## Java Serialization

**[Java Serialization 1](#_Toc1316)**

**[Youtube playlist 2](#_Toc17501)**

**[Github main 2](#_Toc5555)**

**[Chapter 01 - Introduction 3](#_Toc25186)**

**[Youtube 4](#_Toc12595)**

**[Github 4](#_Toc344)**

**[Chapter 02 - Serialization with memory buffer 5](#_Toc2446)**

**[Youtube 5](#_Toc15276)**

**[Github 5](#_Toc26370)**

**[Chapter 03 - Serialization with file 6](#_Toc31262)**

**[Youtube 6](#_Toc13027)**

**[Github 6](#_Toc24062)**

**[Chapter 04 - Serialization versioning 7](#_Toc6492)**

**[Youtube 8](#_Toc14944)**

**[Github 8](#_Toc617)**

**[Chapter 05 - Serialization with array field members 9](#_Toc31680)**

**[Youtube 9](#_Toc25432)**

**[Github 9](#_Toc6635)**

**[Chapter 06 - Serialization with Java Objects as array 10](#_Toc13712)**

**[Youtube 10](#_Toc20020)**

**[Github 10](#_Toc1149)**

**[Chapter 07 - Serialization with Collection field members 11](#_Toc22581)**

**[Youtube 11](#_Toc21443)**

**[Github 11](#_Toc11691)**

**[Chapter 08 - Serialization with Java Objects as Collection 12](#_Toc26666)**

**[Youtube 12](#_Toc5685)**

**[Github 12](#_Toc4330)**

**[Chapter 09 - Serialization with Enum Constants 13](#_Toc31225)**

**[Youtube 13](#_Toc15413)**

**[Github 13](#_Toc8824)**

**[Chapter 10 - Serialization with static fields 14](#_Toc14644)**

**[Youtube 14](#_Toc26406)**

**[Github 14](#_Toc23251)**

**[Chapter 11 - Object graphs 15](#_Toc19314)**

**[Youtube 15](#_Toc2579)**

**[Github 15](#_Toc614)**

**[Chapter 12 - Using transient keyword 16](#_Toc3000)**

**[Youtube 16](#_Toc11282)**

**[Github 16](#_Toc7304)**

**[Chapter 13 - Using writeObject() and readObject() 17](#_Toc843)**

**[Youtube 17](#_Toc24703)**

**[Github 17](#_Toc9881)**

**[Chapter 14 - Using ObjectStreamField 18](#_Toc17568)**

**[Youtube 18](#_Toc15674)**

**[Github 18](#_Toc12363)**

**[Chapter 15 - Protecting sensitive information 19](#_Toc427)**

**[Youtube 19](#_Toc2623)**

**[Github 19](#_Toc17692)**

**[Chapter 16 - How Inheritance Affects Serialization 20](#_Toc30383)**

**[Youtube 21](#_Toc23462)**

**[Github 21](#_Toc7964)**

**[Chapter 17 - Using Externalizable 22](#_Toc8021)**

**[Youtube 22](#_Toc6603)**

**[Github 22](#_Toc26676)**

**[Chapter 18 - Using ObjectInputValidation 23](#_Toc30221)**

**[Youtube 23](#_Toc2554)**

**[Github 23](#_Toc23480)**

**[Chapter 19 - Using writeReplace() and readResolve() 24](#_Toc11292)**

**[Youtube 24](#_Toc24453)**

**[Github 24](#_Toc14142)**

**[Chapter 20 - Singleton pattern and readResolve() 25](#_Toc31527)**

**[Youtube 25](#_Toc11102)**

**[Github 25](#_Toc20314)**

**[Chapter 21 - Using ObjectInputFilter 26](#_Toc3118)**

**[Youtube 27](#_Toc18244)**

**[Github 27](#_Toc15742)**

#### Youtube playlist

<https://youtube.com/playlist?list=PLQDzPczdXrTjGLkI8kd2d0bfNHx0v7dTy>

#### Github main

<https://github.com/backstreetbrogrammer/05_Persistence>

#### Chapter 01 - Introduction

Suppose I want to save the state of one or more objects. If Java didn’t have serialization, I would have to use one of the IO classes to write out the state of the instance variables of all the objects I wanted to save - say to a **csv**, **xml**, **json** or just **plain text**.

