других технологий Microsoft, обеспечивая общее решение, которое помогает автоматизировать мониторинг важных систем и процессов. OpsMgr использует пакеты управления, широко применяемые с базовой операционной системой Windows Server 2012, Exchange Server 2007/2010 или Internet Information Services (IIS), и поэтому требует лишь незначительной настройки после установки.

Средства сторонних разработчиков

Несомненно, среди утилит сторонних разработчиков есть много замечательных средств для анализа мощности и мониторинга производительности. Большинство из них предоставляют дополнительные функции, отсутствующие в мониторе производительности Windows Server 2012 и других средствах, но они стоят дороже и могут выдвигать специальные требования к развертыванию и интеграции в сети организации. Можно попробовать поработать с некоторыми сторонними утилитами, чтобы лучше понять, какие дополнительные возможности они предлагают по сравнению с решениями от Microsoft. Вообще говоря, эти утилиты расширяют возможности, свойственные решениям мониторинга от Microsoft, такие как планирование выполнения, усовершенствованные возможности отчетов, гораздо лучшие возможности хранения данных, возможность мониторинга систем, отличных от Windows, и алгоритмы для последующего анализа тенденций. Перечислим некоторые из этих сторонних средств: AppManager Suite, BMC ProactiveNet Performance Manager, HP Service Health Optimizer, Longitude, NSM.

9.1.2. Монитор производительности

Монитор производительности окно которого показано на рис. 9.1, состоит из трех основных компонентов: инструментов мониторинга, таких как монитор производительности (Performance Monitor), групп сборщиков данных и компонента для формирования отчетов.

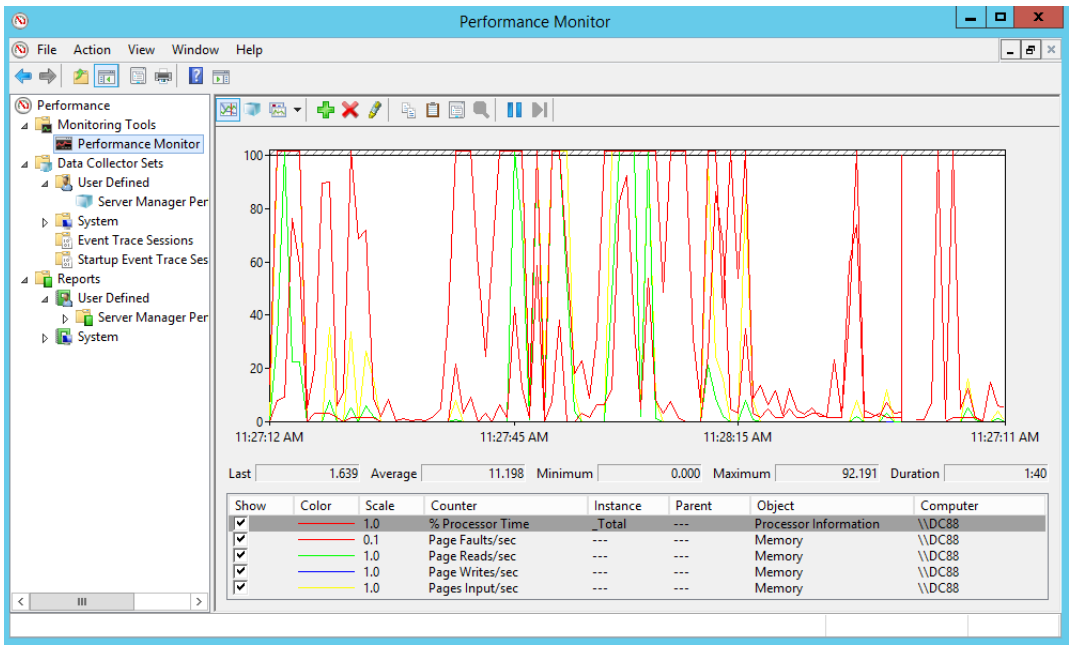


Рис. 9.1. Окно монитора производительности

Используя монитор производительности, администраторы могут обнаруживать узкие места и выявлять проблемы, связанные с использованием ресурсов, в приложениях, процессах или оборудовании. Наблюдение за этими элементами может помочь выявлять и устранять проблемы, планировать изменения мощности и помогать устанавливать эталонные значения, которые в будущем можно будет применять для анализа. При запуске монитора производительности отображаются итоговые данные о производительности системы, показывая текущие значения по использованию памяти, диска, процессора и сети.

Для использования этого средства не нужен этап долгого ознакомления. Монитор производительности можно запустить из диспетчера серверов, выбрав в меню **Tools** пункт **Performance Monitor** (**Сервис -> Монитор производительности**). С помощью этой утилиты можно анализировать данные как в реальном времени, так и сохраненных исторических данных. Анализируемые данные можно просмотреть в виде графиков, диаграмм и отчетов. Данные в формате журнала можно сохранить для дальнейшего применения, чтобы можно было исследовать данные за отдельные короткие периоды времени.

При запуске консоли узел **Системный монитор** отображает оперативную информацию. Каждый вид измеряемой информации называется счетчиком.

Если же нужно собрать информацию за определенный период, нужно создать **Группу сборщиков данных** в одноименном узле консоли. Полученные отчеты будут помещаться в узел консоли **Отчеты**, имеющий такую же структуру, как и **Группы сборщиков данных**. Каждому отчету будет присваиваться имя, содержащее в себе дату старта и порядковый номер отчета за день.

Чтобы просмотреть отчет в графическом виде, нужно перейти в системный монитор и выбрать **Просмотр данных журнала** (рис. 9.2).

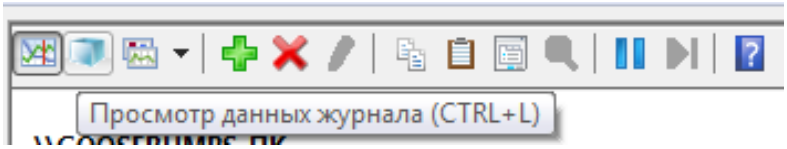


Рис. 9.2. Кнопка **Просмотр данных журнала**

Также в режим системного монитора можно перейти прямо из отчета (рис. 9.3).

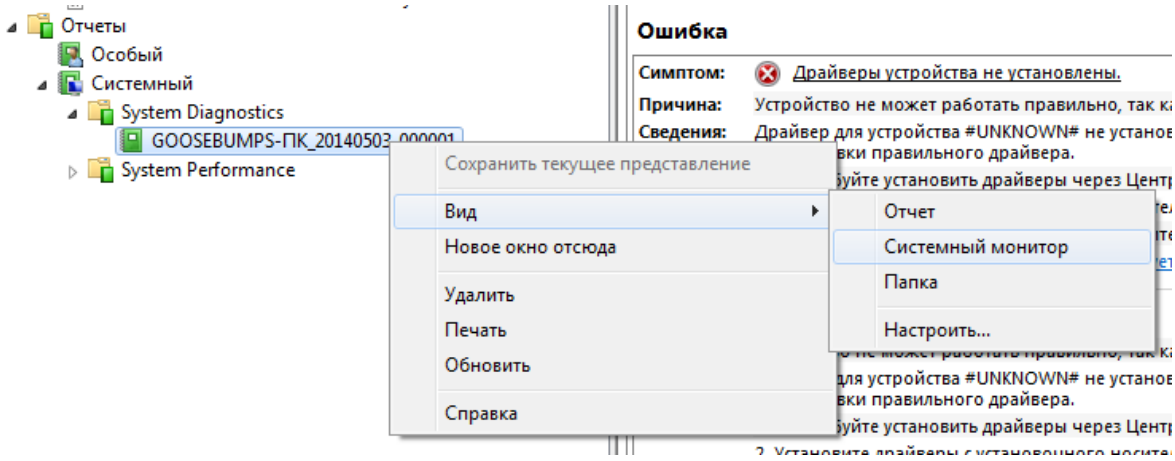


Рис. 9.3. Открытие системного монитора из отчета

По умолчанию информация в системном мониторе отображается в графическом виде. При большом количестве счетчиков консоль теряет наглядность. Можно выделить один счетчик в списке и нажать кнопку **Выделить** (рис.9.4).

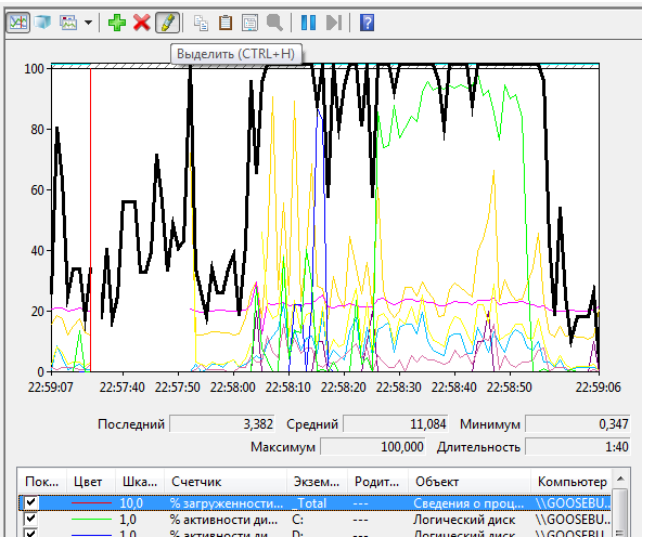


Рис. 9.4. Кнопка **Выделить** в системном мониторе

Также можно переключиться в режим **Отчет**, где наблюдать за счетчиками легче, но не видно динамики (рис. 9.5).

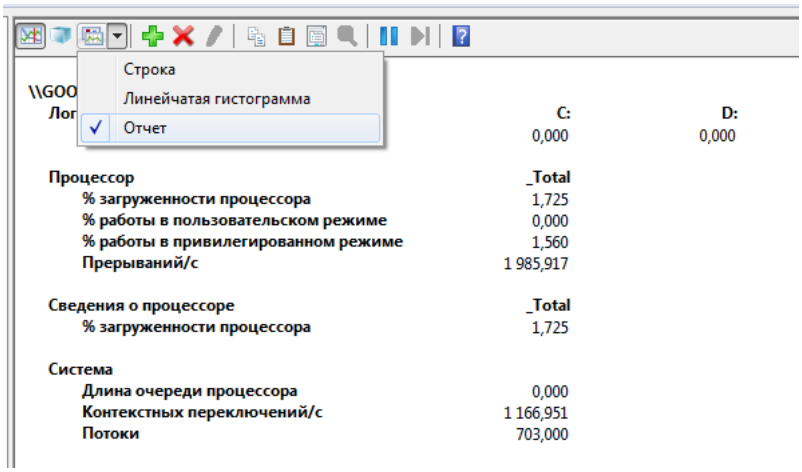


Рис. 9.5. Переключение системного монитора в режим отчета

Работа с некоторыми счетчиками требует досконального понимания работы процессора и операционной системы. Но есть множество вполне очевидных и полезных счетчиков, которыми следует пользоваться.

Добавление счетчика

Сначала в системном мониторе нужно нажать кнопку **Добавить** (рис. 9.6):

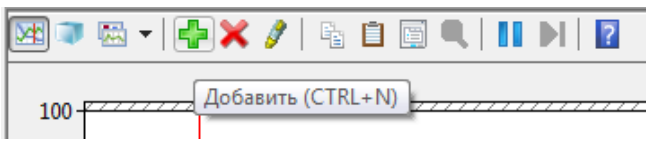


Рис. 9.6. Кнопка **Добавить** в системном мониторе

Затем в открывшемся окне по очереди выбрать компьютер (чаще всего локальный компьютер), развернуть нужную категорию (например, **Логический диск**) и выделить необходимые счетчики (например, **% активности диска**). Далее выбрать нужные объекты, если их несколько (несколько процессоров, дисков,

программ, и т.п.) и нажать кнопку **Добавить>>**. При этом в правом окне формируется список наблюдаемых счетчиков (рис. 9.7). Когда список готов, нажать **ОК**.

