Приложение детализации телефонных соединений
ACViewer

Инструкция по установке

Приложение ACViewer служит для визуализации телефонных соединений сервера Asterisk, который в свою очередь записывает данные детализации в базу данных. Записывать информацию о телефонных соединениях в базу данных сервер Asterisk может как с использованием протокола Radius так и с использованием специального коннектора поставляемого вместе с сервером Asterisk. При описании конфигурации сервера Asterisk используется соединение с базой данных MySQL при помощи коннектора сервера Asterisk.

В данной инструкции будет описана установка приложения на основе дистрибутива CentOS 6.x, с незначительными изменениями возможна установка и на других дистрибутивах Linux.

Установка и настройка сервера баз данных MySQL

База данных используется сервером Asterisk для хранения информации детализации телефонных соединений.

Инсталляция сервера базы данных выполняется командой

```
$ sudo yum groupinstall "Сервер базы данных MySQL"
```

С поставкой приложения ACViewer в директории “mysql-config” находится файл конфигурации сервера MySQL, его требуется скопировать в директорию дистрибутива “/etc” и запустить сервер MySQL

```
$ sudo service mysqld start
```

Дополнительная настройка сервера MySQL

```
$ sudo /usr/bin/mysql_secure_installation
```

При новой установке сервера баз данных MySQL пароль на root пользователя отсутствует, поэтому просто нажимаем Enter. В конфигурации устанавливаем новый пароль на учётную запись root. На большинство вопросов которые будут задаваться в конфигурационном меню подходят ответы заданные по умолчанию.

Активируем запуск сервера MySQL загрузке системы

```
$ sudo chkconfig mysqld on
```

Сервер баз данных готов к работе. После авторизации на сервере MySQL под созданной ранее учётной записью root создаём новую базу данных с указанием имени пользователя и пароля.

```
mysql> CREATE DATABASE acv;
mysql> GRANT ALL PRIVILEGES ON acv.* TO 'acv'@'127.0.0.1' IDENTIFIED BY 'myacv';
mysql> GRANT ALL PRIVILEGES ON acv.* TO 'acv'@'localhost' IDENTIFIED BY 'myacv';
mysql> FLUSH PRIVILEGES;
```

Какие либо таблицы импортировать в созданную базу данных не требуется, после старта приложения ACViewer все нужные таблицы будут созданы автоматически.

Установка и настройка веб сервера Jetty

Веб сервер Jetty является полноценным веб сервером и предназначен для выполнения тех же задач что стоят перед такими серверами как Apache или Nginx. Но в отличии от перечисленных серверов Jetty написан на языке программирования Java, поэтому в систему требуется установить пакеты Java JDK.

```
$ sudo yum install java-1.7.0-openjdk java-1.7.0-openjdk-devel
```

Jetty использует библиотеку коннектора для доступа к серверу MySQL, устанавливаем эту библиотеку в систему.

```
$ sudo yum install mysql-connector-java
```

В CentOS по умолчанию идёт устаревшая версия сервера Jetty, поэтому загружаем архив Jetty версии 9.0.3 с сайта www.eclipse.org

```
$ wget -O jetty-distribution-9.0.3.v20130506.tar.gz
http://eclipse.org/downloads/download.php?file=/jetty/9.0.3.v20130506/dist/jetty-distribution-9.0.3.v20130506.tar.gz
```

Создаём нового пользователя под которым в дальнейшем будет запускаться сервер Jetty в системе

```
$ sudo useradd jetty
```

Распаковываем архив

```
$ tar -zxvf jetty-distribution-9.0.3.v20130506.tar.gz
```

Перемещаем директорию сервера Jetty

```
$ sudo mv jetty-distribution-9.0.3.v20130506 /opt/jetty
```

Для работы потребуется начальная конфигурация сервера Jetty.
Файл тестовой конфигурации “/opt/jetty/start.d/900-demo.ini” удаляем.
Файлы конфигурации коннектора MySQL “jetty-plus.xml” и начальных установок контейнера приложения “webdefault.xml” которые идут с поставкой приложения ACViewer в директории “jetty-config/etc” копируем в директорию Jetty “/opt/jetty/etc”

В файле конфигурации “jetty-plus.xml” убедитесь в соответствии имени базы данных, пользователя и пароля тем что были указаны при создании MySQL базы данных.
В файле конфигурации сервера Jetty “start.ini” убираем комментарии со строк “OPTIONS=jndi” и “etc/jetty-plus.xml”
Файлы контейнера и контекста приложения ACViewer находящиеся в директории “acviewer” копируем в директорию “/opt/jetty/webapps”

Указываем символьную ссылку в jndi директории сервера Jetty на MySQL коннектор и выставляем новые права доступа к файлам

```
$ sudo ln -s /usr/share/java/mysql-connector-java.jar /opt/jetty/lib/jndi/mysql-connector-java.jar
$ sudo chown -R jetty:jetty /opt/jetty
```

Для активации запуска Jetty сервера при загрузке системы потребуется скопировать файл стартового скрипта из директории “jetty-config/bin” поставки ACViewer в директорию “/etc/rc.d/init.d” и добавить его в загрузочную конфигурацию

```
$ sudo chkconfig --add jetty
$ sudo chkconfig jetty on
$ sudo service jetty start
```

На данном этапе приложение ACViewer развёрнуто и выполняется при помощи веб сервера Jetty. При запуске веб сервера Jetty в базе данных MySQL будут автоматически созданы необходимые для работы таблицы. Зайдя браузером по IP адресу сервера на котором развёртывается приложение ACViewer с указанием номера порта 8080 можно авторизоваться с использованием имени “admin” и пароля “admin” заданными по умолчанию в приложении. После успешной авторизации видим интерфейс поиска. Информация о детализации на данном этапе настройки отсутствует.

