

Install Elasticsearch 5.6.16 on Windows

Colin Dunn - 2021-12-23 - Comments (0) - Deskpro Legacy

Preface

Read our news post here for full information on the Log4j2 [0-day vulnerability](#). You do not require advanced system administration skills to follow these instructions, there is no command line interaction involved, but you should involve an experienced user (IT/Tech/System Administrator) where possible. For general guidance on whether this is relevant to you:

- **If you are running Elasticsearch v5.0.0 to v5.6.10, you must follow these instructions to update and patch. ([source](#))**
- **If you are running Elasticsearch v2.x or v5.6.11 or above - you do not need to update, however you must apply [a patch](#) (also step 9-14 of this document) ([source](#))**
- **If you installed Deskpro on Windows with the automatic installer prior to October 18th 2021, you should follow these instructions.**
- **This documentation can be used on any Windows Server 2008, 2012, 2012 R2, 2016, 2019 - as well as Windows 10.**

This process could take up to 20 minutes to complete. Deskpro can operate without the presence of Elasticsearch, if you do not have the time to address this fully now, you should at least disable Elasticsearch entirely in the short term, and revisit this later.

In summary you will:

1. Detect your version of Elasticsearch to confirm if you are affected
2. Disable the Elasticsearch connection
3. Install and configure the new version of Elasticsearch
4. Apply [a patch](#) to fix the vulnerability, restart the Elasticsearch service.
5. Re-enable Elasticsearch

To check your current Elasticsearch version:

Visit your Elasticsearch URL via the browser on the local server.

In most cases this is <http://127.0.0.1:9200> by default. Check Admin > Server >

Elasticsearch for your URL if this is not the case.

To disable Elasticsearch entirely:

Navigate to Admin > Server > Elasticsearch, untick "Enable Elasticsearch" and press save "Save Settings".



This will sever the live connection from the internet into your Elasticsearch service, preventing any exploits. If you are following the below instructions, **we also recommend you to first disable Elasticsearch to address the immediate vulnerability.**

Instructions to install Elasticsearch 5.6.16 (Time to complete: 15-20 minutes)

1. Download the MSI (BETA) version of Elasticsearch 5.6.16. We have tested this installer, it is safe to use.
<https://www.elastic.co/downloads/past-releases/elasticsearch-5-6-16>
2. Click on the .msi installer, this will take you through a simple wizard.
3. You can select "**Use Default Directories**" - unless you specifically want to install this in a custom way.