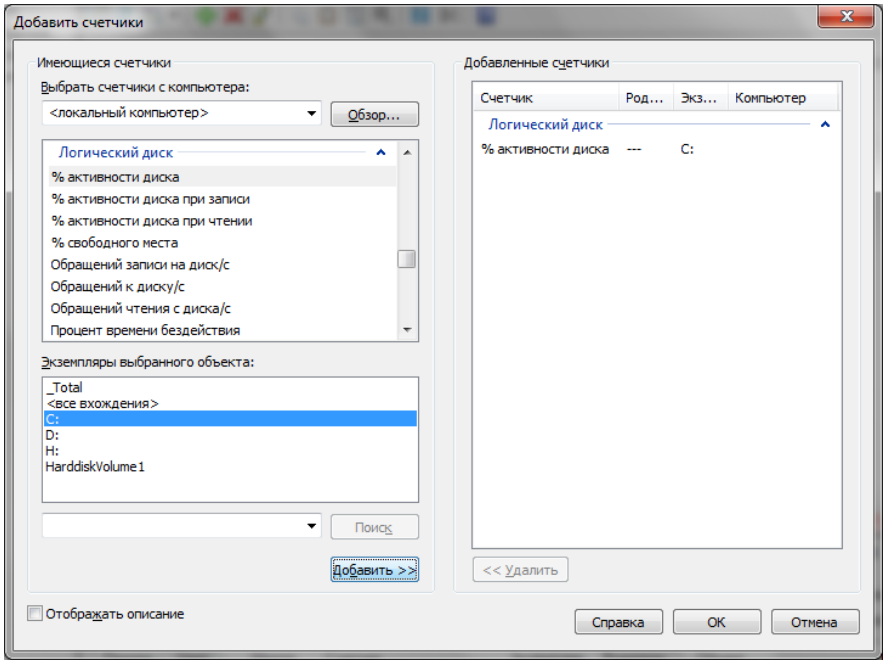
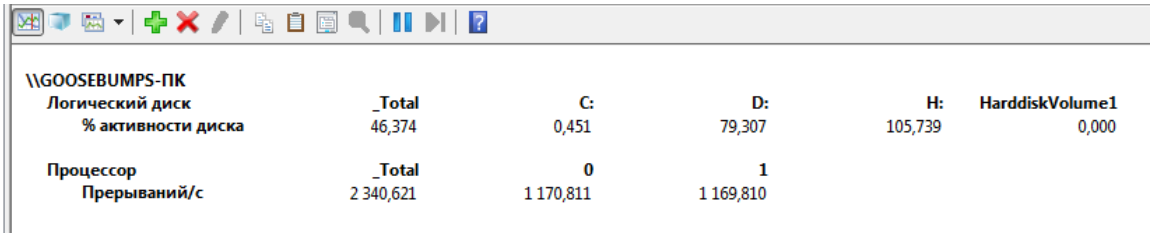


Рис. 9.7. Диалоговое окно для редактирования списка наблюдаемых счетчиков производительности

При выборе экземпляров можно выбрать отдельные экземпляры объектов, а также выбрать специальные значения <все вхождения> и _Total. <все вхождения> позволяет за одно нажатие кнопки добавить в список все существующие в данный момент экземпляры. _Total имеет смысл суммы для количественных счетчиков и смысл среднего арифметического для процентных счетчиков. В примерах ниже 2340=1170+1170, и 46 = (0 + 79 + 106 + 0) **:** 4.



\\GOOSEBUMPS-ПК					
Логический диск	**_Total**	**C:**	**D:**	**H:**	**HarddiskVolume1**
% активности диска	46,374	0,451	79,307	105,739	0,000
Процессор	**_Total**	**0**	**1**		
Прерываний/с	2 340,621	1 170,811	1 169,810		

Рис. 9.8. Эффект суммирования значений счетчиков для разных экземпляров объекта

Группы сборщиков данных

Как уже было сказано, группы сборщиков данных представляют собой коллекции элементов, за которыми будет вестись наблюдение. Можно использовать одну из предварительно определенных групп или же создать собственную группу, чтобы сгруппировать вместе элементы, за которыми нужно вести наблюдение (рис. 9.9). Группы сборщиков данных удобны по нескольким причинам. Это может быть общая тема или смесь элементов. Например, можно создать группу для наблюдения только за памятью или группу для наблюдения за памятью, диском, процессором и многим другим. При необходимости можно запланировать работу таких групп.

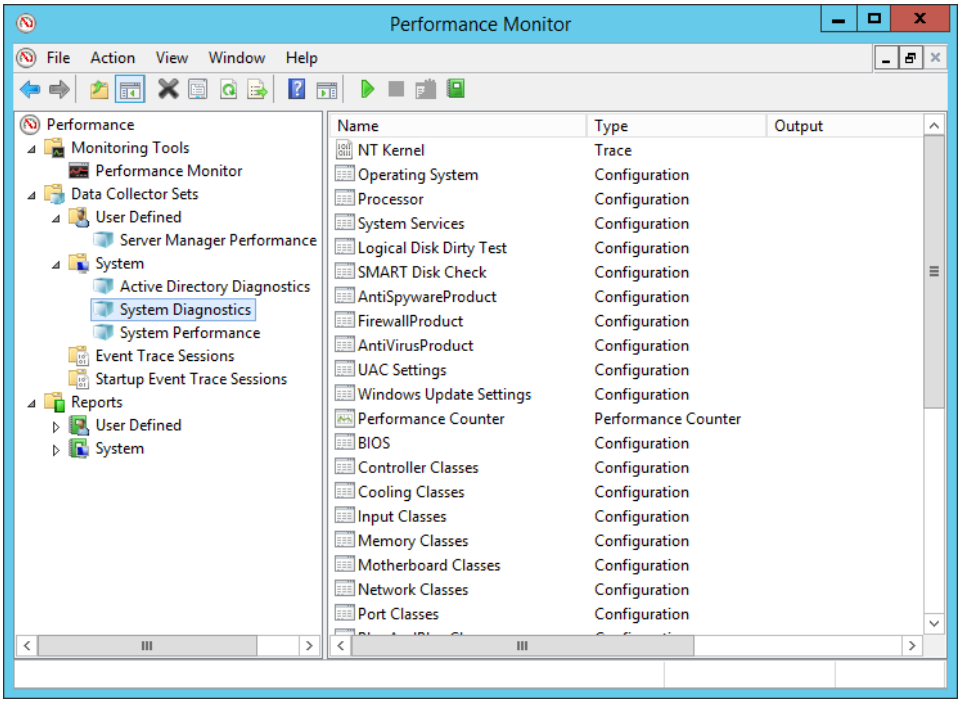


Рис. 9.9. Системные группы сборщиков данных

Сохранение данных о производительности в файле

Если нужно сохранить значения показателей производительности для последующего анализа, создаются группы сборщиков данных (рис. 9.10). Так же, как и при мониторинге, в группу добавляются нужные счетчики, указывается место хранения файлов, условия для запуска и остановки.

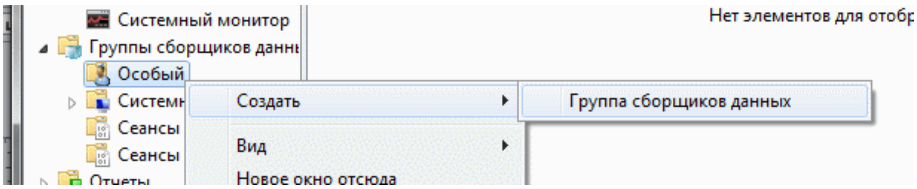


Рис. 9.10. Команда создания новой группы сборщиков данных

В открывшемся окне нужно дать имя группе сборщиков данных и выбрать вариант создания (рис. 9.11), обычно выбирается второй вариант.

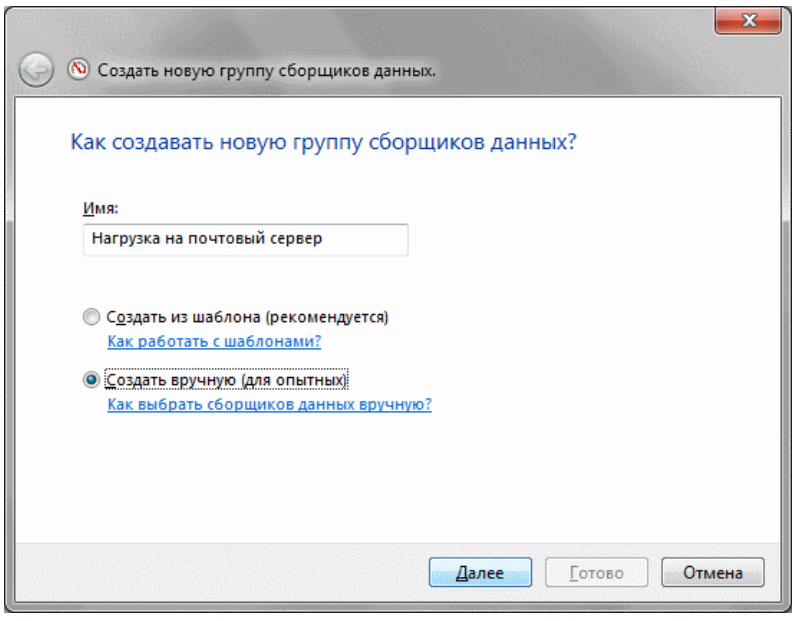


Рис. 9.11. Стартовая страница мастера создания группы сборщиков данных

На следующем экране (рис. 9.12) отметить **Счетчик производительности** (остальные опции часто не нужны).

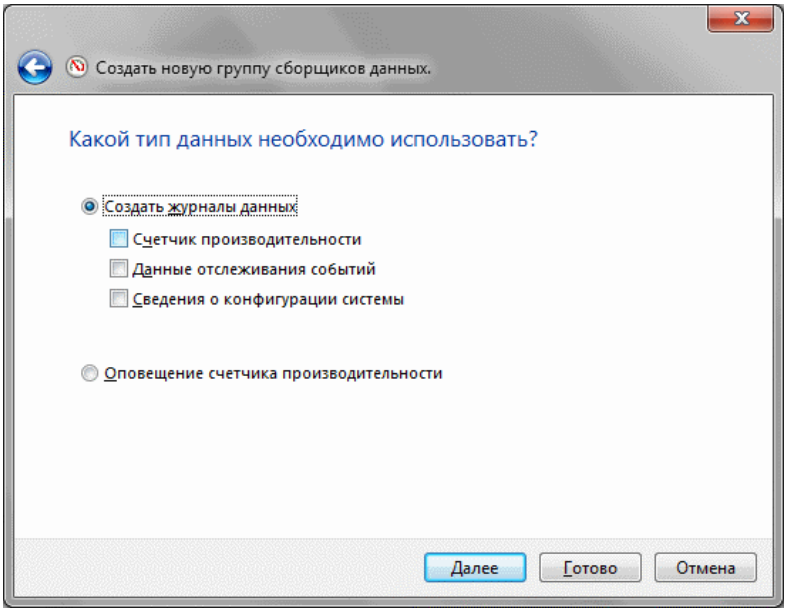


Рис. 9.12. Выбор типа сохраняемых данных

Далее откроется окно для добавления счетчиков (рис. 9.13).

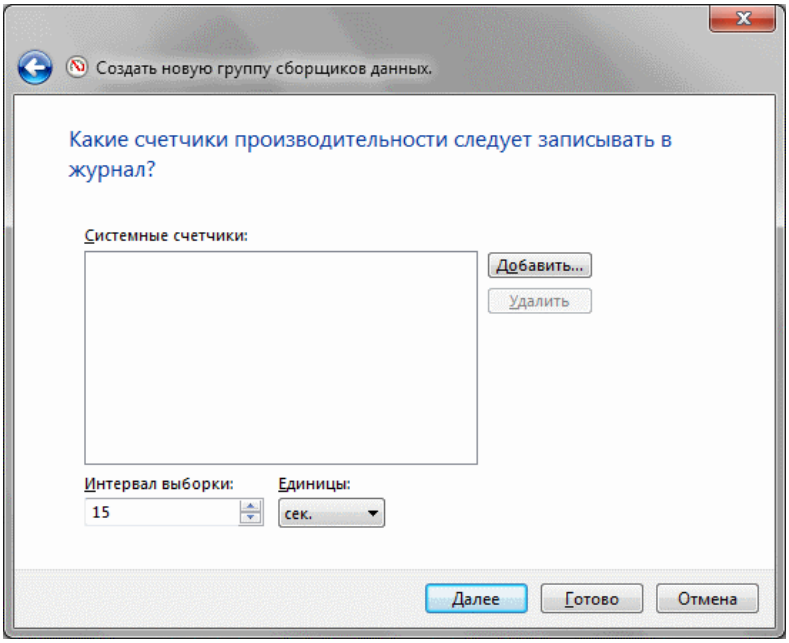


Рис. 9.13. Выбор счетчиков и интервала выборки

Указав список счетчиков, нажать **Далее**. Согласиться в следующем окне с местоположением папки для хранения журналов, нажать **Далее**. В следующем окне выбрать переключатель **Открыть** свойства группы сборщиков данных и нажать **Готово** (рис. 9.14), чтобы перейти к редактированию свойств группы (можно выбрать **Сохранить и закрыть**, если редактирование будет позже или устраивают параметры по умолчанию).

