ТЕМА 4.1. ВВЕДЕНИЕ В ОПЕРАЦИОННУЮ СИСТЕМУ WINDOWS

В данной теме рассматриваются следующие вопросы:

- Принципы организации и структура ОС Windows.
- Принцип модульной структуры ОС Windows.
- Обзор версий Windows.
- Методы инсталляции ОС Windows.
- Организация рабочей среды пользователя.
- Работа с учетными записями пользователей и групп.
- Работа с профилями пользователей.
- Работа с файловой системой.
- Настройка обработки файлов с определенным расширением.
- Мониторинг и оптимизация системы.

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

Экзаменационные вопросы по теме:

- Принципы организации и структура ОС Windows. Обзор версий Windows. Методы инсталляции ОС Windows.
- ОС Windows: организация рабочей среды пользователя, работа с учетными записями пользователей и групп, работа с профилями пользователей.

4.1.1. Принципы организации и структура ОС Windows

Архитектура операционной системы Windows включает ядро операционной системы, системные службы и приложения [1].

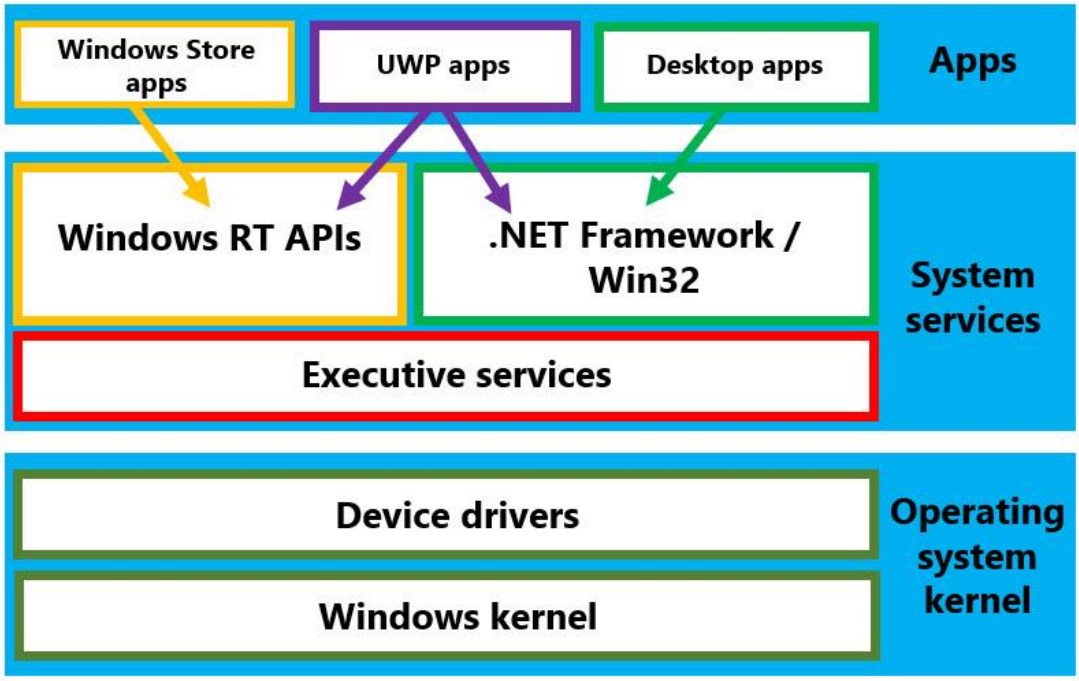


Рис. 4.1.1. Архитектура клиентских версий операционной системы Windows

Ядро операционной системы

На самом низком уровне операционной системы ядро операционной системы состоит из самого ядра Windows и драйверов устройств низкого уровня. Ядро отвечает за прием запросов операционной системы от системных служб. Затем ядро преобразует эти запросы в инструкции для аппаратного обеспечения компьютера, включая центральный процессор (ЦП), память и аппаратные устройства.

При запуске операционной системы сначала инициализируются ядро и связанные с ним низкоуровневые драйверы устройств, а затем службы операционной системы.

Системные службы

Службы операционной системы являются частью операционной системы, а не компонентами, которые вы устанавливаете после развертывания операционной системы. Кроме того, службы операционной системы функционируют без каких-либо действий со стороны пользователя. Фактически они начинаются до того, как пользователь войдет в систему.

И службы операционной системы, и драйверы устройств являются программным обеспечением. Однако разница между ними заключается в том, что драйверы устройств напрямую взаимодействуют с аппаратными устройствами или компонентами. Как правило, системная служба взаимодействует с другими программными компонентами операционной системы.

> *Примечание. С точки зрения управления разница между драйверами устройств и службами более очевидна. Для управления драйверами устройств можно использовать инструмент «Диспетчер устройств», а для управления системными службами — инструмент оснастки консоли управления Microsoft (MMC).*

Системные службы включают в себя различные исполнительные службы, которые обеспечивают различные функции в операционной системе, в том числе:

- Диспетчер ввода-вывода управляет вводом-выводом.
- Диспетчер виртуальной памяти управляет виртуализацией памяти в операционной системе.
- Другие компоненты исполнительной власти контролируют другие аспекты операционной системы.
- Наборы интерфейсов прикладного программирования (API) позволяют Windows поддерживать различные типы приложений. API-интерфейсы среды выполнения Windows (RT) позволяют операционной системе запускать приложения Microsoft Store, тогда как Win32 и связанные наборы API позволяют операционной системе запускать традиционные настольные приложения.

Понимание приложений

На верхнем уровне операционной системы приложения работают путем взаимодействия с пользователем компьютера, а на нижнем уровне — путем интеграции со службами операционной системы. Вы устанавливаете приложения после установки операционной системы, и для их использования вам необходимо запускать приложения вручную.

Начиная с Windows 8.1, Microsoft разработала Windows для поддержки двух разных стилей приложений. Это включало изменение архитектуры операционной системы Windows для обеспечения двух стеков API следующим образом:

- Традиционные настольные приложения, такие как приложения Office, используют API-интерфейсы Win32 и Microsoft .NET Framework.
- Приложения Microsoft Store используют API-интерфейсы Windows RT.

Преимущество этого подхода с двойным стеком заключается в том, что одна и та же операционная система может поддерживать две разные платформы приложений.

В Windows 10 представлена универсальная платформа Windows (UWP), которая представляет собой развитие модели среды выполнения Windows, предоставляющей общую платформу приложений для каждого устройства, способного работать под управлением Windows 10 или более поздней версии. Приложения, разработанные для UWP, могут вызывать API-интерфейсы Win32 и Microsoft .NET Framework, а также API-интерфейсы Windows RT. Это означает, что разработчики могут создать одно приложение, которое будет работать на всех устройствах.

Отличия службы от приложения

Служба – процесс, работающий, даже когда никто не зарегистрирован в системе.

Служба использует несколько потоков.

- Один поток принимает команды от операционной системы (Start, Stop, Pause, Resume и т.п.)
- Второй поток является основным рабочим потоком (обычно он создает еще множество потоков для выполнения отдельных задач). Завершение этого потока завершает работу всей службы.

Управляются диспетчером управления службами (Service Control Manager, SCM).

Службы запускаются в сеансе 0, с активными целостностью системы (System Integrity) и предотвращением выполнения данных (Data Execution Prevention, DEP), содержат идентификатор безопасности, виртуализация файлов и реестра отключены.

Физически может находиться в .EXE или .DLL-файле.

В одном файле может находиться множество служб.

Если служба находится в .DLL-файле, ее запускает `svchost.exe`.

Сравнение служб и драйверов

Информация о службах и драйверах хранится в одном и том же разделе реестра. Различить их можно по параметрам **Start** и **Type**

Параметр **Type** для служб: 10 (автономная), 20 (разделяемая), 110 (интерактивная)

Параметр **Type** для драйверов: 1 (драйвер ядра), 2 (драйвер файловой системы)

Параметр **Start** для служб: 2 (автоматический), 3 (ручной), 4 (отключена)

Параметр **Start** для драйверов: 0 (загрузка), 1 (система)

Реестр Windows

Реестр — это база данных, в которой Windows хранит параметры конфигурации пользователя и компьютера. Всякий раз, когда вы вносите изменения в конфигурацию Windows, это изменение фиксируется в реестре [2].

Реестр Windows организован иерархически. На верхнем уровне имеется пять кустов реестра, которые представляют собой отдельный набор связанных параметров, структурированных как серия ключей, подразделов и значений.

4.1.2. Принцип модульной структуры ОС Windows

Операционная система Windows имеет модульную структуру, что обеспечивает ее работу на самых разных аппаратных платформах, с самыми разными приложениями. Кроме того, этим достигается относительно эффективная возможность модернизации ОС (либо путем замены каких-либо отдельных структурных блоков, либо путем включения новых блоков) [3].

Принцип модульной структуры состоит в том, что за реализацию каждой из функций ОС отвечает отдельный модуль. Все остальные части системы и приложения обращаются к этой функции через стандартный интерфейс. А доступ к основным системным данным можно получить только через определенные функции.

Windows – одна из наиболее многогранных и гибких ОС, она работает на совершенно разных архитектурах и доступна в разных вариантах. На сегодня она поддерживает архитектуры x86, x64, ARM и ARM64. Windows в своё время поддерживала Itanium, PowerPC, DEC Alpha и MIPS. Кроме того, Windows поддерживает целый набор SKU, работающих в различных условиях; от дата-центров, ноутбуков, Xbox и телефонов до встраиваемых версий для интернета вещей, например, в банкоматах [4].

Самый удивительный аспект состоит в том, что ядро Windows практически не меняется в зависимости от всех этих архитектур и SKU. Ядро динамически масштабируется в зависимости от архитектуры и процессора, на котором оно работает, так, чтобы пользоваться всеми возможностями оборудования. Конечно, в ядре присутствует определённое количество кода, связанного с конкретной архитектурой, однако его там минимальное количество, что позволяет Windows запускаться на разнообразных архитектурах.

Windows NT – это, по сути, микроядро, в том смысле, что у него есть своё core Kernel (KE) с ограниченным набором функций, использующее исполняемый уровень (Executive layer, Ex) для выполнения всех политик высокого уровня. EX всё ещё является режимом ядра, так что это не совсем микроядро. Ядро отвечает за диспетчеризацию потоков, синхронизацию между процессорами, обработку исключений аппаратного уровня и реализацию низкоуровневых функций, зависящих от железа. Слой EX содержит различные подсистемы, обеспечивающие набор функциональности, который обычно считается ядром – IO, Object Manager, Memory Manager, Process Subsystem, и т.д.

В Windows 10 появилась поддержка ARM64. Архитектура ARM поддерживает архитектуру big.LITTLE, гетерогенную по своей природе – «большое» ядро работает быстро и

потребляет много энергии, а «малое» ядро работает медленно и потребляет меньше. Идея в том, что малозначительные задачи можно выполнять на малом ядре, экономя таким образом батарею. Для поддержки архитектуры big.LITTLE и увеличения времени работы от батареи при работе Windows 10 на ARM, в планировщик добавили поддержку гетерогенной планировки, учитывающую пожелания приложения, работающего с архитектурой big.LITTLE.

Папка WinSxS

То, что операционная система Windows состоит из многих модулей, можно увидеть, заглянув в папку C:\Windows\WinSxS (SxS означает Side by Side).

WinSxS — служебная папка, которая появилась еще в Windows Vista, и присутствует во всех последующих версиях операционной системы [5].

Здесь хранятся файлы обновлений, конфигурационные данные, резервные копии файлов. Это каталог хранилища компонентов Windows. Именно благодаря ему пользователь может откатить практически любые изменения системы или установить дополнительные компоненты. Содержимое WinSxS используется в откате операционной системы к первоначальным настройкам, а также необходимо для работы Windows.

4.1.3. Обзор версий Windows

Сначала рассмотрим клиентские версии Windows.

Прежде чем устанавливать Windows, важно выбрать наиболее подходящую для вашей организации редакцию. Различные выпуски Windows удовлетворяют потребности потребителей, от частных лиц до крупных предприятий. В этом модуле описаны различные функции каждой редакции, доступной для Windows и более поздних версий.

Таблица 4.1.1. Сравнение выпусков Windows 10/11

Windows 10/Выпуск Windows 11	Аудитория	Доступность
Home	Индивидуальное домашнее использование	Каждый
Pro	Малый и средний бизнес, продвинутые пользователи	Каждый
Pro для рабочих станций	Пользователи с повышенными требованиями к производительности и хранилищу	Каждый
Enterprise	Крупные коммерческие организации	Доступно для корпоративной лицензии. Корпоративное лицензирование Microsoft, Соглашение Microsoft Enterprise, Microsoft Store для образовательных учреждений или программа Microsoft Cloud Solution Provider.
Enterprise LTSC	Крупные корпоративные организации с ограничительными требованиями к изменениям	Корпоративное лицензирование Microsoft, Соглашение Microsoft Enterprise или программа поставщика облачных решений Microsoft.