elasticsearch 5.6.16

Locations Service Configuration Plugins

☒ Use default directories

☐ Use a custom installation directory

C:\Program Files\Elastic\Elasticsearch

BROWSE

☐ Place logs, data, and config in the same directory

Data directory

C:\ProgramData\Elastic\Elasticsearch\data

BROWSE

Configuration directory

C:\ProgramData\Elastic\Elasticsearch\config

BROWSE

Logs directory

C:\ProgramData\Elastic\Elasticsearch\logs

BROWSE

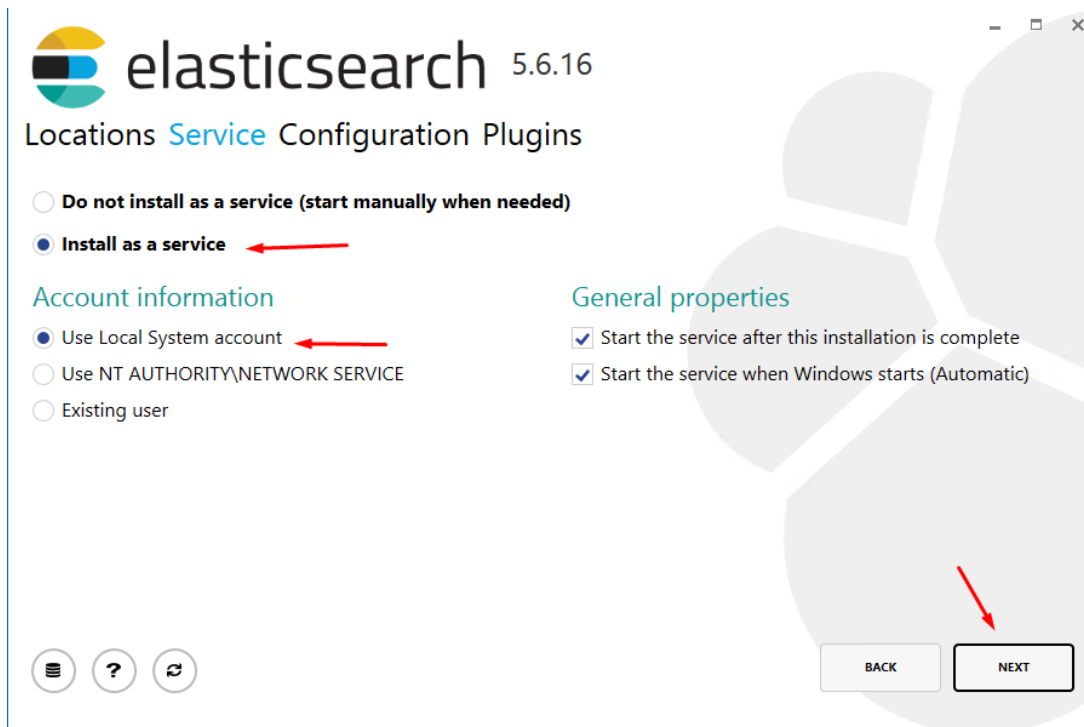


BACK

NEXT

1. You leave the Service settings as default. For clarification, you should have these options selected/enabled:

- Install as a service
- Use Local System account
- Start the service after installation is complete
- Start the service when Windows starts



1. You must set the memory, network host, and ports like so:

- Cluster and Node name can be left as default.
- Memory should be set at minimum to 256MB, in this example, we have gone for 1GB. Be aware of your resource availability when setting this, you can set this higher if you wish to.
- Leave "Lock JVM memory" unticked
- Set the "Network host" to **127.0.0.1**
- Set the HTTP port to **9201**
- Set the transport port to **9301**
- Leave Discover and Unicast host empty.

elasticsearch 5.6.16

Locations Service **Configuration** Plugins

Identifiers

Cluster name

Node name

Roles

☒ Data ☒ Master ☒ Ingest

Memory

1024 MB/4 GB

☐ Lock JVM memory

Network

Network host

HTTP port Transport port

Discovery

Minimum master nodes not set

Unicast Hosts

The existing Elasticsearch service will listen on port 9200 by default, so we will use 9201. This can theoretically be any available port, if you already have a service listening on this port (unlikely in 99.9% of instances), please modify the port number as necessary.

1. Leave all plugin selections empty as default, and proceed to Install.

elasticsearch 5.6.16

Locations Service Configuration **Plugins**

☐ **X-Pack**
X-Pack is an Elastic Stack extension that bundles security, alerting, monitoring, reporting, machine learning, and graph capabilities into one easy-to-install package. While the X-Pack components are designed to work together seamlessly, you can easily enable or disable the features you want to use. X-Pack is a proprietary plugin that falls under the Elastic EULA. By selecting to install X-Pack, A 30 day fully featured trial license is applied upon installation.

☐ **Ingest Attachment Processor**
The ingest attachment plugin lets Elasticsearch extract file attachments in common formats (such as PPT, XLS, and PDF) by using the Apache text and metadata extraction library Tika. You can use the ingest attachment plugin as a replacement for the mapper attachment plugin.

☐ **Ingest GeoIP Processor**
The GeoIP processor adds information about the geographical location of IP addresses, based on data from Geo-IP databases. This processor adds this information by default under the geoip field.

☐ **ICU Analysis**
The ICU Analysis plugin integrates the Lucene ICU module into Elasticsearch, adding extended Unicode support using the ICU libraries, including better analysis of Asian languages, Unicode normalization, Unicode-aware case folding, collation support, and transliteration.

☐ **Japanese (kuromoji) Analysis**
The Japanese (kuromoji) Analysis plugin integrates the Lucene kuromoji analysis module into Elasticsearch.

☐ **Phonetic Analysis**

1. Wait a few minutes for this to install, and exit the controller.

elasticsearch 5.6.16

Elasticsearch installed successfully!

What's Next?