Then I would need to reconstruct the objects that had been saved in the same order of instance fields as it was saved. This is error-prone as we are doing lots of stuff manually here.

Also, if the objects are huge - containing reference to other objects (Object Graphs) and many instance fields, then the manual processing of serialization and deserialization would be very complex and error-prone.

Java’s object serialization allows us to take any object that implements the **Serializable**  
interface and turn it into a **sequence of bytes** that can later be fully restored to regenerate the original object. This is even true across a network, which means that the serialization  
mechanism automatically compensates for differences in operating systems. That is, I can  
create an object on a Windows machine, serialize it, and send it across the network to a Unix  
machine, where it will be correctly reconstructed. I don’t have to worry about the data  
representations on the different machines, the byte ordering, or any other details.



The magic of basic serialization happens with just 2 methods:

* one to serialize objects and write them to a stream
* second to read the stream and deserialize objects

**ObjectOutputStream.writeObject()** // serialize and write

**ObjectInputStream.readObject()** // read and deserialize

###### Youtube

01 - Java Serialization Tutorial Series

<https://youtu.be/F5POMzyLf7c>

02 - Java Serialization - Table Of Contents

<https://youtu.be/W2ZWKwYsNvM>

03 - Java Serialization - Java, Maven and IntelliJ installations

<https://youtu.be/baSkl5eIrNo>

04 - Java Serialization - Maven Project Setup on IntelliJ

<https://youtu.be/eXezwNStAfU>

05 - Java Serialization - Introduction - Theory

<https://youtu.be/Zas-PqxXNE8>

06 - Java Serialization - Introduction - Code Demo 1

<https://youtu.be/KGriEzFUGWA>

07 - Java Serialization - Introduction - Code Demo 2

<https://youtu.be/UylAJ6EOyFg>

###### Github

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/main/java/com/backstreetbrogrammer/chapter01_introduction>

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/test/java/com/backstreetbrogrammer/chapter01_introduction>

#### Chapter 02 - Serialization with memory buffer

The first example is using memory as buffer to where the serialized streams of bytes will be written to and then retrieved from using deserialization.

**Java Object => Serialize to byte array => Memory**

**Memory => Deserialize from byte array => Java Object**

**ByteArrayOutputStream** class is used to serialize to byte array.

This class implements an output stream in which the data is written into a byte array. The buffer automatically grows as data is written to it. The data can be retrieved using **toByteArray()** and **toString()**.

**ByteArrayInputStream** class is used to deserialize from byte array.

This class contains an internal buffer that contains bytes that may be read from the stream. An internal counter keeps track of the next byte to be supplied by the read method.

Drawback using memory buffer is that once the JVM shuts down - the serialized data in memory is erased and can not be used after application restart.

###### Youtube

08 - Java Serialization with memory buffer - Theory

<https://youtu.be/UgUuutfs828>

09 - Java Serialization with memory buffer - Code Demo 1

<https://youtu.be/s0LnxU1zL5A>

10 - Java Serialization with memory buffer - Code Demo 2

<https://youtu.be/CN4vcPtP9Vw>

11 - Java Serialization with memory buffer - Code Demo 3

<https://youtu.be/cdRxfbdJ_ow>

###### Github

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/main/java/com/backstreetbrogrammer/chapter02_serializationwithmemorybuffer>

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/test/java/com/backstreetbrogrammer/chapter02_serializationwithmemorybuffer>

#### Chapter 03 - Serialization with file

It would be incredibly useful if an object could exist and hold its information even while the program wasn’t running. Then, the next time we started the program, the object would be there and it would have the same information or state it had the previous time the program was running.

Object serialization allows us to implement persistence. Persistence means that an object’s lifetime is not determined by whether a program is executing; the object lives in between invocations of the program. By taking a serializable object and writing it to disk (via file), then restoring that object when the program is reinvoked, we’re able to produce the effect of persistence.