Pro Education	Сравнимо с Pro для сотрудников школы, администраторов, учителей и учащихся.	Доступно для клиентов с корпоративной лицензией для учебных заведений.
Education	Сравнимо с Enterprise для школьного персонала, администраторов, учителей и учащихся.	Доступно для клиентов с корпоративной лицензией для учебных заведений.
IoT Core/ Enterprise	Устройства стационарного назначения и бытовые устройства	Доступно через дистрибьюторов Windows IoT

Подробное описание версий можно найти по следующей ссылке:

https://learn.microsoft.com/en-us/training/modules/explore-windows-editions/2-examine-client-editions-capabilities

Enterprise LTSC

Enterprise Long Term Service Channel (LTSC) — это специальная версия Enterprise, которую Microsoft не будет обновлять новыми функциями. Enterprise LTSC получает только обновления безопасности и другие важные обновления. Вы можете установить Enterprise LTSC на устройства, работающие в известной неизменяемой среде. Типичным примером может служить ПК, используемый как часть медицинской или промышленной системы. Эти среды обычно представляют собой закрытые системы, разработанные с учетом определенной спецификации, на которую могут повлиять традиционные обновления. Различия между Enterprise LTSC и стандартной версией Enterprise включают в себя:

- Не получает обновлений функций
- Нет браузера Microsoft Edge (можно установить отдельно)
- Нет клиента Microsoft Store
- Многие встроенные универсальные приложения для Windows отсутствуют.

Microsoft выпускает обновленную версию выпуска LTSC примерно каждые три года. Windows Enterprise LTSC 2021 — это текущий выпуск, включающий накопительные обновления до версии 21H2 включительно.

Минимальные требования к оборудованию для Windows 10

Для установки Windows 10 устройства должны соответствовать следующим минимальным требованиям к оборудованию [6]:

Процессор: 1 гигагерц (ГГц) или более быстрый процессор или система на кристалле (SOC).

Оперативная память: 1 ГБ для 32-битной версии или 2 ГБ для 64-битной версии.

Место на жестком диске: 16 ГБ для 32-битной версии или 20 ГБ для 64-битной версии.

Видеокарта: DirectX 9 или новее с драйвером Windows Display Driver Model (WDDM) 1.0.

Дисплей: 800x600 пикселей

Минимальные требования к оборудованию для Windows 11

Для установки или обновления до Windows 11 устройства должны соответствовать следующим минимальным требованиям к оборудованию:

Процессор: 1 гигагерц (ГГц) или выше с двумя или более ядрами на совместимом 64-разрядном процессоре или системе на кристалле (SoC).

Оперативная память: 4 гигабайта (ГБ) или больше.

Память: 64 ГБ или больше доступного хранилища.

Для загрузки обновлений и включения определенных функций может потребоваться дополнительное пространство для хранения.

Видеокарта: совместима с DirectX 12 или более поздней версии, с драйвером WDDM 2.0.

Прошивка системы: UEFI, поддержка безопасной загрузки.

TPM: доверенный платформенный модуль (TPM) версии 2.0.

Дисплей: Дисплей высокой четкости (720p), монитор 9 дюймов или больше, 8 бит на цветовой канал.

Подключение к Интернету: подключение к Интернету необходимо для выполнения обновлений, а также для загрузки и использования некоторых функций.

> *Для Windows 11 Home Edition требуется подключение к Интернету и учетная запись Microsoft для завершения настройки устройства при первом использовании.*

Серверные версии Windows Server

Последняя LTSC-версия Windows Server сегодня — это Windows Server 2022. Также поддерживается и Windows Server 2019.

Windows Server 2022 обеспечивает расширенную многоуровневую безопасность, гибридные возможности с Azure и гибкую платформу приложений [7]. Он имеет встроенные возможности защищенного ядра, помогающие защитить оборудование, встроенное ПО и возможности ОС Windows Server от расширенных угроз безопасности. Серверы с защищенным ядром основаны на таких технологиях, как System Guard в Защитнике Windows и безопасности на основе виртуализации, что позволяет снизить риск, связанный с уязвимостями встроенного ПО и современными вредоносными программами.

Соединение также более защищено, чем раньше, благодаря более быстрым и защищенным зашифрованным соединениям HTTPS, стандартному шифрованию SMB AES 256 и ряду других.

По сравнению с более ранними выпусками Server, Windows Server 2022 также улучшает управление гибридными серверами за счет значительно улучшенного управления виртуальными машинами, улучшенного средства просмотра событий и большего количества функций, доступных в Windows Admin Center. В контейнеры Windows внесены улучшения, такие как меньшие размеры изображений для более быстрой загрузки, упрощенная реализация сетевой политики и инструменты контейнеризации для приложений .NET.

Существует три редакции Windows Server 2022:

- Standard
- Datacenter
- Datacenter: Azure Edition

Редакция **Standard** включает основную функциональность, кроме Hotpatching и SDN. Но Storage Replica ограничен одной группой ресурсов до 2TB и количество автоматически лицензируемых машин ограничено двумя.

Редакция **Datacenter** поддерживает все функции, кроме Hotpatching и SMB over QUIC.

Редакция **Datacenter: Azure Edition** является самым премиальным из трех и, как следует из названия, поддерживается в Azure (Azure IaaS или Azure Stack HCI — 21H2) и предлагает определенные функции, недоступные за пределами этих сред (горячее обновление, SMB через QUIC) и расширенная сеть Azure). Особенно полезна здесь функция горячего исправления (Hotpatching), которая позволяет администраторам применять исправления без перезагрузки, а также SMB через QUIC для безопасного доступа к общим файлам через Интернет без хлопот, связанных с настройкой VPN.

Требования к оборудованию:

Оперативная память: минимум 512 МБ

Сетевые адаптеры: Ethernet (не менее 1 гигабит в секунду)

Процессор: 1,4 ГГц, минимум 64-разрядный

Требования к дисковому пространству: минимум 32 ГБ данных.

Другие:

- Прошивка с поддержкой безопасной загрузки и система на базе UEFI 2.3.1c
- Монитор с минимальным разрешением Super VGA (1024 x 768) и графическое устройство
- Доверенный платформенный модуль (TPM), позволяющий получить определенные функции.

В портфолио Microsoft есть еще одна операционная система, основанная на Windows Server, но имеющая другое имя. Это **Azure Stack HCI**. Она имеет собственную сертификацию оборудования, лицензируется по подписке и может быть установлен только на «голое железо», но не на виртуальную машину. В отличие от Server 2022, она получает обновления функций через короткие промежутки времени [8].

Microsoft позиционирует Azure Stack HCI как конкурента Windows Server в области гиперконвергентных инфраструктур. В будущем только он получит все необходимые новые функции для этого варианта использования.

4.1.4. Методы инсталляции ОС Windows

Когда требуется развернуть новые серверы или рабочие станции, то одним из главных вопросов является следующий: будет ли осуществляться сборка и развертывание этих систем вручную, или же процесс развертывания систем будет автоматизирован. Автоматизация развертывания систем не является задачей, которую можно выполнить в течение нескольких часов или дней, во всяком случае, не в первый раз. Наоборот, построение функциональной инфраструктуры развертывания операционных систем требует тщательного планирования, иногда — дорогих лицензий, и многих часов, дней или недель тестирования и настройки образов и механизмов автоматизации. Существует несколько разных вариантов развертывания сервера Windows и настольных операционных систем бизнес-класса. Это могут быть ручная установка, полностью автономные (не обслуживаемые) установки, автономные готовые или дополнительно настроенные установки, а также развертывания заготовленных и, возможно, специально настроенных образов операционной системы.

Ручная установка с использованием установочного носителя

Устанавливать систему вручную не очень сложно. Нужно воспользоваться установочным носителем и пройти все этапы установки, документируя по мере продвижения все настройки.

Этот способ иногда необходим, когда у администратора нет образа, подходящего для определенной аппаратной платформы, или когда регулярно развертывается только небольшое количество систем, а время, необходимое на создание автоматических установок или установок с использованием образов, не ограничено и не является ключевым фактором для организации.

Автономная (необслуживаемая) установка

Автономные установки могут быть полезными при развертывании большого количества настольных компьютеров и серверов, на которых установлено одинаковое оборудование.

Файл автономной установки представляет собой файл, содержащий ответы на все вопросы, задаваемые во время ручной установки. Конфигурационные файлы автономной

установки обычно называют файлами ответов. Опции в некоторых файлах ответов автономной установки могут включать принятие лицензионного соглашения конечным пользователем, ввод лицензионного ключа, вариант форматирования жесткого диска, определение раздела или размера тома для операционной системы и многое другое. Теперь это называется файлом необслуживаемой установки (unattended installation file).

Сервер развертывания Windows выполняет некоторые из задач автономной установки, в основном задачу развертывания готового образа при присоединении к домену Active Directory. Если стандартная установка WDS по каким-то причинам неприемлема, можно создать автономные файлы для выполнения шагов установки: специальное разбиение жестких дисков на разделы, присоединение к домену, создание учетной записи локального администратора и ряд других. Создание и тестирование автономных файлов – утомительное занятие, для которого необходим диспетчер образов систем Windows (Windows System Image Manager) из инструментального набора оценки и развертывания Windows (Windows Assessment and Deployment Kit) или же ручное редактирование XML-файлов.

Установка, сопровождаемая производителем

Некоторые производители поставляют носитель автономной установки, который сразу же после запуска предлагает администратору ответить на несколько вопросов, и оставшаяся часть установки происходит в автономном режиме. Этот распространенный сценарий встречается в секторе розничных продаж для домашних пользователей, а также для серверов и настольных компьютеров, поставляемых с установленными операционными системами.

Эти типы установок обычно включают лицензированное программное обеспечение от поставщика комплектного оборудования (Original Equipment Manufacturer — OEM). Здесь важно сказать следующее: если организация планирует выбрать вариант автономного развертывания серверов или настольных компьютеров с помощью систем развертывания или клонирования образов, то лицензию и носитель для операционной системы OEM использовать нельзя, поскольку это, как правило, противоречит лицензионному соглашению.

Серверные системы часто продаются с уже установленными операционными системами (OEM). Но многие серверы все-таки поставляются без операционных систем и требуют покупки или лицензирования установочного носителя. Многие производители предлагают установочные CD-диски, которые сначала выполняют опрос администратора, а затем по результатам этого опроса создают автономные файлы для установки серверной операционной системы Windows. В зависимости от ситуации и устанавливаемого ПО, это весьма удобный вариант, т.к. обычно он содержит все необходимые для оборудования драйверы и поддерживающее ПО для наблюдения за этим оборудованием.

Создание копий или образов систем

Создание копий или образов систем может быть полезно при развертывании нескольких идентичных настольных компьютеров и серверов. Вы создаете настольный компьютер или сервер, подготавливаете систему для клонирования или создания образа и копируете или захватываете образ системы с помощью средств сторонних разработчиков или средств развертывания от Microsoft, таких как WDS. Продукты Microsoft поддерживают клонирование и создание образов серверов и настольных компьютеров только в том случае, если для генерирования идентификаторов безопасности (Security Identifier — SID) нового компьютера используется утилита Sysprep.exe. Служба Windows Deployment Services может использоваться для развертывания установочных образов, а также специально настроенных или снятых установочных образов на серверах и настольных компьютерах, работающих под управлением Windows.

Microsoft и независимые поставщики программного обеспечения уже многие годы поддерживают создание образов и быстрое развертывание систем Windows. В настоящее время у Microsoft имеются три различных средства развертывания образов: служба развертывания Windows (Windows Deployment Services), диспетчер настроек системного центра (System Center Configuration Manager) и инструментальный набор развертывания Microsoft (Microsoft Deployment Toolkit - MDT). В более ранних версиях Microsoft Windows Server также поставлялись средства развертывания как часть ОС и в виде отдельных пакетов компонентов.

Структура WIM-файла

WIM — это формат образа диска на основе файлов, который впервые был представлен в Windows Vista®. Файлы WIM представляют собой сжатые пакеты, содержащие несколько связанных файлов. Формат WIM-файла оптимизирован для максимального сжатия с использованием LZX или для быстрого сжатия с использованием XPRESS.

Структура файла WIM содержит до шести типов ресурсов: заголовок, файловый ресурс, ресурс метаданных, таблицу поиска, данные XML и таблицу целостности. На рис. 4.1.2 показан общий макет WIM-файла, который содержит два образа.

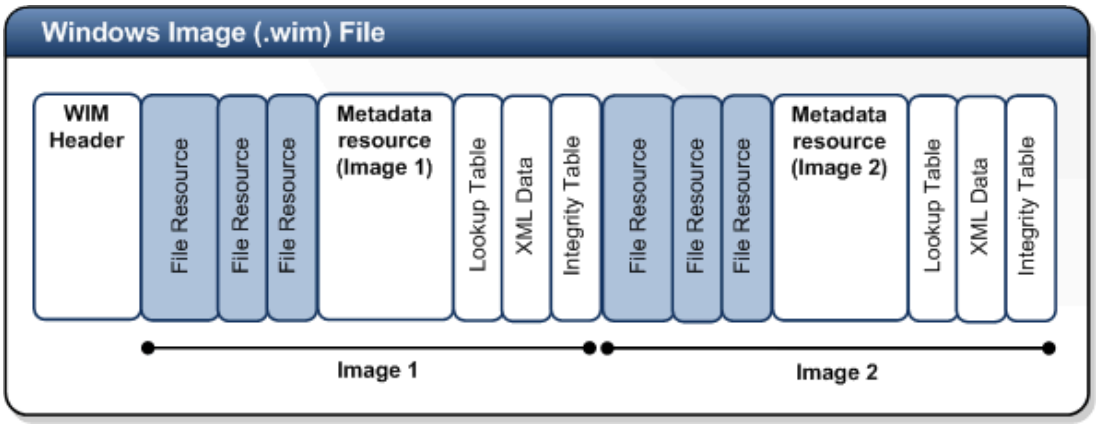


Рис. 4.1.2. Структура WIM-файла

Заголовок WIM. Определяет содержимое WIM-файла, включая расположение ключевых ресурсов (ресурс метаданных, таблицу поиска, данные XML) и различные атрибуты WIM-файла (версия, размер, тип сжатия).

