**JDBC**

JDBC – стандарт для взаимодействия Java-приложения с реляционными БД, представляет собой набор классов и интерфейсов для работы с различными реляционными БД. Реализация интерфейсов JDBC API осуществляется за счет JDBC-драйвера.

JDBC-драйвер – jar-файл, который обеспечивает взаимодействие между Java-приложением и конкретной БД. Предоставляет реализацию JDBC API для конкретной реляционной БД (адаптер Java-приложения к БД – преобразует запрос на Java в формат, который БД сможет обработать и выполнить).

Стандартизированный API обеспечивает независимость Java-приложения от БД, с которой она взаимодействует, то есть можно легко переключаться между разными БД, изменив драйвер на соответствующий, при этом не меняя реализацию приложения.

**Общий план подключения и работы:**

1) Подключение драйвера к проекту – добавление его в classpath(file-> proj structure-> modules)

2) Загрузка класса этого драйвера и его регистрация – с помощью Class.forName() или DriverManager.registerDriver() – с JDBC 4 это происходит автоматически при создании подключения.

Class.*forName*("org.postgresql.Driver");  
  
Driver driver = new org.postgresql.Driver();  
DriverManager.*registerDriver*(driver);

3) Создание подключения (получение объекта Connection) с помощью DriverManager.getConnection().

4) Дальнейшая работа с классами, представляющими работу с SQL запросами (Statement, PreparedStatment, CallableStatment).

**Классы**

*DriverManager* – Класс, предназначенный для работы с драйверами и установления соединения между Java приложением и БД. Основное назначение – регистрация драйверов и установление соединения.

registerDriver() – явно можно не вызывать, т.к. метод вызывается в static блоке класса Driver при его загрузке.

getConnection() – опрашивает каждый загруженный драйвер для определения того, с которым можно установить соединение (действует простым перебором и устанавливает соединение с первым соответствием)

*Connection* – устанавливается с помощью DriverManager.getConnection(), посредством передачи в него данных для подключения. Включает в себя методы для работы с транзакциями (commit, rollback, setautocommit, savepoint), работа со специальными типами (blob, clob, array, xml), исполнение SQL запросов (statement, preparestatment, callablestatment).

**Классы для работы с запросами**

***Statement*** – Для работы SQL операторов без параметров, то есть статических SQL выражений, так как подвержены SQL инъекциям, поскольку он выполняет SQL-запрос без дополнительной проверки.

Execute() – Исполняет SQL-запрос, возвращает Boolean, поэтому предпочтительное использование – DDL операции, что не подразумевает возвращаемые данные (возвращает true, если результат запроса resultset и false в остальных случаях). При этом все таки можно получить кол-во измененных записей или ResultSet посредством вызова getUpdateCount(), getResultSet() и др. на соответствующем Statement.

executeUpdate() – отличается возвращаемым значением, возвращает число затронутых операцией записей (-1 если таких нет). Используется, когда не требуется получить множество результатов запроса.

executeQuerry() – возвращает resultset, который содержит множество результатов запроса, используется, в случае, если запрос подразумевает возвращение некоторого множества. Используется в запросах типа select или запросах, использующих returning.

***ResultSet*** – содержит набор данных для извлечения. Сразу после получения набора данных его курсор находится перед первой записью и чтобы сделать её текущей необходимо вызвать метод next().  
Содержание полей текущей записи доступно через вызовы методов getInt(), getFloat(), getString(), getDate() и т.д.

***Batch*** – структура для группировки запросов, подразумевающих возвращение кол-ва измененных строк или отсутствие значения (не Select) для каждого запроса (при использовании executeUpdate вернется только число обновлений для последнего запроса). Необходим для оптимизации производительности путем уменьшение накладных расходов на связь с базой данных за счет уменьшения числа обращений между приложением и базой данных.

Взаимодействие осуществляется посредством методов addBatch() – добавляет запрос в пакет, executeBatch() – исполняет пакет запросов, clearBatch()- очищает пакет.