**Java Object => Stream of bytes => File**

**File => Deserialize from stream of bytes => Java Object**

**FileOutputStream** class is used to write the serialized stream of bytes to file on the disk.

This class is an output stream for writing data to a File and is meant for writing streams of raw bytes such as image data.

**FileInputStream** class is used to read the stream of bytes from the file.

This class obtains input bytes from a file in a file system and is meant for reading streams of raw bytes such as image data.

###### Youtube

12 - Java Serialization with file - Theory

<https://youtu.be/v3nMZmeRT4c>

13 - Java Serialization with file - Code Demo

<https://youtu.be/O9HMVSqezGU>

###### Github

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/main/java/com/backstreetbrogrammer/chapter03_serializationwithfile>

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/test/java/com/backstreetbrogrammer/chapter03_serializationwithfile>

#### Chapter 04 - Serialization versioning

Suppose we have a class and we have serialized its object to a file on the disk, and due to some new requirements, we added/removed one field from our class. Or just added a new utility method to it. Now, if we try to deserialize the already serialized object, we will get **InvalidClassException**.

When we serialize a class, each class has a unique identification number associated with it.  
Its also called stream unique identifiers, more commonly known as **serial versionUIDs**.  
  
If we do not specify this number by declaring a static final long field named **serialVersionUID**,   
the system automatically generates it at runtime by applying a cryptographic hash function (SHA-1) to the structure of the class.  
  
This value is affected by the names of the class, the interfaces it implements, and most of its members, including synthetic members generated by the compiler.  
  
If we change any of these things, for example, by adding a convenience method, the generated serial version UID **changes**.

If we fail to declare a serial version UID, compatibility will be broken, resulting in an **InvalidClassException** at runtime.  
  
The basic idea is a class could have been serialized with an older version of the class and deserialized with a newer version of the class.  
  
The **serialVersionUID** helps inform the JVM that the stored data may not match the new class definition.   
  
Thus, if an older version of the class is encountered during deserialization, a **java.io.InvalidClassException** is thrown.  
  
***Conclusion***: It's a good practice to declare a static **serialVersionUID** variable in every class that implements Serializable.

In **IntelliJ IDE**, we can generate **serialVersionUID** using the following action:

Ctrl + Shift + A (will launch *Actions* tab menu) => type ‘**Serializable class without**’ and select the item to toggle it on/off.

OR

File -> Settings -> Editor -> Inspections -> Java -> Serialization issues:

Find ‘**Serializable class without** **serialVersionUID**’ and check it.

Now, for each class implementing **Serializable** interface will show warning if no **serialVersionUID** is declared.

Press “Alt + Enter” and Click on “Create constant field serialVersionUID in …” and **serialVersionUID** will be generated and declared in the class.

OR, we can just declare any random number like 1L or 42L and declare in the class.

For example:

private static final long serialVersionUID = 1L; // 1L or 2L or 3L - any number can be chosen

###### Youtube

<https://www.youtube.com/playlist?list=PLQDzPczdXrTjGLkI8kd2d0bfNHx0v7dTy>

###### Github

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/main/java/com/backstreetbrogrammer/chapter04_serializationversioning>

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/test/java/com/backstreetbrogrammer/chapter04_serializationversioning>

#### Chapter 05 - Serialization with array field members

Suppose we have a class which has array of primitives or array of Objects as its field members. In this scenario, we need to ensure that every element in the array is Serializable, otherwise the serialization will fail.

###### Youtube

<https://www.youtube.com/playlist?list=PLQDzPczdXrTjGLkI8kd2d0bfNHx0v7dTy>

###### Github

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/main/java/com/backstreetbrogrammer/chapter05_serializationwitharrayfields>

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/test/java/com/backstreetbrogrammer/chapter05_serializationwitharrayfields>

#### Chapter 06 - Serialization with Java Objects as array

If we have an array of a serializable class objects, the whole array can be serialized in one go by just calling **writeObject()** method from **ObjectOutputStream** class. We need to ensure that every element in the array is Serializable, otherwise the serialization will fail.