Файловые ресурсы. Серия пакетов, содержащих данные, например, исходные файлы.

Ресурс метаданных. Содержит информацию о файлах, которые включены в образ, включая структуру каталогов и атрибуты файлов. Для каждого образа в WIM-файле есть один ресурс метаданных.

Lookup Table. Содержит расположение файлов ресурсов в WIM-файле.

XML Data. Содержит дополнительные данные об изображении.

Таблица целостности. Содержит информацию о хэш-безопасности, которая используется для проверки целостности изображения во время операции приложения.

Для работы с WIM-файлами используют программы ImageX и DISM из состава WADK. DISM также входит в состав Windows. Эти программы обладают сходной функциональностью, но запись параметров выполняется по-другому. Для иллюстрации различий приведены некоторые примеры.

Создание нового образа на основе жесткого диска с установленной операционной системой:

```
imagex /capture <другие параметры>
DISM /Capture-Image <другие параметры>
```

Применение WIM-файла к жесткому диску (то есть, копирование файлов из WIM-файла на жесткий диск):

`imagex /apply <другие параметры>`

`DISM /Apply-Image <другие параметры>`

Смонтировать (отобразить) WIM-файл на папку на диске и предоставить доступ к его содержимому посредством обычных файловых операций:

`imagex /mount image_file image_number <другие параметры>`

`DISM /Mount-Image /ImageFile:<path_to_image_file> <другие параметры>`

Использование файлов ответов

Во время стандартной установки Windows мастер установки задает оператору различные вопросы, например, параметры разметки жесткого диска, лицензионный ключ, имя пользователя и т. д. Такие параметры можно вручную указать в файле ответов, и он обеспечит автоматический ответ во время установки. Файл ответов — это текстовый файл в формате XML с именем `Autounattend.xml`.

Чтобы выбрать файл ответов во время установки, нужно загрузить среду предустановки Windows и выполнить команду `setup.exe` с параметром `/unattend:filename`. При отсутствии параметра `/unattend` программа установки будет искать файл с именем `Autounattend.xml` в корневых папках всех доступных дисков. Поэтому проще всего записать файл ответа на USB-устройство флэш-памяти, вставить его в компьютер, а затем загрузить этот компьютер с установочного диска Windows.

Так как файл ответов — это текстовый файл, его можно создать в любом текстовом редакторе, взяв за отправную точку образец в комплекте средств для развертывания и оценки Windows (Windows ADK) в папке `C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Deployment Tools\Samples\Unattend`.

Но намного удобнее использовать специальную программу — диспетчер установки Windows® (Windows SIM). Созданные вручную файлы ответов также необходимо проверять в диспетчере установки Windows.

Иногда можно использовать нескольких файлов ответов. Например, в ходе установки Windows можно использовать общий файл ответов, который содержит сведения о компании и поддержке. После завершения установки и при запуске средства `Sysprep` можно применить второй файл ответов для добавления дополнительных настроек.

Набор инструментальных средств Windows Assessment and Deployment Kit

Комплект средств для развертывания и оценки Windows (Windows ADK) содержит средства, необходимые для настройки образов Windows для широкомасштабного развертывания, а также для проверки качества и производительности системы, добавленных компонентов и приложений. Может быть бесплатно загружен с сайта Microsoft.

Инструменты Windows ADK можно разделить на две категории.

- Набор средств оценки Windows и набор средств оценки производительности Windows, используемые для оценки качества и производительности систем и компонентов.
- Средства развертывания, такие как WinPE, Sysprep и DISM, и другие средства, которые можно использовать для настройки и развертывания образов Windows 10.

Ниже перечислены инструменты, входящие в Windows 10 ADK:

- Windows Configuration Designer
- Windows Preinstallation Environment (WinPE)
- Deployment Image Servicing and Management (DISM)

- Windows System Image Manager (WSIM)
- Windows Assessment Toolkit
- Windows Performance Toolkit
- User State Migration Toolkit (USMT)
- Volume Activation Management Tool (VAMT)
- User Experience Virtualization (UE-V)
- Application Virtualization (App-V)

Кратко опишем некоторые инструменты.

Windows Preinstallation Environment (Windows PE). Минимальная операционная система, предназначенная для подготовки компьютера для установки и обслуживания Windows. Работает целиком в оперативной памяти, то есть не требует жесткий диск. Для предотвращения использования WinPE в производственной среде она автоматически перезагружается через 72 часа, при этом теряются все настройки. Также недоступны многие функции Windows.

User State Migration Tool (USMT) (Инструмент миграции состояния пользователей (USMT)). Инструмент USMT переносит данные пользовательских учетных записей и настройки приложений на целевую машину. Это экономит время администратора, но не воссоздает систему в первоначальном состоянии.

Deployment Tools (Инструменты развертывания). Инструменты развертывания требуются для выполнения автономной установки потому, что именно они выполняют такую автоматизированную установку. Фактически это подмножество инструментов для ADK. Оно содержит несколько поддерживающих программ, таких как инструмент обслуживания и управления образами (Deployment Image Servicing and Management — DISM), инструмент активации OEM (OEM Activation) и диспетчер образов систем Windows (Windows System Image Manager), а также другие средства.

Служба Windows Deployment Services

WDS — это серверная роль в Windows Server, которая спроектирована для оказания помощи организациям, использующим доменную службу Active Directory, при развертывании систем Windows. Система WDS обычно настраивается для обеспечения служб хранения и извлечения образов, необходимых для их развертывания, клиентских компонентов, таких как образы загрузки PXE, и управляющих компонентов, используемых для конфигурирования параметров WDS, в том числе добавление образов на сервер WDS и создание мультивещательных передач.

Загрузочные образы

Загрузочный образ содержит клиент Windows Deployment Services и среду Windows PE (Windows Preinstallation Environment — предустановочная среда Windows), которая, по сути, является операционной системой в миниатюре, предназначенной для соединения системы с сервером WDS и предоставления средств для выбора и установки установочною образа WDS.

Загрузочный образ, имеющийся на установочном носителе Windows Server 2012, имеет имя boot.wim и может использоваться для загрузки систем, которые будут устанавливать образы Windows Vista SP1, Windows Server 2008 или более поздние серверные и настольные операционные системы x64. Загрузочный образ Windows Server может применяться также для установки образов с помощью мультивещательных передач. Если предполагается развертывать образы x86, то по опыту лучше загружать эти системы, используя совместимый загрузочный образ x86 Windows 10. Это упростит проблему доставки драйверов и ручной их вставки в случае необходимости.

Установочные образы

Установочный образ на самом деле является установочным носителем Windows, который упакован в одном WIM-файле. В зависимости от носителя, используемого для предоставления WIM-файлов, он может содержать множество разных установочных образов.

Например, организации, получающие лицензионный носитель от Microsoft, могут получить DVD-диск Microsoft Windows Server, который содержит вариант полной установки и образы Server Core для редакций Standard и Datacenter. На сервере WDS обычно требуется только один загрузочный образ на платформу x86 или x64, однако он может содержать множество разных установочных образов.

Образы обнаружения

Образ обнаружения создается из загрузочного образа и используется для запуска системы и загрузки среды Windows Preinstallation Environment (Windows PE), а также для нахождения сервера WDS и соединения с ним. Образ обнаружения обычно используется, если сеть или система не поддерживает загрузку PXE. Образы обнаружения могут экспортироваться в файлы ISO, затем записываться или сохраняться на переносимых носителях, таких как CD-диски, DVD-диски или карты памяти USB. В некоторых случаях, когда оборудование не является загрузочным и правильно подключено к серверу WSD, использующему загрузочный образ, образ обнаружения может быть протестирован в качестве альтернативы и развертыванию установочного образа, и захвату системы в образ.

Образы захвата

Образ захвата тоже создается из загрузочного образа, но вместо запуска установки, как у установочного образа, обеспечивает запуск утилиты захвата WDS. Утилита захвата WDS используется для связи с системой, готовой для создания образа или клонирования, с использованием соответствующих инструментов подготовки системы, с системой WSD для создания нового установочного образа, который позднее можно развернуть на клиентах WDS. Прежде чем применять образ захвата, производится настройка системы с ОС посредством добавления приложений, специальных конфигураций и других изменений в системе, необходимых для определенной организации. Когда система будет готова к созданию образа, она подготавливается с помощью утилиты sysprep (от Microsoft). Эта утилита используется для очистки идентификатора безопасности (SID) компьютера и конфигураций операционной системы, являющихся специфическими для системы, на основе которой будет создан образ. Но зачастую перед запуском sysprep приходится выполнять дополнительные действия, которые обеспечат успешный захват, например, очистку ключей реестра для конкретных приложений, удаление пользовательских профилей и, возможно, удаление самих приложений. Чтобы быть уверенным в сторонних приложениях или даже разработанных Microsoft, просмотрите документацию производителя, обращая особое внимание на создание образов, клонирование и работу с утилитой sysprep.

Набор инструментальных средств Microsoft Deployment Toolkit

Microsoft Deployment Toolkit — единый набор средств и процессов для автоматизации развертывания серверных и настольных систем. В дополнение к уменьшению времени развертывания и стандартизации настольных и серверных образов, MDT упрощает работу со средствами безопасностью и текущими конфигурациями. MDT основывается на базовых средствах развертывания из комплекта средств для развертывания и оценки Windows (Windows ADK) с дополнительным руководством и функциями, которые уменьшают сложность задачи и время, необходимое для развертывания в корпоративной среде.

Набор инструментов Microsoft Deployment Toolkit (MDT) поддерживает три типа развертываний: Zero Touch Installation (ZTI), Lite Touch Installation (LTI) и User Driven Installation (UDI). ZTI — полностью автоматизированная схема развертывания, при которой установка не требует взаимодействия с пользователем. Для развертывания UDI требуется полное ручное вмешательство для ответа на каждое приглашение на установку, например, имя машины, пароль или язык. Для развертывания ZTI и UDI требуются инфраструктура Microsoft System Center. Для развертывания ZTI требуется постоянное сетевое подключение к точке распространения. Для развертывания LTI требуется ограниченное взаимодействие с пользователем. Для развертывания LTI требуется очень небольшая инфраструктура, поэтому его можно установить из общего сетевого ресурса или носителя с помощью USB флеш-накопителя или оптического диска.

4.1.5. Организация рабочей среды пользователя

Рабочая среда пользователя состоит из настроек рабочего стола, например, цвета экрана, настроек мыши, размера и расположения окон, из настроек процесса обмена информацией по сети и с устройством печати, переменных среды, параметров реестра и набора доступных приложений [9].

Для управления средой пользователя предназначены следующие средства Windows:

Сценарий входа в сеть (сценарий регистрации) представляет собой командный файл, имеющий расширение .bat, или исполняемый файл с расширением .exe, который выполняется при каждой регистрации пользователя в сети. Сценарий может содержать команды операционной системы, предназначенные, например, для создания соединения с сетью или для запуска приложения. Кроме того, с помощью сценария можно устанавливать значения переменных среды, указывающих пути поиска, каталоги для временных файлов и другую подобную информацию.

Профили пользователей. В профиле пользователя хранятся все настройки рабочей среды компьютера, на котором работает Windows 2000, определенные самим пользователем. Это могут быть, например, настройки экрана и соединения с сетью.

Сервер сценариев Windows (Windows Scripting Host, WSH). Сервер сценариев независим от языка и предназначен для работы на 32-разрядных платформах Windows. Он включает в себя как ядро сценариев Visual Basic Scripting Edition (VBScript), так и JScript. Сервер сценариев Windows предназначен для выполнения сценариев прямо на рабочем столе Windows или на консоли команд. При этом сценарии не надо встраивать в документ HTML.

Большинство настроек рабочей среды пользователя можно настроить с помощью **групповых политик**.

4.1.6. Работа с учетными записями пользователей и групп

Локальные учетные записи пользователей определяются локально на устройстве и могут назначаться только на этом устройстве. Локальные учетные записи пользователей — это субъекты безопасности, которые используются для защиты и управления доступом к ресурсам на устройстве для служб или пользователей [10].

Учетные записи локальных пользователей по умолчанию — это встроенные учетные записи, которые создаются автоматически при установке операционной системы. Учетные записи локальных пользователей по умолчанию не могут быть удалены или удалены и не предоставляют доступ к сетевым ресурсам.

