Администрирование в информационных системах

Веб-службы и сервисы

Администрирование веб-служб

Службы ИНТЕРНЕТ в Windows Server 2003

- Информационные службы Интернета (IIS) вместе с продуктами семейства Microsoft Windows Server 2003 обеспечивают комплексные, надежные, масштабируемые, безопасные и регулируемые возможности веб-сервера при работе с внутренними и внешними сетями, а также с Интернетом.
- IIS является инструментом для создания мощных коммуникационных платформ динамических сетевых приложений.
- Различные организации используют IIS для поддержки и управления веб-страниц в Интернете или во внутренней сети, для поддержки и управления FTP-узлами, для маршрутизации новостей и почты, которые используют протоколы NNTP и SMTP.

Возможности служб IIS

- IIS 6.0 поддерживает последние веб-стандарты, такие как Microsoft ASP.NET, XML и протокол SOAP, для разработки, реализации и управления веб-приложениями.
- IIS 6.0 включает новые возможности для достижения высокой производительности, надежности, масштабируемости и безопасности большого числа веб-узлов на одном или нескольких серверах IIS.

Повышенная надежность служб IIS 6.0

- IIS 6.0 обладает повышенной надежностью по сравнению с предыдущими версиями благодаря новой архитектуре обработки запросов, которая обеспечивает **изолированную среду** для выполнения приложений.
- Это позволяет отдельным веб-приложениям работать независимо друг от друга в виде независимых рабочих процессов.

Режимы работы

- IIS 6.0 можно настроить либо для работы в режиме изоляции рабочих процессов, в котором любой процесс запускается в изолированной среде, либо в режиме изоляции IIS 5.0, в котором можно запускать веб-приложения, несовместимые с режимом изоляции рабочих процессов.
- В режиме изоляции рабочих процессов можно изолировать любой объект или процесс — от отдельного веб-приложения до нескольких узлов, обеспечив их работу в виде самостоятельного независимого рабочего процесса службы веб-публикации.
- Это позволит исключить возможность сбоя в работе одного приложения или узла из-за сбоя другого. Изоляция приложений или узлов в отдельные процессы упрощает ряд задач по управлению.

Группы приложений

- Режим изоляции рабочих процессов позволяет клиентам создавать несколько групп приложений, где каждая группа приложений может иметь уникальную конфигурацию.
- При этом повышается производительность и надежность, поскольку эти группы приложений получают ответы на запросы непосредственно из ядра, а не от службы Интернета.
- Группа приложений может быть настроена в режиме изоляции рабочих процессов для обслуживания любых объектов — от одного веб-приложения до нескольких веб-приложений и узлов.
- Назначение приложения группе приложений позволяет еще глубже изолировать приложения и выполняется так же просто, как назначение этому приложению группы в метабазе, к которой оно должно маршрутизироваться.
- Узлы по умолчанию считаются обычным приложением, где корневое пространство имен "/" настраивается в качестве приложения.

Обеспечение безопасности

- IIS 6.0 предоставляет набор средств и технологий обеспечения безопасности, гарантирующих согласованность содержимого веб- и FTP-узлов, а также передаваемых через эти узлы данных.
- Функции обеспечения безопасности IIS решают следующие связанные с безопасностью задачи:
  - проверка подлинности клиента и сервера,
  - управление доступом,
  - шифрование потока данных,
  - использование цифровых сертификатов,
  - аудит.