Similarly, while deserialization, the whole array object can be read by calling **readObject()** method from **ObjectInputStream** class.

###### Youtube

<https://www.youtube.com/playlist?list=PLQDzPczdXrTjGLkI8kd2d0bfNHx0v7dTy>

###### Github

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/main/java/com/backstreetbrogrammer/chapter06_serializationwitharrayobjects>

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/test/java/com/backstreetbrogrammer/chapter06_serializationwitharrayobjects>

#### Chapter 07 - Serialization with Collection field members

Suppose we have a class which has collection of objects say **List** as its field members. In this scenario, we need to ensure that every element in the collection is Serializable, otherwise the serialization will fail.

Please note that while the collection interfaces like **List**, **Set**, etc. are **NOT** serializable, the concrete collection classes like **ArrayList**, **HashSet** etc. **ARE** serializable.

###### Youtube

<https://www.youtube.com/playlist?list=PLQDzPczdXrTjGLkI8kd2d0bfNHx0v7dTy>

###### Github

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/main/java/com/backstreetbrogrammer/chapter07_serializationwithlistfields>

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/test/java/com/backstreetbrogrammer/chapter07_serializationwithlistfields>

#### Chapter 08 - Serialization with Java Objects as Collection

If we have a collection (List, Set, etc) of a serializable class objects, the whole collection can be serialized in one go by just calling **writeObject()** method from **ObjectOutputStream** class. We need to ensure that every element in the collection is Serializable, otherwise the serialization will fail.

Similarly, while deserialization, the whole collection object can be read by calling **readObject()** method from **ObjectInputStream** class.

###### Youtube

<https://www.youtube.com/playlist?list=PLQDzPczdXrTjGLkI8kd2d0bfNHx0v7dTy>

###### Github

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/main/java/com/backstreetbrogrammer/chapter08_serializationwithlistobjects>

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/test/java/com/backstreetbrogrammer/chapter08_serializationwithlistobjects>

#### Chapter 09 - Serialization with Enum Constants

As per Java specifications, Enum constants are serialized differently than ordinary serializable objects.

The serialized form of an enum constant consists solely of its **name**; field values of the constant are not present in the form.

To **serialize** an enum constant, **ObjectOutputStream**writes the value returned by the enum constant’s **name()**method.

For reference,

* **name()** is an instance method which returns the name of the instance.
* **valueOf()** is a static method taking a String and returning the enum instance with that name.
* **values()** is a static method returning all the enum instances.

To **deserialize** an enum constant, **ObjectInputStream**reads the constant name from the stream; the deserialized constant is then obtained by calling the **valueOf()** method, passing the constant’s enum type along with the received constant name as arguments.

Few more points to take note of:

* enum types have a fixed **serialVersionUID**of **0L** and cannot be changed
* process by which enum constants are serialized **cannot** be customized: any class-specific **writeObject()**, **readObject()**, **readObjectNoData()**, **writeReplace()**, and **readResolve()**methods defined by enum types are ignored during serialization and deserialization

###### Youtube

<https://www.youtube.com/playlist?list=PLQDzPczdXrTjGLkI8kd2d0bfNHx0v7dTy>

###### Github

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/main/java/com/backstreetbrogrammer/chapter09_serializationwithenum>

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/test/java/com/backstreetbrogrammer/chapter09_serializationwithenum>

#### Chapter 10 - Serialization with static fields

Static fields are NEVER saved as part of the object’s state.

We should think of static variables purely as CLASS variables. They have nothing to do with individual instances. And serialization applies only to OBJECTS.

Suppose we have 3 instances of a Serializable class => all of which were serialized at **different** times, and thus all of which were saved when the value of a static variable in the class was different.

Now, if static variables were serializable, which of the 3 instances would win ? OR, Which instance’s static value would be used to replace the one currently in the one and only class that’s currently loaded ? => this is a problem… that’s why, static fields are never part of serialization / deserialization process.