Учетные записи локальных пользователей по умолчанию используются для управления доступом к ресурсам локального устройства на основе прав и разрешений, назначенных учетной записи. Учетные записи локальных пользователей по умолчанию и создаваемые локальные учетные записи пользователей находятся в папке **Пользователи**. Папка

Пользователи находится в папке Локальные пользователи и группы в локальной консоли управления Майкрософт (MMC). Управление компьютером — это набор средств администрирования, которые можно использовать для управления локальным или удаленным устройством.

Администратор

Учетная запись локального администратора по умолчанию — это учетная запись пользователя для системного администрирования. У каждого компьютера есть учетная запись администратора (SID S-1-5-домен-500, отображаемое имя — Администратор). Учетная запись администратора — это первая учетная запись, которая создается при установке Windows.

Учетная запись администратора имеет полный контроль над файлами, каталогами, службами и другими ресурсами на локальном устройстве. Учетная запись администратора может создавать других локальных пользователей, назначать права пользователей и назначать разрешения. Учетная запись администратора может в любое время управлять локальными ресурсами, изменив права и разрешения пользователя.

Учетную запись администратора по умолчанию нельзя удалить или заблокировать, но ее можно переименовать или отключить.

Программа установки Windows отключает встроенную учетную запись администратора и создает другую локальную учетную запись, которая является членом группы администраторов.

Участники групп "Администраторы" могут запускать приложения с повышенными разрешениями, не используя параметр Запуск от имени администратора. Быстрое переключение пользователей более безопасно, чем использование **runas** или повышение прав пользователей.

По умолчанию учетная запись администратора входит в группу Администраторы. Рекомендуется ограничить число пользователей в группе "Администраторы", так как члены группы "Администраторы" имеют разрешения на полный доступ на устройстве.

Учетную запись администратора нельзя удалить из группы администраторов.

Гость

Гостевая учетная запись позволяет случайным или разовым пользователям, у которых нет учетной записи на компьютере, временно войти на локальный сервер или клиентский компьютер с ограниченными правами пользователя. По умолчанию учетная запись гостя отключена и имеет пустой пароль. Так как учетная запись гостя может предоставлять анонимный доступ, она считается угрозой безопасности. По этой причине рекомендуется оставить учетную запись гостя отключенной, если только ее использование не требуется.

По умолчанию учетная запись "Гость" является единственным членом группы SID S-1-5-32-546 "Гости" по умолчанию, которая позволяет пользователю войти на устройство.

При включении гостевой учетной записи предоставляйте только ограниченные права и разрешения. По соображениям безопасности гостевую учетную запись нельзя использовать в сети и делать доступной для других компьютеров.

Кроме того, гостевой пользователь в гостевой учетной записи не должен иметь возможности просматривать журналы событий. После включения гостевой учетной записи рекомендуется часто отслеживать гостевую учетную запись, чтобы гарантировать, что другие пользователи не смогут использовать службы и другие ресурсы. Сюда относятся ресурсы, которые непреднамеренно были оставлены доступными предыдущим пользователем.

Управление учетной записью локального пользователя

Учетные записи локальных пользователей по умолчанию и созданные вами учетные записи локальных пользователей находятся в папке «Пользователи». Папка "Пользователи" находится в папке "Локальные пользователи и группы".

Вы можете использовать локальные пользователи и группы для назначения прав и разрешений только на локальном сервере, чтобы ограничить возможность локальных пользователей и групп выполнять определенные действия. Право разрешает пользователю выполнять определенные действия на сервере, такие как резервное копирование файлов и папок или выключение сервера. Разрешение на доступ — это правило, связанное с объектом, обычно с файлом, папкой или принтером. Он регулирует, какие пользователи могут иметь доступ к объекту на сервере и каким образом.

Вы не можете использовать локальные пользователи и группы в контроллере домена. Однако вы можете использовать локальных пользователей и группы на контроллере домена для удаленных компьютеров, которые не являются контроллерами домена в сети.

Вы также можете управлять локальными пользователями с помощью NET.EXE USER и управлять локальными группами с помощью NET.EXE LOCALGROUP или с помощью различных командлетов PowerShell и других технологий сценариев.

Применение ограничений локальной учетной записи

Контроль учетных записей (UAC) — это функция безопасности, которая информирует вас о том, что программа вносит изменения, требующие административных разрешений. UAC работает путем настройки уровня разрешений учетной записи пользователя. По умолчанию контроль учетных записей настраивается для уведомления при попытке приложений внести изменения в компьютер, но вы можете изменить это, когда управление учетными записями уведомляет вас.

Контроль учетных записей позволяет рассматривать учетную запись с правами администратора как учетную запись обычного пользователя, не являющегося администратором, до тех пор, пока не будут запрошены и утверждены полные права, также называемые повышением прав. Например, контроль учетных записей позволяет администратору вводить учетные данные во время сеанса пользователя, не являющегося администратором, для выполнения случайных административных задач без необходимости переключать пользователей, выходить из нее или использовать команду **Запуск от имени** (`runas`).

Кроме того, UAC может потребовать от администраторов специального одобрения приложений, вносящих общесистемные изменения, прежде чем этим приложениям будет предоставлено разрешение на запуск, даже в пользовательском сеансе администратора.

Учетные записи для служб

Учетная запись **SYSTEM** используется операционной системой и службами, работающими под управлением Windows. В операционной системе Windows существует множество служб и процессов, которым требуется возможность внутреннего входа, например, во время установки Windows. Учетная запись SYSTEM была разработана для этой цели, и Windows управляет правами пользователя учетной записи SYSTEM. Это внутренняя учетная запись, которая не отображается в диспетчере пользователей и не может быть добавлена ни в какие группы.

С другой стороны, учетная запись SYSTEM отображается на томе файловой системы NTFS в диспетчере файлов в разделе Разрешения меню Безопасность. По умолчанию учетной записи SYSTEM предоставляются разрешения на полный доступ ко всем файлам в томе NTFS. Здесь учетная запись SYSTEM имеет те же функциональные права и разрешения, что и учетная запись администратора.

Предоставление разрешений на доступ к файлам группе администраторов учетной записи не означает неявное предоставление разрешений учетной записи SYSTEM. Разрешения учетной записи SYSTEM можно удалить из файла, но мы не рекомендуем их удалять.

Учетная запись **NETWORK SERVICE** — это предопределенная локальная учетная запись, используемая диспетчером управления службами (SCM). Служба, работающая в контексте учетной записи NETWORK SERVICE, предоставляет учетные данные компьютера удаленным серверам.

Учетная запись **LOCAL SERVICE** — это предопределенная локальная учетная запись, используемая диспетчером управления службами. Она имеет минимальные привилегии на локальном компьютере и предоставляет анонимные учетные данные в сети.

4.1.7. Работа с профилями пользователей

Система создает профиль пользователя при первом входе пользователя на компьютер. При последующих входах система загружает профиль пользователя, а затем другие системные компоненты настраивают среду пользователя в соответствии с информацией в профиле [11].

Типы профилей пользователей

- **Локальные профили пользователей**. Локальный профиль пользователя создается при первом входе пользователя на компьютер. Профиль хранится на локальном жестком диске компьютера. Изменения, внесенные в профиль локального пользователя, относятся к пользователю и компьютеру, на котором внесены изменения.
- **Перемещаемые профили пользователей**. Перемещаемый профиль пользователя — это копия локального профиля, которая копируется в общую папку сервера и хранится в ней. Этот профиль загружается на любой компьютер, на который пользователь входит в сеть. Изменения, внесенные в перемещаемый профиль пользователя, синхронизируются с серверной копией профиля при выходе пользователя из системы. Преимущество перемещаемых профилей пользователей заключается в том, что пользователям не нужно создавать профиль на каждом компьютере, который они используют в сети.
- **Обязательные профили пользователей**. Обязательный профиль пользователя — это тип профиля, который администраторы могут использовать для указания параметров для пользователей. Только системные администраторы могут вносить изменения в обязательные профили пользователей. Изменения, внесенные пользователями в параметры рабочего стола, теряются при выходе пользователя из системы.
- **Временные профили пользователей**. Временный профиль выдается каждый раз, когда ошибка препятствует загрузке профиля пользователя. Временные профили удаляются в конце каждого сеанса, а изменения, внесенные пользователем в параметры рабочего стола и файлы, теряются при выходе пользователя из системы. Временные профили доступны только на компьютерах под управлением Windows 2000 и более поздних версий.

Профиль пользователя состоит из следующих элементов:

- **Куст реестра**. Куст реестра — это файл `NTuser.dat`. Куст загружается системой при входе пользователя и сопоставляется с разделом реестра HKEY_CURRENT_USER. Куст реестра пользователя поддерживает настройки и конфигурацию на основе реестра.
- **Набор папок профилей, хранящихся в файловой системе**. Файлы профилей пользователей хранятся в каталоге `Profiles` в папке для каждого пользователя.

Папка профиля пользователя — это контейнер для приложений и других системных компонентов для заполнения вложенными папками и данными для каждого пользователя, такими как документы и файлы конфигурации. Обозреватель Windows широко использует папки профилей пользователей для таких элементов, как рабочий стол пользователя, меню "Пуск" и папка "Документы".

Профили пользователей предоставляют следующие преимущества:

- Когда пользователь входит на компьютер, система использует те же параметры, которые использовались при последнем выходе пользователя.
- При совместном использовании компьютера с другими пользователями каждый пользователь получает настроенный рабочий стол после входа в систему.
- Параметры в профиле пользователя уникальны для каждого пользователя. Другие пользователи не могут получить доступ к параметрам. Изменения, внесенные в профиль одного пользователя, не влияют на профили других пользователей или других пользователей.

Локальные профили пользователей

Для обеспечения безопасности Windows требуется профиль пользователя для каждой учетной записи пользователя на компьютере. Система автоматически создает локальный профиль пользователя для каждого пользователя при первом входе пользователя на компьютер. Система автоматически поддерживает параметры рабочей среды каждого пользователя в профиле пользователя на локальном компьютере [12].

Управление профилями пользователей в Windows Vista и более поздних версиях осуществляется с помощью элемента панели управления **Учетные записи пользователей**.

Профиль пользователя не загружается автоматически при входе пользователя с помощью функции **LogonUser**. Чтобы загрузить профиль пользователя программным способом, используйте функцию **LoadUserProfile**. Чтобы выгрузить профиль пользователя, загруженный **LoadUserProfile**, вызовите функцию **UnloadUserProfile**.

Перемещаемые профили пользователей

Если компьютер работает под управлением Windows 2000 Server или более поздней версии в сети, пользователи могут хранить свои профили на сервере. Эти профили называются перемещаемыми профилями пользователей [13].

Перемещаемые профили пользователей имеют следующие преимущества.

- **Автоматическая доступность ресурсов**. Уникальный профиль пользователя автоматически становится доступным при входе на любой компьютер в сети. Пользователям не нужно создавать профиль на каждом компьютере, который они используют в сети.
- **Упрощенная замена и резервное копирование компьютеров**. Когда необходимо заменить компьютер пользователя, его можно легко заменить, так как все данные профиля пользователя хранятся отдельно в сети, независимо от отдельного компьютера. Когда пользователь впервые входит на новый компьютер, серверная копия профиля пользователя копируется на новый компьютер.

Профиль пользователя не загружается автоматически при входе пользователя с помощью функции **LogonUser**. Чтобы загрузить перемещаемый профиль пользователя программным способом, используйте функцию **LoadUserProfile**. Чтобы выгрузить перемещаемый профиль пользователя, загруженный **LoadUserProfile**, вызовите функцию **UnloadUserProfile**.

Обязательный профиль пользователя

Обязательный профиль пользователя — это особый тип предварительно настроенного перемещаемого профиля пользователя, который администраторы могут использовать для указания параметров для пользователей. С помощью обязательных профилей пользователей пользователь может изменять свой рабочий стол, но изменения не сохраняются при выходе пользователя из системы. При следующем входе пользователя будет загружен обязательный профиль пользователя, созданный администратором. Существует два типа обязательных профилей: обычные обязательные профили и супер-обязательные профили [14].

Профили пользователей становятся обязательными, когда администратор переименовывает файл `NTuser.dat` (куст реестра) на сервере в `NTuser.man`. Расширение `.man` приводит к тому, что профиль пользователя будет доступен только для чтения.

Профили пользователей становятся супер обязательными, если имя папки пути к профилю заканчивается на `.man`; например, `\\server\share\mandatoryprofile.man\`.

Суперобязательные профили пользователей похожи на обычные обязательные профили, за исключением того, что пользователи с суперобязательными профилями не могут войти в систему, если сервер, на котором хранится обязательный профиль, недоступен. Пользователи с обычными обязательными профилями могут войти в систему с локально кэшируемой копией обязательного профиля.

Только системные администраторы могут вносить изменения в обязательные профили пользователей.

Расширение профиля для каждой версии Windows

Имя папки, в которой вы храните профиль, должно использовать правильное расширение для операционной системы, к которой он будет применен. В следующей таблице перечислены правильные расширения для каждой версии операционной системы.

Таблица 4.1.2.

