

Администрирование информационных систем

Администрирование почтового
сервера

Основные понятия

- Электронная почта – служба по пересылке и получению писем (электронных сообщений) между пользователями компьютерной сети
- Ящик, почтовый ящик – место хранения сообщений (обычно папка на почтовом сервере)
- Почтовый сервер – компьютер, осуществляющий получение, хранение и доставку почты по запросам пользователей. Также этот термин подразумевает специализированное программное обеспечение, выполняющее необходимые функции обслуживания почтовых клиентов.
- Спам – массовая рассылка корреспонденции рекламного характера лицам, не выразившим желания её получать

Основные понятия

Релей (relay) – узел, занимающийся получением/пересылкой сообщений и/или писем электронной почты:

- обеспечивает приём сообщения, хранение (от минут до нескольких дней) и пересылку сообщения (получателю или следующему релею).
- может проверять сообщения на вирусы, спам, осуществлять проверку прав на отправку сообщения.
- может проверять отправителя или не требовать авторизации (открытый релей).

Основные задачи администратора почтового сервера

- Установка и конфигурирование почтового сервера.
- Управление почтовыми отделениями.
- Управление доступом пользователей, создание, изменение, удаление почтовых ящиков.
- Резервное копирование и восстановление пользовательских данных.
- Обеспечение безопасности, конфиденциальности, целостности и доступности данных.

Электронная почта

- Электронная почта – важное средство обмена информацией в современном мире.
- Обмен электронными почтовыми сообщениями основан на использовании клиент-серверной архитектуры.
- Можно выделить следующие компоненты службы:
 - MTA (Mail Transfer Agent – агент пересылки почты) – отвечает за пересылку почты между почтовыми серверами;
 - MDA (Mail Delivery Agent – агент доставки почты) – отвечает за доставку почты конечному пользователю от сервера;
 - MUA (Mail user agent – почтовый агент пользователя, почтовый клиент) – программа, обеспечивающая пользовательский интерфейс для работы с почтой.

Электронная почта: алгоритм работы

- Клиент создает письмо (используя MUA, например, Outlook или Веб-интерфейс).
- Далее, по указанию «Отправить», MDA клиента пересылает письмо на почтовый сервер, инициирует дальнейшие действия и помещает его в соответствующую папку почтового ящика – то есть, например, в папку «Отправленные».
- В этот момент за доставку письма принимается MTA: если почтовый сервер отправителя и получателя совпадают, то письмо перемещается в соответствующую папку получателя; если же нет, то адрес доставки уточняется с помощью служб DNS и происходит пересылка сообщения на соответствующий почтовый сервер.
- При следующем посещении сети пользователем служба MDA получателя проверит состояние почтового ящика и «обнаружит» появление письма. После этого получатель может быть извещен уведомлением.
- Получатель «забирает» письмо – информация пересылается клиенту.

Электронная почта: протоколы

- Существует несколько сетевых протоколов используемых для приема-передачи, а также управления почтовыми сообщениями:
 - SMTP
 - POP3
 - IMAP
- Почтовых протоколы бывают двух видов:
 - протоколы принудительной доставки (передача почты инициируется отправителем) – например, SMTP;
 - протоколы доставки по запросу (передача инициируется получателем сообщения) - POP3, IMAP.

Доставка по запросу

- Последнее звено в цепи доставки почты обычно составляют серверы доставки по запросу.
- Наиболее популярные протоколы данного класса – POP (Post Office Protocol) и IMAP (Internet Message Access Protocol).
- Данные протоколы используются, когда конечным получателем является рабочая станция, на которой не запущен сервер принудительной доставки.
- Различия в работе протоколов:
 - **POP3** – почта на сервере хранится временно, в ограниченном объёме, а пользователь периодически скачивает письма к себе, тем самым очищая ящик;
 - **IMAP** – вся корреспонденция, связанная с почтовым ящиком (включая копии отправленных писем), хранится на сервере, а пользователь обращается к хранилищу для просмотра существующих и написания новых писем.

Настройка почтового сервера (POP3 на примере Windows Server)

- Службы электронной почты Windows Server 2003 включают службу POP3, обеспечивающую получение электронной почты, и службу SMTP, обеспечивающую передачу электронной почты.
- Служба POP3 может быть использована для хранения учетных записей электронной почты и управления ими на почтовом сервере.
- После того как компьютер будет настроен как почтовый сервер, пользователи смогут подключаться к почтовому серверу и получать электронную почту на локальные компьютеры при помощи клиента электронной почты, поддерживающего протокол POP3, например Microsoft Outlook.

Настройка службы POP3.