Проверка подлинности

Метод	Уровень безопасности	Способ Отправки паролей	Использование с прокси-серверами и брандмауэрами	Требования к клиенту
Анонимная проверка подлинности	Отсутствует	Не применяется	Доступно	Любой обозреватель
Обычная проверка подлинности	Низкий	Открытый текст в кодировке Base64	Доступно, но отправка пароля незащищенным текстом через прокси-сервер или брандмауэр рискованна, поскольку кодировка Base64 не зашифрована и легко декодируется	Большинство обозревателей
Краткая проверка подлинности	Средний	Хешированная	Доступно	Internet Explorer 5 или более поздней версии
Расширенная краткая проверка подлинности	Средний	Хешированная	Доступно	Internet Explorer 5 или более поздней версии
Встроенная проверка подлинности Windows	Высокий	Хешированная при использовании NTLM. Билет Kerberos при использовании Kerberos	Недоступно, за исключением использования через подключение PPTP	Internet Explorer 2.0 или более поздние версии для NTLM; Windows 2000 или более поздние версии с Internet Explorer 5 или более поздними версиями для Kerberos
Проверка подлинности сертификатов	Высокий	Отсутствует	Доступно при использовании подключения SSL	Internet Explorer и Netscape
Проверка подлинности .NET Passport	Высокий	Зашифрована	Доступно при использовании подключения SSL	Internet Explorer и Netscape

Управление доступом

- Правильное управление доступом к содержимому веб- и FTP-узлов является основным элементом организации защищенного веб-сервера.
- Используя возможности Windows и системы безопасности IIS, можно эффективно управлять доступом пользователей к содержимому веб- и FTP-узлов. Управление доступом может быть организовано на нескольких уровнях, от всего веб- или FTP-узла до отдельных файлов.
- Каждой учетной записи предоставляются права пользователя и разрешения.
  - **Права пользователя** являются правами на выполнение определенных действий на компьютере или в сети.
  - **Разрешения** представляют правила, связанные с

Схема управление доступом

- Клиент запрашивает ресурс на сервере.
- IP-адрес клиента проверяется на ограничения IP-адресов, заложенные в IIS. Если IP-адресу отказано в доступе, запрос отклоняется и пользователю возвращается сообщение «403 Доступ запрещен».
- Сервер, если это задано в настройке, запрашивает у клиента информацию для проверки подлинности. Обозреватель либо приглашает пользователя указать имя и пароль, либо предоставляет эту информацию автоматически.
- IIS проверяет допустимость учетной записи пользователя. Если учетная запись пользователя не является допустимой, запрос отклоняется и пользователю возвращается сообщение «401 Отказано в доступе».
- IIS проверяет наличие у пользователя веб-разрешений для запрашиваемого ресурса. Если таких разрешений нет, запрос отклоняется и пользователю возвращается сообщение «403 Доступ запрещен».
- Добавляются любые модули безопасности, такие как олицетворение Microsoft ASP.NET.
- IIS проверяет для ресурса разрешения NTFS на статические файлы, ASP-страницы и CGI-файлы. Если у пользователя нет разрешений NTFS, запрос отклоняется и пользователю возвращается сообщение «401 Отказано в доступе».
- Если у пользователя имеются разрешения NTFS, запрос

Шифрование

- Шифрованием называют преобразование элементов информации с помощью математической функции, после которого восстановление исходной информации становится исключительно трудным для всех, кроме лица, которому адресована информация. Основой этого процесса является математическое значение, которое называют *ключом*, используемое функцией для однозначного сложного преобразования информации.
- Веб-сервер использует для защиты связи с пользователями в значительной степени один и тот же процесс шифрования. После установления защищенной связи специальный *ключ сеанса* используется и веб-сервером, и веб-обозревателем пользователя как для шифрования, так и для расшифровки информации. Например, когда правомочный пользователь пытается загрузить файл с веб-узла, для которого требуется безопасный канал связи, веб-сервер использует ключ сеанса для шифрования файла и относящихся к нему заголовков HTTP. После получения зашифрованного файла веб-обозреватель использует копию того же ключа сеанса для восстановления файла.
- Этот метод шифрования, несмотря на защиту, имеет существенный недостаток: при создании защищенного канала по незащищенной сети может передаваться копия ключа сеанса. Это означает, что компьютерному взломщику, желающему нарушить систему безопасности подключения, достаточно перехватить ключ сеанса. Для предотвращения таких ситуаций на веб-сервере применяется дополнительный способ шифрования.