Версия операционной системы клиента	Версия операционной системы сервера	Расширение профиля
Windows 8.1	Windows Server 2012 R2	V4
Windows 10 версии 1607 и более поздних версий	Windows Server 2016 и более поздние версии	V6

Например, если профиль создается для Windows v20H2, путь к папке профиля может быть `\\server\share\profile.v6` с расширением, указывающим версию.

Расширенную информацию можно найти по ссылке:

https://learn.microsoft.com/en-us/training/modules/manage-user-profiles/

4.1.8. Работа с файловой системой

Оболочка предоставляет несколько способов управления файловой системой. Оболочка предоставляет функцию **`SHFileOperation`**, которая позволяет приложению перемещать, копировать, переименовывать и удалять файлы программными средствами. Оболочка также поддерживает некоторые дополнительные возможности управления файлами [15].

- HTML-документы можно подключить к связанным файлам, таким как графические файлы или таблицы стилей. При перемещении или копировании документа подключенные файлы также автоматически перемещаются или копируются.
- Для систем, доступных для нескольких пользователей, управление файлами можно осуществлять для каждого пользователя. Пользователи имеют простой доступ к файлам данных, но не к файлам, принадлежащим другим пользователям.

- Если файлы документов добавляются или изменяются, их можно добавить в список последних документов оболочки. Когда пользователь щелкает команду Документы в меню Пуск, появляется список ссылок на документы.

Пространство имен не является статическим, и приложения обычно должны управлять файловой системой, выполняя одну из следующих операций.

- Копирование объекта в другую папку.
- Перемещение объекта в другую папку.
- Удаление объекта.
- Переименование объекта.

Все эти операции выполняются с помощью **SHFileOperation**. Эта функция принимает один или несколько исходных файлов и создает соответствующие целевые файлы. В случае операции удаления система пытается поместить удаленные файлы в корзину.

Можно также перемещать файлы с помощью функции перетаскивания .

Чтобы использовать функцию, необходимо заполнить элементы структуры **SHFILEOPSTRUCT** и передать их в **SHFileOperation**. Ключевыми элементами структуры являются **pFrom** и **pTo**.

Элемент **pFrom** — это строка с двойным завершением **NULL**, которая содержит одно или несколько имен исходных файлов. Это могут быть полные пути или стандартные подстановочные знаки DOS, такие как *.*. Хотя этот элемент объявлен как строка, завершающаяся **нулевым** значением, он используется в качестве буфера для хранения нескольких имен файлов. Каждое имя файла должно заканчиваться обычным символом **NULL**. Чтобы указать конец **pFrom**, в конце конечного имени необходимо добавить дополнительный символ **NULL**.

Элемент **pTo** — это строка с двойным **нулем**, как **и pFrom**. Элемент **pTo** содержит имена одного или нескольких полных имен назначения. Они упаковываются в **pTo** так же, как и для **pFrom**. Если **pTo** содержит несколько имен, необходимо также установить флаг **FOF_MULTIDESTFILES** в элементе **fFlags**. Использование **pTo** зависит от операции, как описано здесь.

- Если для операций копирования и перемещения все файлы находятся в одном каталоге, **pTo** содержит полное имя каталога. Если файлы находятся в разных местах назначения, **pTo** также может содержать один полный каталог или имя файла для каждого исходного файла. Если каталог не существует, система создает его.
- Для операций переименования **pTo** содержит один полный путь к каждому исходному файлу в **pFrom**.
- Для операций удаления **pTo** не используется.

Синтаксис функции SHFileOperationA [16]:

```
int SHFileOperationA(
  [in, out] LPSHFILEOPSTRUCTA lpFileOp );
```

Синтаксис структуры SHFILEOPSTRUCT [17]:

```
typedef struct _SHFILEOPSTRUCTA {
  HWND         hwnd;
  UINT         wFunc;
  PCZZSTR      pFrom;
  PCZZSTR      pTo;
  FILEOP_FLAGS fFlags;
  BOOL         fAnyOperationsAborted;
  LPVOID       hNameMappings;
  PCSTR        lpszProgressTitle;
} SHFILEOPSTRUCTA, *LPSHFILEOPSTRUCTA;
```

Параметр `wFunc` указывает, какую операцию выполнить. Принимает одно из следующих значений: `FO_COPY`, `FO_DELETE`, `FO_MOVE`, `FO_RENAME`.

Для однопоточных приложений в современных версиях Windows рекомендуется использовать интерфейс **`IFileOperation`** [18].

`IFileOperation` предлагает множество преимуществ по сравнению со старой функцией **`SHFileOperation`**.

- Использование **`IShellItem`** для идентификации элементов, а не строковых путей. **`SHFileOperation`** требовало, чтобы строки пути и назначения заканчивались двумя нулевыми символами, а не стандартным одним нулевым символом, который сам использовался для разделения нескольких путей в строке. Идентификация элемента с помощью **`IShellItem`** более надежна и менее подвержена ошибкам программирования. Это также позволяет вам получить доступ к элементам нефайловой системы, таким как виртуальные папки. Несколько элементов в одной операции можно передать как **`IShellItemArray`**, **`IDataObject`** или коллекцию, доступ к которой осуществляется через **`IEnumShellItems`**, а не как строку.
- Более точные отчеты об ошибках через значения `HRESULT` в сочетании с таким API, как **`FormatMessage`**. Коды возврата из **`SHFileOperation`** могут вводить в заблуждение или быть неточными.
- Расширяемость. Возможности **`IFileOperation`**, как интерфейса модели компонентных объектов (COM), могут быть расширены третьей стороной для удовлетворения их конкретных потребностей, хотя это должно быть очень редким случаем. Windows предоставляет реализацию **`IFileOperation`** по умолчанию, которая должна удовлетворить потребности большинства пользователей.
- Улучшенная обратная связь о прогрессе. Подробный ход операции, включая уведомления о начале и завершении определенных операций над отдельными элементами, а также общий прогресс, можно получить во время операции. Хотя **`SHFileOperation`** действительно предоставлял пользовательский интерфейс прогресса, он не был таким подробным.
- Больше функциональности. В дополнение к функциям копирования, удаления, перемещения и переименования, предоставляемым **`SHFileOperation`**, **`IFileOperation`** позволяет применять значения свойств и создавать новые элементы.
- Больше контроля над операцией. В дополнение к флагам операций, распознаваемым **`SHFileOperation`**, в **`IFileOperation::SetOperationFlags`** распознаются новые флаги, которые определяют расширенные параметры операции.
- За один вызов можно выполнять различные операции. Например, вы можете переместить набор файлов, скопировать другие, переименовать папку и применить свойства к еще одному элементу за одну операцию. **`SHFileOperation`** может выполнять только одну операцию — копирование, перемещение, переименование или удаление — одновременно.

4.1.9. Настройка обработки файлов с определенным расширением

Сопоставления файлов определяют, как оболочка обрабатывает тип файла в системе [19].

Сопоставления файлов управляют следующими функциями:

- Какое приложение запускается, когда пользователь дважды щелкает файл.
- Какой значок отображается для файла по умолчанию.
- Отображение типа файла при просмотре в Windows Обозреватель.
- Какие команды отображаются в контекстном меню файла.

- Другие функции пользовательского интерфейса, такие как подсказки, сведения о плитке и область сведений.

Разработчики приложений могут использовать сопоставления файлов для управления тем, как оболочка обрабатывает пользовательские типы файлов, или для связывания приложения с существующими типами файлов. Например, при установке приложения приложение может проверка наличие существующих сопоставлений файлов, а также создать или переопределить эти сопоставления файлов.

Пользователи могут управлять некоторыми аспектами сопоставлений файлов, чтобы настроить обработку типа файла оболочкой с помощью пользовательского интерфейса **`Open With…`** или редактирования реестра.

Как работают сопоставления файлов

Файлы предоставляются в оболочке как элементы оболочки. Для управления сопоставлениями файлов разработчики приложений могут зарегистрировать сопоставление между типом файла и обработчиками (COM-объекты, предоставляющие функциональные возможности для элементов оболочки типа файла). Когда оболочке требуется запросить сопоставления файлов для типа файла, она создает массив разделов реестра, содержащий связи для этого типа файла, и проверяет эти ключи на наличие соответствующих сопоставлений файлов.

Типы общедоступных и частных файлов

Общедоступные типы файлов также известны как популярные или спорные типы, так как конкурирующие приложения могут быть связаны с этими типами файлов [20]. Характеристики общедоступных типов файлов:

- Как правило, они определяются органами по стандартам и/или продвигаются их определяющими организациями как форматы обмена.
- Они часто обмениваются между компьютерами и пользователями для различных целей.
- Они должны поддерживаться на разных платформах.
- Приложения от нескольких поставщиков, скорее всего, будут обрабатывать их.

Некоторые примеры типов файлов, которые считаются общедоступными, — это типы файлов изображений .png, .gif, .jpg и .bmp, а также типы звуковых файлов WAV, .mp3 и AU.

В отличие от открытых типов файлов, частные или защищаемые типы файлов обычно имеют формат, который реализуется и понимается только одним приложением или поставщиком. В результате типы частных файлов обычно не подвержены конфликтам между приложениями. Некоторые типы файлов могут начинаться как частные типы файлов, но позже становятся общедоступными типами файлов.

Программные идентификаторы

Оболочка использует подраздел реестра с программным идентификатором (ProgID) для связывания типа файла с приложением и управления поведением связи. Записи ProgID, используемые для сопоставления файлов, находятся в HKEY_CLASSES_ROOT реестра [21].

Правильный формат имени ключа ProgID — [поставщик или приложение]. [Компонент]. [Версия], разделенная точками и без пробелов, как в **Word. Document.6**. Часть версии является необязательной, но настоятельно рекомендуется.

В следующем примере раздела реестра показан узел ключа ProgID сопоставления файлов:

```
HKEY_CLASSES_ROOT
   Vendor.App.1
      (Default) = My Friendly Name
      AllowSilentDefaultTakeOver
      AppUserModelID = Vendor.Application
      EditFlags = 0x00000001
      FriendlyTypeName = @%SystemRoot%\shell32.dll,-154
      InfoTip = @%SystemRoot%\shell32.dll,-54
      CurVer
         (Default) = Vendor.App.1
      DefaultIcon
         (Default) = %SystemRoot%\shell32.dll,-1
```

Регистрация типа файла

Чтобы связать тип файла с существующим приложением, найдите ProgID для приложения в реестре. Чтобы связать тип файла с новым приложением, определите ProgID для приложения.

Подразделы расширения имени файла имеют следующую общую форму: `extension=ProgID`. Подразделы расширения имени файла хранятся в поддереве `HKEY_CLASSES_ROOT`.

Важно включить в реестр начальную точку (.) при создании подразделов типов файлов. Например, если требуется, чтобы файлы с коротким расширением `.myp` и длинным расширением `.myp-file` открывался с помощью приложения MyProgram, используйте следующий синтаксис:

```
HKEY_CLASSES_ROOT
   .myp
      (Default) = ApplicationVendor.MyProgram
   .myp-file
      (Default) = ApplicationVendor.MyProgram
   ApplicationVendor.MyProgram
      (Default) = MyProgram Application
```

Как показано в предыдущем примере, если вы также регистрируете расширение короткого имени файла (MYP), необходимо также создать подраздел для длинного расширения (MYP-file).

Записи расширения типа файлов в реестре имеют несколько необязательных подразделов и атрибутов.

Общая форма подраздела расширения имени файла выглядит следующим образом. Все типы записей относятся к типу REG_SZ.

```
HKEY_CLASSES_ROOT
   .ext
      (Default) = ProgID.ext.1
      Content Type = MIME content type
      PerceivedType = PerceivedType
      OpenWithProgids
         ProgID2.ext.1
         ProgID3.ext.1
      ProgID.ext.1
         shellnew
```

Чтобы глобально зарегистрировать тип файла на определенном компьютере, создайте запись для этого типа файла в подразделе `HKEY_LOCAL_MACHINE\Software\Classes`.

Чтобы сделать регистрацию типа файла видимой только для текущего пользователя, создайте запись для этого типа файла в подразделе `HKEY_CURRENT_USER\Software\Classes`.

Приложение может предоставлять собственную реализацию команды, например, **open** или **play**, как показано в следующем примере реестра.

```
HKEY_CLASSES_ROOT
   Applications
      ApplicationName.exe
         shell
            verb
```

4.1.10. Мониторинг и оптимизация системы

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.

4.1.10.1. 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 последних версиях Windows 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— 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 и большинством других технологий Microsoft, обеспечивая общее решение, которое помогает автоматизировать мониторинг важных систем и процессов.

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 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.

4.1.10.2. Монитор производительности

Монитор производительности, окно которого показано на рис. 4.1.3, состоит из трех основных компонентов: инструментов мониторинга, таких как монитор производительности (Performance Monitor), групп сборщиков данных и компонента для формирования отчетов.