[Open Elasticsearch in the browser](#)

[Read "The Definitive Guide" for free online!](#)

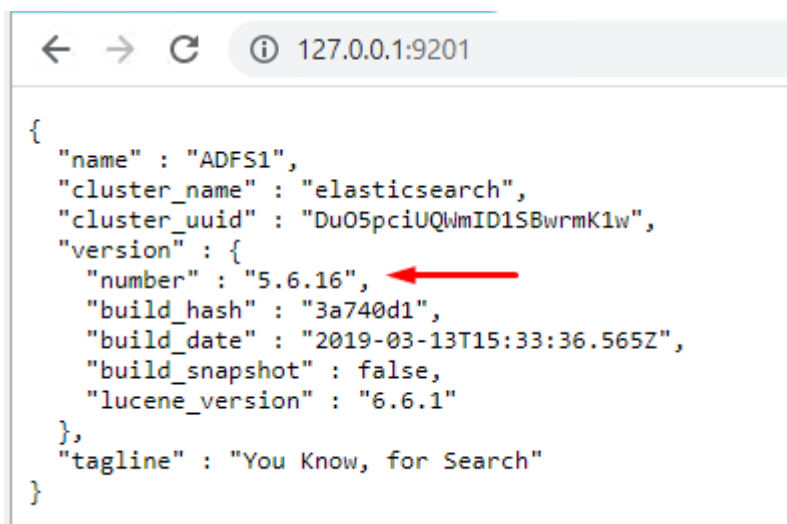
[Read the 5.6 API reference](#)

[Find a client for your favorite language](#)

☐ Open the Elastic Stack documentation after exiting

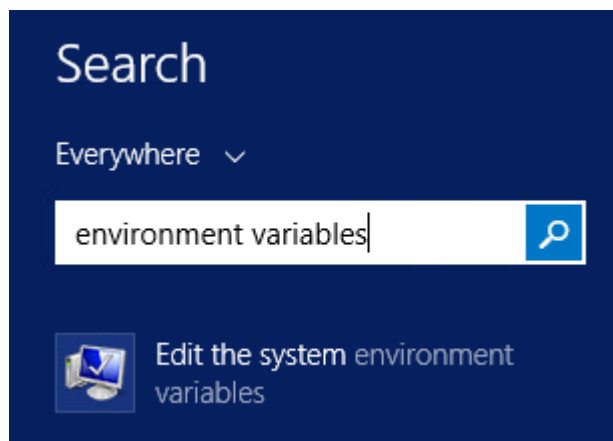


1. Visit <http://127.0.0.1:9201> via the browser on the local server, verify the service has been installed, and is listening.

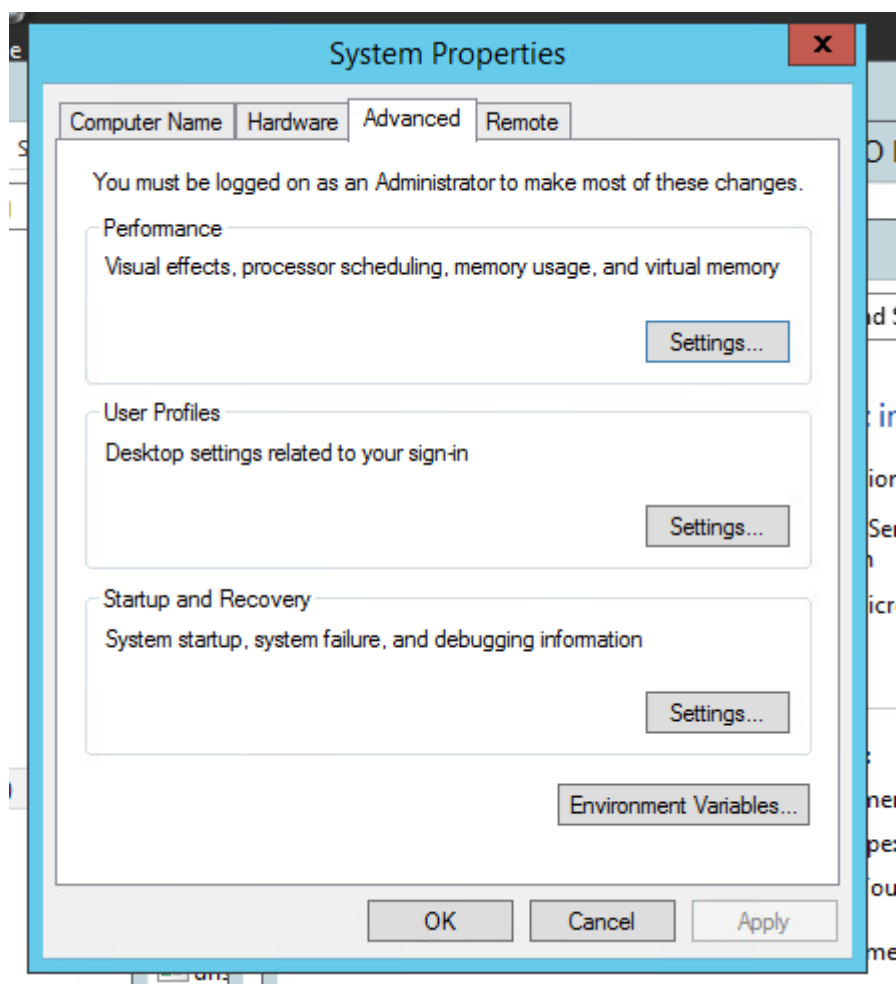
A screenshot of a web browser window. The address bar shows "127.0.0.1:9201". The page content is a JSON object representing the Elasticsearch status. A red arrow points to the "number" field in the "version" object, which is "5.6.16".

```
{
  "name" : "ADFS1",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "DuO5pciUQWmID1SBwrmK1w",
  "version" : {
    "number" : "5.6.16",
    "build_hash" : "3a740d1",
    "build_date" : "2019-03-13T15:33:36.565Z",
    "build_snapshot" : false,
    "lucene_version" : "6.6.1"
  },
  "tagline" : "You Know, for Search"
}
```