Шифрование с открытым ключом

- Средство безопасности веб-сервера, работающее по протоколу SSL, использует метод шифрования, известный под именем шифрования с *открытым ключом* для защиты ключа сеанса от перехвата при передаче. Шифрование с открытым ключом, в котором используются два дополнительных ключа, *закрытый* и *общий*, выполняется следующим образом:
  - Веб-обозреватель пользователя устанавливает защищенную связь (https://) с веб-сервером.
  - Веб-обозреватель пользователя и сервер вступают в диалог, чтобы определить уровень шифрования, который должен использоваться для защиты подключений.
  - Веб-сервер отправляет обозревателю его открытый ключ.
  - Веб-обозреватель шифрует сведения, используемые при создании ключа сеанса, с помощью открытого ключа и отправляет их на сервер.
  - С помощью закрытого ключа сервер расшифровывает сообщение, создает ключ сеанса, шифрует его с помощью открытого ключа и отправляет обозревателю.
  - Ключ сеанса используется как сервером, так и веб-обозревателем для шифрования и расшифровывания передаваемых данных.

Сертификаты

- Сертификаты содержат сведения, используемые для проверки подлинности пользователей сети. Как и обычные формы установления подлинности, сертификаты позволяют веб-серверам и пользователям проверить подлинность друг друга перед установлением соединения.
- Сертификаты содержат также значения для шифрования, или *ключи*, которые используются для установления соединения по протоколу SSL между клиентом и сервером. При использовании соединения SSL такие данные, как номера банковских карт, передаются по сети в зашифрованном виде, поэтому не могут быть перехвачены и использованы неавторизованными лицами.
- Существуют два типа сертификатов, используемых протоколом SLL, — серверные и клиентские сертификаты. Каждый из них имеет свой формат и назначение.
  - *Серверные сертификаты* содержат сведения о сервере, что позволяет клиенту однозначно идентифицировать сервер до передачи важной информации.
  - *Клиентские сертификаты* содержат личные данные клиентов, запрашивающих доступ к узлу, и позволяют идентифицировать пользователей перед предоставлением доступа к ресурсам узла.

Аудит

- Для отслеживания действий пользователей и обнаружения попыток несанкционированного доступа к каталогам и файлам в системе NTFS можно использовать средства аудита.
- В журнал аудита могут быть записаны следующие события:
  - успешные и неуспешные попытки входа пользователей в систему;
  - попытки доступа пользователей к запрещенным учетным записям;
  - попытки выполнения пользователями запрещенных команд.

Администрирование IIS

- Для удовлетворения потребностей различных групп пользователей IIS предоставляет широкий спектр средств управления и администрирования.
- Администраторы могут настроить сервер, на котором работает IIS 6.0, с помощью:
  - Диспетчера IIS
  - Административных сценариев
  - Редактируя неформатированный файл конфигураций IIS
  - Удаленного доступа.

Неформатированная метабаза

- Метабаза является хранилищем для большинства значений конфигурации IIS. Ее модернизация привела к значительному ускорению процессов запуска и завершения работы сервера, а также к увеличению общей производительности и удобства использования самой метабазы. Данная версия IIS включает в себя редактируемый вручную или программно неформатированный файл конфигураций метабазы .XML. Для хранения метабазы используются два неформатированных файла формата .XML:
  - файл **MetaBase.xml** содержит значения конфигурации IIS;
  - файл **MBSchema.xml** хранит схему метабазы XML и следит за правильностью ее настройки.

Сценарии администрирования

- Администрирование из командной строки позволяет выполнять задачи управления более эффективно.
- IIS предоставляет сценарии для следующих задач:
  - создание, удаление, запуск, остановка и регистрация веб-узлов;
  - создание, удаление, запуск, остановка и регистрация FTP-узлов;
  - создание и удаление виртуальных веб-каталогов;
  - создание и удаление приложений;
  - экспорт и импорт конфигурации IIS;
  - создание резервных копий и восстановление

Создание веб-узлов

- Сценарий для командной строки iisweb.vbs, хранящийся в папке *корневой_каталог_системы*\system32, используется для создания конфигураций веб-узлов на локальных и удаленных компьютерах под управлением операционной системы из семейства Windows Server 2003 с установленной службой версией IIS 6.0.
- Команда не создает и не удаляет содержимое, она настраивает структуру каталога и некоторые файлы конфигурации IIS.
- **Синтаксис**
  - **iisweb /create** *путь имя_узла* [**/b** *порт*] [**/i** *IP-адрес*] [**/d** *заголовок_узла*] [**/dontstart**]