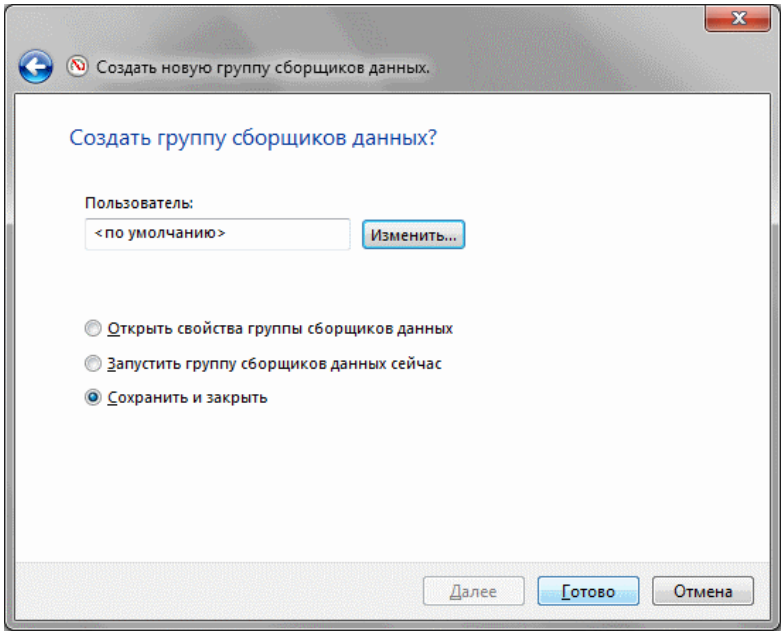


Рис. 9.14. Последняя страница мастера создания группы сборщиков данных

При создании группы сборщиков данных одновременно создается сборщик данных по имени DataCollector01, в котором хранятся выбранные во время создания группы счетчики. При необходимости в группу можно добавить дополнительные сборщики данных.

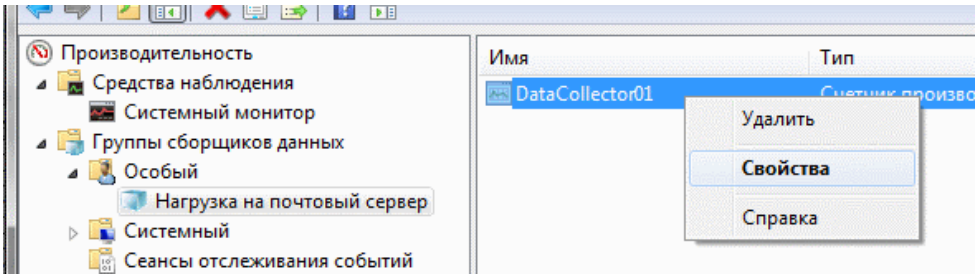


Рис. 9.15. Сборщик данных по имени DataCollector01

Если открыть свойства сборщика данных, можно изменить список счетчиков и формат данных (рис. 9.16). Обычно выбирается формат **Двоичный** (Binary), тогда результаты можно будет просмотреть в этой же консоли, в Системном мониторе. Если же анализ будет проводиться сторонней программой, тогда можно использовать остальные форматы, CSV и TSV-файлы можно открывать с помощью Excel или импортировать в базу данных, вариант SQL помещает данные непосредственно в базу данных.

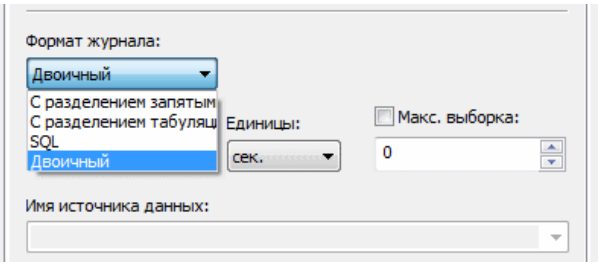


Рис. 9.16. Выбор формата файла журнала

Второй настраиваемый параметр — интервал выборки (рис. 9.17), то есть периодичность измерений. При поиске неисправностей обычно устанавливается небольшой интервал (1-5 секунд), чтобы не пропустить важного события. При

анализе долговременных трендов можно установить период 1–15 минут и даже больше (например, свободное место на диске).

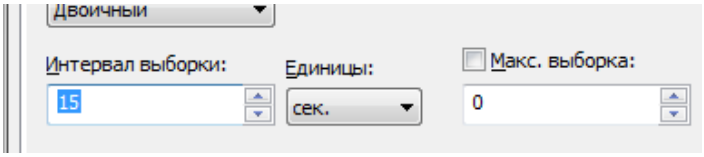


Рис. 9.17. Выбор интервала выборки

При настройках группы сборщиков данных по умолчанию, доступен только ручной запуск (команда **Пуск** контекстного меню, рис. 9.18). Когда группа запущена, ее иконка изменяется ( ). После остановки группы в узле консоли **Отчеты->Особый->Имя набора** появится папка, имя которой автоматически генерируется на основе имени компьютера, даты запуска и порядкового номера журнала за этот день.

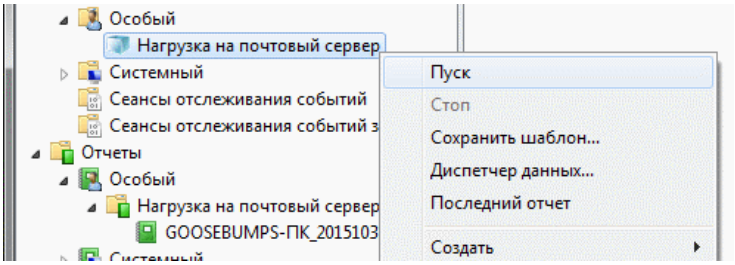


Рис. 9.18. Ручной запуск группы сборщиков данных

Просмотр сохраненных данных

Перейти к просмотру сохраненных данных можно одним из следующих способов:

1. В Системном мониторе нажать кнопку **Просмотр данных журнала**, затем выбрать переключатель **Файлы журнала**, нажать кнопку **Добавить** (рис. 9.19) и выбрать нужный файл.

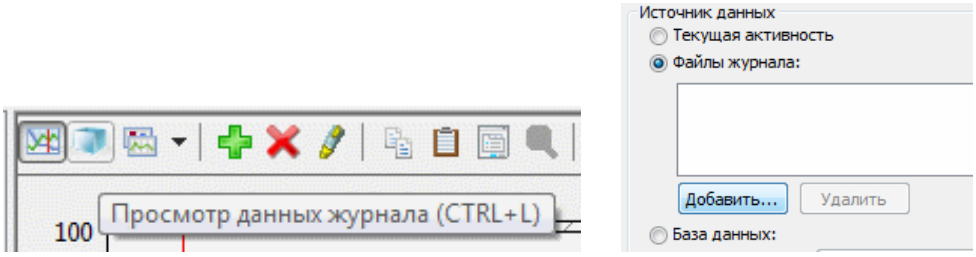


Рис. 9.19. Добавление файла журнала

2. Открыть **Системный монитор** из узла **Отчеты**.

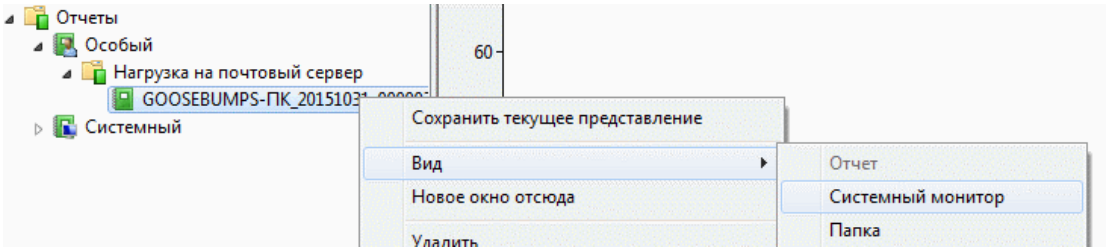


Рис. 9.20. Запуск системного монитора из узла Отчеты

3. Выполнить двойной щелчок мышью на соответствующем файле *.blg в проводнике Windows (рис. 9.21).

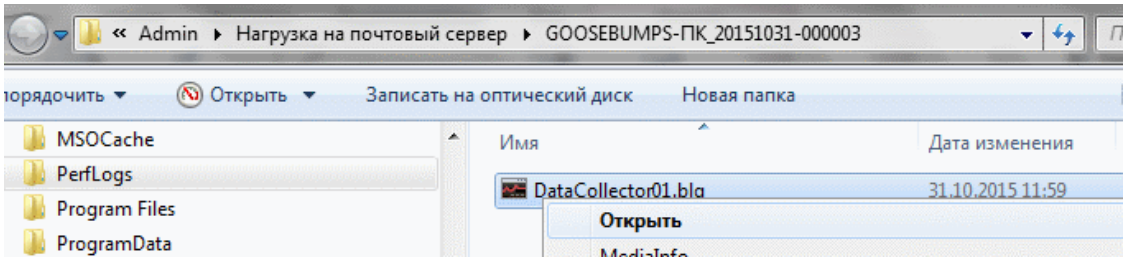


Рис. 9.21. Открытие информации о производительности в проводнике Windows

Откроется окно системного монитора с горизонтальной полосой прокрутки, где можно выбрать исследуемый диапазон времени (рис. 9.22).

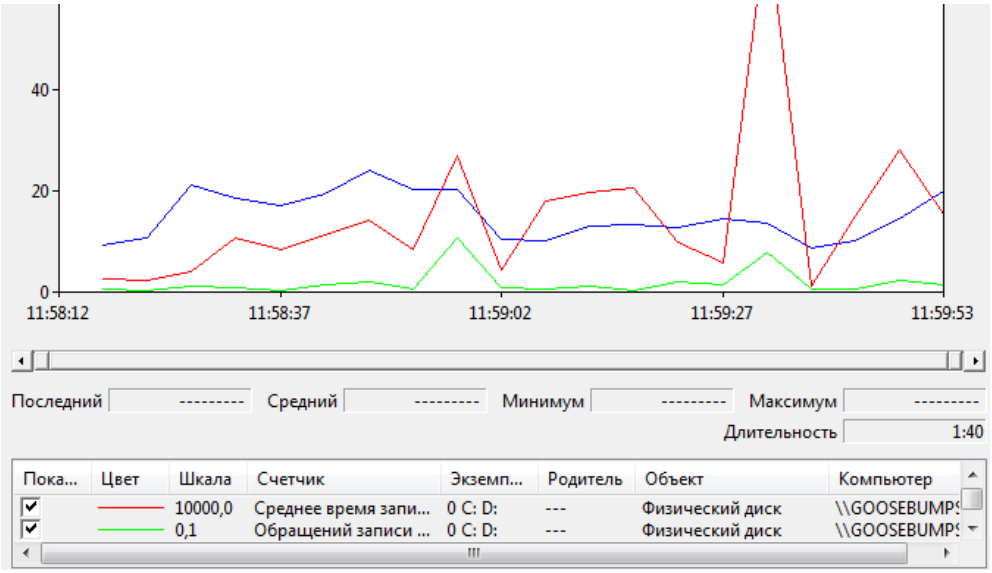


Рис. 9.22. Отображение информации о производительности из файла

Отчеты

Как упоминалось ранее, монитор производительности включает обновленный механизм формирования отчетов, а также несколько шаблонных диагностических отчетов и отчетов о производительности. Кроме того, отчеты можно создавать вручную или генерировать из групп сборщиков данных. Для диагностики и оценки производительности системы можно воспользоваться тремя готовыми системными отчетами: диагностика Active Directory (Active Directory Diagnostics), диагностика системы (System Diagnostics) и производительность системы (System Performance). Чтобы получить отчет по диагностике системы, потребуется выполнить перечисленные ниже действия.

1. Раскройте узлы **Data Collector Sets** (Группы сборщиков данных) и **System** (Система) в дереве консоли монитора производительности.

2. Щелкните правой кнопкой мыши либо на наборе **System Diagnostics** (Диагностика системы), либо на наборе **System Performance** (Производительность системы) и выберите в контекстном меню пункт **Start** (Запустить). ОС Windows начнет сбор данных для отчета.