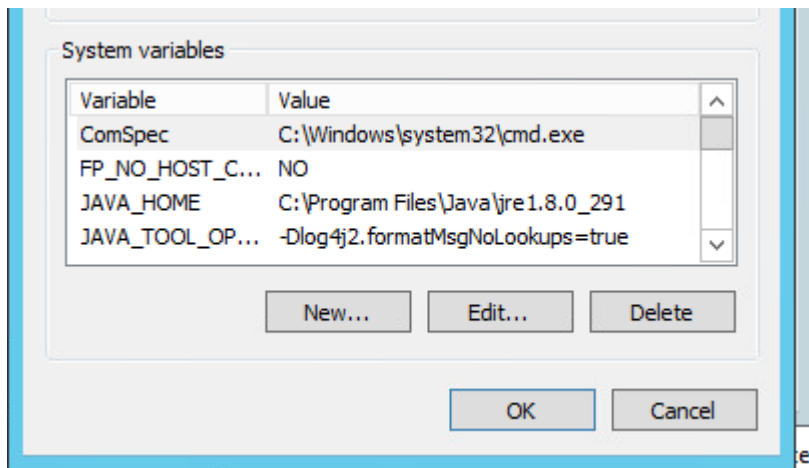
1. Search for "Environment Variables" in the start menu and click on "Edit the system environment variables" (or go to Control Panel > System and Security > System > Advanced system settings)



1. Click on "Environmental Variables"

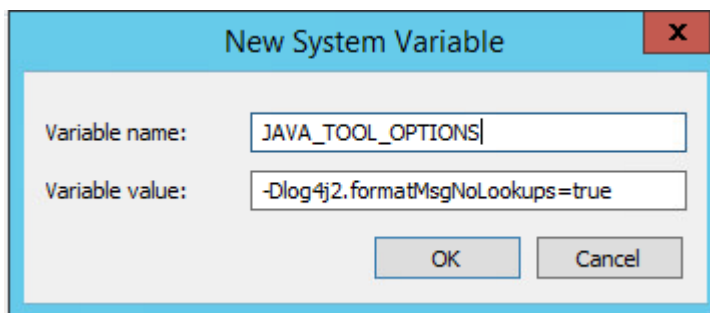


1. . Click on "New"