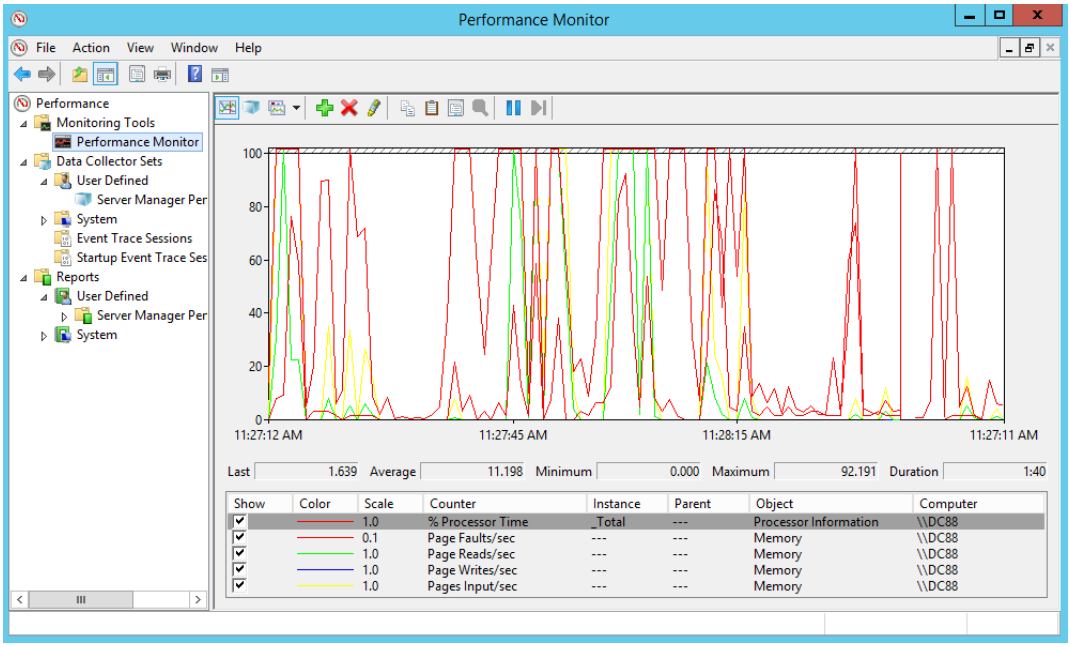


Рис. 4.1.3. Окно монитора производительности

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. 4.1.4).

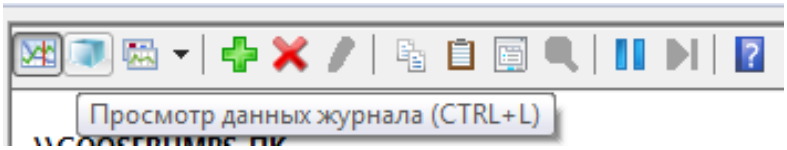


Рис. 4.1.4. Кнопка Просмотр данных журнала

Также в режим системного монитора можно перейти прямо из отчета (рис. 4.1.5).

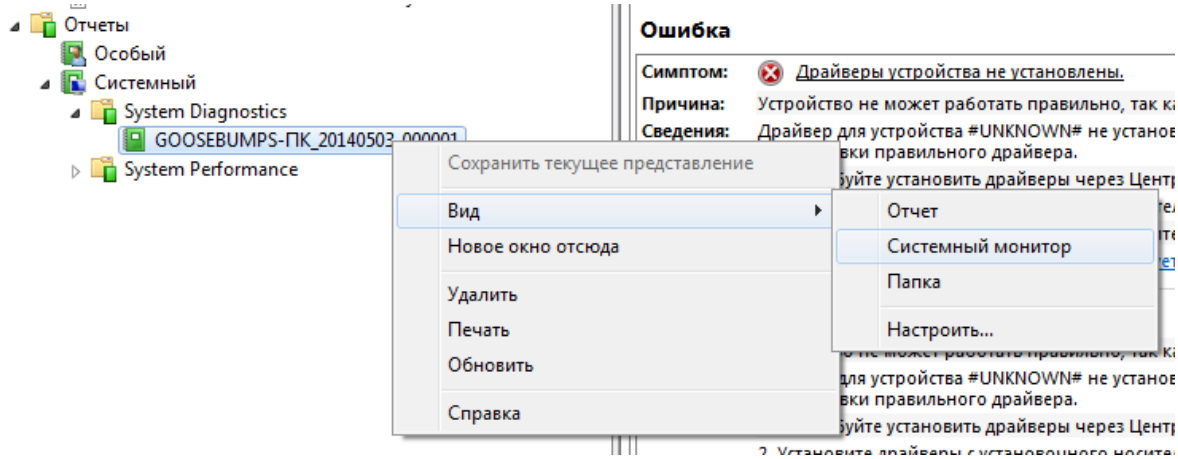


Рис. 4.1.5. Открытие системного монитора из отчета

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.4.1.6).

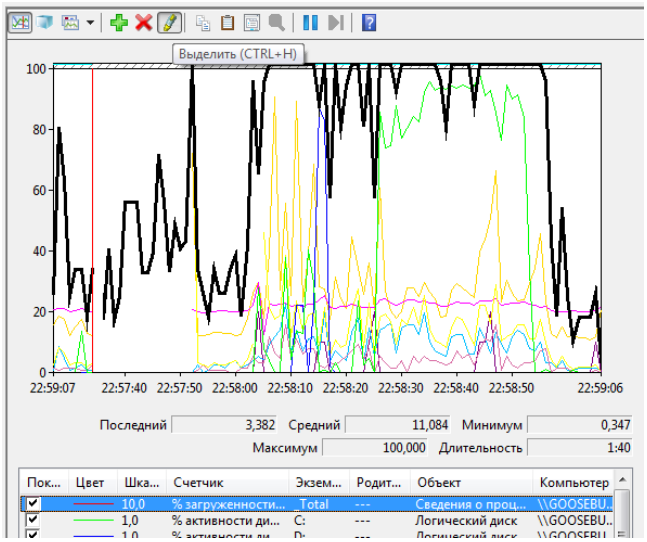


Рис. 4.1.6. Кнопка **Выделить** в системном мониторе

Также можно переключиться в режим **Отчет**, где наблюдать за счетчиками легче, но не видно динамики (рис. 4.1.7).

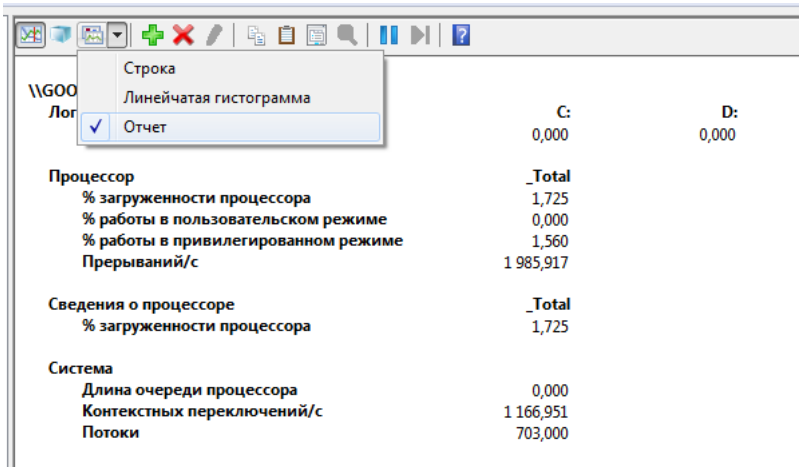


Рис. 4.1.7. Переключение системного монитора в режим отчета

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. 4.1.8):

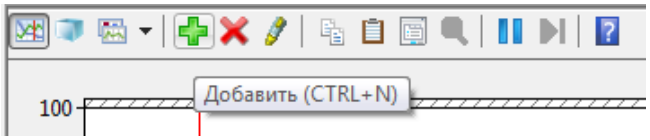


Рис. 4.1.8. Кнопка **Добавить** в системном мониторе

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. 4.1.9). Когда список готов, нажать **ОК**.

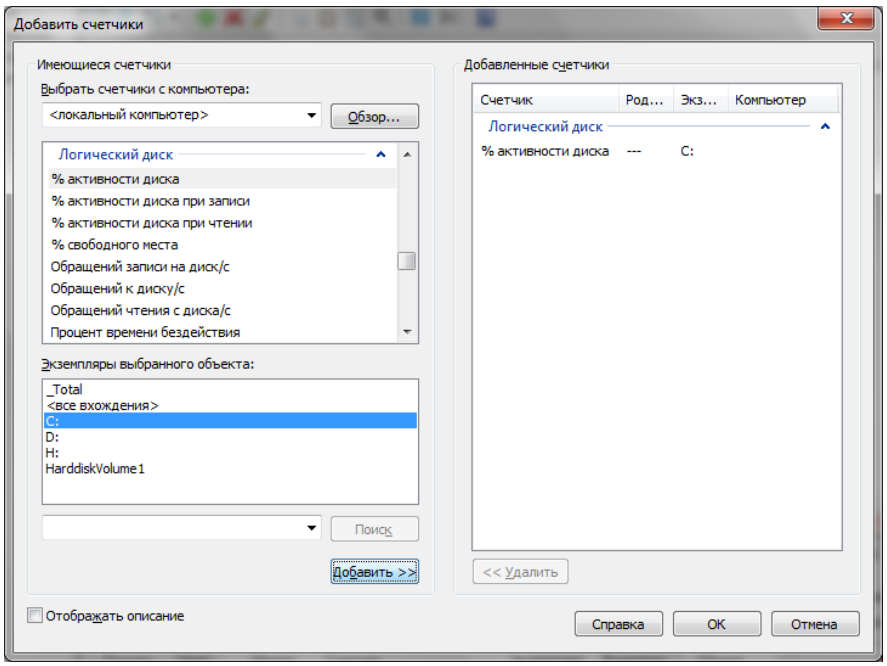
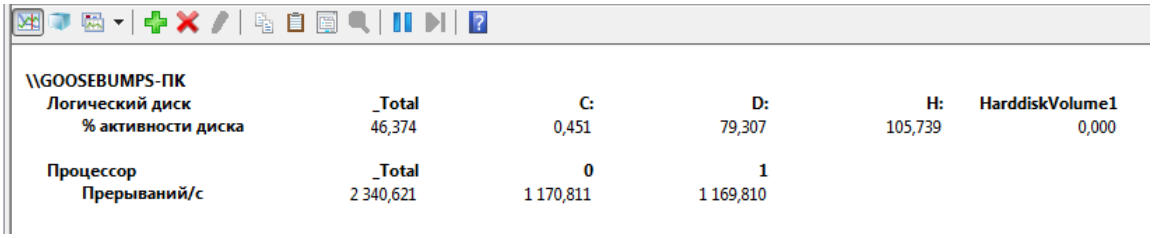


Рис. 4.1.9. Диалоговое окно для редактирования списка наблюдаемых счетчиков производительности

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. 4.1.10. 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. 4.1.11). 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.

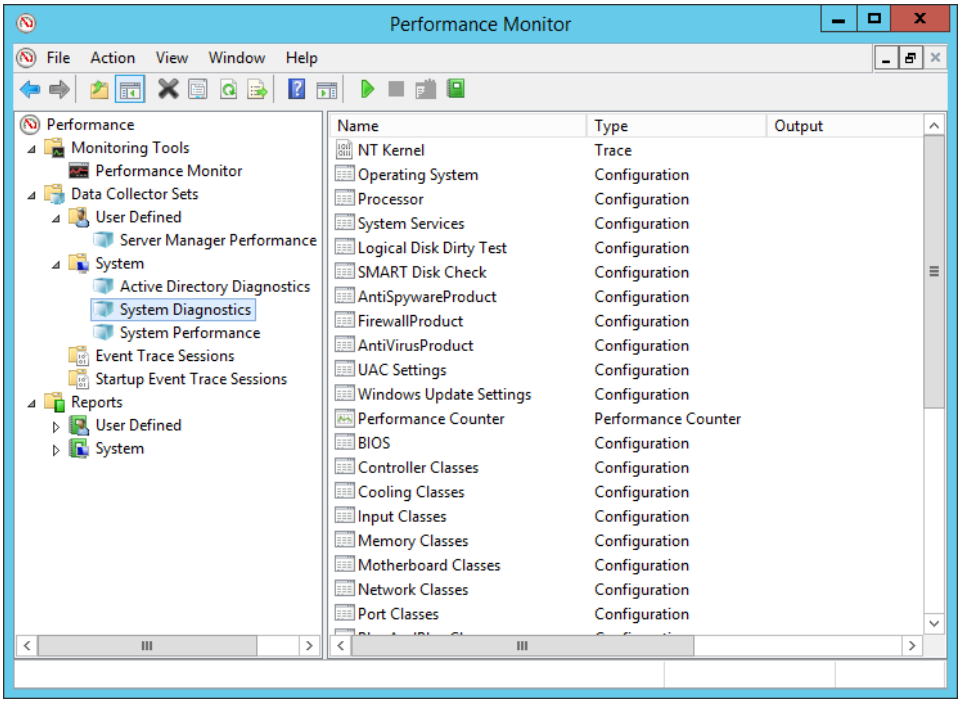


Рис. 4.1.11. Системные группы сборщиков данных

Сохранение данных о производительности в файле

Если нужно сохранить значения показателей производительности для последующего анализа, создаются группы сборщиков данных (рис. 4.1.12). Так же, как и при мониторинге, в группу добавляются нужные счетчики, указывается место хранения файлов, условия для запуска и остановки.