Удаление веб-узлов

- **Синтаксис**
  - **iisweb /delete** *веб_узел* [*веб_узел*...] [**/s** *компьютер* [**/u** [*домен*\] *пользователь***/p** *пароль*]]
- **Пример**
- В следующем примере удаляются несколько конфигураций веб-узлов на удаленном компьютере.
- Веб-узлы «Finance», «Work Group» и «Logo» расположены на сервере SRV01. В команде первые два узла определяются по имени, а веб-узел «Logo» — по пути к метабазе, «W3SVC/79116006». К тому же в команде используется параметр **/s** для ввода имени удаленного компьютера, а также параметры **/u** и **/p** для запуска команды с разрешениями

Запуск, приостановка и остановка веб-узлов

- Запуск веб-узла выполняется командой
  - **iisweb/start** *веб_узел* [*веб_узел*...] [**/s** *компьютер* [**/u** [*домен*\] *пользователь***/p** *пароль*]]
- Остановка веб-узла выполняется командой
  - **iisweb/stop** *веб_узел* [*веб_узел*...] [**/s** *компьютер* [**/u** [*домен*\] *пользователь***/p** *пароль*]]
- Приостановка веб-узла выполняется командой
  - **iisweb/pause** *веб_узел* [*веб_узел*...]

Управление ftp-узлом

- Сценарий для командной строки iisftp.vbs, хранящийся в папке *корневой_каталог_системы*\system32, используется для создания конфигураций FTP-узлов (File Transfer Protocol) на локальных и удаленных компьютерах под управлением одной из операционных систем семейства Windows Server 2003 с установленной версией IIS 6.0.
- Данная команда не создает и не удаляет содержимое, а производит настройку структуры каталога и файлов конфигурации IIS.
- При использовании сценария iisftp.vbs для создания нового FTP-узла задаются только основные свойства, необходимые для создания узла и определения его содержимого.
- Сценарий iisftp.vbs использует те же свойства по умолчанию, которые диспетчер IIS использует при создании новых FTP-узлов, и следует тем же правилам наследования свойств. Для настройки дополнительных свойств FTP-узла следует использовать диспетчер IIS.

Создание, удаление, запуск и остановка ftp-узла

- Для создания, запуска, остановки и удаления ftp-узла используются команды подобные командам управления веб-узлами:
  - Создание:
    - **iisftp /create** *путь имя_узла* [**/b** *порт*] [**/i** *IP_адрес*] [**/dontstart**] [**/isolation** {*AD*|*локальный*} [**/domain** *имя_домена* **/Admin** [*домен*\] *пользователь* **/AdminPwd***пароль*]] [**/s** *компьютер* [**/u** [*домен*\] *пользователь***/p** *пароль*]]
  - Запуск
    - **iisftp/start** *FTP_узел* [*FTP_узел*...] [**/s** *компьютер* [**/u** [*домен*\] *пользователь***/p** *пароль*]]
  - Остановка
    - **iisftp/stop** *FTP_узел* [*FTP_узел*...] [**/s** *компьютер* [**/u** [*домен*\] *пользователь***/p** *пароль*]]
  - Удаление
    - **iisftp /delete** *FTP_узел* [*FTP_узел*...] [**/s** *компьютер* [**/u** [*домен*\] *пользователь***/p** *пароль*]]