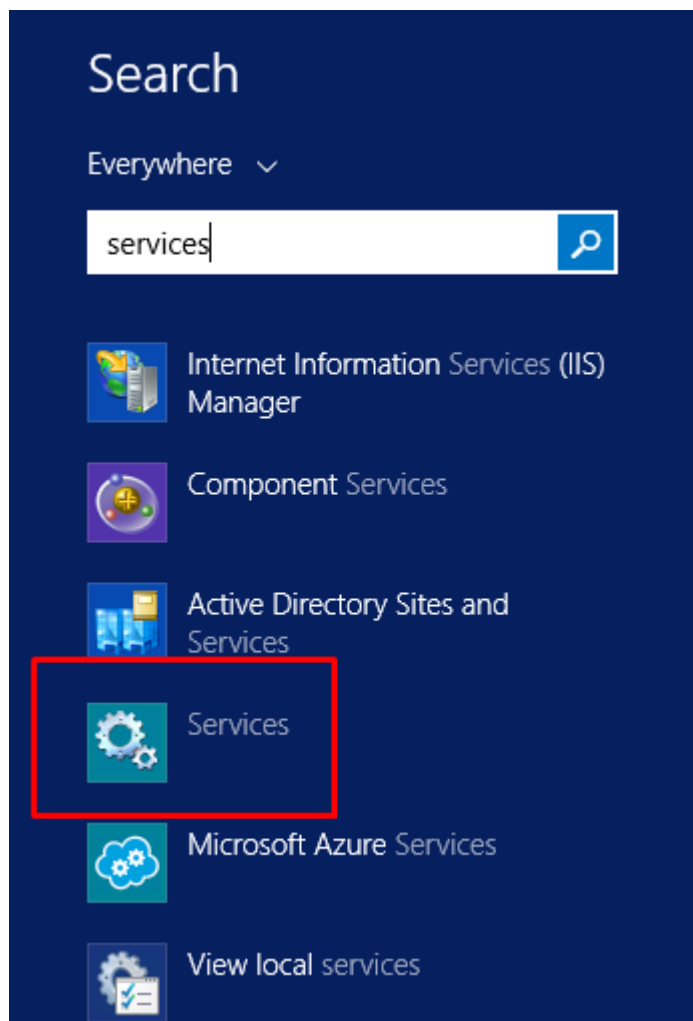


1. For the "Variable name" enter: JAVA_TOOL_OPTIONS

For the "Variable value" enter: -Dlog4j2.formatMsgNoLookups=true

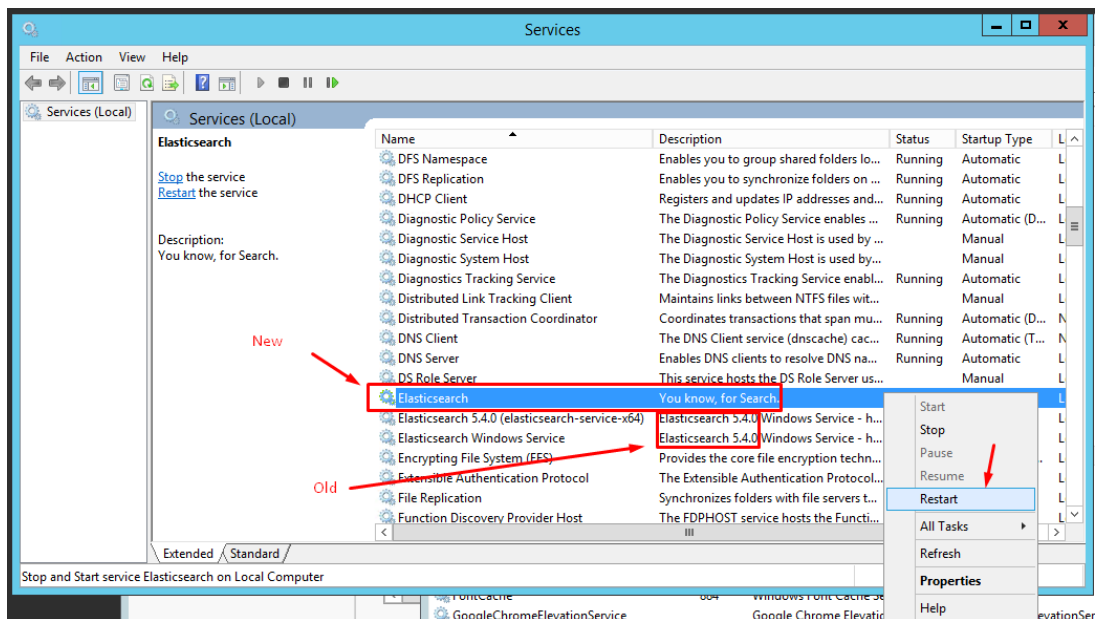


1. Press "OK" on the Window, "OK" again, and "OK" once more, till the system properties window is closed. You can try and open this up again, to confirm the changes have applied.
2. You must restart the Elasticsearch service after applying this. Open the "Start" menu and Search for Services, Open "Services"