Предварительная подготовка сервера

Прежде чем компьютер будет настроен как почтовый сервер, необходимо убедиться в следующем:

- сервер, на который будут установлены службы электронной почты, настроен для подключения к Интернету;
- доступен раздел с файловой структурой NTFS. Можно повысить безопасность, обеспечиваемую дисковыми квотами, используя раздел NTFS;
- доменное имя электронной почты зарегистрировано;
- MX-запись (Mail eXchanger) для доменного имени электронной почты существует и соответствует имени сервера;
- сервер настроен на статическую адресацию;
- включен брандмауэр Windows;
- мастер настройки безопасности установлен и активен.

Настройка службы POP3.

Создание почтовых ящиков

- Для того чтобы отправлять или получать электронную почту, каждый пользователь должен иметь уникальный почтовый ящик в домене электронной почты.
- Почтовые ящики можно создавать как с помощью оснастки службы POP3, так и из командной строки.
- Средство администрирования службы POP3 с помощью командной строки – команда winpop:

```
winpop [add {имя_домена | имя_пользователя@имя_домена [/createuser пароль]]]
[delete {имя_домена | имя_пользователя@имя_домена [/deleteuser]]]
[list {имя_домена}]
[lock {имя_домена | имя_пользователя@имя_домена}]
[unlock {имя_домена | имя_пользователя@имя_домена}]
[stat {имя_домена}]
[changepwd имя_пользователя@имя_домена новый_пароль]
[createquotafile имя_пользователя@имя_домена [/user:имя_пользователя]]
[migrateToAD имя_пользователя@имя_домена]
[help]
```

Настройка службы POP3

Метод проверки подлинности

Возможные варианты:

Метод проверки подлинности	Рекомендации к использованию
<i>Локальные учетные записи Windows</i>	Почтовый сервер не является рядовым сервером Active Directory, и предполагается сохранять учетные записи пользователей на серверах, на которых установлена служба POP3
<i>Интегрированные с Active Directory</i>	Почтовый сервер является контроллером домена или рядовым сервером
<i>Зашифрованный файл паролей</i>	Почтовый сервер не использует Active Directory, или не предполагается использовать учетные записи для службы POP3 на локальном компьютере

Протоколы принудительной доставки почты

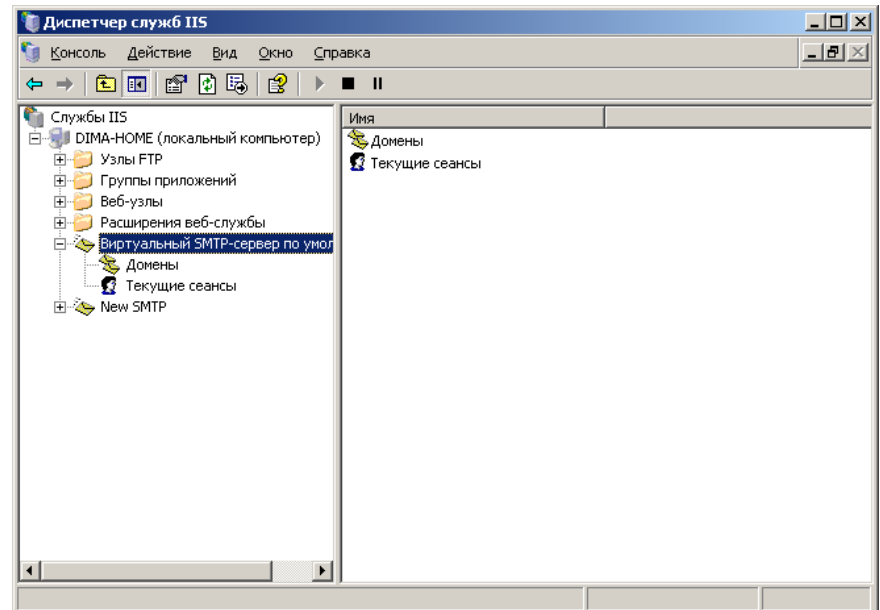
- Почтовые серверы могут отправлять почту не только между пользователями одного компьютера, но и на другие компьютеры. Для таких процессов используются **ретрансляторы почты** – система, принимающая почту от одного компьютера и посылающая на другой.
- В качестве протокола принудительной доставки почтовых сообщений обычно выступает протокол SMTP (Simple Mail Transport Protocol).
- Важная особенность при работе такого протокола – компьютер-получатель должен быть доступен.

Серверы принудительной доставки ПОЧТЫ

- Серверы принудительной доставки почты – важнейший компонент в системе обмена электронной почты.
- Для UNIX систем примерами могут служить следующие популярные почтовые сервера:
 - sendmail;
 - qmail;
 - exim;
 - postfix
- Для Windows систем можно использовать специализированные серверы (такие как Exchange) или службу SMTP, входящую в состав IIS, службу pop3, входящую в состав Windows Server 2003 R2.