Работает только с сущностью Statement.

***PreparedStatment*** – наследник statement, предназначен для SQL-запросов с параметрами и часто выполняемых операторов. Предварительно компилирует запрос, который может содержать входные параметры и выполняться несколько раз, с разным набором данных параметров, так же СУБД может определить такой запрос как ранее исполняемый и кэшировать его, за счет чего увеличится производительность. Так же защищает от SQL-инъекций.

SQL инъекции – внедрение вредоносного SQL запроса в основной запрос. Внедрение происходит за счет наличия параметров, которые приходят в приложение извне и используются для подстановки в основной запрос.

String line = "Select \* from new\_table where id =";  
String id = "31"; //обычный параметр, полученный от пользователя  
String injection = "31 or 1=1";//параметр с инъекцией  
try (Connection connect = DriverManager.*getConnection*("jdbc:postgresql://localhost:5432/northwind", "user", "user")) {  
 Statement statement = connect.createStatement();  
 ResultSet result = statement.executeQuery(line + id);  
 while (result.next()) {  
 System.*out*.println(result.getInt("id") + " " + result.getString("name"));  
 }  
 ResultSet injResult = statement.executeQuery(line + injection);  
 System.*out*.println("\_\_\_\_\_\_\_\_");  
 while (injResult.next()) {  
 System.*out*.println(injResult.getInt("id") + " " + injResult.getString("name"));  
 }//получаем все записи из-за того, что выполняется одно из условий SQL-выражения  
}

Варианты инъекций – Drop table, or 1=1, or ‘’ = ‘’, Union и тд.

Отличие в синтаксисе – запрос передается при создании PreparedStatment, а параметры изменяемые параметры в таком запросе заменяются на ‘?’. При вызове исполняющего метода (одного из execute) в него передаются нужные параметры для исполнения.

String query = """  
 insert into new\_table(name)  
 values (?),(?);  
 """; //Вопросы указывают на изменяемые параметры  
try (Connection connection = DriverManager.*getConnection*("jdbc:postgresql://localhost:5432/northwind", "user", "user")) {  
 PreparedStatement prep = connection.prepareStatement(query);  
 prep.setString(1, "new name");  
 prep.setString(2, "another name");  
 //Каждый знак вопроса задается определенным числовым типом с помощью метода set и передается его номер  
 int updateNumber = prep.executeUpdate(); //Исполняется как Statement  
 System.*out*.println(updateNumber);  
}

***CallableStatment*** – для вызова хранимых процедур c помощью preparecall(). Имеет такой же принцип, как и PreparedStatment

String procedure = """  
 call sum\_values(?,?);  
 """;  
try (Connection connection = DriverManager.*getConnection*("jdbc:postgresql://localhost:5432/northwind", "user", "user")) {  
 CallableStatement callable = connection.prepareCall(procedure);  
 callable.setInt(1, 10);  
 callable.setInt(2, 35);  
 ResultSet result = callable.executeQuery();  
 while(result.next()){  
 System.*out*.println(result.getInt(1));  
 }  
}

SetTimeOut – устанавливает максимальное время ожидания запроса к БД.

SetfetchSize – определяет максимальный размер результирующего набора, который будет получать приложение. Т.е. результат общей выборки не изменится, но приложение будет получать ее пакетами указанного размера, что уменьшает нагрузку на клиентскую часть за счет уменьшения кол-ва записей, которые нужно хранить, при этом увеличивает кол-во запросов к БД.

SetMaxRows – устанавливает максимальное значение результирующего набора.

Для работы с Null результатами в resultset нужно использовать getObject и передать класс, в который кастить Class.class

Для получения ключей сгенерированных автоматически нужно выставить флаг RETURNING\_GENERATED\_KEYS при обращении к statement

Для возврата вставленных данных нужно использовать returning в sql запросе и получить его соответствующим execute и обработать полученный resultset или с помощью executeUpdate путем передачи в него массива.