###### Youtube

<https://www.youtube.com/playlist?list=PLQDzPczdXrTjGLkI8kd2d0bfNHx0v7dTy>

###### Github

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/main/java/com/backstreetbrogrammer/chapter10_serializationwithstaticfields>

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/test/java/com/backstreetbrogrammer/chapter10_serializationwithstaticfields>

#### Chapter 11 - Object graphs

Java's default serialization process is fully **recursive**, so whenever we try to serialize one object, the serialization process try to serialize all the fields (primitive and reference) with our class (except **static**and **transient**fields).

The reference to objects fields are serialized and Java serialization takes care of saving that object’s entire “object graph”. That means a deep copy of everything the saved objects needs to be stored.

Just remember to implement the Serialization interface for all the objects in the “object graph” - otherwise we will get **NotSerializableException**.

###### Youtube

<https://www.youtube.com/playlist?list=PLQDzPczdXrTjGLkI8kd2d0bfNHx0v7dTy>

###### Github

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/main/java/com/backstreetbrogrammer/chapter11_objectgraphs>

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/test/java/com/backstreetbrogrammer/chapter11_objectgraphs>

#### Chapter 12 - Using transient keyword

Suppose one of the objects in the “object graph” is not accessible (meaning we can’t modify it due to permission issues) and not marked as Serializable. In that case, are we blocked to Serialize our main class which has reference to that read-only object?

One option is to subclass that read-only class, but it may be marked as **final**.

OR, we don’t know if the read-only class object has other similar objects in its own “object graph”.

There are other private members fields (primitive and reference) of a class which contains sensitive data like passwords, or it doesn’t make sense to serialize it - like the state of an in-memory Thread.

That’s where the **transient** modifier comes in. By marking the members fields (primitive and reference) as transient, these fields are NOT serialized just like **static** fields.

What happens to data marked **transient** on **deserialization**? It reverts to  
its default Java values, such as **0.0D** for **double**, **false** for **boolean** or **null** for an **object**.

###### Youtube

<https://www.youtube.com/playlist?list=PLQDzPczdXrTjGLkI8kd2d0bfNHx0v7dTy>

###### Github

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/main/java/com/backstreetbrogrammer/chapter12_transient>

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/test/java/com/backstreetbrogrammer/chapter12_transient>

#### Chapter 13 - Using writeObject() and readObject()

Just based on the above example, if one of the reference object is not accessible and we had to mark it as **transient**. While deserialization, the **transient** reference object will come as default value of null. What can we do to somehow make sure that it matches the same object state when it was saved ?

Java serialization has a special mechanism just for this - a set of private methods we can implement such that it will be invoked automatically during serialization and deserialization.

These 2 special methods we define must have signatures that look EXACTLY like this:

1. For serialization

private void writeObject(ObjectOutputStream stream) {

// code for saving the object

}

1. For deserialization:

private void readObject(ObjectlnputStream stream) {

// code for restoring the same object as it was saved although if its transient

}

By implementing these 2 methods, we can customize or control the default Java serialization process.

Also, we can call the methods like **ObjectOutputStream.defaultWriteObject()** and ObjectInputStream.defaultReadObject() to invoke the default Java serialization process inside **writeObject()** and **readObject()** methods respectively.

###### Youtube

<https://www.youtube.com/playlist?list=PLQDzPczdXrTjGLkI8kd2d0bfNHx0v7dTy>

###### Github

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/main/java/com/backstreetbrogrammer/chapter13_writeObjectReadObject>

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/test/java/com/backstreetbrogrammer/chapter13_writeObjectReadObject>

#### Chapter 14 - Using ObjectStreamField

In case of **transient** keyword, we chose which member fields (primitive and reference) of a class SHOULD NOT participate in serialization and deserialization process. This is also called as *blacklisting*.

Using **ObjectStreamField** class and **ObjectOutputStream.putFields** and **ObjectInputStream.readFields,** we can choose which member fields (primitive and reference) of a class SHOULD participate in serialization and deserialization process. This is also called as *whitelisting*.

Ideally *whitelisting* should be preferred over *blacklisting* as we have full control on which fields to serialize or not.

