Визитка

АРСЕНИЙ АНКУДИНОВ, *инженер-программист*

Визитка

ВАЛЕНТИНА ЮГАЙ, *инженер-тестер*

Отказоустойчивый антивирусный сервер

Антивирусные сервера для повышения надежности могут быть объединены в кластер серверов. В результате администратор безопасности может управлять параметрами защиты станций сети с разных антивирусных серверов — вне зависимости от того, к какому серверу кластера подсоединены станции антивирусной сети

Использование группы серверов в целях обеспечения отказоустойчивости было возможно уже в Dr.Web Enterprise Suite 6.0. В этой версии можно было использовать единую базу – балансировщики, автоматически распределяющие запросы станций по активным серверам, плюс станции имели возможность не только подключения к конкретному серверу, но и использования мультикастинга. Однако для полноценного кластера не хватало гибкости в назначении и применении настроек к станциям сети. Появление в Dr.Web Enterprise Suite 10.0 кластерного протокола решило эту проблему.

Первое, что необходимо для создания кластера – это единая база данных, с которой будут работать все антивирусные сервера кластера (и, соответственно, в конфигурационных файлах drwcsd.conf всех серверов кластера должна быть прописана одна внешняя БД).

Как и в случае простого использования базы данных (без организации кластера) каждый из серверов обращается к базе данных независимо и все данные серверов хранятся раздельно. Везде, где это актуально, сервер забирает из БД только записи, привязанные к его ID, который является уникальным для каждого сервера. Использование единой базы данных уже позволяет серверам работать с агентами, присоединенными к иным серверам. Но организация кластера дает возможность агентам получать изменения не только при следующем подключении.

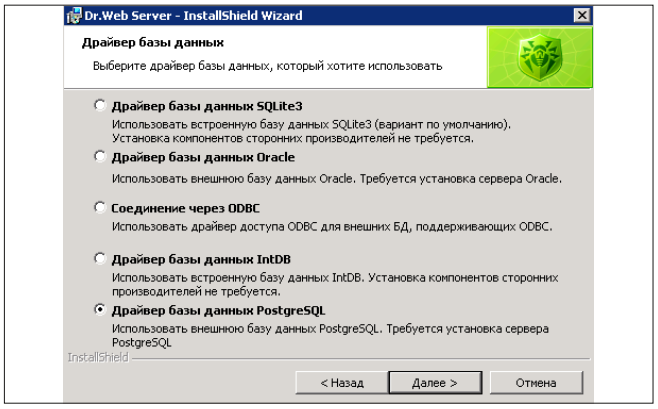
Для примера рассмотрим ситуацию, когда в качестве такой единой базы данных используется PostgreSQL. В данном примере мы не будем использовать кластерный вариант БД, он также возможен, в том числе с реализацией кластеров типа master-slave или multi-master.

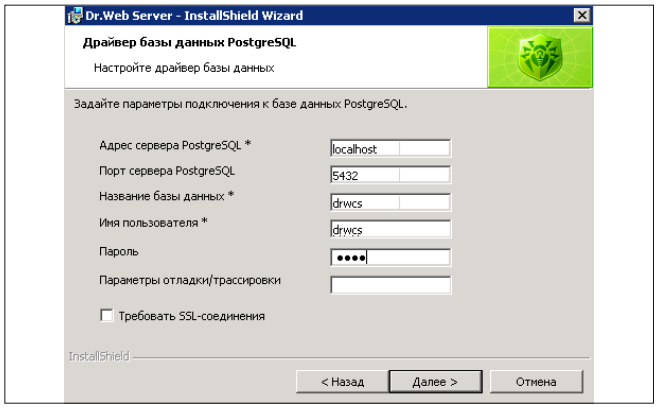
Сам процесс установки PostgreSQL не имеет никаких особенностей, но в отличии от ситуации, когда данная база использовалась для шестой версии, установка ODBC-драйвера больше не требуется. Отметим, что переход в Dr.Web Enterprise Suite 10.0 на использование собственного драйвера кроме всего прочего решил проблему с утечками памяти, возникавшими в библиотеке этой СУБД.

