Администрирование информационных систем

Веб-сервер

Основные определения

- Веб-сервер — сервер, который обрабатывает HTTP-запросы от клиентов. Работает с текстами, изображениями, медиа-потоками и другими данными. Термин подразумевает как ПО, так и ТО – зависимо от контекста.
- Клиент – под этим термином понимается пользователь услугами веб-сервера, то есть веб-браузер или любая другая программа (например, антивирус) или устройство, которое выполняет к нему запрос.
- Веб-сайт – набор логически связанных между собой страниц, с общими доменным именем и IP-адресом.
- Хостинг – услуга по хранению файлов сайта и размещению его в сети Интернет.

Существующие веб-серверы

- Apache — свободный веб-сервер для UNIX-подобных ОС
- IIS – разработка компании Microsoft, распространяется с ОС семейства Windows.
- nginx – свободный веб-сервер.
- lighttpd – свободный веб-сервер.
- Google Web Server – веб-сервер, основанный на Apache и доработанный компанией Google.
- Resin – свободный веб-сервер приложений.
- Cherokee – свободный веб-сервер, управляемый только через web-интерфейс.
- Rootage – веб-сервер, написанный на java.
- THTTPD – простой, маленький, быстрый и безопасный веб-сервер.
- Open Server – бесплатная программа с графическим интерфейсом использует множество исключительно свободного программного комплекса.
- H2O – свободный быстрый веб-сервер, написанный на C.

Функционал веб-сервера (на примере IIS)

- Информационные службы Интернета (IIS) вместе с продуктами семейства Microsoft Windows обеспечивают комплексные, масштабируемые и регулируемые возможности веб-сервера при работе с внутренними и внешними сетями, а также с Интернетом с достаточно высоким уровнем надежности и безопасности.
- IIS является инструментом для создания мощных коммуникационных платформ динамических сетевых приложений.
- IIS используется 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.

Основные возможности служб IIS

- Поддержка веб-стандартов, таких как Microsoft ASP.NET, XML и протокол SOAP, для разработки, реализации и управления веб-приложениями.
- Особая архитектура обработки запросов, которая обеспечивает изолированную среду для выполнения приложений - это позволяет отдельным веб-приложениям работать независимо друг от друга в виде независимых рабочих процессов.
- Для удобства работы администратора службы IIS предоставляют ряд средств управления и администрирования сервера – это:
  - диспетчер IIS;
  - административные сценарии;
  - возможность редактирования неформатированного файла конфигураций IIS;
  - удаленный доступ.

IIS: режимы работы

- IIS 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.

IIS: 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.

IIS: о безопасности

- IIS 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.
- 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 работы с учетом прав доступа

- 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 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.

IIS: неформатированная метабаза

- Метабаза является хранилищем для большинства значений конфигурации IIS. IIS включает в себя редактируемый вручную или программно неформатированный файл конфигураций метабазы .XML. Обычно 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.
- Поскольку оба файла являются неформатированными, то их можно прочитать только с помощью соответствующего редактора.

IIS: 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 конфигурации IIS.