###### Youtube

<https://www.youtube.com/playlist?list=PLQDzPczdXrTjGLkI8kd2d0bfNHx0v7dTy>

###### Github

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/main/java/com/backstreetbrogrammer/chapter14_usingobjectstreamfield>

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/test/java/com/backstreetbrogrammer/chapter14_usingobjectstreamfield>

#### Chapter 15 - Protecting sensitive information

When developing a class that provides controlled access to resources, care must be taken to protect sensitive information and functions. During deserialization, the private state of the object is restored. To avoid compromising a class, the sensitive state of an object must not be restored from the stream, or it must be re-verified by the class.

The easiest technique is to mark fields that contain sensitive data as private **transient**. Transient fields are not persistent and will not be saved by any persistence mechanism. Marking the field will prevent the state from appearing in the stream and from being restored during deserialization. Since writing and reading (of private fields) cannot be superseded outside of the class, the **transient** fields of the class are safe.

However, if we really want to serialize secured or confidential fields, we should use encryption and decryption of the field.

###### Youtube

<https://www.youtube.com/playlist?list=PLQDzPczdXrTjGLkI8kd2d0bfNHx0v7dTy>

###### Github

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/main/java/com/backstreetbrogrammer/chapter15_securedFields>

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/test/java/com/backstreetbrogrammer/chapter15_securedFields>

#### Chapter 16 - How Inheritance Affects Serialization

If a superclass is **Serializable**, then all subclasses are automatically Serializable without having to explicitly mark the subclass as **Serializable**.

If a class does NOT explicitly extend any other class and does NOT implement Serializable, then we can confirm that the class is NOT serializable as class **Object** does NOT implement **Serializable**.

Now suppose a subclass implements **Serializable** but the super class does NOT. How is this going to affect serialization?

When an object is constructed using **new** (as opposed to being **deserialized**), following things happen in this sequence:

1. All **instance variables** are assigned **default** values - like int as 0, double as 0D, boolean as false, String as null, etc.
2. The **constructor** is invoked, which immediately invokes the superclass constructor OR another overloaded constructor, until one of the overloaded constructors invokes the superclass constructor.
3. All **superclass** constructors complete.
4. Instance variables that are initialized as part of their declaration are assigned their initial value overriding the default values they’re given prior to the superclass constructors completing.
5. The constructor completes.

BUT, these things do NOT happen when an object is deserialized.

If the constructor were invoked, and/or variables were assigned the values given in their declarations, the object we are trying to restore would revert to its original state, rather than coming back reflecting the changes in its state that happened sometime after it was created.

In other words, we want only the values saved as part of the serialized state of the object to be reassigned.

If the superclass is not Serializable, the instance variables in the subclass (which implements Serializable) will be serialized and deserialized correctly, but the **inherited variables** from the non-serializable superclass will come back with their default/initially assigned values rather than the values they had at the time of serialization.

Thus, if a subclass implements **Serializable** but the super class does NOT, then any instance variables INHERITED from that superclass will be reset to the values they were given during the original construction of the object. This is because the non-serializable class constructor WILL run.

In fact, every constructor ABOVE the first non-serializable class constructor will also run in the inheritance tree.

###### Youtube

<https://www.youtube.com/playlist?list=PLQDzPczdXrTjGLkI8kd2d0bfNHx0v7dTy>

###### Github

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/main/java/com/backstreetbrogrammer/chapter16_inheritance>

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/test/java/com/backstreetbrogrammer/chapter16_inheritance>

#### Chapter 17 - Using Externalizable

If we want to fully control serialization and override JVM default serialization process, we can implement the **Externalizable** interface and override its methods **writeExternal()** and **readExternal()**.

Using **Externalizable**, complete serialization/deserialization logic becomes our responsibility.

We need to tell what to serialize using **writeExternal()** method and what to deserialize using **readExternal().** With implementation of **writeExternal()** and **readExternal()**, methods **writeObject()** and **readObject()** becomes redundant and do not get called.

We can even serialize/deserialize **static** and **transient** variables although it will be a bad practice to do so.

When an **Externalizable** object is reconstructed, the object is created using public no-arg constructor ***before*** the **readExternal()** method is called.