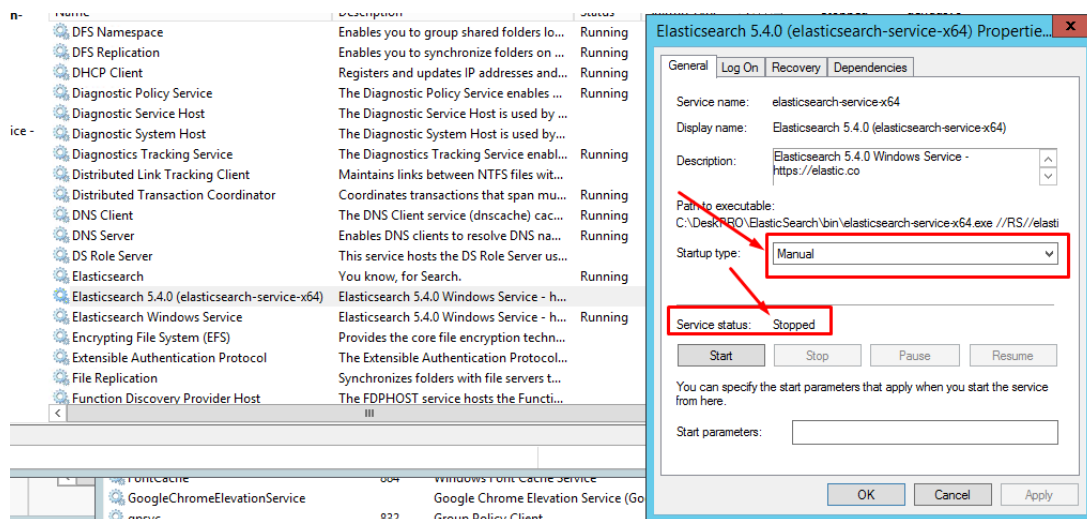
1. Locate the NEW Elasticsearch service, right click, and **restart**. The previous Elasticsearch services should be labelled with the old version 5.4.0.

If you are not sure, restart all of the Elasticsearch services. This is the only way to apply the above patch.