Добавляем правило которое позволит использовать в работе порт 80

```
$ sudo iptables -t nat -I PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 8080
$ sudo service iptables save
```

Установка и настройка сервера телефонии Asterisk

Для установки сервера Asterisk потребуется установить защиту основного репозитория и подключить репозиторий EPEL.
Для защиты основного репозитория задействуем yum плагин “yum-plugin-protectbase”

```
$ sudo yum install yum-plugin-protectbase
```

после установки в файле конфигурации репозитория к основному репозиторию и репозиторию обновлений выставляем опцию “protect = 1”

Подключаем EPEL репозиторий для платформы x86

```
$ sudo yum install http://download.fedoraproject.org/pub/epel/6/i386/epel-release-6-8.noarch.rpm
```

или для платформы x86_64
```
$ sudo yum install http://download.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm
```

После обновления базы данных о пакетах можно устанавливать сервер Asterisk
```
$ sudo yum install asterisk
```

С поставкой ACViewer в директории “asterisk-config” идёт файл конфигурации коннектора Asterisk к базе данных MySQL, его требуется скопировать в директорию конфигурации сервера Asterisk “/etc/asterisk”. Убедитесь в соответствии имени базы данных, пользователя и пароля в файле конфигурации тем что были указаны при создании MySQL базы данных.

Запускаем сервер Asteirsk и активируем его запуск при загрузке системы
```
$ sudo service asterisk start
$ sudo chkconfig asterisk on
```

Заходим на консоль управления сервером Asterisk и убеждаемся что соединение с базой даных MySQL установлено
```
localhost*CLI> cdr mysql status
```

Дальнейшая конфигурация сервера Asterisk зависит от требований администратора системы. Как минимум требуется создать простой план соединений и убедиться в том что сделанные телефонные соединения отображаются в веб интерфейсе ACViewer.
Файлы аудио записей размещаются в директории “/var/spool/asterisk/monitor”, на указанные директории потребуется выставить соответствующие права доступа (r-x).
Дополнительно в директории asterisk-config представлен образец конфигурации плана соединений для записи голосов оператора и абонента в файл, а также текстовая конфигурация планировщика задач cron с помощью которой можно установить длительность хранения аудио записей на накопителе в 90 дней.

Настройка шифрования передаваемых данных

Для создания защищённого HTTPS соединения потребуется создать ключ и сертификат при помощи OpenSSL и затем экспортировать в хранилище ключей поставляемое с веб сервером Jetty.

Создание кюча.
```
$ openssl genrsa -des3 -out jetty.key
```

В процессе генерации ключа у вас будет запрошен пароль для защиты ключа. Ведите самостоятельно придуманный пароль и затем подтвердите ввод пароля.

Создание сертификата
```
$ openssl req -new -x509 -key jetty.key -out jetty.crt
```

В процессе генерации сертификата у вас будет запрошен придуманный ранее пароль к ключу. Если не планируется обращаться в удостоверяющий центр для подписи сертификата то при вводе дополнительной информации допустимо оставлять те значениями что предлагаются по умолчанию за исключением свойства “Common Name”. В свойстве “Common Name” указывается имя домена либо имя хоста.

Конвертация в PKCS12 формат контейнера

Для хранения ключа и сертификата с использованием JSSE технологии конвертируем созданный ключ и сертификат в формат PKCS12.

```
$ openssl pkcs12 -inkey jetty.key -in jetty.crt -export -out jetty.pkcs12
```

В процессе конвертации у вас будет вновь запрошен придуманный ранее пароль к ключу и предложено ввести пароль который будет использоваться для экспорта содержимого контейнера PKCS12 контейнера. В качестве пароля экспорта содержимого указываем значение “keypwd” (без кавычек). Данный пароль указан по умолчанию в файле конфигурации веб сервера Jetty, в дальнейшем его можно сменить.

Импорт ключа и сертификата с использованием PKCS12 контейнера.

Импортируем ключ и сертификат из формата контейнера PKCS12 в контейнер который взаимодействует с веб сервером Jetty с использованием технологии JSSE. Данный контейнер представлен в Jetty файлом “keystore”. Для работы с контейнером ключа в формате JSSE вместе с Java поставляется утилита keytool.

```
$ sudo keytool -importkeystore -srckeystore jetty.pkcs12 -srcstoretype PKCS12
-destkeystore /opt/jetty/etc/keystore
```

В процессе импорта будет запрошен пароль на повышение привилегий для возможности записи информации в файл контейнера JSSE.

Далее будет предложено ввести пароль для доступа к контейнеру JSSE (“storepwd” без кавычек). Данный пароль является паролем по умолчанию для контейнера JSSE, в дальнейшем его можно сменить.

В завершении будет предложено ввести пароль для экспорта содержимого контейнера в формате PKCS12.

После выполнения введённой команды появится сообщение об успешном импорте ключа.

Включение шифрования передаваемых данных

После импорта ключа требуется задействовать шифрование передаваемых данных в файле конфигурации. Для этого в файле “start.ini” снимаем комментарий со строк “etc/jetty-ssl.xml” и “etc/jetty-https.xml”.

Кроме того, для автоматического перенаправления запроса на порт зашифрованного соединения потребуется заменить файл конфигурации контекста тем файлом конфигурации что находится в директории “secure-context” архива ACViewer

Созданные в процессе импорта ключа файлы “jetty.key”, “jetty.pkcs12”, “jetty.crt” более не потребуются и их можно удалить.