If a public no-arg constructor is not present then a **InvalidClassException** is thrown at runtime.

###### Youtube

<https://www.youtube.com/playlist?list=PLQDzPczdXrTjGLkI8kd2d0bfNHx0v7dTy>

###### Github

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/main/java/com/backstreetbrogrammer/chapter17_externalizable>

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/test/java/com/backstreetbrogrammer/chapter17_externalizable>

#### Chapter 18 - Using ObjectInputValidation

Suppose we have done the deserialization of a complete object graph and now we want to validate the invariants of the objects.

We can do that by implementing **ObjectInputValidation** interface and overriding the **validateObject()** method from it.

The method **validateObject()** will automatically get called when we register this validation by calling **ObjectInputStream.registerValidation()** from **readObject()** method.

It is very useful to verify that stream has not been tampered with, or that the data makes sense before handing it back to your application.

If the object cannot be made valid, it should throw the **InvalidObjectException**. Any exception that occurs during a call to **validateObject()** will terminate the validation process, and the **InvalidObjectException** will be thrown.

###### Youtube

<https://www.youtube.com/playlist?list=PLQDzPczdXrTjGLkI8kd2d0bfNHx0v7dTy>

###### Github

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/main/java/com/backstreetbrogrammer/chapter18_objectinputvalidation>

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/test/java/com/backstreetbrogrammer/chapter18_objectinputvalidation>

#### Chapter 19 - Using writeReplace() and readResolve()

The **writeReplace()** method allows the developer to provide a replacement object that will be serialized instead of the original one. The **writeReplace()** method is run ***before* writeObject()** and allows us to replace the object that gets serialized.

Similarly, **readResolve()** method is used during deserialization process to allow the developer to replace the deserialized object by another one of our choice. The **readResolve()** method is run ***after* readObject()** method is called.

###### Youtube

<https://www.youtube.com/playlist?list=PLQDzPczdXrTjGLkI8kd2d0bfNHx0v7dTy>

###### Github

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/main/java/com/backstreetbrogrammer/chapter19_writeReplaceReadResolve>

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/test/java/com/backstreetbrogrammer/chapter19_writeReplaceReadResolve>

#### Chapter 20 - Singleton pattern and readResolve()

In software engineering, the **singleton** pattern is a software design pattern that restricts the instantiation of a class to a singular instance. The pattern is useful when exactly one object is needed to coordinate actions across a system.

More specifically, the singleton pattern allows objects to:

* Ensure they only have one instance
* Provide easy access to that instance
* Control their instantiation by hiding the constructors of a class

As we know that deserialization process will always contain the “copy” of the original object => thus it will break the singleton design pattern as only ONE and SAME instance has to be there in a current JVM run.

In other words, any class would no longer be a singleton if it implements **Serializable** interface. It doesn’t matter whether the class uses the **default serialized form** or a **custom serialized form**, nor does it matter whether the class provides an explicit **readObject()** method.

Any **readObject()** method, whether explicit or default, returns a newly created instance, which will not be the same instance that was created at class initialization time.

To solve this issue, the **readResolve()** method allows to substitute another instance for the

one created by **readObject()**.

If the class of an object being deserialized defines a **readResolve()** method with the proper declaration, this method is invoked on the newly created object after it is deserialized.

The object reference returned by this method is then returned in place of the newly created

object. No reference to the newly created object is retained, so it immediately becomes eligible for garbage collection.

###### Youtube

<https://www.youtube.com/playlist?list=PLQDzPczdXrTjGLkI8kd2d0bfNHx0v7dTy>

###### Github

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/main/java/com/backstreetbrogrammer/chapter20_singleton>

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/test/java/com/backstreetbrogrammer/chapter20_singleton>

#### Chapter 21 - Using ObjectInputFilter

Deserialization of untrusted data can lead to vulnerabilities that allow an attacker to execute arbitrary code.

The **readObject()** method in **ObjectInputStream** class will construct any sort of serializable object that can be found on the classpath before passing it back to the caller.