После установки PostgreSQL открываем SQL Shell и в появившемся окне на вопросы:

```
Server [localhost]:
Database [postgres]:
Port [5432]:
Username [postgres]:
```

Рисунок 1. Выбираем нужную базу данных и указываем параметры доступа





следует ответить нажатием на клавишу <ENTER> либо ввести актуальные данные, если они отличаются от предложенных по умолчанию, затем следует ввести пароль, который был задан при установке PostgreSQL.

Создаем новую базу данных, ее владельца и его пароль. В дальнейшем он будет использоваться для подключения к базе данных:

```
create user drwcs;
alter user drwcs password 'xxxx';
create database drwcs with owner=drwcs;
```

По умолчанию Dr.Web Enterprise Suite 10.0 предполагает использование кодировки UTF8, поэтому можно создать базу данных с указанием данной кодировки:

```
create database drwcs owner=drwcs encoding='UTF8';
```

В конфигурационном файле pg_hba.conf необходимо разрешить доступ к базе данных со всех машин кластера и после внесения изменений не забыть перезапустить сервис базы данных.

В тестовых целях первый сервер антивирусного кластера установим на той же машине, где мы развертывали базу данных. При создании кластера необходимо учесть, что для возможности работы с одной базой данных все антивирусные сервера кластера должны быть одинаковой версии. В дальнейшем обновлять серверы в пределах кластера следует только из установочных пакетов. При этом требуется остановить все серверы и осуществить обновление по очереди. Обновление через Центр Управления (переход на новую ревизию) применять не следует, поскольку при использовании общей базы данных после обновления первого сервера кластера, все оставшиеся серверы не смогут продолжить функционирование и обновление.

В ходе установки указываем создать новую базу данных, для первой установки ключи шифрования не задаем – они будут сформированы автоматически.

Выбираем нужную базу данных и указываем параметры доступа (см. рис. 1).

В том случае, что что-то было указано не верно, причину проблем можно будет найти в файле initdb.log, подкаталога var каталога установки Dr.Web Enterprise Suite (в зависимости от битности дистрибутива это по умолчанию каталоги C:\Program Files (x86)\DrWeb Server или C:\Program Files\DrWeb Server).

Для организации кластера используется специальный кластерный протокол. Протокол позволяет серверам обмениваться информацией быстрее, чем в случае с серверами, объединёнными посредством межсерверных связей. Поэтому по завершении установки заходим на закладку «Модули» группы настроек «Конфигурация DrWeb Server» и проверяем, что флаг «Протокол “Cluster Protocol Module”» установлен (см. рис. 2).

Заходим на соседнюю закладку «Кластер» и задаем необходимые параметры:

Multicast-группа – IP-адрес multicast-группы, через которую сервера кластера будут осуществлять обмен информацией (по сути, мультикаст-группа тождественна мультикастному IP-адресу, на который датаграммы отправляются и, соответственно, получаются всеми узлами, которые добавились в эту группу). Теоретически возможно использование нескольких мультикаст-групп. В этом случае каждый из серверов должен входить только в одну мультикаст-группу. Пересечений мультикаст-групп быть не должно;

Порт – номер порта сетевого интерфейса, к которому привязывается транспортный протокол для передачи информации в multicast-группу. В качестве Порта выбирается любой свободный порт;

Интерфейс – IP-адрес сетевого интерфейса, к которому привязывается транспортный протокол для передачи обновлений в multicast-группу. В качестве Интерфейса используется любой сетевой адрес, по которому сервер видит остальные сервера (например, интерфейс VPN, если сервера связываются между собой посредством VPN), совпадения его с адресом Центра управления не требуется.

В рассматриваемом случае на всех серверах кластера была реализована ситуация, когда все сервера поднимали транспорт на всех интерфейсах. Поэтому в настройках были указаны следующие настройки:

- Multicast-группа: 232.0.0.1
- Порт: 11111
- Интерфейс: 0.0.0.0

В иных случаях (например, когда одна из сетей является внешней для кластера, и через нее подключаются агенты, а вторая является внутрикластерной) кластерный протокол лучше связывать только с интерфейсами внутренней сети, указывая вместо 0.0.0.0 внутренние адреса, например, 192.168.1.1,192.168.1.2, и т.д. (см. рис. 3).