3. Когда вы соберете достаточно данных, снова щелкните правой кнопкой мыши на наборе и выберите в контекстном меню пункт **Stop** (Остановить).

4. Раскройте узлы **Reports** (Отчеты), **System** (Система) и щелкните на наборе, который выбирался ранее. Дважды щелкните на отчете, показанном ниже набора производительности.

Отчёт будет скомпилирован и выведен на экран, как было показано на рис. 9.23.

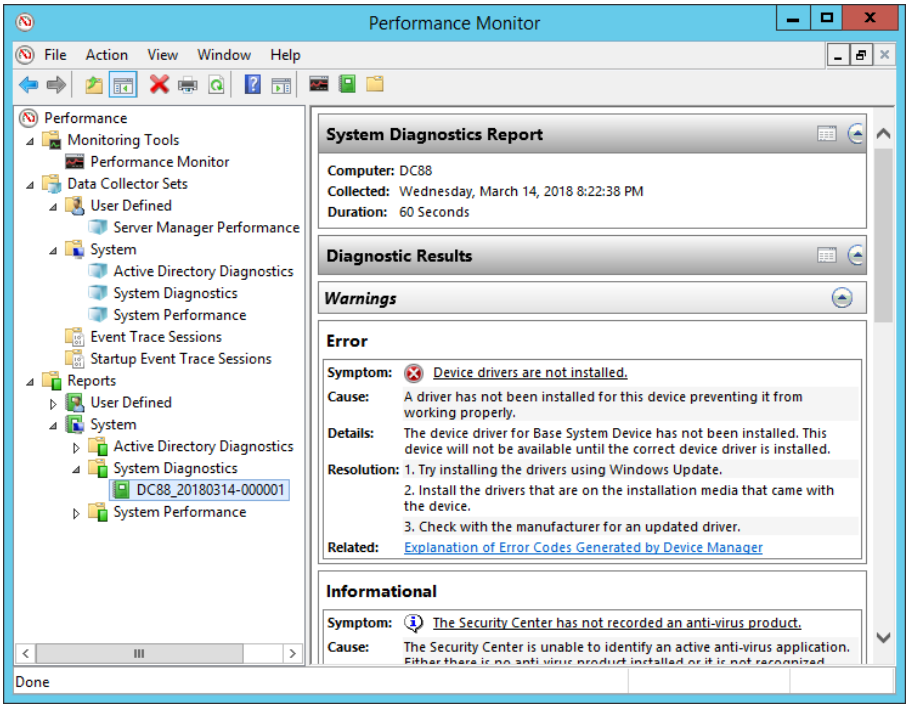


Рис. 9.23. Отчет для набора «Диагностика системы»

9.1.3. Оповещения

Оповещения счетчика производительности позволяют настраивать задачу для запуска, когда счетчик производительности, например, доступное дисковое пространство или память, становится ниже или превышает определенное значение. Чтобы настроить оповещение счетчика производительности, вы создаете новый набор сборщиков данных, выбираете опцию «Создать вручную» и выбираете опцию «Оповещения счетчика производительности», как показано на рис. 9.24.

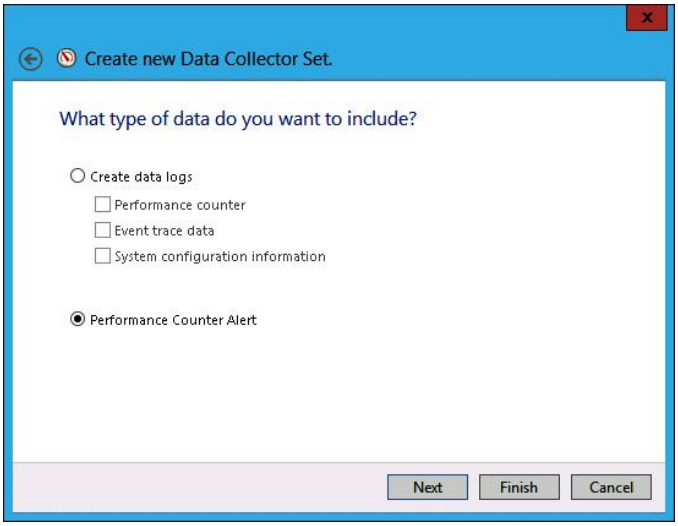


Рис.9.24. Создание оповещения счетчиков производительности

Вы добавляете счетчик производительности, пороговое значение и должно ли срабатывать оповещение, если значение превышает или падает ниже этого

значения. На рис. 9.25 показано оповещение, которое запускается, когда объем доступной памяти становится ниже 512 мегабайт.

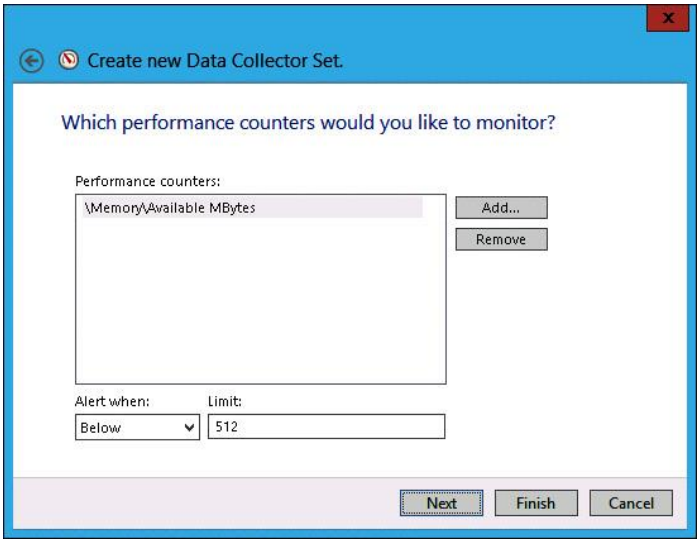


Рис. 9.25. Установка порога срабатывания

Когда вы создаете оповещение, все, что оно делает при срабатывании — это записывает событие в журнал событий. Вы также можете настроить оповещение для запуска запланированной задачи при запуске. Вы делаете это, редактируя свойства оповещения и указывая имя запланированной задачи на вкладке «Задача», как показано на рис. 9.26.

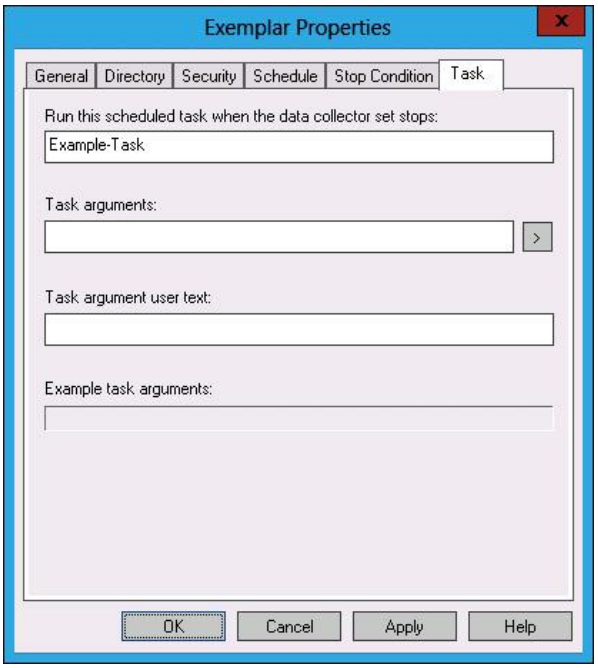


Рис. 9.26. Запуск запланированной задачи

Более подробно о работе со счетчиками производительности можно прочитать в следующих статьях.

http://www.oszone.net/12774/perfmon1
http://www.oszone.net/12885/perfmon2
http://www.oszone.net/12948/perfmon3
http://www.oszone.net/13493/perfmon4

9.2. Журналы событий Windows

Журнал событий (Event Log) — в Microsoft Windows стандартный способ записи и централизованного хранения информации о важных программных и аппаратных событиях. Служба журналов событий сохраняет события от различных источников в едином журнале событий, программа просмотра событий позволяет пользователю наблюдать за журналом событий, программный интерфейс (API) позволяет приложениям записывать в журнал информацию и просматривать существующие записи. Также можно настроить централизованную подписку для сбора нужной информации на одном сервере.

9.2.1. Административная консоль «Просмотр событий»

Для работы с журналами используется консоль **Просмотр событий** (Event Viewer, `eventvwr.msc`, рис. 9.27).

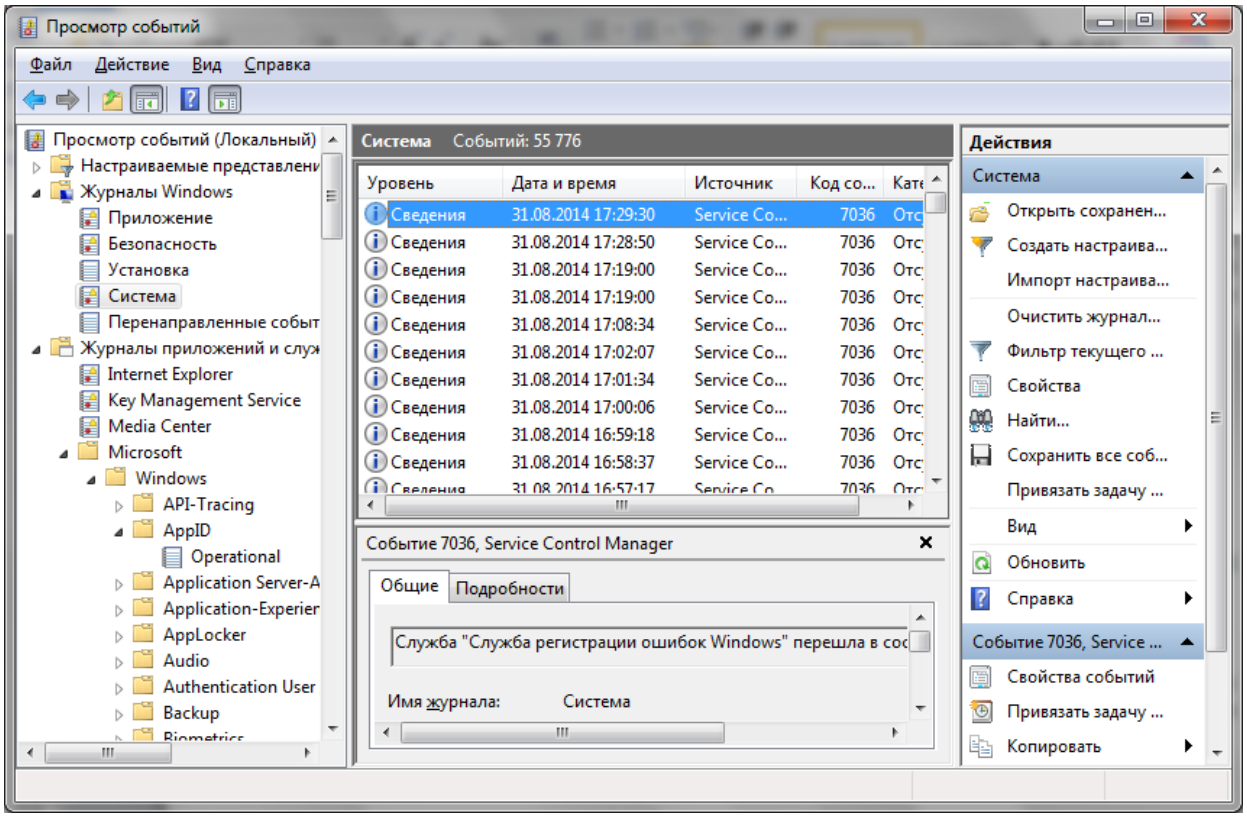


Рис. 9.27. Консоль Просмотр событий

После установки операционной системы имеются следующие журналы событий:

файл журнала **приложений** (Application) — для событий приложений и служб;

файл журнала **безопасности** (Security) — для событий системы аудита;

файл журнала **системы** (System) — для системных событий, например, от драйверов устройств.

Начиная с Windows Server 2008 и Windows Vista многие компоненты Windows и приложения имеют собственные журналы событий. Они отображаются в узле Журналы приложений и служб\Microsoft\Windows. В англоязычной литературе эти дополнительные журналы называются Crimson Channel.

События от каждого источника могут включаться в определяемые отдельно для каждого источника категории. События должны принадлежать к одному из пяти предопределённых типов (уровней).

