Администрирование в информационных системах

Веб-службы и сервисы
Администрирование веб-служб

Понятие веб-службы

- **Веб-служба**, *веб-сервис* (*web service*) — программная система, идентифицируемая строкой URI (*Uniform Resource Identifier*), общедоступные интерфейсы которой определены на языке XML.
- Программные системы могут взаимодействовать с ней посредством сообщений, основанных на XML, и передаваемых с помощью интернет-протоколов.

Основные понятия

- **URI** (***Uniform Resource Identifier***) — единообразный идентификатор ресурса —короткая последовательность символов, идентифицирующая абстрактный или физический ресурс.
- **Единый указатель ресурсов** (***URL — Uniform Resource Locator***) — определитель местонахождения ресурса.

Структура URL

- <схема>://<логин>:<пароль>@<хост>:<порт>/<URL-путь>
  - *схема* - схема обращения к ресурсу, в большинстве случаев имеется в виду сетевой протокол
  - *логин* - имя пользователя, используемое для доступа к ресурсу
  - *пароль* - пароль, ассоциированный с указанным именем пользователя *хост* полностью прописанное доменное имя хоста в системе DNS или IP-адрес хоста в форме четырёх десятичных чисел, разделённых точками.
  - *порт* - порт хоста для подключения
  - *URL-путь* уточняющая информация о месте нахождения ресурса (зависит от протокола)
- Например:
  - ftp://user:p@$$word@ftp.company.com/MyLib

Достоинства веб-служб

- Веб-службы обеспечивают взаимодействие программных систем независимо от платформы;
- Веб-службы основаны на базе открытых стандартов и протоколов. Благодаря использованию XML достигается простота разработки и отладки веб-служб;
- Интернет-протокола HTTP обеспечивает возможность взаимодействия программных систем через межсетевой экран.

Службы ИНТЕРНЕТ в Windows Server 2003

- Информационные службы Интернета (IIS) 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.
  - IIS 6.0 поддерживает последние веб-стандарты, такие как Microsoft ASP.NET, XML и протокол SOAP, для разработки, реализации и управления веб-приложениями.

Возможности IIS

- IIS 6.0 обладает повышенной надежностью по сравнению с предыдущими версиями благодаря новой архитектуре обработки запросов, которая обеспечивает **изолированную среду** функционирования 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.

Группы приложений

- Режим изоляции рабочих процессов позволяет клиентам создавать несколько групп приложений, где каждая группа приложений может иметь уникальную конфигурацию.
- Группа приложений может быть настроена в режиме изоляции рабочих процессов для обслуживания любых объектов — от одного веб-приложения до нескольких веб-приложений и узлов.
- 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,
  - управление доступом,
  - шифрование,
  - сертификаты,
  - 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

- 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 объектом, таким как файл или папка, которые определяют, какие учетные записи могут получить доступ к объекту.

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 выполняется.

Шифрование

- **Шифрованием** – преобразование элементов информации с помощью математической функции, после которого восстановление исходной информации является 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.

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

- Цифровые сертификаты содержат сведения, используемые для проверки подлинности пользователей сети.
- Сертификаты содержат также значения для шифрования, или *ключи*, которые используются для установления соединения по протоколу SSL между клиентом и сервером.
- Существуют два типа сертификатов, используемых протоколом SSL, — 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

- Средства аудита используются для отслеживания действий пользователей и обнаружения попыток несанкционированного доступа к каталогам и файлам в системе NTFS.
- 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 служб 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 служб IIS;
  - Административных сценариев;
  - Файла конфигураций IIS;
  - Удаленного доступа.

Использование файлов конфигурации

- Метабаза является хранилищем для большинства значений конфигурации IIS. Средства IIS включает в себя редактируемый 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.
- Для служб 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 конфигурации IIS.

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**] [**/s** *компьютер* [**/u** [*домен*\]*пользователь*/**p** *пароль*]]

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 пользовательской учетной записи «Администратор».
- **iisweb /delete Finance "Work Group" W3SVC/79116006 /s SRV01 /u Alice /p p@##word**

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…*] [**/s** *компьютер* [**/u** [*домен*\]*пользователь*/**p** *пароль*]]

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.
  - 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.

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.
  - 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.
  - 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 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 полностью копирует конфигурацию IIS (метабазу и схему) на другой компьютер.

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.
- Для полного или частичного копирования конфигурации метабазы с одного сервера на другой используйте сценарий iiscnfg.vbs.

Управление резервными копиями

- 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.

Копирование конфигурации

- Операция **/copy** не копирует содержимое сервера, например веб-страницы и файлы FTP, связанное с конфигурацией IIS.
- Операция **/copy** изменяет свойства метабазы, связанные с компьютером и системой, таким образом, что они становятся применимы на конечном компьютере.
  - Настройки путей к каталогам и файлам при этом не производится. В результате пути конфигурации могут оказаться недействительными на конечном компьютере.

Установка дополнительных компонентов