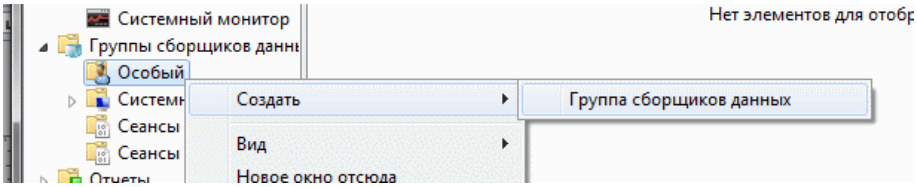


Рис. 4.1.12. Команда создания новой группы сборщиков данных

В открывшемся окне нужно дать имя группе сборщиков данных и выбрать вариант создания (рис. 4.1.13), обычно выбирается второй вариант.

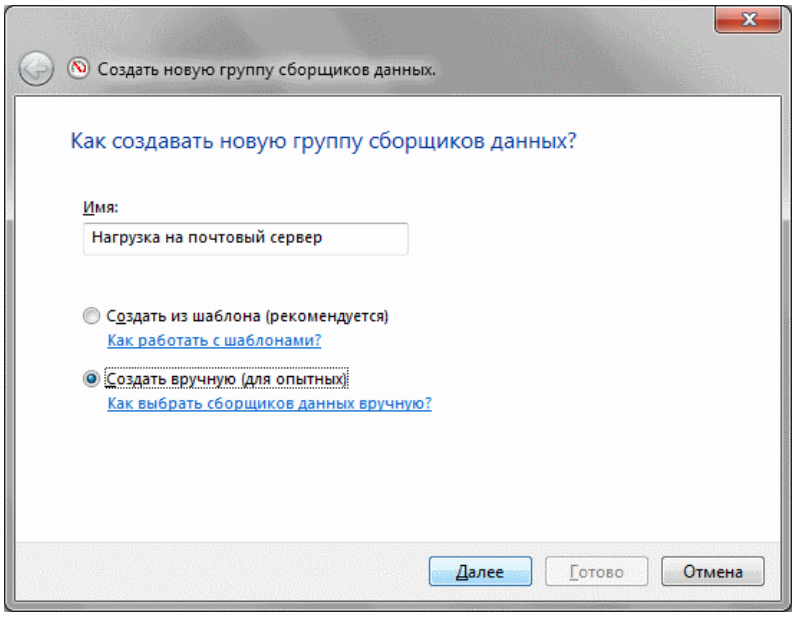


Рис. 4.1.13. Стартовая страница мастера создания группы сборщиков данных

На следующем экране (рис. 4.1.14) отметить **Счетчик производительности** (остальные опции часто не нужны).

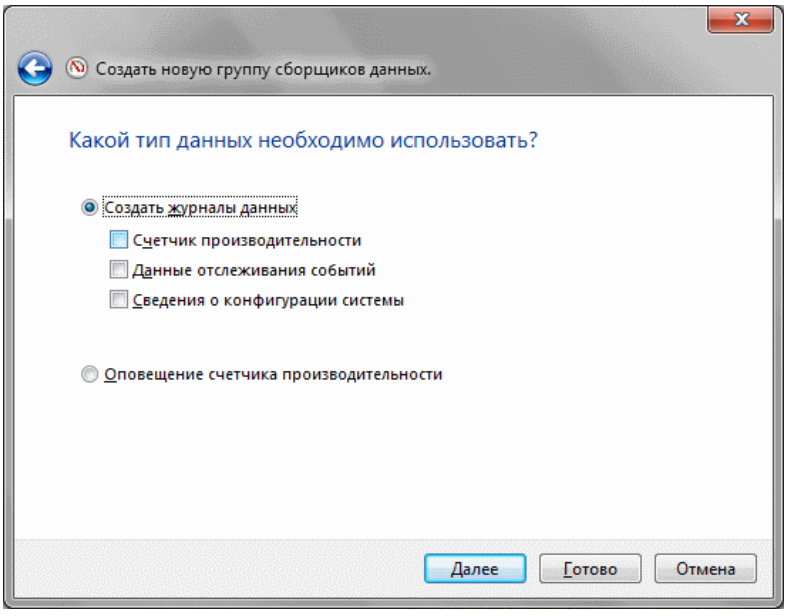


Рис. 4.1.14. Выбор типа сохраняемых данных

Далее откроется окно для добавления счетчиков (рис. 4.1.15).

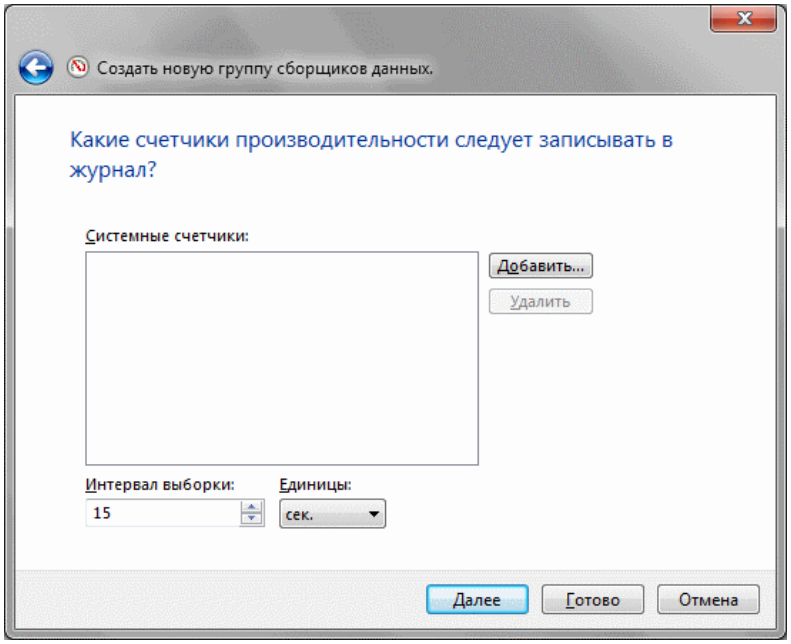


Рис. 4.1.15. Выбор счетчиков и интервала выборки

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. 4.1.16), чтобы перейти к редактированию свойств группы (можно выбрать **Сохранить и закрыть**, если редактирование будет позже или устраивают параметры по умолчанию).

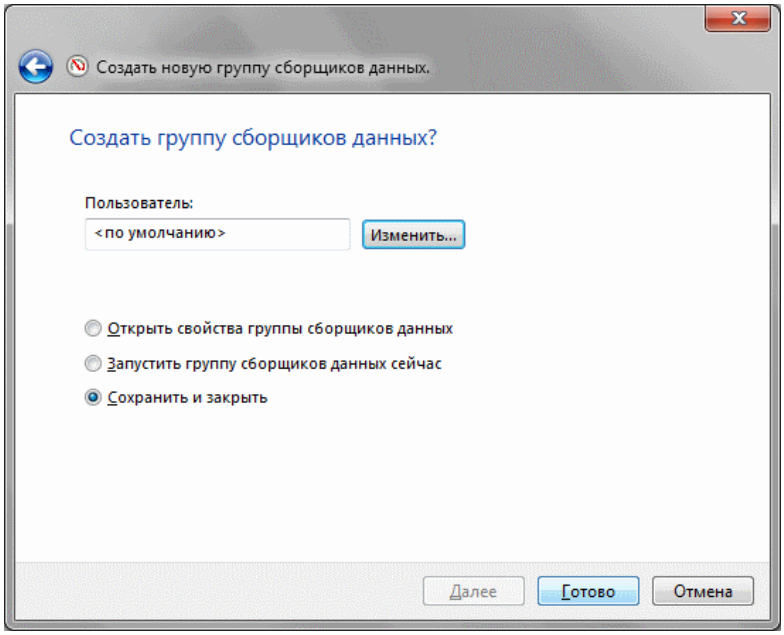


Рис. 4.1.16. Последняя страница мастера создания группы сборщиков данных

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.

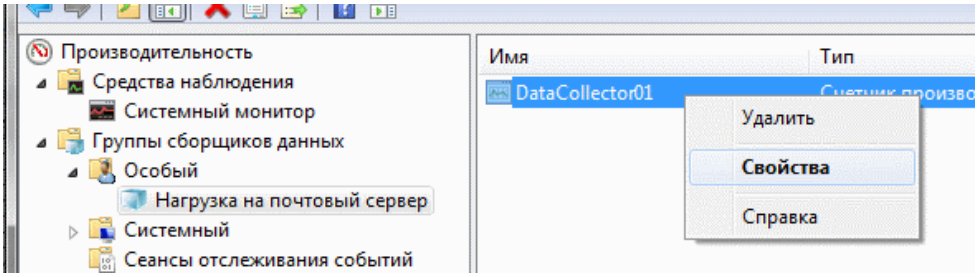


Рис. 4.1.17. Сборщик данных по имени DataCollector01

Если открыть свойства сборщика данных, можно изменить список счетчиков и формат данных (рис. 4.1.18). 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.

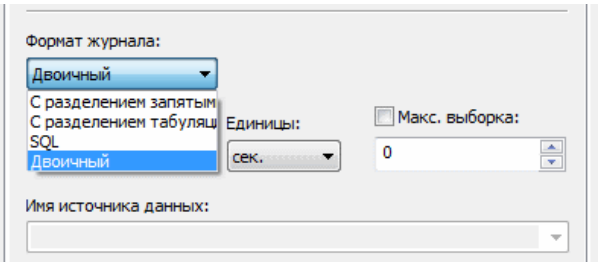


Рис. 4.1.18. Выбор формата файла журнала

Второй настраиваемый параметр — интервал выборки (рис. 4.1.19), 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).

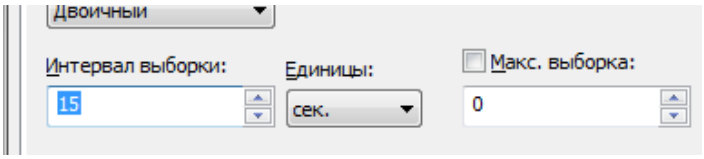


Рис. 4.1.19. Выбор интервала выборки

При настройках группы сборщиков данных по умолчанию, доступен только ручной запуск (команда **Пуск** контекстного меню, рис. 4.1.20). 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.

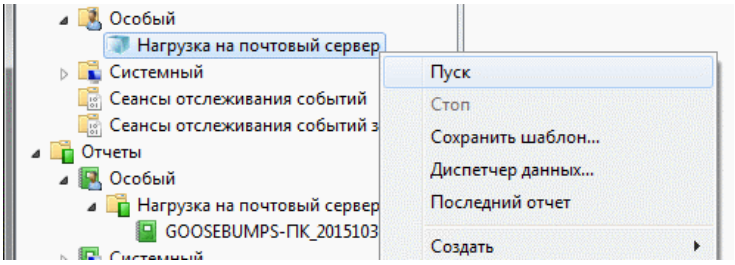


Рис. 4.1.20. Ручной запуск группы сборщиков данных

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. 4.1.21) и выбрать нужный файл.

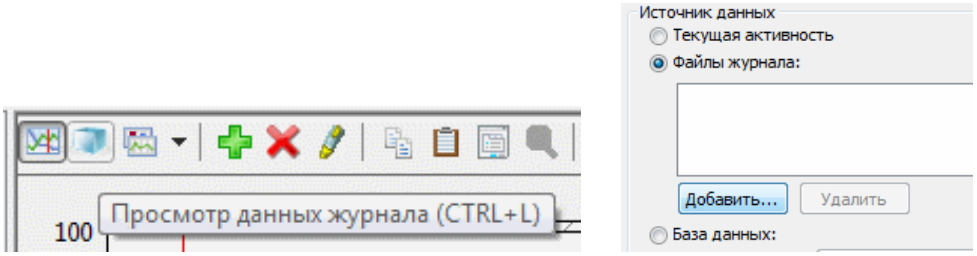


Рис. 4.1.21. Добавление файла журнала

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

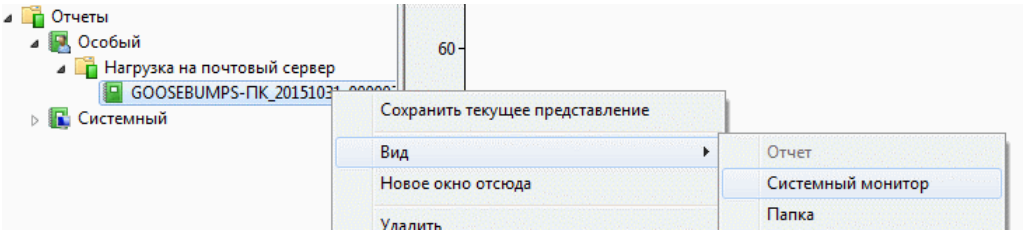


Рис. 4.1.22. Запуск системного монитора из узла Отчеты

3. Выполнить двойной щелчок мышью на соответствующем файле `*.blg` в проводнике Windows (рис. 4.1.23).