Сведения. События указывают редкие и важные успешные операции.

Предупреждение. События указывают проблемы, которые не требуют немедленного вмешательства, но могут привести к ошибкам в будущем. Примером такого рода событий может служить исчерпание ресурсов.

Ошибка. События указывают существенные проблемы, обычно приводящие к потере функциональности или данных. Примером может служить невозможность запуска службы при загрузке.

Аудит успеха. События безопасности, которые происходят при успешном обращении к наблюдаемым ресурсам. Примером может служить успешный вход в систему.

Аудит неудачи. События безопасности, которые происходят при неуспешном обращении к наблюдаемым ресурсам. Примером может служить попытка открыть файл пользователем, не имеющим соответствующих прав доступа.

Запись о событии (рис. 9.28) включает в себя: идентификатор события, тип события, источник события, категорию события, массив строк и дополнительные, специфичные для события, двоичные данные. Каждый источник событий должен зарегистрировать свой файл сообщений, в котором хранятся строки описания идентификаторов сообщений, категорий и параметров.

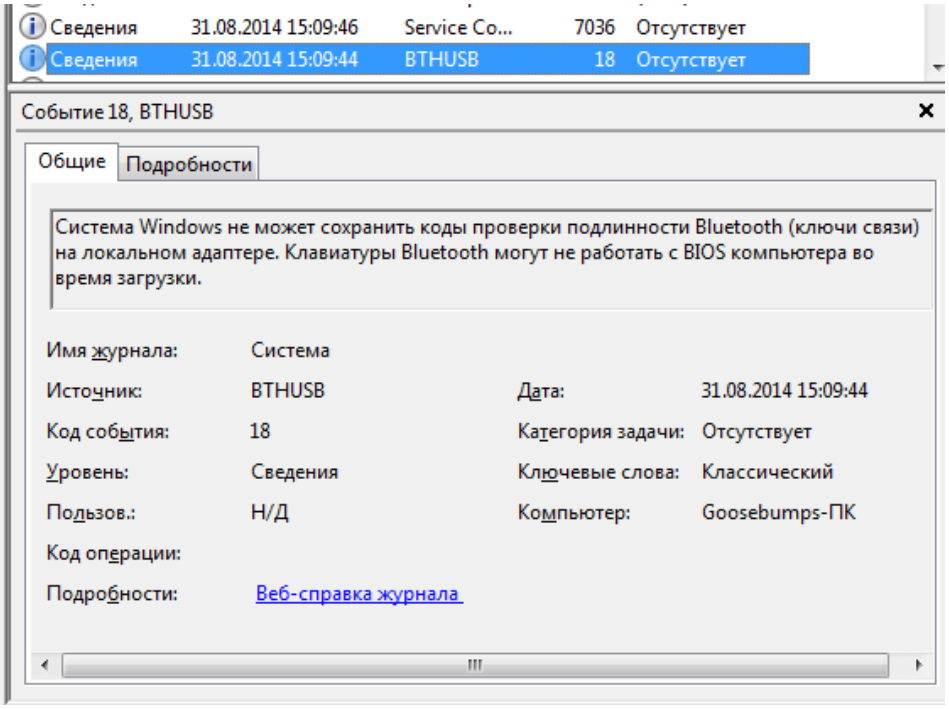


Рис. 9.28. Запись о событий

Источник события — это текстовый идентификатор, под которым служба или программа зарегистрировала себя в системе событий Windows. Если нужно найти только события от одной программы, то можно или отсортировать события по столбцу «Источник», либо создать фильтр, либо создать представление (описано ниже). В иллюстрации ниже (рис. 9.29) отмечены SkypeUpdate и Диспетчер печати, которые могут помещать события в журнал.

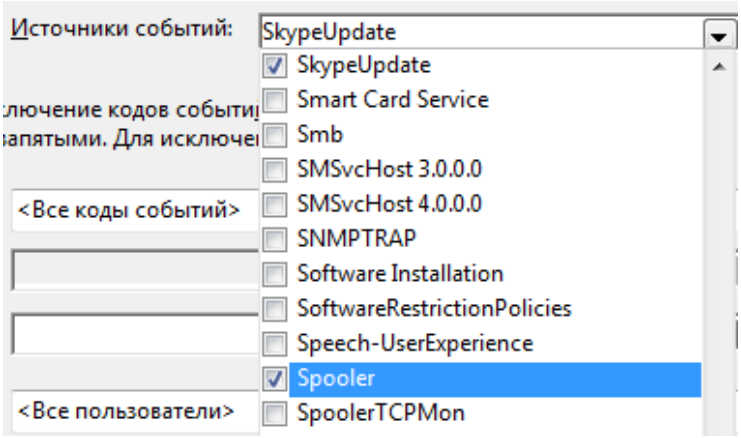


Рис. 9.29. Выбор источников событий Windows

В реестре имеется запись о каждом источнике событий. Здесь следует обратить внимание на два параметра: CategoryMessageFile и EventMessageFile. Эти параметры указывают на .EXE или .DLL, в котором находится текстовое описание событий. Это сделано для экономии места в журнале событий. То есть, разработчик приложения нумерует все события, о которых он хочет уведомить администратора компьютера. Текстовые описания этих событий хранятся внутри приложения. В журнал событий помещается только номер события и параметры. Когда консоль отображает содержимое журнала, она сначала находит в приложении описание события по его номеру, затем подставляет параметры и выводит на экран результат.

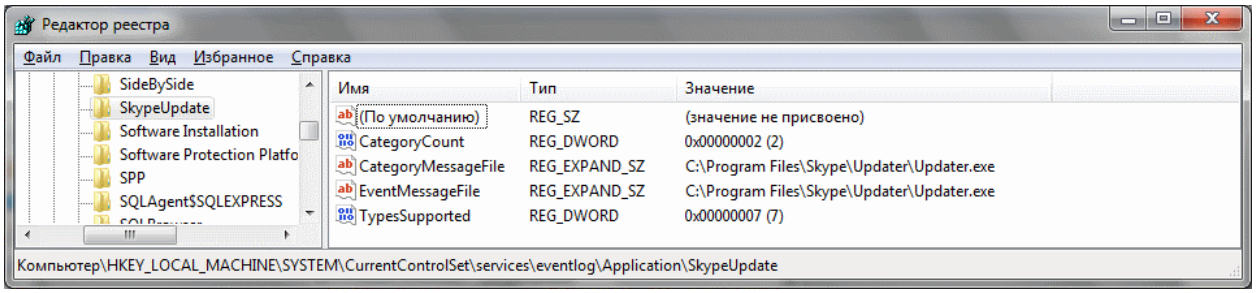


Рис. 9.30. Информация о журнале событий в реестре Windows

Журналы событий обычно содержат огромное количество событий, большинство из которых не представляют интереса, так как они происходят регулярно и лишь фиксируют принятый порядок вещей, например, успешный запуск многочисленных служб.

Есть по крайней мере две ситуации, когда нужно ограничить вывод информации какой-то частью: 1) поиск неисправности в какой-либо подсистеме; 2) младшему администратору делегировали часть административных функций, например, управление DNS-сервером, и ему нужно видеть только свои события. Порядок действий в обоих случаях сходен. Поэтому рассмотрим процесс на примере поиска событий об обновлении Skype.

Если операция поиска разовая и нет необходимости выполнять ее многократно на регулярной основе, то нужно использовать фильтрацию текущего журнала (рис. 9.31).

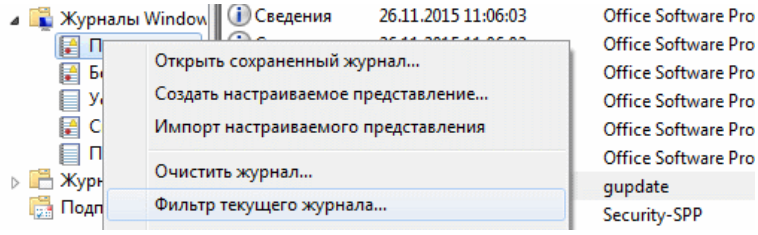


Рис. 9.31. Включение фильтра для текущего журнала

В открывшемся окне указать критерии поиска. Можно ограничить диапазон поиска по времени, выбрать уровни событий, источники, коды и другие параметры (рис. 9.32).

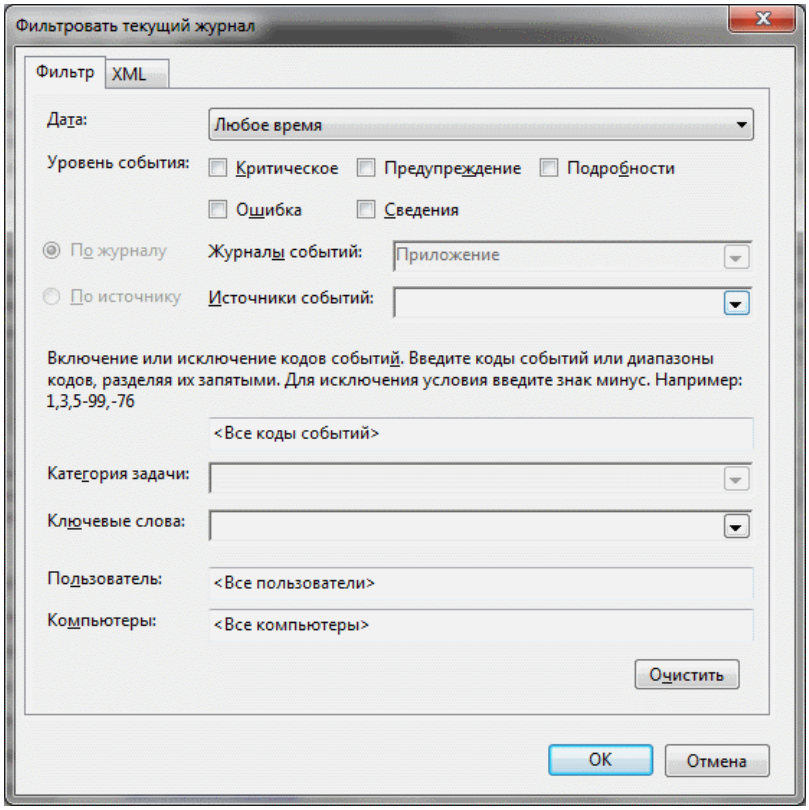


Рис. 9.32. Диалоговое окно для настройки фильтра журнала

Для нашей задачи нужно выбрать все уровни событий и источник данных SkypeUpdate, затем нажать OK.

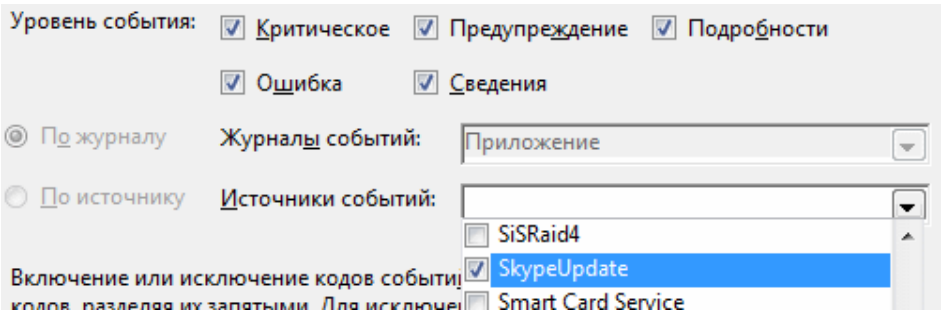


Рис. 9.33. Выбор источников событий для фильтра журнала

После выполнения этих действий в рабочей панели консоли останутся лишь события с источником SkypeUpdate, все остальные исчезнут (рис. 9.34). Чтобы не ввести в заблуждение администратора, в режиме фильтрации в верхней части панели отображается информационное сообщение с параметрами фильтрации.