Виртуальные каталоги

- Сценарий для командной строки iisvdir.vbs, хранящийся в папке *корневой_каталог_системы*\system32, используется для создания виртуальных веб-каталогов на локальных и удаленных компьютерах под управлением операционной системы из семейства Windows Server 2003 с установленной версией IIS 6.0.
- Команда не создает и не удаляет содержимое, она настраивает структуру виртуального каталога и файлы конфигурации IIS.
- При использовании сценария iisvdir.vbs для создания нового виртуального веб-каталога задаются только основные свойства, необходимые для создания узла и определения его содержимого.
- Сценарий iisvdir.vbs использует те же свойства по умолчанию, которые диспетчер IIS использует при создании новых виртуальных каталогов, и следует тем же правилам наследования свойств.
- Для настройки дополнительных свойств каталога следует использовать диспетчер IIS.
- Например, для создания виртуального каталога используется команда:
  - **iisvdir /create** *веб_узел*[/*виртуальный_путь*] *имя физический_путь* [**/s** *компьютер* [**/u** [*домен*\]*пользователь***/p** *пароль*]]

Управление конфигурациями IIS

- Для создания и управления файлами конфигурации IIS на компьютерах под управлением операционной системы из семейства Windows Server 2003 с установленной версией IIS 6.0, используются два сценария для командной строки, хранящихся в папке *корневой_каталог_системы*\System32.
- Сценарий iisback.vbs создает архивные копии конфигурации IIS (метабазы и схемы) локального или удаленного компьютера и управляет ими.
- Сценарий iiscnfg.vbs импортирует и экспортирует все или выбранные элементы метабазы IIS на локальном или удаленном компьютере, или

