## Веб-администрирование, веб-сервисы

Базовые сведения об IIS

Информационные службы интернета (Internet Information Services, IIS) представляют собой пакет приложений для интернета, выпускаемый компанией Microsoft. Информационные службы интернета – это не просто веб-сервер. Они обеспечивают поддержку всемирной сети, протоколов передачи файлов (FTP), протоколов передачи новостей интернета (NNTP) и простых сообщений электронной почты (SMTP). IIS полностью интегрированы в операционную систему, совместимы с приложениями Microsoft .NET и позволяют организациям реализовывать интернетвозможности, дополняющие их инфраструктуру.

Службы IIS

Существует несколько служб для поддержки IIS, их перечень приведен в панели управления службами в WS03. Набор служб зависит от установленных компонентов IIS. Если компонент не установлен, то связанная с ним служба в панели управления службами не отображается. Служба IIS Admin является главной службой администрирования IIS, остальные службы зависят от нее. При остановке службы остальные службы IIS будут также остановлены. FTP Publishing. Обеспечивает работу FTP-сервера в IIS. World Wide Web Publishing. Обеспечивает работу веб-сервера в IIS. Simple Mail Transfer Protocol (SMTP). Обеспечивает работу сервера SMTP в IIS. Network News Transfer Protocol (NNTP). Обеспечивает работу NNTP-сервера в IIS. HTTP SSL. Необходима для выполнения службой WWW Publishing функции сертификации SSL. Службы связаны между собой таким образом, что службу, для функционирования которой необходима работа другой службы, нельзя включить без второй службы. Эти зависимости показаны на вкладке Dependencies окна Properties (Свойства) службы.

Служба веб-публикации

Служба веб-публикации предоставляет конечным пользователям IIS средства веб-публикации, направляя HTTP-запросы клиентов на веб-узлы, размещенные на сервере IIS. Служба веб-публикации управляет основными компонентами IIS, которые обрабатывают HTTP-запросы, а также устанавливают параметры и управляют работой веб-приложений.

Служба веб-публикации запускается в виде файла Iisw3adm.dll в программе Svchost.exe

Служба FTP

Служба FTP обеспечивает полную функциональность IIS по управлению и обработке файлов.

Cлужбы FTP поддерживает изоляцию пользователей на уровне узла, что помогает администраторам обеспечить безопасность веб-узлов и их использование на коммерческой основе.

Служба FTP запускается как файл Ftpsvc.dll в программе Inetinfo.exe

Служба SMTP

IIS позволяет отправлять и получать сообщения электронной почты с помощью службы SMTP.

Службу SMTP также можно использовать для получения сообщений с отзывами от клиентов веб-узла.

Служба SMTP не обеспечивает полной функциональности служб электронной почты.

Служба SMTP запускается как файл Smtpsvc.dll в программе Inetinfo.exe

Служба NNTP

Для обслуживания локальных дискуcсионных групп на одном компьютере можно использовать службы NNTP. Поскольку данное средство полностью совместимо с протоколом NNTP, для участия в обсуждениях группы новостей пользователи могут воспользоваться любым клиентом для просмотра новостей.

Сценарий Rfeed, находящийся в папке inetsrv, обеспечивает поддержку службой NNTP IIS загрузки новостей.

Поддержка службой NNTP репликации отсутствует. Для загрузки новостей или репликации групп новостей для нескольких компьютеров следует использовать сервер Exchange.

Служба NNTP запускается как файл Nntpsvc.dll в программе Inetinfo.exe

Служба IIS Admin

Служба IIS Admin управляет метабазой IIS и производит обновление системного реестра Microsoft Windows для службы веб-публикации, а также служб FTP, SMTP и NNTP.

Метабаза является хранилищем данных конфигурации IIS.

Служба IIS Admin предоставляет доступ к данным метабазы другим приложениям, включая основные компоненты IIS, встроенные в IIS приложения и приложения сторонних производителей, не входящие в комплект IIS, такие как средства управления и наблюдения.