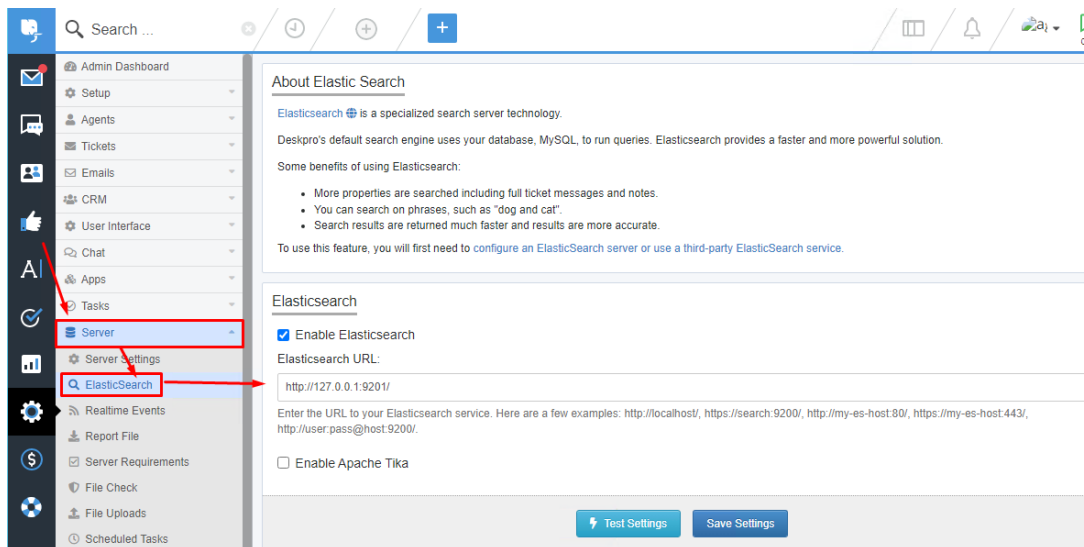


1. Disable the previous services entirely. Right click on the defunct services, and select properties.

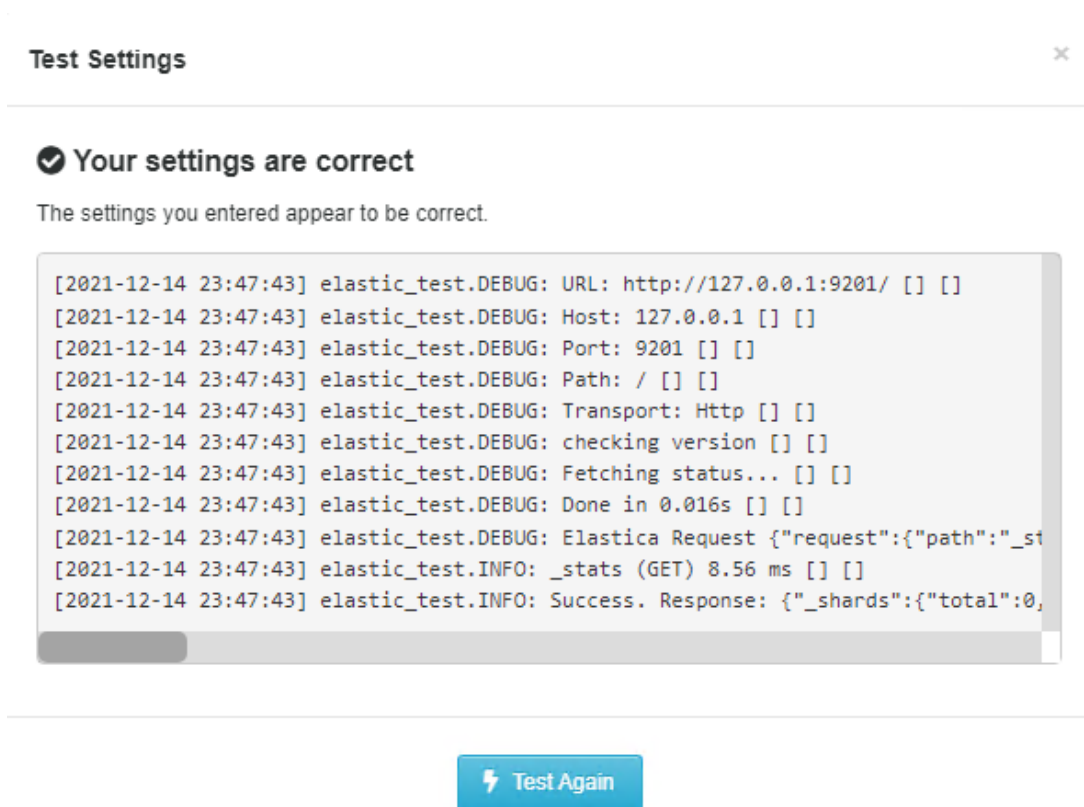
Ensure the old services are both **stopped**, and the **Startup type is set to disabled**. You will get a warning from the Deskpro Manager that some services are not working, this can be ignored.



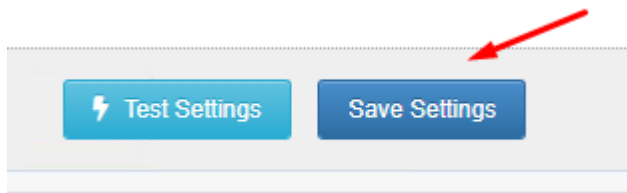
1. Log into your Deskpro Administrator area, navigate to Server > Elasticsearch, and enter in the new URL: <http://127.0.0.1:9201>



1. Click on "Test Settings" to do a soft-test of the server. You should see a window pop up confirming the new URL is correct, and responding properly



1. Close out of this, and click "Save Settings". The Elasticsearch index will automatically attempt to re-index itself.



1. Allow this to run for a number of minutes, to hours (depending on the size of your index) You may see an error suggesting your Elasticsearch service is down, you usually are able to refresh, and this will clear itself up.

When complete, Deskpro will show "The Elasticsearch index was initialized on:" - and display the objects inn Elasticsearch, compared to those in Deskpro. The numbers on each side of the graph should be more or less equal.

1. Final check, search for a string, in your search box, and ensure the "Sort By:" options are displaying, and output different results. If Elasticsearch is not working, these options will not display.