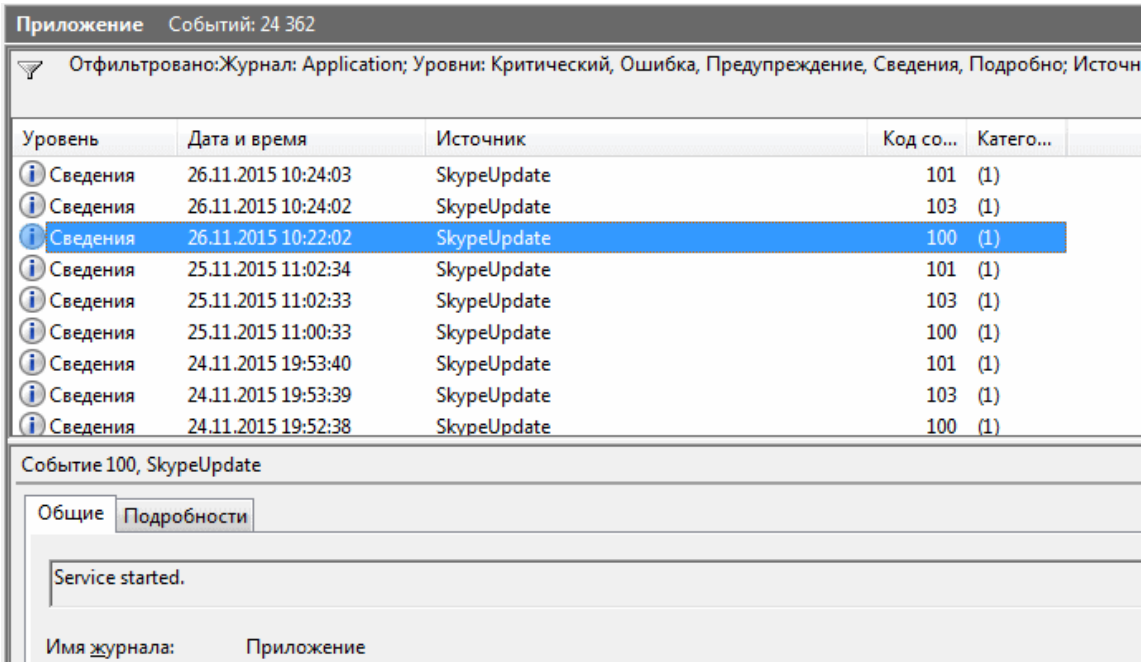


Рис. 9.34. Информационное сообщение о фильтрации

Из скриншота выше мы видим, что ежедневно запускается служба SkypeUpdate (событие 100), через две минуты срабатывает таймаут по ничегонеделанию (событие 103) и еще через секунду служба останавливается (событие 101). Это регулярное поведение, и такое поведение должно и такая последовательность событий может игнорироваться при ежедневном анализе.

Чтобы выключить фильтрацию, нужно выбрать команду **Очистить фильтр** (рис. 9.35). После этого снова будут отображаться все события.

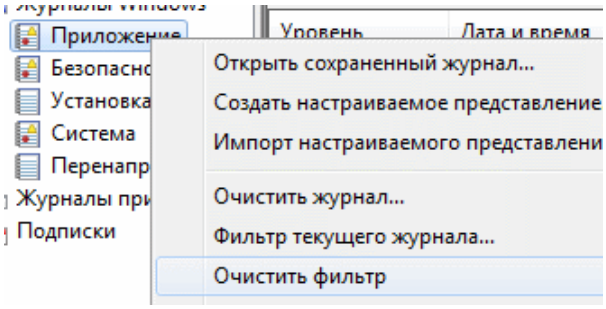


Рис. 9.35. Команда Очистить фильтр

9.2.2. Создание настраиваемых представлений

Если администратор отвечает за некоторый круг обязанностей, и ему интересен лишь некоторое подмножество событий, за которым он будет следить очень часто, то ему следует создать настраиваемое представление (Custom View). Для этого нужно щелкнуть правой кнопкой мыши на узле **Настраиваемые представления** и выбрать команду **Создать настраиваемое представление…** (рис. 9.36).

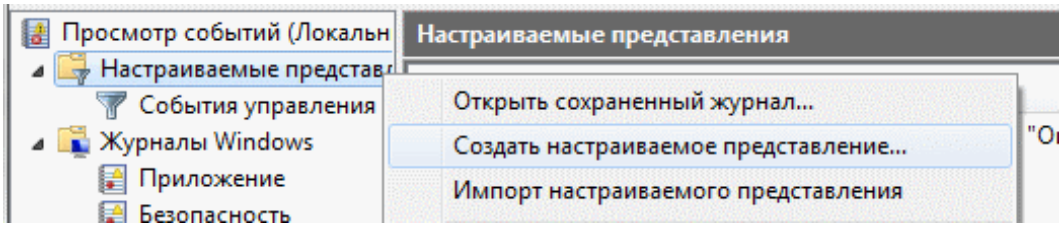


Рис. 9.36. Создание настраиваемого представления

Откроется такое же окно, как и при создании фильтра, отличающееся только заголовком (рис. 9.37).

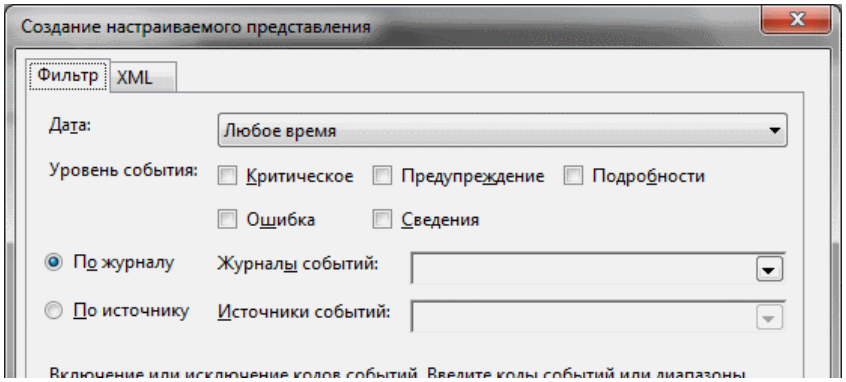


Рис. 9.37. Окно настройки фильтра для настраиваемого представления

Нужно заполнить критерии отбора событий и нажать **ОК**. Появится окно, в котором нужно дать имя настраиваемому представлению и указать его место в дереве представлений (рис. 9.38), затем нажать **ОК**. Здесь же можно создать папки для группировки представлений.

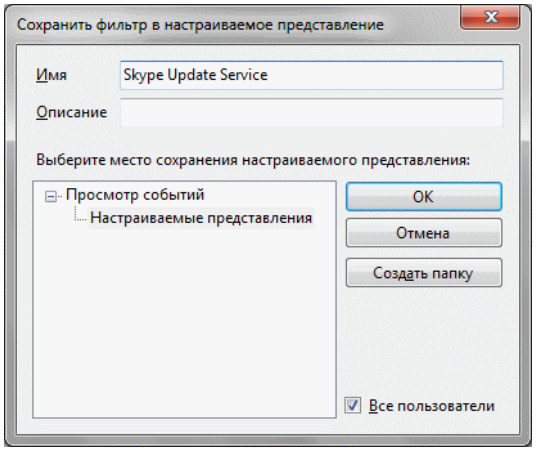


Рис. 9.38. Сохранение фильтра для настраиваемого представления

Теперь представление всегда можно увидеть на его месте (рис.9.39).

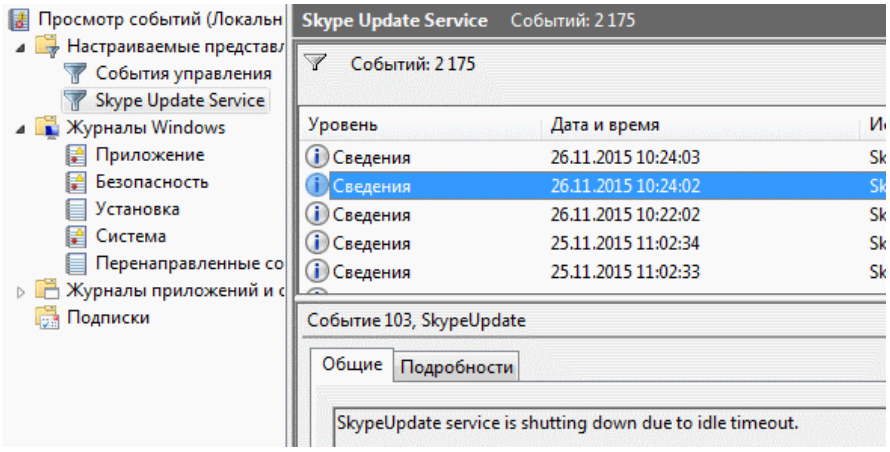


Рис. 9.39. Узел настраиваемых представлений в консоли Просмотр событий

9.3. Методика устранения неисправностей

Когда происходит сбой системы или событие, влияющее на производительность системы, вы должны иметь возможность исправить проблему или решить проблему быстро и эффективно. С таким большим количеством переменных и возможностей в современной сетевой среде способность быстро определять основную причину зависит от наличия логической и всеобъемлющей методологии устранения неполадок. Вы также должны понимать доступные инструменты, чтобы определить основную причину и внести исправления в окружающую среду, если это возможно.

9.3.1. Разработка методологии устранения неполадок

Устранение неполадок, особенно при работе с технологией, может быть многоэтапным процессом с большим количеством потенциальных корневых причин и несколькими попытками решить проблему до того, как будет определена фактическая первопричина. Методология устранения неполадок может помочь организовать весь процесс устранения неполадок от начального сбора информации до тестирования возможных исправлений для обеспечения правильной работы исправлений и ее поддержки.

Основные понятия и методы должны быть поняты и соблюдаться на протяжении всего процесса устранения неполадок, чтобы обеспечить решение проблемы наиболее эффективным способом.

Оценка воздействия

Понимание того, как проблема влияет на сетевую среду и операции вашей организации, является очень важной частью процесса устранения неполадок. Для проблемы, которая влияет на критически важные сервисы, такие как операции с пунктами продажи в загруженном розничном магазине, может потребоваться временное частичное исправление или обходное решение, до тех пор, пока не будет определена и исправлена основная причина проблемы.

По мере продолжения процесса устранения неполадок временное исправление, возможно, потребуется переоценить, чтобы обеспечить максимально возможную поддержку остальной среды. Наконец, как только исходная проблема была определена и исправлена, метод замены временного исправления постоянным решением должен быть определен и реализован таким образом, который оказывает наименьшее влияние на действия вашей организации.

Коммуникация с клиентами

Почти каждая проблема, которую вы устраняете, повлияет на хотя бы одного человека в вашей организации. Те, кто пострадал, должны конкретно знать, как эта проблема повлияет на них в будущем. Кроме того, они должны быть проинформированы о ходе процесса устранения неполадок, временных оценках для разрешения и изменений процесса, которые могут потребоваться от них из-за временного исправления. Когда проблема была исправлена, и среда вернулась в полностью работоспособное состояние, им также необходимо получить уведомление о том, что проблема устранена. Все эти предметы относятся к категории коммуникаций.

Коммуникация является одним из наиболее важных компонентов процесса устранения неполадок и часто игнорируется. Коммуникация может состоять из личного общения, телефонных звонков, электронных писем или обновления билета службы поддержки с прогрессом в устранении неполадок.

Если есть ряд людей, затронутых проблемой, ваши методы коммуникации, возможно, необходимо будет скорректировать, чтобы гарантировать, что информация достигает заинтересованных лиц наиболее эффективно. Например, если проблема затрагивает весь отдел, вы можете выбрать одного человека из этого отдела, обычно менеджера, для непосредственного общения. Любая информация о процессе устранения неполадок затем передается менеджером другим сотрудникам отдела. Это гарантирует, что вы сможете сосредоточиться на процессе устранения неполадок и возлагаете на менеджера ответственность за то, чтобы его сотрудники знали о состоянии и ходе процесса устранения неполадок.

Документация

На протяжении всего процесса устранения неполадок документация должна поддерживаться на всех уровнях. Исходные симптомы, затронутые люди и системы, потенциальные причины, а также неудачные и успешные попытки решить проблему необходимо записать и соответствующим образом задокументировать, чтобы обеспечить постоянный прогресс в процессе устранения неполадок.

Невозможность документировать процесс устранения неполадок может привести к игнорированию симптомов, недопониманию или сбою в работе, неудачным попыткам решения, предпринимаемым несколько раз, или даже к возврату к нормальной работе, не зная специфики разрешения или если было завершено постоянное исправление. Как только проблема будет решена, ваша надлежащая документация по разрешению и шаги, предпринятые для достижения этой резолюции, могут помочь вам ускорить процесс устранения неполадок по аналогичным вопросам.

9.3.2. Этапы типичной методологии устранения неполадок

В любой методологии устранения неполадок, особенно в тех случаях, когда несколько человек могут участвовать в процессе устранения неполадок, важно иметь установленный процесс устранения неполадок. При использовании этого процесса, обнаруженная проблема проходит через несколько этапов, каждый из которых приближает вопрос к окончательному решению.