Служба IIS Admin запускается как файл Iisadmin.dll в программе Inetinfo.exe

Режимы изоляции IIS

В IIS 6.0 имеются два различных режима работы, которые называются режимами изоляции приложений (режимами изоляции): режим изоляции рабочих процессов и режим изоляции IIS 5.0.

В обоих режимах в качестве средства прослушивания протокола HTTP используется файл HTTP.sys, внутренние процессы работы в этих двух режимах принципиально отличаются.

Режим изоляции рабочих процессов позволяет воспользоваться всеми преимуществами усовершенствованной архитектуры IIS 6.0 и использует основной компонент рабочих процессов. Режим изоляции IIS 5.0 предназначен для запуска приложений, рассчитанных для работы со специальными средствами и возможностями IIS 5.0.

Выбор режима изоляции приложений IIS влияет на производительность, надежность, безопасность и доступность различных средств.

Режим изоляции рабочих процессов является наиболее предпочтительным для IIS 6.0, так как он предоставляет более надежную платформу для работы приложений.

Режим изоляции рабочих процессов также обеспечивает повышенный уровень безопасности благодаря тому, что по умолчанию приложениям, работающим в рабочих процессах, назначаются учетные записи NetworkService.

Приложениям, работающим в режиме изоляции IIS 5.0, назначаются учетные записи LocalSystem, что предоставляет доступ и возможность вмешательства практически во все ресурсы компьютера.

Режим изоляции рабочих процессов

Использование режима изоляции рабочих процессов открывает такие возможности, как объединение приложений в группы, а также использование средств перезапуска и определения работоспособности.

На рисунке видно, что код приложения загружается только в рабочий процесс.

Примерами кодов приложений являются приложения ASP и ASP.NET.

Модули выполнения для этих программных платформ реализованы как расширения интерфейса ISAPI.

Пошаговая процедура обработки запроса в режиме изоляции рабочих процессов выглядит следующим образом.

1. Запрос поступает в программу HTTP.sys.
2. Программа HTTP.sys определяет допустимость запроса. Если запрос является недопустимым, то клиенту возвращается код для недопустимого запроса.
3. Если запрос является допустимым, то программой HTTP.sys проверяется наличие соответствующего ответа в кэше режима ядра.
4. При наличии ответа в кэше он отправляется программой HTTP.sys немедленно.
5. При отсутствии ответа в кэше программа HTTP.sys определяет нужную очередь запросов, и данный запрос помещается в эту очередь.
6. Если этой очереди не назначен ни один рабочий процесс, то программа HTTP.sys отправляет службе веб-публикации запрос на запуск рабочего процесса.
7. Запрос извлекается рабочим процессом из очереди запросов и обрабатывается.
8. Ответ возвращается рабочим процессом программе HTTP.sys.
9. Программа HTTP.sys отправляет ответ клиенту и заносит запрос в журнал, если заданы соответствующие настройки

Структура каталогов IIS

ASP Compiled Templates - Содержит используемый шаблон ASP.

History - Содержит историю изменений метабазы, позволяющую выполнять откат изменений в метабазе.

iisamdpwd - Содержит ASP-страницы, относящиеся к аутентификации IIS Admin.

MetaBack - Каталог по умолчанию для резервных файлов метабазы.

Веб-сайт администрирования

В IIS 6 веб-сайт администрирования позволяет управлять всем сервером Windows из локального или удаленного веб-браузера. Он функционирует через SSL, используя порт 8098 по умолчанию. Для доступа к веб-сайту администрирования введите в строке адреса браузера https://имя\_компьютера:8098 (где имя\_компьютера представляет собой имя компьютера, который необходимо администрировать).

Файлы справки IIS

Все файлы справки IIS 6 перемещены в централизованное место расположения вместе с остальными файлами справки Windows. Самым простым способом вызова справки IIS является выбор команды Help/Help Topics (Справка/Вызов справки) в консоли MMC.

Учетные записи, используемые в IIS

Поскольку функционирование всех компонентов WS03 рассматривается с точки зрения безопасности, и для доступа необходима учетная запись, IIS устанавливает две учетные записи и одну группу в базу данных учетных записей для использования их в работе. Эти элементы позволяют IIS выполнять программы и рабочие процессы, а пользователям – осуществлять доступ к сайту.