Введя нужные параметры, нажимаем «Сохранить» и перезагружаем сервер.

В целях тестирования функционирования кластера установим защиту на одну из станций сети.

Рисунок 2. Проверка флагов при конфигурации

В целях исключения дублирования запросов к БД рекомендуется в серверном расписании задания Purge Old Data, Backup sensitive data, Purge old stations, Purge expired stations, Purge unsent IS events выполнять только на одном из серверов. Если один из серверов расположен на том же сервере, что и база данных, то логично, чтобы эти задания выполнялись на нем.

Процедура установки защиты полностью аналогична Dr.Web Enterprise Suite 6.0, за исключением того, что в десятой версии, если не было выбрано автоматическое подтверждение новых станций сети, все такие станции попадают в группу Newbies, где им нужно назначить группу (см. рис. 6).

Третьим требованием для функционирования кластера является то, что на всех серверах должны быть одинаковые ключи шифрования drwcsd.pub и drwcsd.pri. В зависимости от того, как в дальнейшем будет развертываться кластер могут потребоваться или оба ключа или только drwcsd.pri. Заходим на страницу «Ключи шифрования» и экспортируем нужные файлы (см. рис. 4).

Продолжим создавать узлы кластера. В ходе установки антивирусных сервером мы можем указать ранее экспортированный drwcsd.pri (см. рис. 5).

Рисунок 3. Указание параметров интерфейсов

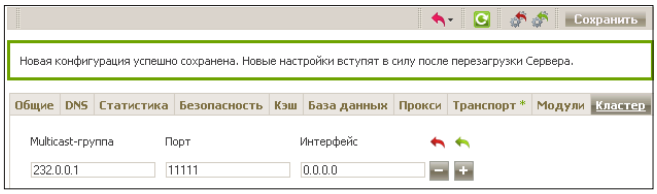


Рисунок 4. Экспорт ключей шифрования

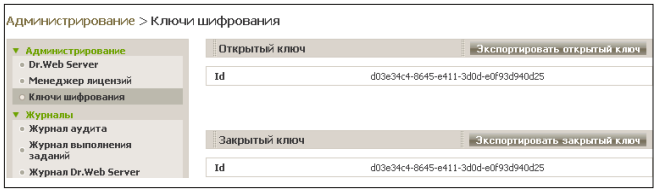
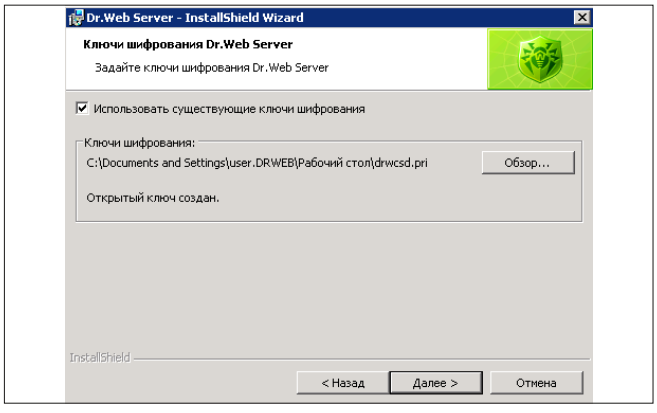


Рисунок 5. Указание ранее экспортированного ключа шифрования



Если не указать данный ключ при установке, то сразу после установки сервера необходимо заменить оба ключа, при этом после замены сервер нужно перезапустить. Ключ drwcsd.pub находится в папках Installer и webmin\install каталога установки, а drwcsd.pri – в папке etc.

В ходе установки сервера рекомендуется выбирать установку с использованием внутренней базы данных, что позволит избежать потенциальных проблем с инициализацией уже существующей базы данных. Поэтому сразу после установки необходимо перейти на закладку «База данных», ввести необходимые параметры – и перезагрузить сервер (см. рис. 7).

