

Wissensdatenbank > Deskpro Legacy > Install Elasticsearch 5.6.16 on Windows

### Install Elasticsearch 5.6.16 on Windows

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

## Preface

Read our news post here for full information on the Log4j2 <u>0-day vulnerability</u>. 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 <u>a patch</u> (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 <u>a patch</u> 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 <a href="http://lz7.0.0.1:9200">http://lz7.0.0.1:9200</a> 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".

🚯 Apps		
⊘ Tasks	-	Elasticsearch
Server	-	Enable Elasticsearch
Server Settings		
Q ElasticSearch		Save Settings
Realtime Events		
🛓 Report File		The Elasticsearch Engine is an optional technology. It's currently provided without charge but may require a license in the future.
Server Requirements		

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

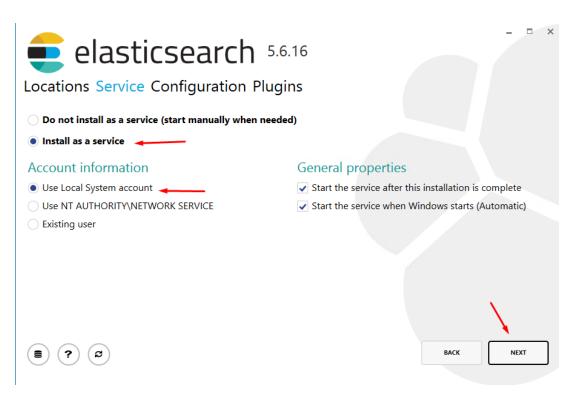
you to first disable Elasticsearch to address the immediate vulnerability.

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

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

	ticsearch 5.6.16 e Configuration Plugins		- • ×
OUse a custom install	ation 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
		васк	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

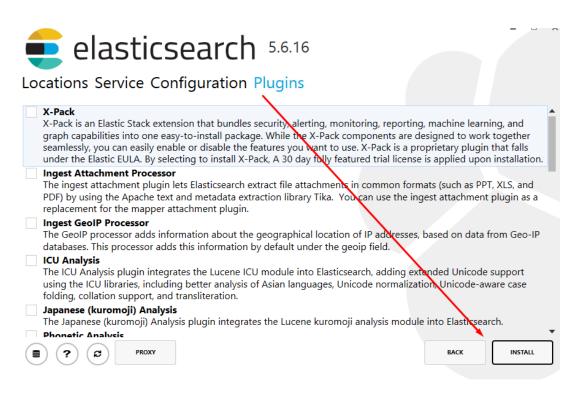


- 1. You must set the memory, network host, and ports like so:
- Cluster and Node name can be left as default.
- Memory should be set at minimum to 256MB, in this example, we have gone for 1GB.
   Be aware of your resource availability when setting this, you can set this higher if you wish to.
- Leave "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.

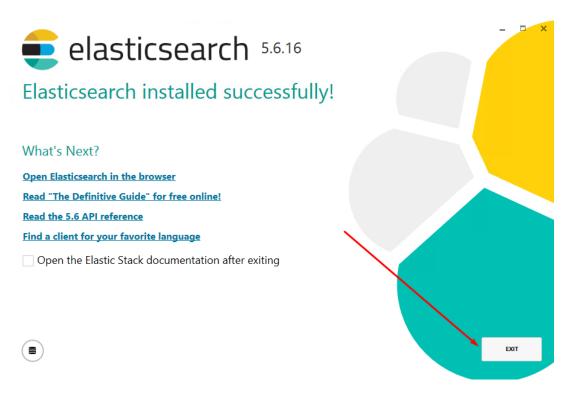
elasticsearch 5.6.16 Locations Service Configuration Plugins						
Identifiers		Network		(Optional)		
Cluster name	elasticsearch	Network host	127.0.0.1			
Node name	ADFS1	HTTP port	9201 +- Transport port	9301 +-		
Roles	Data Master Ingest	Discovery		(Optional)		
Memory	1024 MB/4 GB	Unicast Hosts	ster nodes not set	+-		
Lock JVM r	nemory	+ -				
	3		ВАСК	NEXT		

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.