IUSR\_COMPUTERNAME

Учетная запись обеспечивает анонимный доступ к веб-сайту при подключении пользователя к веб-странице без представления входных данных. Такой пользователь по умолчанию является членом группы Guest (Гость).

IWAM\_COMPUTERNAME

Учетная запись используется для запуска рабочих процессов и является членом группы IIS\_WPG.

IIS\_WPG

Члены этой группы могут запускать рабочие процессы. Любая учетная запись, выполняющая рабочие процессы, должна быть членом данной группы. Это учетная запись с низким уровнем безопасности, обладающая правами сетевой службы. Процессы, использующие уровень прав Network Service (Сетевая служба), осуществляют доступ к серверу так, как если бы они находились вне сервера, и поэтому не имеют прямого доступа к операционной системе.

Что такое метабаза IIS

Метабаза является иерархически организованным хранилищем данных о конфигурации IIS и схем, используемых при настройке.

Конфигурация метабазы и схемы для IIS 4.0 и IIS 5.0 хранились в файле двоичного формата, что затрудняло его чтение и редактирование.

В IIS 6.0 вместо одного двоичного файла (MetaBase.bin) используются текстовые XML-файлы MetaBase.xml и MBSchema.xml.

Файлы конфигурации хранятся на компьютере в папке systemroot\System32\Inetsrv. Только Администраторы могут просматривать и изменять эти файлы.

Сведения о конфигурации IIS хранятся в файле MetaBase.xml, а схема метабазы хранится в файле MBSchema.xml.

При запуске IIS эти файлы считываются уровнем хранилища и затем записываются в метабазу в памяти с помощью объектов ABO (Admin Base Objects).

Сведения о настройке метабазы

Предусмотрено несколько способов для изменения значений, хранящихся в метабазе. Значения в метабазе можно записывать и считывать с помощью следующих ресурсов:

* Диспетчер IIS. Приложение, предоставляющее интерфейс пользователя; позволяет изменять метабазу, находящуюся в памяти (наиболее безопасный способ обновления метабазы).
* Интерфейсы ADSI (Active Directory Service Interfaces). Набор интерфейсов программирования, которые можно использовать в командной строке или в сценарии.
* Интерфейсы WMI (Windows Management Instrumentation). Набор интерфейсов программирования, которые можно использовать в командной строке или в сценарии.
* COM-библиотека или исполняемая программа. Библиотека динамической компоновки COM-объектов (.dll) или исполняемая программа (.exe), такая как MetaEdit, которую можно использовать для настройки метабазы в памяти. MetaEdit — инструментальное средство Майкрософт для редактирования метабазы.

Изменения параметров конфигурации, выполненные с помощью указанных средств, заносятся в метабазу, находящуюся в памяти, посредством объектов ABO (Admin Base Objects).

Метабаза в памяти представляет собой копию файлов MetaBase.xml и MBSchema.xml в файловом кэше IIS

Каждому объекту IIS ADSI соответствует раздел в схеме метабазы.

Методы Get, Put и SetInfo — три из восьми методов объекта Windows ADSI, содержащихся во всех объектах ADSI.

С их помощью можно получать и задавать значения свойств, а также сохранять сведения в метабазе.

Adsutil.vbs

Adsutil.vbs — служебная программа администрирования IIS, использующая язык VBScript и интерфейсы ADSI для управления конфигурацией IIS.

Сценарий следует запускать с помощью программы CScript, компонента сервера сценариев Windows (Windows Script Host).

Журнал метабазы

Метабаза в IIS периодически резервируется и сортируется по версиям. При этом используются два номера версии: главный и дополнительный.

По умолчанию сохраняются десять копий метабазы, что позволяет осуществлять откат, восстанавливая одну из предыдущих версий. Количество резервируемых версий настраивается с помощью редактирования свойства MaxHistoryFiles метабазы. Как правило, число сохраняемых копий не должно быть меньше десяти. При каждом сохранении метабазы ее резервная копия и соответствующая схема записываются в папку history. IIS проверяет количество пар резервных файлов, и если оно становится больше, чем значение параметра MaxHistoryFiles, то удаляются наиболее старые пары.