Необходимо отметить, что за исключением первого сервера кластера, не рекомендуется вводить боевые сервера в кластер с иной внешней или внутренней базы – это приведет как минимум к потере данных (информации о станциях, статистики, настроек – за исключением настроек, хранящихся в конфигурационных файлах), так как при импорте данные, имеющиеся в базе полностью затираются. Максимум, что можно сделать, – импортировать ряд настроек.

Желательное требование к серверам кластера – в конфигурационном файле Центра управления webmin.conf для всех серверов должно быть прописано одинаковое DNS-имя сервера (в центре управления этот параметр задается в поле «Название»), а в случае реализации системы балансировки запросов агентов между серверами на DNS-сервере в сети регистрируется общее имя кластера для каждого отдельного сервера и задается метод балансировки нагрузки (см. рис. 8).

Отдельно нужно остановиться на использовании на серверах кластера лицензионных ключей. В вышеописанном случае, если запросы станций динамически распределяются при каждом подключении согласно логике динамического распределения нагрузки, то в случайный момент на каждом из серверов может оказаться занято на одного и того же агента по одному месту в лицензии, что приведет к превышению лицензии. В связи с этим при динамическом распределении запросов не рекомендуется использовать Менеджер лицензий для распространения лицензий по отдельным серверам, желательно использовать отдельные ключи на каждом сервере. Механизма совместного управления агентами и лицензиями так, чтобы этого не потребовалось, на данный момент нет. Однако, в случае, когда динамическое распределение не используется и агенты постоянно присоединены к одному серверу можно использовать Менеджер лицензий и одинаковый ключ (в десятой версии используется не пара ключей, а один agent.key) для всех серверов.

После того, как на новом сервере сети будут указаны необходимые параметры на закладке «Кластер», переходим на страницу статистики и убеждаемся, что кластер заработал (см. рис. 9).

Для того, чтобы нам с вами окончательно убедиться в работоспособности кластера, на любом из серверов кластера выбираем станцию, подключенную к иному серверу, вносим изменения в ее настройки – и убеждаемся, что изменения применились на станции сразу – без необходимости переподключения станции или инициации ее нового запроса. EOF

Рисунок 6. Назначение группы

Рисунок 7. Вводим только самые необходимые данные для настроек сервера

Рисунок 8. Заполнение поля «Название» для прописания одинакового DNS-имя сервера

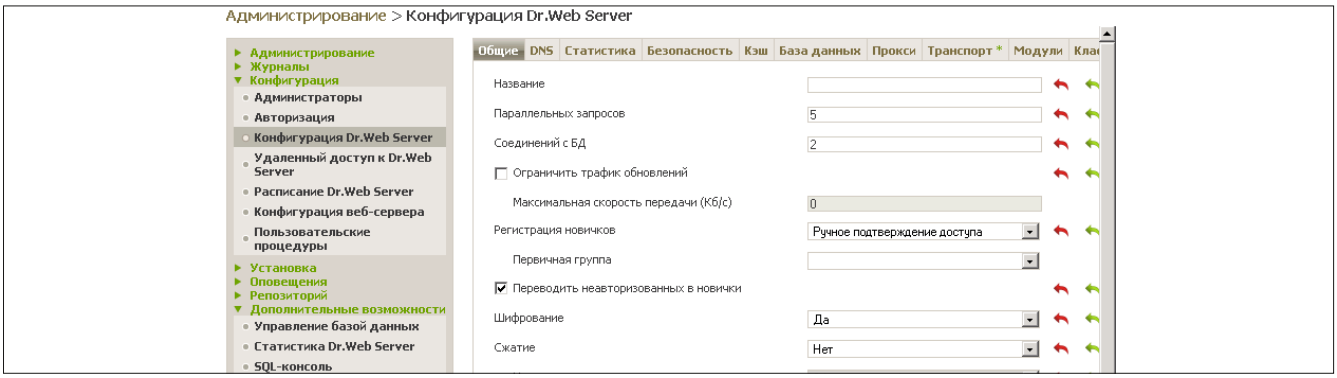


Рисунок 9. Просмотр статистики – наш кластер работает!