1. **Определите проблему**. Первым шагом в процессе устранения неполадок является правильное определение проблемы. Это означает, что вы получили конкретную информацию о симптомах, наблюдаемых теми, кто испытывает эту проблему. Это может состоять из физических описаний от конечных пользователей (мой экран был пустым, когда я нажал кнопку запуска) или наблюдение за проблемой самостоятельно. Обеспечение того, чтобы вы понимали масштаб и факты проблемы, очень важны. Неправильная или неполная информация может привести к неправильным предположениям об устранении неполадок и может привести к устранению всех предполагаемых основных причин без фактического разрешения.

2. **Соберите исходную информацию**. Следующим шагом в этом процессе является сбор соответствующей информации о проблеме. Как правило, эта сборка состоит из действий, таких как расширенное наблюдение за симптомами, проведение диагностических тестов на пораженном аппаратном и программном обеспечении или получение технической информации от поставщиков или поставщиков затронутых предметов.

3. **Определите вероятные причины проблемы**. После того как соответствующая информация будет собрана, список вероятных причин должен быть записан и, как правило, ранжирован, чтобы сначала выявить наиболее вероятные причины. По мере продолжения процесса устранения неполадок причины проверяются один за другим, это может привести к устранению причин, отличных от проверяемой причины. Это также может привести к добавлению новых причин в список в результате большей информации, собранной во время тестирования.

4. **Разработайте план действий**. Затем вы должны определить план действий для проверки наиболее вероятной причины или причин. Этот план может включать один или несколько шагов и должен быть документирован, чтобы убедиться, что он выполнен правильно и что его можно повторить при необходимости в процессе устранения неполадок.

Кроме того, ваш план развития должен позволить откат после реализации, если план действий не решит проблему.

5. **Внедрите план действий**. После того, как план будет установлен, план должен быть реализован и процесс документирован.

6. **Проверьте результаты плана действий**. После того как реализация плана будет завершена, вы должны проверить среду, чтобы определить, исправлена ли проблема. Вы также должны убедиться, что ваши действия не оказали негативного влияния на затронутые системы и пользователей.

7. **Документируйте результаты плана действий и повторите шаги плана действий, если это необходимо**. Затем результаты вашего плана действий должны быть задокументированы. Если результат плана действий скорректировал вопрос удовлетворительным образом, вы должны перейти к последнему этапу закрытия проблемы и доработать документацию. Если ваш план действий не увенчался успехом, вы должны отменить шаги плана действий. Затем переходите к следующей вероятной причине в списке и начинайте шаги плана действий по этой причине, повторяя процесс до тех пор, пока причина не будет определена и не будет достигнуто разрешение.

8. **Пометьте проблему как решенную и обновите документацию**. После того как вы определили проблему как решенную, любые временные исправления или обходные пути должны быть удалены и затронутые пользователи должны быть проинформированы о разрешении. Кроме того, документация по разрешению и шаги, предпринятые в процессе устранения неполадок, должны быть завершены и записаны таким образом, чтобы обеспечить последующую ссылку или каталогизацию. Это может быть с помощью специализированного приложения для службы техподдержки, документа Microsoft Office Word или Microsoft Office Excel® или просто записи в блокноте.

9.4. Другие программы для мониторинга

9.4.1. Zabbix

Zabbix — это решение распределенного мониторинга корпоративного класса с открытыми исходными кодами, созданное Алексеем Владышевым. настоящее время активно разрабатывается и поддерживается компанией Zabbix SIA.

Zabbix предназначен для мониторинга многочисленных параметров сети, жизнеспособности и целостности серверов. Zabbix использует гибкий механизм оповещений, что позволяет пользователям конфигурировать основанные на e-mail уведомления практически для любого события. Это позволяет быстро реагировать на проблемы с серверами. Zabbix предлагает отличные функции отчетности и визуализации данных, основанные на данных истории.

Zabbix поддерживает как опрос узлов, так и отправку сведений. Все отчеты и статистика Zabbix, также как и параметры настройки, доступны через Веб-интерфейс (рис. 9.40). Веб-интерфейс обеспечивает доступ к информации о состоянии вашей сети и жизнеспособности ваших серверов из любого места. Правильно настроенный Zabbix может сыграть важную роль в мониторинге ИТ инфраструктуры. Это верно и для маленьких организаций с несколькими серверами и для больших организаций со множеством серверов.

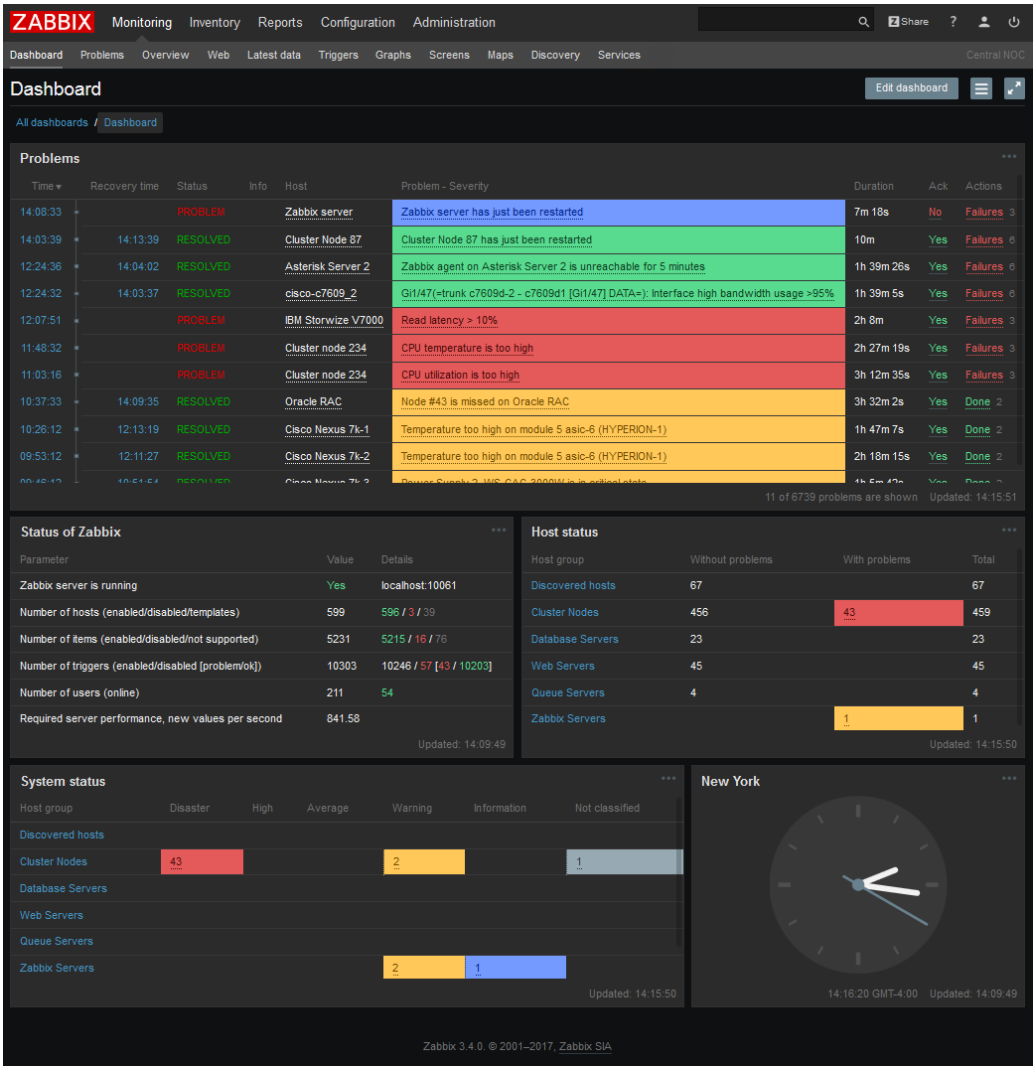


Рис. 9.40. Внешний вид панели управления Zabbix

Источник: https://habrahabr.ru/company/zabbix/blog/336084/

Zabbix бесплатен. Zabbix написан и распространяется под лицензией GPL General Public License версии 2. Это означает, что его исходный код свободно распространяется и доступен для неограниченного круга лиц. Коммерческая поддержка доступна и осуществляется самой компанией Zabbix.

Для хранения данных используется MySQL, PostgreSQL, SQLite или Oracle Database, веб-интерфейс написан на PHP. Поддерживает несколько видов мониторинга:

Simple checks — может проверять доступность и реакцию стандартных сервисов, таких как SMTP или HTTP, без установки какого-либо программного обеспечения на наблюдаемом хосте;

Zabbix agent — может быть установлен на UNIX-подобных или Windows-хостах для получения данных о нагрузке процессора, использования сети, дисковом пространстве и так далее;

External check — выполнение внешних программ, также поддерживается мониторинг через SNMP.

Основные возможности:

- Распределённый мониторинг — до нескольких тысяч узлов. Конфигурация младших узлов полностью контролируется старшими узлами, находящимися на более высоком уровне иерархии.
- Сценарии на основе мониторинга;
- Автоматическое обнаружение;
- Централизованный мониторинг журналов
- Веб-интерфейс для администрирования и настройки
- Отчётность и тенденции
- SLA-мониторинг
- Поддержка высокопроизводительных агентов (zabbix-agent) практически для всех платформ
- Комплексная реакция на события
- Поддержка SNMP v1, 2, 3
- Поддержка SNMP-ловушек
- Поддержка IPMI
- Поддержка мониторинга JMX-приложений
- Поддержка выполнения запросов в различные базы данных без необходимости использования сценарной обвязки
- Расширение за счёт выполнения внешних скриптов
- Гибкая система шаблонов и групп
- Возможность создавать карты сетей.

Поддерживаемые платформы (сервер и агент): AIX, FreeBSD, HP-UX, Linux, Mac OS, OpenBSD, SCO OpenServer, Solaris, Tru64/OSF; кроме того, реализованы агенты для Novell Netware и операционных систем семейства Windows.

Архитектура

Zabbix состоит из нескольких основных программных компонентов, функции которых изложены ниже.

Сервер

Zabbix сервер является основным компонентом, которому агенты сообщают информацию и статистику о доступности и целостности. Сервер является главным хранилищем, в котором хранятся все данные конфигурации, статистики, а также оперативные данные.

База данных

Как таковая вся информация о конфигурации, а так же данные собранные Zabbix, хранятся в базе данных.

Веб-интерфейс

Для легкого доступа к Zabbix из любого места и с любой платформы, поставляется интерфейс на основе Веб. Интерфейс является частью Zabbix сервера и обычно (но не обязательно) работает на том же самой физической машине, что и сервер.

Прокси

Zabbix прокси может собирать данные о производительности и доступности от имени Zabbix сервера. Прокси является опциональной частью Zabbix; однако он может быть полезен чтобы распределить нагрузку одного Zabbix сервера.

Агент

Zabbix агенты разворачиваются на наблюдаемых системах для активного мониторинга за локальными ресурсами и приложениями, и для отправки собранных данных Zabbix серверу или прокси.

Поток данных

Кроме того, важно сделать шаг назад и взглянуть на весь поток данных в Zabbix. Для того чтобы создать элемент данных, который будет собирать данные, вы должны сначала создать узел сети. Перемещаясь в другой конец спектра Zabbix, у вас должен быть элемент данных, чтобы создать триггер. У вас должен быть триггер, чтобы создать действие.

Таким образом, если вы хотите получать оповещения о слишком высокой загрузке CPU на Сервере X, вы сначала должны создать запись о узле сети для Сервера X, затем элемент данных для наблюдения за CPU, затем триггер, который сработает, если загрузка CPU будет слишком высокой, а затем действие которое отправит вам email.

Хотя может показаться, что требуется слишком много шагов, использование шаблонов значительно упрощает процесс. Однако, такое построение системы позволяет создавать очень гибкие инсталляции.

Документацию по Zabbix можно найти по следующей ссылке.

Zabbix documentation in Russian
https://www.zabbix.com/documentation/3.2/ru/start

9.4.2. Pandora FMS

Pandora FMS (для Pandora Flexible Monitoring System) — программное обеспечение для мониторинга компьютерных сетей (рис. 9.41). Pandora FMS позволяет визуализировать состояние и производительность нескольких параметров из разных операционных систем, серверов, приложений и аппаратных систем, таких как брандмауэры, прокси, базы данных, веб-серверы или маршрутизаторы.

