Upgrading Elasticsearch from 5.1 to 5.2

I decided to upgrade my Elasticsearch installation over 3 nodes - following the documentation in Rolling Upgrades

After the initial steps:

```
curl -XPUT 'localhost:9200/_cluster/settings?pretty' -H 'Content-Type: application/json' -d'
{
  "transient": {
    "cluster.routing.allocation.enable": "none"
  }
}'
curl -XPOST 'localhost:9200/_flush/synced?pretty'
```

I upgraded **elkserver1** with:

```
root@elkserver1:~# service elasticsearch stop
root@elkserver1:~# apt-get install elasticsearch
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  linux-headers-4.4.0-53 linux-headers-4.4.0-53-generic linux-headers-4.4.0-57 linux-headers-4.4.0-57-generic
  linux-image-4.4.0-53-generic linux-image-4.4.0-57-generic linux-image-extra-4.4.0-53-generic
  linux-image-extra-4.4.0-57-generic
Use 'sudo apt autoremove' to remove them.
The following packages will be upgraded:
  elasticsearch
1 upgraded, 0 newly installed, 0 to remove and 63 not upgraded.
Need to get 33.4 MB of archives.
After this operation, 236 kB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/5.x/apt stable/main amd64 elasticsearch all 5.2.0 [33.4 MB]
Fetched 33.4 MB in 3s (9,591 kB/s)
(Reading database ... 218942 files and directories currently installed.)
Preparing to unpack .../elasticsearch_5.2.0_all.deb ...
Unpacking elasticsearch (5.2.0) over (5.1.1) ...
Processing triggers for systemd (229-4ubuntu13) ...
Processing triggers for ureadahead (0.100.0-19) ...
Setting up elasticsearch (5.2.0) ...

Configuration file '/etc/elasticsearch/elasticsearch.yml'
 ==> Modified (by you or by a script) since installation.
 ==> Package distributor has shipped an updated version.
   What would you like to do about it ?  Your options are:
    Y or I  : install the package maintainer's version
    N or O  : keep your currently-installed version
      D     : show the differences between the versions
      Z     : start a shell to examine the situation
 The default action is to keep your current version.
*** elasticsearch.yml (Y/I/N/O/D/Z) [default=N] ?
Installing new version of config file /etc/elasticsearch/jvm.options ...
Installing new version of config file /usr/lib/systemd/system/elasticsearch.service ...
Installing new version of config file /etc/init.d/elasticsearch ...
Processing triggers for systemd (229-4ubuntu13) ...
Processing triggers for ureadahead (0.100.0-19) ...
root@elkserver1:~# service elasticsearch start
```

But it did not start - looking at the log I found:

```
[2017-02-07T19:56:57,523][ERROR][o.e.b.Bootstrap          ] Exception
java.lang.IllegalArgumentException: Plugin [x-pack] is incompatible with Elasticsearch [5.2.0]. Was designed
for version [5.1.1]
        at org.elasticsearch.plugins.PluginInfo.readFromProperties(PluginInfo.java:108) ~[elasticsearch-5.2.0.
jar:5.2.0]
        at org.elasticsearch.plugins.PluginsService.getPluginBundles(PluginsService.java:292) ~[elasticsearch-
5.2.0.jar:5.2.0]
        at org.elasticsearch.plugins.PluginsService.<init>(PluginsService.java:131) ~[elasticsearch-5.2.0.jar:
5.2.0]
        at org.elasticsearch.node.Node.<init>(Node.java:297) ~[elasticsearch-5.2.0.jar:5.2.0]
        at org.elasticsearch.node.Node.<init>(Node.java:232) ~[elasticsearch-5.2.0.jar:5.2.0]
        at org.elasticsearch.bootstrap.Bootstrap$6.<init>(Bootstrap.java:241) ~[elasticsearch-5.2.0.jar:5.2.0]
        at org.elasticsearch.bootstrap.Boots
```

DOH - Read the fucking manual - Step 4: Upgrade any plugins

So I removed and added the X-Pack again:

```
root@elkserver1:/usr/share/elasticsearch# bin/elasticsearch-plugin remove x-pack
root@elkserver1:/usr/share/elasticsearch# bin/elasticsearch-plugin install x-pack
-> Downloading x-pack from elastic
[=================================================] 100%
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@     WARNING: plugin requires additional permissions     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
* java.lang.RuntimePermission accessClassInPackage.com.sun.activation.registries
* java.lang.RuntimePermission getClassLoader
* java.lang.RuntimePermission setContextClassLoader
* java.lang.RuntimePermission setFactory
* java.security.SecurityPermission createPolicy.JavaPolicy
* java.security.SecurityPermission getPolicy
* java.security.SecurityPermission putProviderProperty.BC
* java.security.SecurityPermission setPolicy
* java.util.PropertyPermission * read,write
* java.util.PropertyPermission sun.nio.ch.bugLevel write
* javax.net.ssl.SSLPermission setHostnameVerifier
See http://docs.oracle.com/javase/8/docs/technotes/guides/security/permissions.html
for descriptions of what these permissions allow and the associated risks.

Continue with installation? [y/N]
```

And restarted Elasticsearch, and It cam up alright.

After a short while, **elkserver3** and **elkserver2** got the same (x-pack excluded) - between node upgrades went aproximatly 10 minutes.

And then I enabled Shard allocation again:

```
curl -XPUT 'localhost:9200/_cluster/settings?pretty' -H 'Content-Type: application/json' -d'
{
  "transient": {
    "cluster.routing.allocation.enable": "all"
  }
}'
```

During the entire upgrade, Cluster health was either red or yellow - and I was somewhat concerned about the state of everything in the cluster.

But it came back to green and the number of unassigned shards went towards a nice 0 (zero)

This actually costed me some data loss... first of all, after rebooting my elkserver1, the filebeat service did not start and I did not realized this for 2 days.

Before that realization, searching is the "syslog-*" index gave me "Courier Fetch: X of 5 shards failed" and looking at the Shards from the Upgrade time and onwards for the syslog-* index, size was closed to 0.

I never found the reason, but ended up deleting the "closed to 0 ones" in Kibana with "DELETE /syslog-dd.mm.yyyy" and then everything worked again. The X-Pack could be a possibility, but all other index'es works and have worked fine the entire time.

Also, the "Courier Fetch: X of 5 shards failed" is a common problem it seems, when googling it.

But I should have closed all Logstash instances before the upgrade....