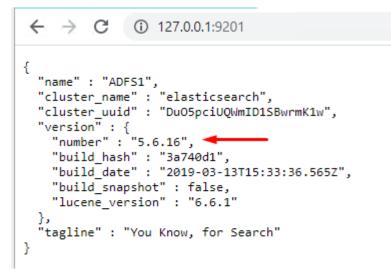
1. Leave all plugin selections empty as default, and proceed to Install.



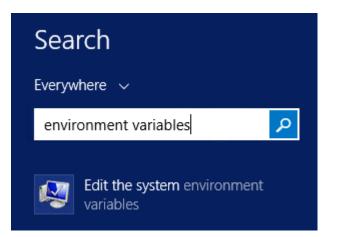
1. Wait a few minutes for this to install, and exit the controller.



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



 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"

	System Properties	
ļ	Computer Name Hardware Advanced Remote	
	You must be logged on as an Administrator to make most of these changes.	
	Performance Visual effects, processor scheduling, memory usage, and virtual memory	
	Settings	
	User Profiles	
	Desktop settings related to your sign-in	
	Settings	
	Startup and Recovery	
	System startup, system failure, and debugging information	
	Settings	
	Environment Variables	
	OK Cancel Apply	
_		

1. . Click on "New"

Variable	Value	^		
ComSpec	C:\Windows\system32\cmd.exe			
FP_NO_HOST_C	NO			
JAVA_HOME	C:\Program Files\Java\jre1.8.0_291			
JAVA_TOOL_OP	-Dlog4j2.formatMsgNoLookups=true	~		
[	New Edit Delet			
l	New Edit Delet	e		
	200 (AMA)			

1. . For the "Variable name" enter: JAVA\_TOOL\_OPTIONS

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

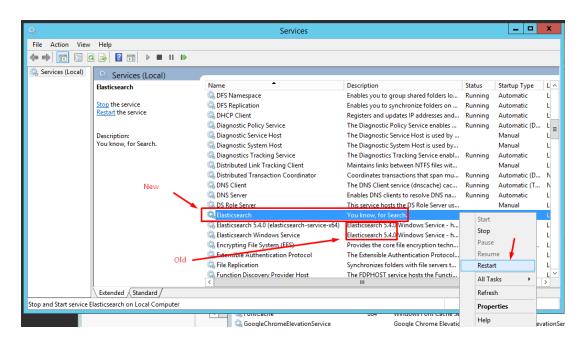
New System Variable		
Variable name: Variable value:	JAVA_TOOL_OPTIONS -Dlog4j2.formatMsgNoLookups=true OK Cancel	

- 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"

Search				
Everyw	/here ~			
servi	ces 🔎			
	Internet Information Services (IIS) Manager			
	Component Services			
	Active Directory Sites and Services			
Ö,	Services			
<b>@</b>	Microsoft Azure Services			
۲¢	View local 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.

n-	nome	Description	Status	
	🔍 DFS Namespace	Enables you to group shared folders lo	Running	Elasticsearch 5.4.0 (elasticsearch-service-x64) Propertie
	CFS Replication	Enables you to synchronize folders on	Running	
	Client DHCP Client	Registers and updates IP addresses and	Running	General Log On Recovery Dependencies
	Capital Diagnostic Policy Service	The Diagnostic Policy Service enables	Running	Service name: elasticsearch-service-x64
	🔍 Diagnostic Service Host	The Diagnostic Service Host is used by		
ice -	🖏 Diagnostic System Host	The Diagnostic System Host is used by		Display name: Elasticsearch 5.4.0 (elasticsearch-service-x64)
	🔍 Diagnostics Tracking Service	The Diagnostics Tracking Service enabl	Running	Description: Elasticsearch 5.4.0 Windows Service -
	Distributed Link Tracking Client	Maintains links between NTFS files wit		https://elastic.co
	Distributed Transaction Coordinator	Coordinates transactions that span mu	Running	Pathto executable:
	🔍 DNS Client	The DNS Client service (dnscache) cac	Running	Pathop executable: C:\DeskNBO\ElasticSearch\bin\elasticsearch-service-x64.exe //RS//elasti
	C DNS Server	Enables DNS clients to resolve DNS na	Running	
	🔍 DS Role Server	This service hosts the DS Role Server us		Startup type: Manual 🗸
	🔍 Elasticsearch	You know, for Search.	Running	
	Elasticsearch 5.4.0 (elasticsearch-service-x64)	Elasticsearch 5.4.0 Windows Service - h		
	🖳 Elasticsearch Windows Service	Elasticsearch 5.4.0 Windows Service - h	Running	Service status: Stopped
	🔍 Encrypting File System (EFS)	Provides the core file encryption techn		
	🖳 Extensible Authentication Protocol	The Extensible Authentication Protocol		Start Stop Pause Resume
	Sile Replication	Synchronizes folders with file servers t		You can specify the start parameters that apply when you start the service
	Runction Discovery Provider Host	The FDPHOST service hosts the Functi		from here.
	<	III		
				Start parameters:
	roncache	004 WINDOWS FOR CACHE SE		
	GoogleChromeElevationService	Google Chrome Elevatio	n Service (Go	OK Cancel Apply
	C gpsvc	832 Group Policy Client		