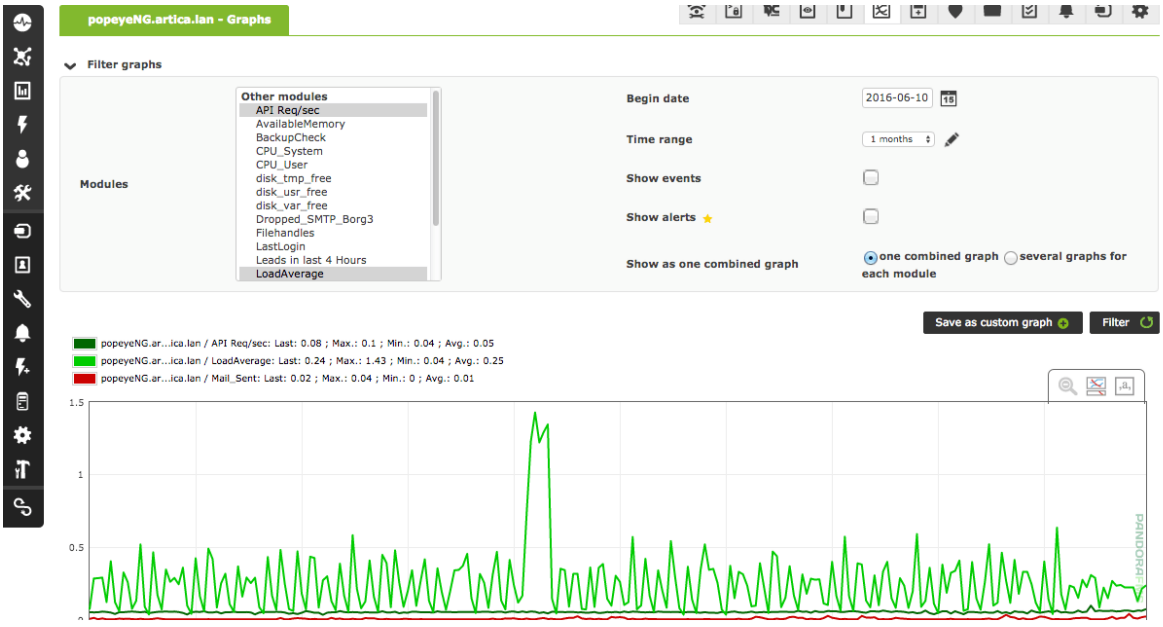


Рис. 9.41. Отображение средней нагрузки в программе Pandora FMS

Источник: https://blog.pandorafms.org/zabbix-vs-nagios-vs-pandorafms-an-in-depth-comparison/

Pandora FMS может быть развернута практически в любой операционной системе. Он имеет удаленный мониторинг (WMI, SNMP, TCP, UDP, ICMP, HTTP ...), а также может использовать агенты. Агент доступен для каждой платформы. Он также может контролировать аппаратные системы с стеком TCP / IP, такими как балансировочные балансы нагрузки, маршрутизаторы, сетевые коммутаторы, принтеры или брандмауэры.

Pandora FMS имеет несколько серверов, которые обрабатывают и получают информацию из разных источников, используя WMI для сбора удаленной информации Windows, интеллектуального сервера, подключаемого сервера, который делает сложные пользовательские сетевые тесты, расширенный сервер экспорта для репликации данных между различными сайтами Pandora FMS, сервера обнаружения сети и консоли SNMP Trap. Архитектура программы показана на рис. 9.42.

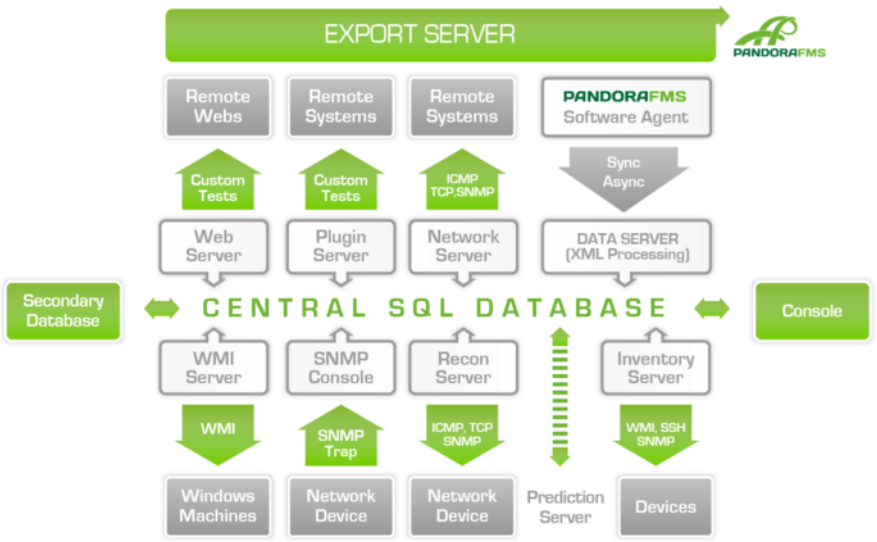


Рис. 9.42. Архитектура программы Pandora FMS
Источник: https://en.wikipedia.org/wiki/Pandora_FMS

Pandora FMS выпущена на условиях GNU General Public License, и является бесплатным программным обеспечением.

9.4.3. Nagios

Nagios — программа с открытым кодом, предназначенная для мониторинга компьютерных систем и сетей: наблюдения, контроля состояния вычислительных узлов и служб, оповещения администратора в том случае, если какие-то из служб прекращают (или возобновляют) свою работу (рис.9.43).

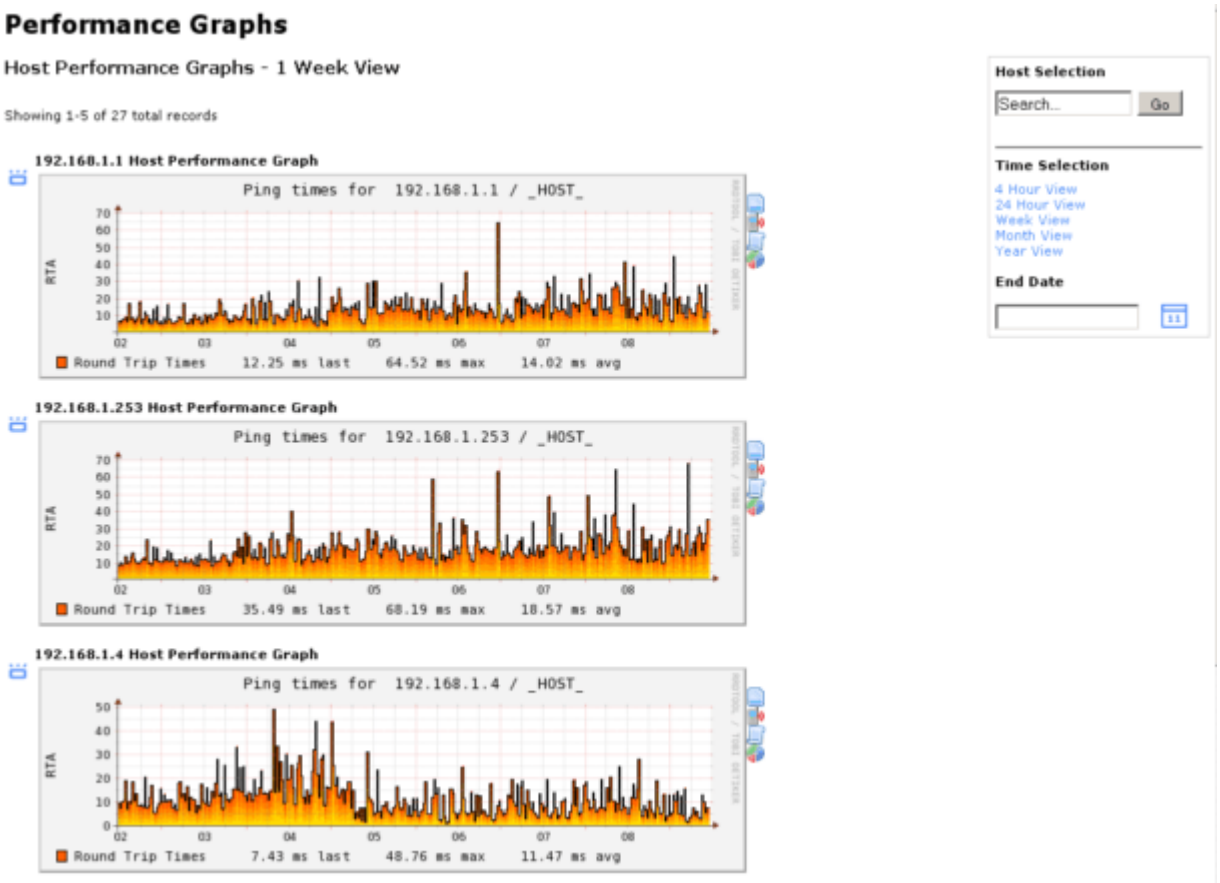


Рис.9.43. Диаграммы производительности в программе Nagios
Источник: https://blog.pandorafms.org/zabbix-vs-nagios-vs-pandorafms-an-in-depth-comparison/

Nagios первоначально была создана под именем Netsaint, разработана Этаном Галстадом (Ethan Galstad). Он же поддерживает и развивает систему сегодня, совместно с командой разработчиков, которые занимаются как официальными, так и неофициальными плагинами.

Первоначально Nagios была разработана для работы под Linux, но она также хорошо работает и под другими ОС, такими как Sun Solaris, FreeBSD, AIX и HP-UX.

Обзор возможностей:

- Мониторинг сетевых служб (SMTP, POP3, HTTP, NNTP, ICMP, SNMP)
- Мониторинг состояния хостов (загрузка процессора, использование диска, системные логи) в большинстве сетевых операционных систем
- Поддержка удаленного мониторинга через шифрованные туннели SSH или SSL
- Простая архитектура модулей расширений (плагинов) позволяет, используя любой язык программирования по выбору (Shell, C++, Perl, Python, PHP, C# и другие), легко разрабатывать свои собственные способы проверки служб
- Параллельная проверка служб
- Возможность определять иерархии хостов сети с помощью «родительских» хостов, позволяет обнаруживать и различать хосты, которые вышли из строя, и те, которые недоступны
- Отправка оповещений в случае возникновения проблем со службой или хостом (с помощью почты, пейджера, смс, или любым другим способом, определенным пользователем через модуль системы)
- Возможность определять обработчики событий произошедших со службами или хостами для проактивного разрешения проблем
- Автоматическая ротация лог-файлов
- Возможность организации совместной работы нескольких систем мониторинга с целью повышения надёжности и создания распределенной системы мониторинга
- Включает в себя утилиту nagiostats, которая выводит общую сводку по всем хостам, по которым ведется мониторинг.

9.4.4. Ganglia

Ganglia — масштабируемая распределённая система мониторинга кластеров параллельных и распределённых вычислений и облачных систем с иерархической структурой. Позволяет отслеживать статистику и историю (загруженность процессоров, сети) вычислений в реальном времени для каждого из наблюдаемых узлов.

Проект создан в 1998 году в Калифорнийском университете в Беркли как продолжение проекта Millennium, который был инициирован Национальным научным фондом США.

Система построена по иерархическому принципу для интеграции кластеров. Для мониторинга состояния кластеров и их объединения используется древовидная система, основанная на P2P-соединениях и широковещательных протоколах.

Использует такие технологии, как XML для представления данных, XDR для сжатия данных, RRDtool для хранения и визуализации данных. Для отображения страниц статистики используется шаблонизатор TemplatePower[6].

Система портирована на широкий спектр операционных систем и процессорных архитектур, известно об её использовании более чем 500 кластерах по всему миру. Существуют сборки для следующих операционных систем: Linux (i386, x86-64, SPARC, DEC Alpha, powerpc, m68k, MIPS, ARM, PA-RISC, S390), FreeBSD, NetBSD, OpenBSD, DragonflyBSD, Mac OS X, Solaris (SPARC), AIX, IRIX, Tru64, HP-UX и Windows NT/XP/2000/2003/2008[7]. Используется для связи кластеров в университетских кампусах по всему миру и может масштабироваться для обработки кластеров имеющих до 2000 узлов в своем составе.

Необходимые пакеты для установки Ganglia присутствуют в большинстве репозиториев современных дистрибутивов Linux.