Служба SMTP

- В IIS 6 входит служба простого протокола электронной почты (SMTP).
- При пересылке сообщения SMTP-сервер вначале устанавливает соединение с ближайшим узлом.
- Если это соединение не установлено или по каким-либо причинам недоступно, SMTP-сервер отклоняет прием сообщения от клиента и уведомляет его об ошибке.
- По умолчанию SMTP-сервер напрямую соединяется с сервером, на котором находится домен-получатель сообщения.
- Средства администрирования IIS позволяют сконфигурировать SMTP-сервер для распространения служб обмена сообщениями на разнообразные платформы.
- Управлять службой SMTP можно с помощью Диспетчера служб IIS.



Параметры конфигурации

- При работе с SMTP-сервером администратор должен контролировать следующие параметры:
 - Аутентификацию клиентов на SMTP-сервере перед отправкой сообщения;
 - Передачу сообщений клиента на SMTP-сервер;
 - Отправку сообщений с SMTP-сервера;
 - Маршрутизацию сообщений с SMTP-сервера;
 - Настройки SMTP для заданного домена SMTP.

Создание и настройка виртуального сервера

- Для выполнения отправки электронных сообщений через сервер под управлением Windows Server 2003 на нем должна быть запущена служба SMTP. Если данная служба установлена и работает, для ее использования необходим **виртуальный сервер SMTP**.
- По умолчанию такой сервер создается при установке службы SMTP.
- При добавлении виртуального SMTP-сервера мастер создания выполняет базовую настройку виртуального SMTP-сервера.
- В отличие от FTP- и веб-серверов, виртуальные SMTP-серверы не могут быть созданы из файлов конфигурации или посредством выполнения сценария.

Запуск, приостановка и остановка виртуальных серверов SMTP

- Виртуальный сервер SMTP может находиться в одном из состояний – **выполняется, приостановлен и остановлен**.
- Запуск виртуального SMTP-сервера позволяет ему отвечать на запросы.
- Во время приостановки виртуальный сервер не отвечает на новые запросы об отправке сообщений, однако продолжает обработку имеющихся.
- При полной остановке виртуальный сервер перестает отвечать на любые запросы и обрабатывать очереди сообщений.
- Следует учесть, что:
 - запуск, приостановка или остановка службы SMTP распространяется на все виртуальные серверы SMTP, находящиеся на узле;
 - остановка служб (вызванная ошибками в приложении или по указанию администратора системы) приведет к остановке всех виртуальных серверов системы;
 - управление службой SMTP может осуществляться посредством команд командной строки или через консоль управления Службы (Services).

Домены SMTP

Домена SMTP не совпадают с сетевыми доменами или доменами, относящимися к DNS. Домен SMTP предназначен для отправки сообщений.

- SMTP-сервер может иметь от одного до трех типов доменов:
 - Локальный. Сообщения с адресами электронной почты, использующие локальный домен, обслуживаются локальным сервером.
 - Псевдоним (alias). Это домен, имеющий ту же конфигурацию, что и локальный домен, но другое доменное имя.
 - Удаленный. Сообщения с адресами электронной почты, не использующими локальное имя домена, обслуживаются удаленным сервером.
- Каждый виртуальный сервер SMTP должен иметь хотя бы один локальный домен.
- Каждый виртуальный сервер должен содержать, хотя бы один домен по умолчанию.
- Имя домена по умолчанию присоединяется к адресам электронной почты, в которых не указано имя домена.

Создание виртуального сервера

- Мастер создания виртуального SMTP-сервера позволяет выполнить создание в несколько этапов. Параметры, заданные при создании, впоследствии могут быть изменены, за исключением домашнего каталога:
 - Этап 1. Указание имени виртуального сервера (используется для идентификации сервера в Диспетчере IIS).
 - Этап 2. Задание IP-адреса виртуального SMTP-сервера (значение по умолчанию – все незанятые).
 - Этап 3. Выбор домашнего каталога (домашним каталогом является путь к месту расположения в главном сервере, в который SMTP-служба записывает сообщения и файлы).
 - Этап 4. Определение домена по умолчанию (домен по умолчанию – имя домена, присоединяемое к данному имени учетной записи в процессе аутентификации).

Структура домашнего каталога

- В домашнем каталоге виртуального SMTP-сервера создаются следующие подкаталоги:
 - BadMail. Каталог для записи сообщений, вернувшихся с отчетом о невозможности доставки.
 - Drop. Каталог для записи всех входящих сообщений данного домена.
 - Pickup. Каталог для записи сообщений, используемых службой сообщений.
 - Queue. Каталог, в котором сообщения электронной почты ставятся в очередь для использования удаленно инициированной доставки при наличии поддержки удаленного домена.