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

Ģ	Q Search	◎/ ④ /    /  +	/ 💷 / 🔔 / 🙈 -	On
	<ul> <li>Admin Dashboard</li> <li>Setup</li> </ul>	About Elastic Search		
	🚨 Agents 👻	Elasticsearch 🌐 is a specialized search server technology.		
	Tickets -	Deskpro's default search engine uses your database, MySQL, to run queries. Elasticsearch provides a faster and more pow	erful solution.	
24	🖂 Emails 🔹	Some benefits of using Elasticsearch:		
	🚢 CRM 👻	More properties are searched including full ticket messages and notes.		
<b>1</b>	User Interface	<ul> <li>You can search on phrases, such as "dog and cat".</li> <li>Search results are returned much faster and results are more accurate.</li> </ul>		
. \	Q₁ Chat ·	To use this feature, you will first need to configure an ElasticSearch server or use a third-party ElasticSearch service.		
A	& Apps 🔹			
$\bigotimes$	🕑 Tasks 🔍	Elasticsearch		
	Server -	Z Enable Elasticsearch		
	Server Settings	Elasticsearch URL:		
	Q ElasticSearch	http://127.0.0.1:9201/		
	Realtime Events	Enter the URL to your Elasticsearch service. Here are a few examples: http://localhost/, https://search:9200/, http://my-es-ho	ost:80/, https://my-es-host:443/,	
	🛓 Report File	http://user:pass@host:9200/.		
\$	Server Requirements	Enable Apache Tika		
	File Check			
۲	1 File Uploads	Fest Settings		
	Scheduled Tasks			

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

×

#### Test Settings

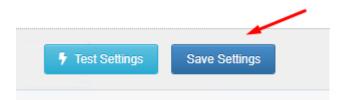
#### Your settings are correct

The settings you entered appear to be correct.

```
[2021-12-14 23:47:43] elastic_test.DEBUG: URL: http://127.0.0.1:9201/ [] []
[2021-12-14 23:47:43] elastic_test.DEBUG: Host: 127.0.0.1 [] []
[2021-12-14 23:47:43] elastic_test.DEBUG: Port: 9201 [] []
[2021-12-14 23:47:43] elastic_test.DEBUG: Path: / [] []
[2021-12-14 23:47:43] elastic_test.DEBUG: Transport: Http [] []
[2021-12-14 23:47:43] elastic_test.DEBUG: checking version [] []
[2021-12-14 23:47:43] elastic_test.DEBUG: Fetching status... [] []
[2021-12-14 23:47:43] elastic_test.DEBUG: Done in 0.016s [] []
[2021-12-14 23:47:43] elastic_test.DEBUG: Elastica Request {"request":{"path":"_st
[2021-12-14 23:47:43] elastic_test.INFO: _stats (GET) 8.56 ms [] []
[2021-12-14 23:47:43] elastic_test.INFO: Success. Response: {"_shards":{"total":0,
]
```



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



 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.

 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.