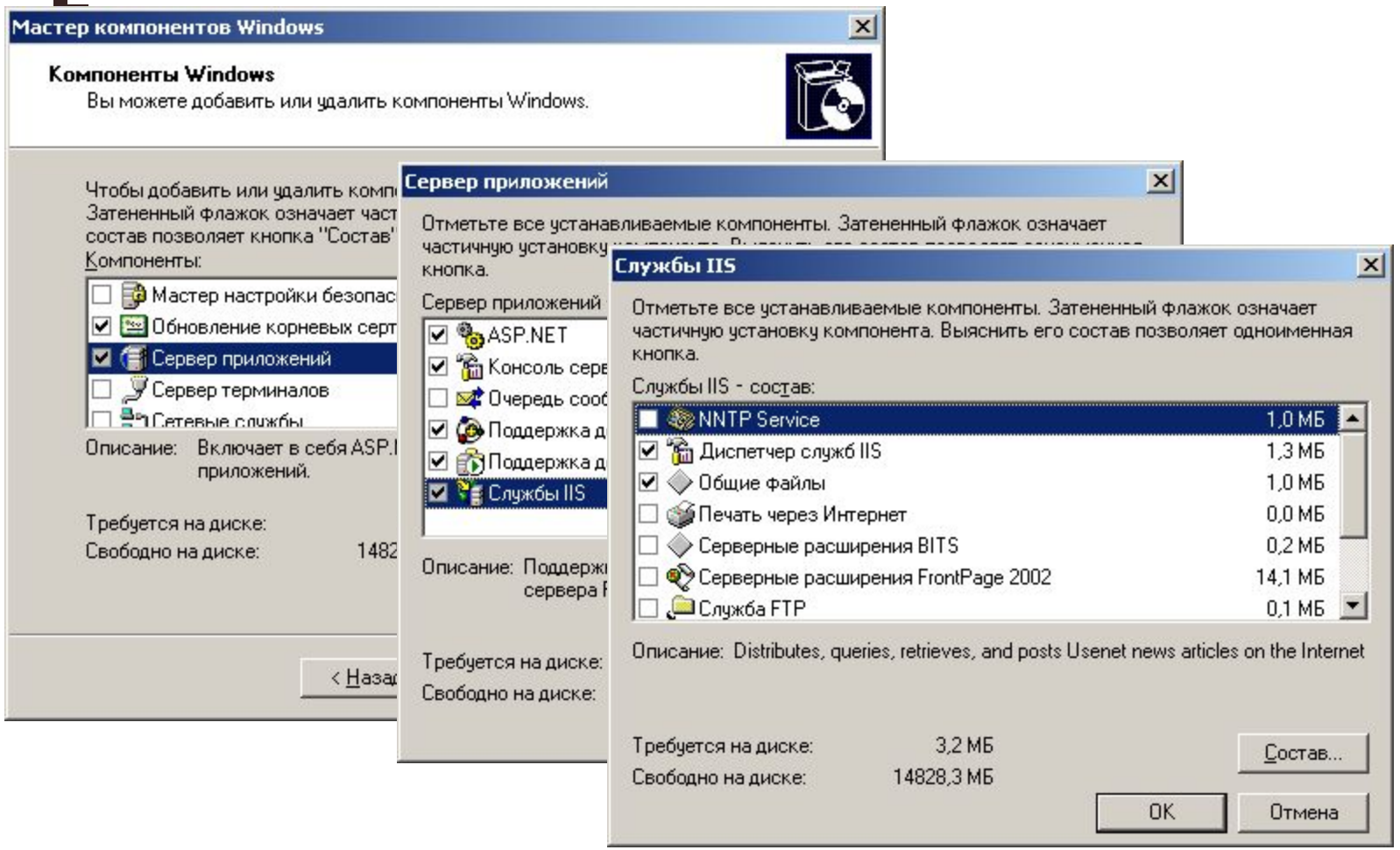
Управление резервными копиями

- При каждой операции архивирования (**/backup**) создается два файла: файл .MD*x* для хранения метабазы и файл .SC*x* для хранения схемы, где *x* является номером версии резервной копии. Служба IIS и сценарий iisback.vbs сохраняют файлы резервных копий в папке *корневой_каталог_системы*\System32\inetsrv\MetaBack.
- Метабаза и схема конфигурации IIS включают свойства системы и свойства сеанса.
- Не следует выполнять копирование или импорт метабазы или схемы одного сервера IIS на другой сервер IIS, не внося изменений.
- Для полного или частичного копирования конфигурации метабазы с одного сервера на другой используйте сценарий iiscnfg.vbs.
- Создание резервной копии:
  - **iisback /backup** [**/b** *имя_резервной_копии*] [**/v** {*Integer* | **HIGHEST_VERSION** | **NEXT_VERSION**}] [**/overwrite**] [**/e** *пароль_шифрования*] [**/s** *компьютер* [**/u** [*домен*\]*пользователь***/p** *пароль*]]
- Восстановление из резервной копии
  - **iisback /restore/b** *имя_резервной_копии* [**/v** {*целое* | **HIGHEST_VERSION**}] [**/e** *пароль_шифрования*] [**/s** *компьютер* [**/u** [*домен*\]*пользователь***/p** *пароль*]]
- Удаление архивной конфигурации
  - **iisback /delete** [**/b***имя_резервной_копии*] [**/v** {*целое* | **HIGHEST_VERSION**}] [**/s***компьютер* [**/u** [*домен*\]*пользователь***/p***пароль*]]
- Вывод списка резервных копий
  - **iisback /list** [**/s** *компьютер* [**/u** [*домен*\]*пользователь***/p** *пароль*]]

Копирование конфигураций

- Сценарий для командной строки iiscnfg.vbs, хранящийся в папке *корневой_каталог_системы*\system32, используется для копирования метабазы и схемы IIS с одного компьютера на другой. Оба компьютера должны работать под управлением одной из операционных систем семейства Windows Server 2003 с установленной версией IIS 6.0.
- Операция копирования (**/copy**) сценария iisback.vbs используется для создания резервной копии исходной метабазы и схемы. Затем резервные копии файлов (.MD*x* и .SC*x*) копируются на конечный компьютер, при этом сценарий iisback.vbs заменяет метабазу и схему конечного компьютера резервной копией.
- Все эти операции можно выполнить вручную, однако операция **/copy** представляет собой удобный одношаговый способ репликации конфигурации IIS. Операция **/copy** обладает возможностями сценария iissync.exe, средства, ранее включавшегося в Windows.
- Операция **/copy** не копирует содержимое сервера, например веб-страницы и файлы FTP, связанное с конфигурацией IIS. Вместо этого операция **/copy** изменяет свойства метабазы, связанные с компьютером и системой, таким образом, что они

Установка дополнительных компонентов



Диспетчер служб IIS