Thus, if a rogue process sent us very large arrays or instances of classes that could be considered dangerous, we could perhaps check the generated instances using the **ObjectInputValidation** interface, but at that point the instance had already been constructed. We might already have run out of memory on the server or been hacked in some way.

It also means that if an attacker is able to put malicious data into the serialized object, this will cause serious security issues to the system.

To prevent Java deserialization vulnerabilities, an application has to restrict a set of classes which may be deserialized.

To do so, we can use serialization filters via **ObjectInputFilter** interface introduced in Java 9.

It has a method **checkInput(FilterInfo)**, and the **FilterInfo** provides the following filters choices to check:

* serialClass(): the class of an object being deserialized
* arrayLength(): the number of array elements when deserializing an array of the class
* depth(): the depth of the object graph at that point
* references(): the current number of object references
* streamBytes(): the current number of bytes consumed

The method **checkInput(FilterInfo)** returns either **Status.UNDECIDED**, **Status.ALLOWED**, or **Status.REJECTED**.

We should use **ALLOWED** if we want the object to be accepted, or we would mark them as **REJECTED** if we want this to be rejected.

**UNDECIDED** means we allow later filters to override but currently, it is undecided, not allowed and not rejected.

We can implement serialization filters in 2 ways:

* Custom filters by implementing **checkInput(FilterInfo)** method of **ObjectInputFilter** interface
* Pattern-based filters which can accept or reject specific classes, packages, or modules => A class that matches a pattern that is preceded by ! is rejected. A class that matches a pattern without ! is accepted.

###### Youtube

<https://www.youtube.com/playlist?list=PLQDzPczdXrTjGLkI8kd2d0bfNHx0v7dTy>

###### Github

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/main/java/com/backstreetbrogrammer/chapter21_serializationfilters>

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/test/java/com/backstreetbrogrammer/chapter21_serializationfilters>

#### Chapter 22 - Serialization Proxy Pattern

As we have seen that deserialization of untrusted data can lead to vulnerabilities that allow an attacker to execute arbitrary code. The decision to implement **Serializable** increases the likelihood of bugs and security problems as it allows instances to be created without the usage of new operator or using constructors.

Also, the serialized data may contain sensitive information if not protected properly allowing the hackers to peep in using this security hole.

This is where **Serialization Proxy Pattern** comes in which greatly ***reduces*** all these risks.

Steps to design the pattern:

* In the serializable Java POJO class, define a **private static nested class** with all the fields same as enclosing class and marked as **final**
* This inner static class should also implement **Serializable** interface and is called the **serialization proxy** of the enclosing class
* This inner static class should only have a single constructor for which the parameter type is the enclosing class
* Implement the **writeReplace()** method in enclosing class which returns an instance of inner serialization proxy class using the above single constructor
* Implement the **readObject()** method in enclosing class which should throw **InvalidObjectException**
* Finally, provide a **readResolve()** method in the inner serialization proxy class that returns the equivalent instance of the enclosing class

Serialization Proxy Pattern helps protect the original enclosing class instance to serialize using **writeReplace()** method and the attacker can not get the same instance as we have implemented the **readObject()** method to throw Exception.

Under the hood, the private inner serialization proxy class is taking care of serializing and deserializing the logical equivalent instance of the enclosing class in a secured way.

Serialization proxy pattern has two limitations:

* It is not compatible with classes that are extendable by their users or the classes which can be subclassed. Better to chose it for **final** classes.
* It is not compatible with some classes whose object graphs contain circularities: if we attempt to invoke a method on such an object from within its serialization proxy’s **readResolve()** method, we’ll get a **ClassCastException** because we don’t have the object yet, only its serialization proxy.

Thus, consider the serialization proxy pattern whenever we have to write a **readObject()** or **writeObject()** method on a class that is not extendable by its clients.

###### Youtube

<https://www.youtube.com/playlist?list=PLQDzPczdXrTjGLkI8kd2d0bfNHx0v7dTy>

###### Github

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/main/java/com/backstreetbrogrammer/chapter21_serializationfilters>

<https://github.com/backstreetbrogrammer/05_Persistence/tree/main/src/test/java/com/backstreetbrogrammer/chapter21_serializationfilters>