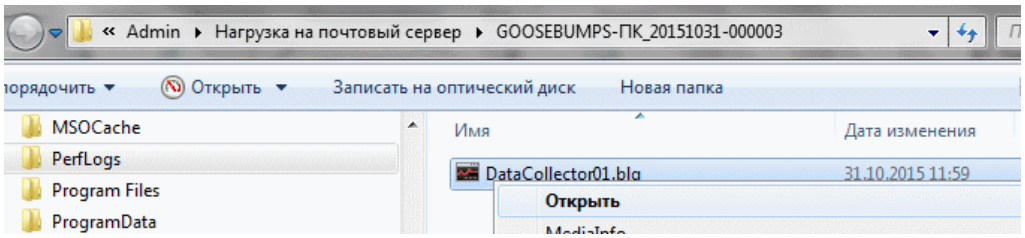


Рис. 4.1.23. Открытие информации о производительности в проводнике Windows

Откроется окно системного монитора с горизонтальной полосой прокрутки, где можно выбрать исследуемый диапазон времени (рис. 4.1.24).

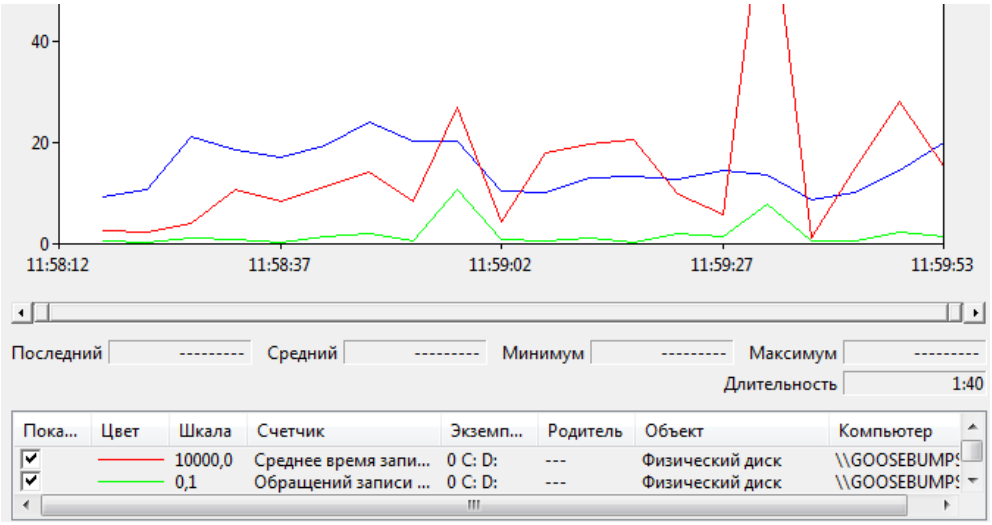


Рис. 4.1.24. Отображение информации о производительности из файла

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. 4.1.25.

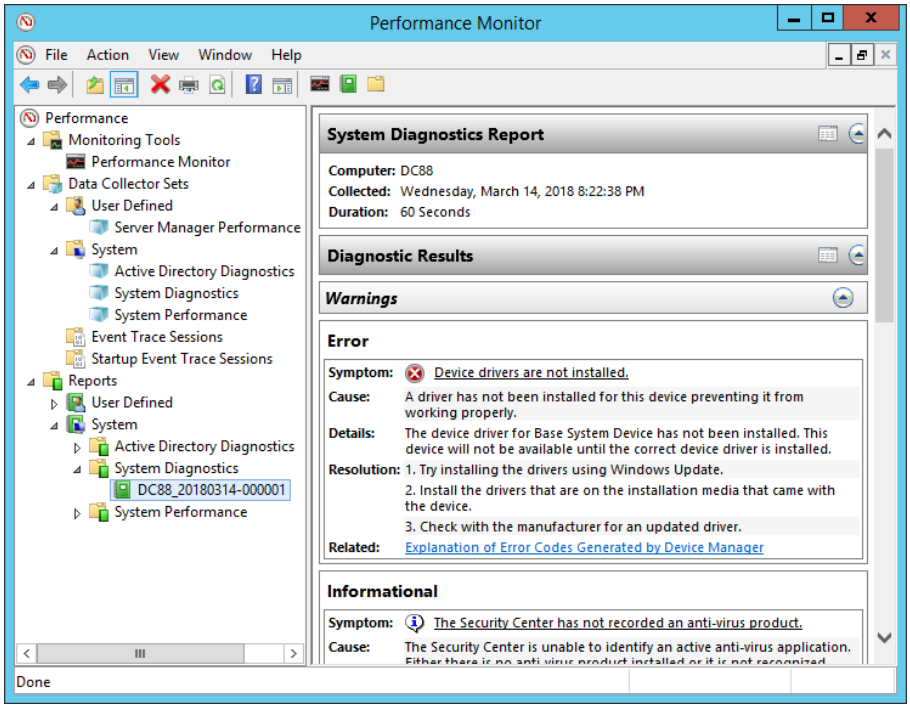


Рис. 4.1.25. Отчет для набора «Диагностика системы»

4.1.10.3. 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. 4.1.26.

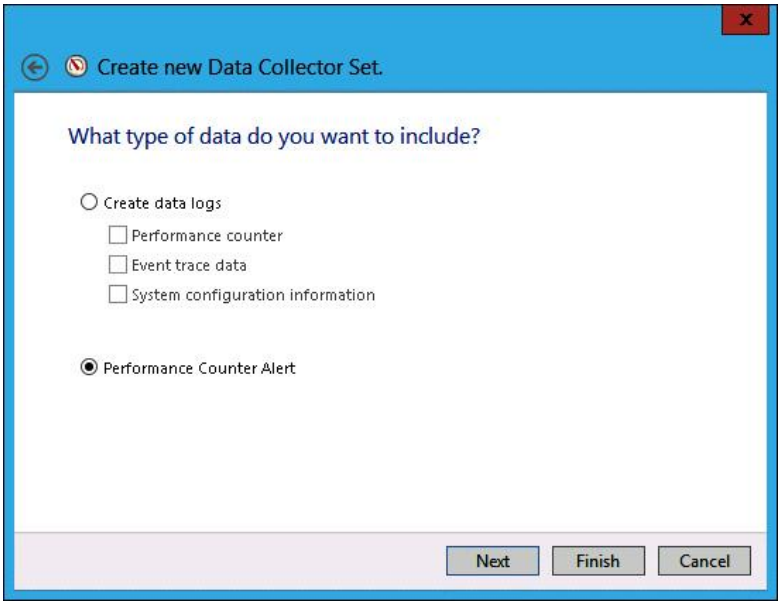


Рис. 4.1.26. Создание оповещения счетчиков производительности

Вы добавляете счетчик производительности, пороговое значение и должно ли срабатывать оповещение, если значение превышает или падает ниже этого значения. На рис. 4.1.27 показано оповещение, которое запускается, когда объем доступной памяти становится ниже 512 мегабайт.

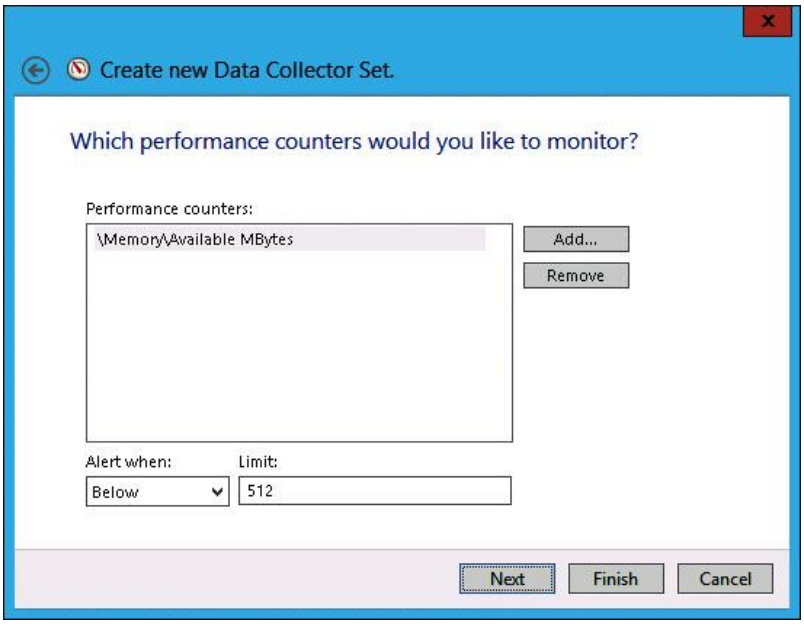


Рис. 4.1.27. Установка порога срабатывания

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. 4.1.28.

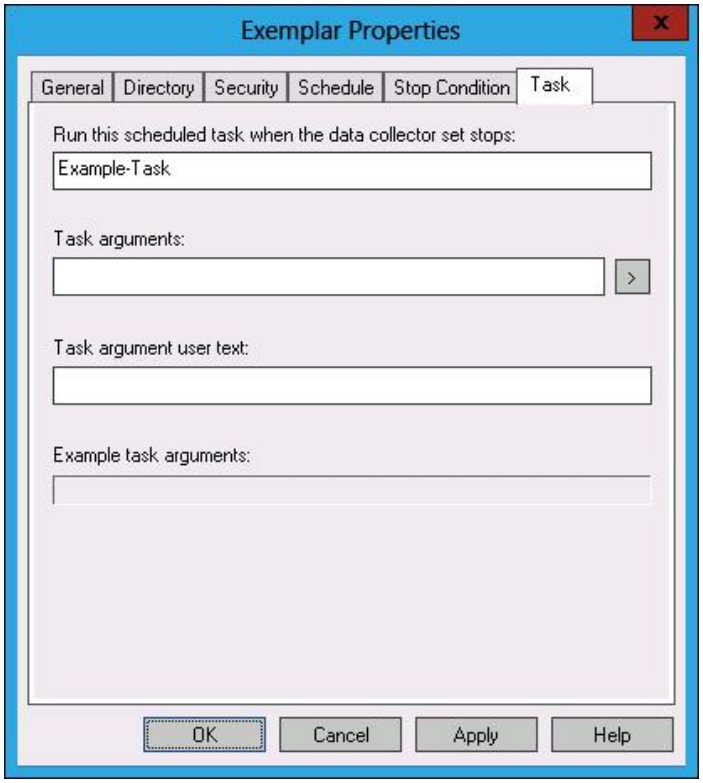


Рис. 4.1.28. Запуск запланированной задачи

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

Список использованных источников

1. Examine the Windows client architecture

https://learn.microsoft.com/en-us/training/modules/explore-windows-architecture/3-examine-windows-client-architecture

2. Examine the Windows registry

https://learn.microsoft.com/en-us/training/modules/explore-windows-architecture/4-examine-windows-registry

3. Архитектура операционной системы Windows xp

https://studfile.net/preview/5368363/page:3/

4. Единое ядро Windows

https://habr.com/ru/articles/428469/

5. Папка WinSxS — зачем она нужна и можно ли ее удалить?

https://club.dns-shop.ru/blog/t-328-prilojeniya/36072-papka-winsxs-zachem-ona-nujna-i-mojno-li-ee-udalit/

6. Изучите требования к оборудованию

https://learn.microsoft.com/en-us/training/modules/explore-windows-editions/4-examine-hardware-requirements

7. Сравнение и обсуждение выпусков Windows Server 2022

https://www.thewindowsclub.com/windows-server-2022-editions-compared?expand_article=1

8. Windows Server 2022: Comparison of editions and features

https://4sysops.com/archives/windows-server-2022-comparison-of-editions-and-features/

9. Управление рабочей средой пользователя

https://studfile.net/preview/8511263/page:5/

10. Локальные учетные записи

https://learn.microsoft.com/ru-ru/windows/security/identity-protection/access-control/local-accounts

11. Сведения о профилях пользователей

https://learn.microsoft.com/ru-ru/windows/win32/shell/about-user-profiles

12. Профили локальных пользователей

https://learn.microsoft.com/ru-ru/windows/win32/shell/local-user-profiles

13. Перемещаемые профили пользователей
https://learn.microsoft.com/ru-ru/windows/win32/shell/roaming-user-profiles

14. Обязательные профили пользователей
https://learn.microsoft.com/ru-ru/windows/win32/shell/mandatory-user-profiles

15. Управление файловой системой
https://learn.microsoft.com/ru-ru/windows/win32/shell/manage

16. SHFileOperationA function (shellapi.h)
https://learn.microsoft.com/en-us/windows/win32/api/shellapi/nf-shellapi-shfileoperationa

17. SHFILEOPSTRUCTA structure (shellapi.h)
https://learn.microsoft.com/en-us/windows/win32/api/shellapi/ns-shellapi-shfileopstructa

18. Интерфейс IFileOperation (shobjidl_core.h)
https://learn.microsoft.com/en-us/windows/win32/api/shobjidl_core/nn-shobjidl_core-ifileoperation

19. Как работают сопоставления файлов
https://learn.microsoft.com/ru-ru/windows/win32/shell/fa-how-work

20. Типы файлов
https://learn.microsoft.com/en-us/windows/win32/shell/fa-file-types

21. Программные идентификаторы
https://learn.microsoft.com/ru-ru/windows/win32/shell/fa-progids