Резервирование и восстановление метабазы

Несмотря на то, что можно использовать файлы истории для восстановления файлов конфигурации метабазы, выполнение ее резервного копирования имеет некоторые преимущества. Одним из них является то, что файлы истории метабазы используются только на том компьютере, на котором они были созданы, в то время как резервные копии можно восстановить на любом другом компьютере. Резервирование метабазы выполняется по запросу через IIS MMC.

Пулы приложений

IIS вводит принципиально новый способ поддержки приложений. Пулы приложений позволяют выполнять код в изолированной среде. Каждый пул приложения обслуживается одним или несколькими рабочими процессами.

При запуске IIS служба веб-администрирования (Web Administration Service) инициализирует таблицу маршрутизации пространства имен http.sys с одной записью для каждого приложения. Эта таблица определяет, к какому пулу приложений должно быть маршрутизировано приложение. При получении запроса http.sys дает WAS команду на запуск одного или нескольких рабочих процессов для поддержки этого пула приложения. Такая изоляция процессов в целом повышает стабильность веб-сервера.

Мониторинг состояния

WAS имеет возможность контролировать состояние ("здоровье") IIS посредством отслеживания рабочих процессов и мониторинга степени их исправности. Это позволяет предотвратить отказы IIS. WAS отслеживает рабочие процессы посредством отправки пинг-запросов через установленные промежутки времени.

Если рабочий процесс не отвечает на пинг-запрос, WAS завершает процесс и запускает новый, что сохраняет возможность системы отвечать на системные запросы даже в случае "зависания" рабочего процесса. При возникновении сбоя в рабочем процессе и его "зависании" http.sys будет выдавать последовательные запросы до тех пор, пока WAS не запустит новый рабочий процесс для поддержки этого пула приложения. Конечный пользователь столкнется с временной потерей обслуживания приложениями в данном пуле приложений, в то время как ключевые веб-службы и другие приложения продолжат свою работу.

Веб-наборы

Для поддержки одного пула приложений можно установить несколько рабочих процессов. Такие структуры называются веб-наборами. Веб-наборы улучшают мультипроцессорную масштабируемость, так как каждый рабочий процесс становится родственным отдельному процессору для увеличения количества обращений в кэш этого процессора. При возникновении перегрузки рабочего процесса его поддерживают другие рабочие процессы.

Этот подход снижает необходимость перезагрузки сервера даже при обновлении компонентов, так как просто перезапускается пул приложения. Количество запросов в очереди для каждого пула приложения указывается в http.sys при выполнении рабочего процесса в режиме изоляции. По достижении этого лимита новые запросы к пулу приложения не обрабатываются, и пользователь получает сообщение об ошибке HTTP 503.

Источники:

<https://ideafix.name/UNIVERSITY/NETWORK3/1.pdf>

<https://docplayer.ru/38212052-Administrirovanie-v-informacionnyh-sistemah-lekciya-4-udalennoe-administrirovanie.html>

<https://perviydoc.ru/v32633/%D0%B0%D0%B4%D0%BC%D0%B8%D0%BD%D0%B8%D1%81%D1%82%D1%80%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D1%85_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC._%D0%B2%D0%B5%D0%B1-%D1%81%D0%BB%D1%83%D0%B6%D0%B1%D1%8B_%D0%B8_%D1%81%D0%B5%D1%80%D0%B2%D0%B8%D1%81%D1%8B._%D0%BB%D0%B5%D0%BA%D1%86%D0%B8%D1%8F_3._%D0%B0%D0%B4%D0%BC%D0%B8%D0%BD%D0%B8%D1%81%D1%82%D1%80%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%B2%D0%B5%D0%B1-%D1%83%D0%B7%D0%BB%D0%BE%D0%B2._%D1%81%D0%BB%D1%83%D0%B6%D0%B1%D1%8B_iis>