



BroadBot Installation Manual

IG-001

Table of Contents

1.	Introduction.	3
2.	Pre-requisites.	3
3.	Installation Procedure for Windows Operating Systems	3
4.	Post-installation.	6
5.	Uninstall or Roll-back.	8
6.	Installation Procedure for Centos/Debian:.....	10
7.	Points to Note:	11
8.	Troubleshooting:.....	12

1. Introduction.

Built on the Elastic Stack, BroadBot was designed with simplicity in mind. We want to give users insight to any malicious activity happening on their local machine and/or network, without needing the knowledge or spending the time putting everything together themselves.

BroadBot is an open source offering of Invinsec's SIEMaaS. Please visit our Web site <https://www.invinsec.com/> for a full product breakdown.

2. Pre-requisites.

Before running BroadBot Installer, please do check out the requirements below:

We strongly recommend using the latest JDK 8 (at least u20 or higher). If that is not an option, use JDK 7.0 update u55. Do note that the Java Virtual Machine (JVM) versions are critical for a stable environment as an incorrect version can corrupt the data underneath as explained in this blog post.

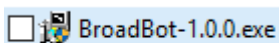
Download the latest JDK from Oracle's site. The software and installation instructions can be found here: <http://www.oracle.com/technetwork/java/javase/downloads/index.html>

Important: Please note that even though JRE includes a JVM, BroadBot installation requires JDK instead. This is a requirement because Elastic will be run as a Windows Service. Further reading: <https://www.elastic.co/guide/en/elasticsearch/reference/current/windows.html>

3. Installation Procedure for Windows Operating Systems

Once all prerequisite checks and controls are positively finished, the install process can start.

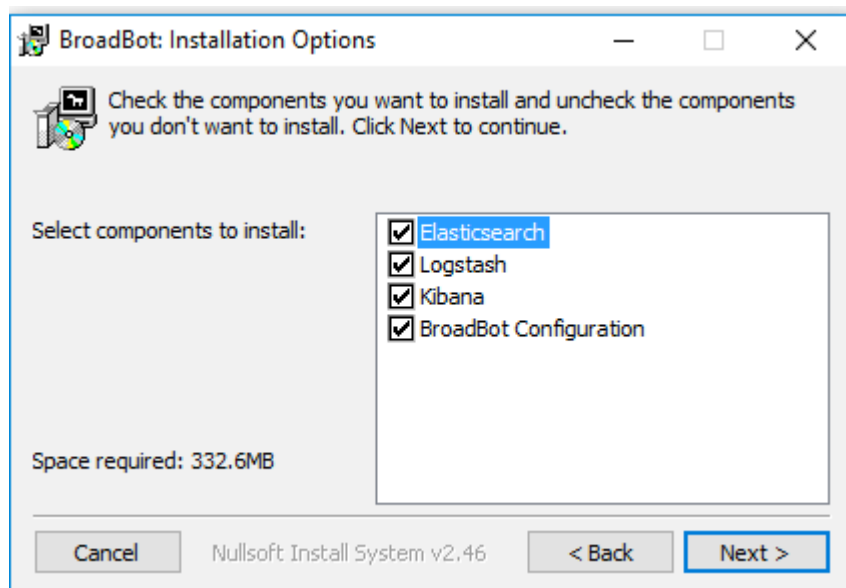
Run the BroadBot-1.0.0.exe to start the setup of BroadBot, if prompted, give administrative permissions.



Read the Licence agreement and accept the terms as shown below:

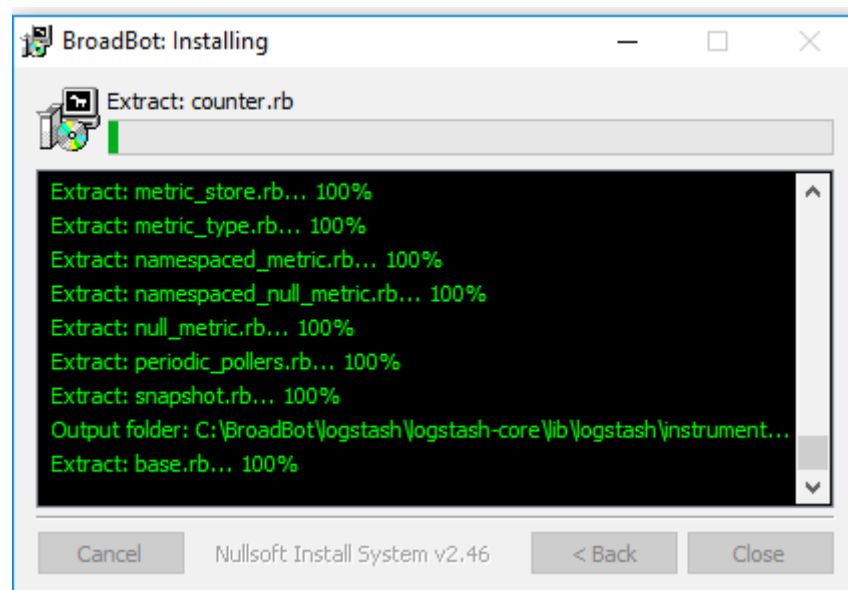
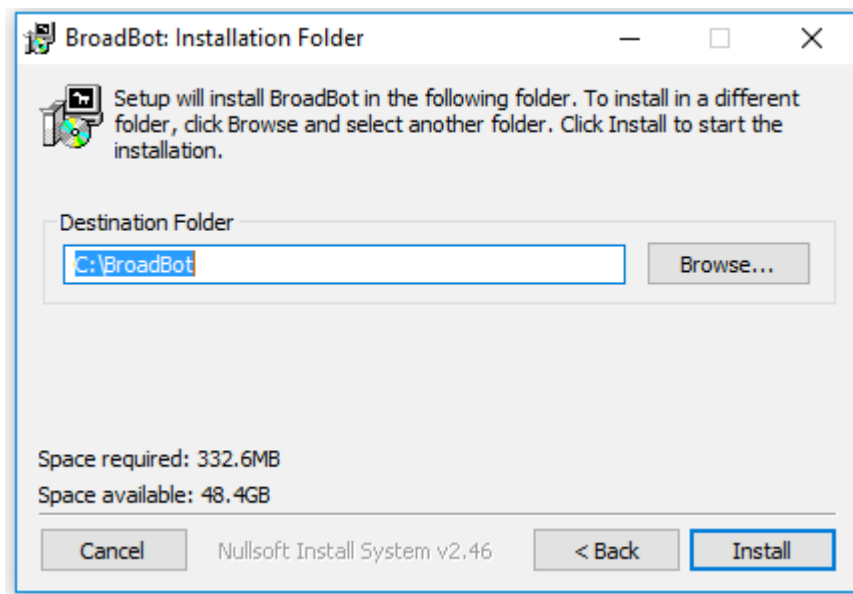


By default, all components are selected for the installation. Leave as is for a full installation:

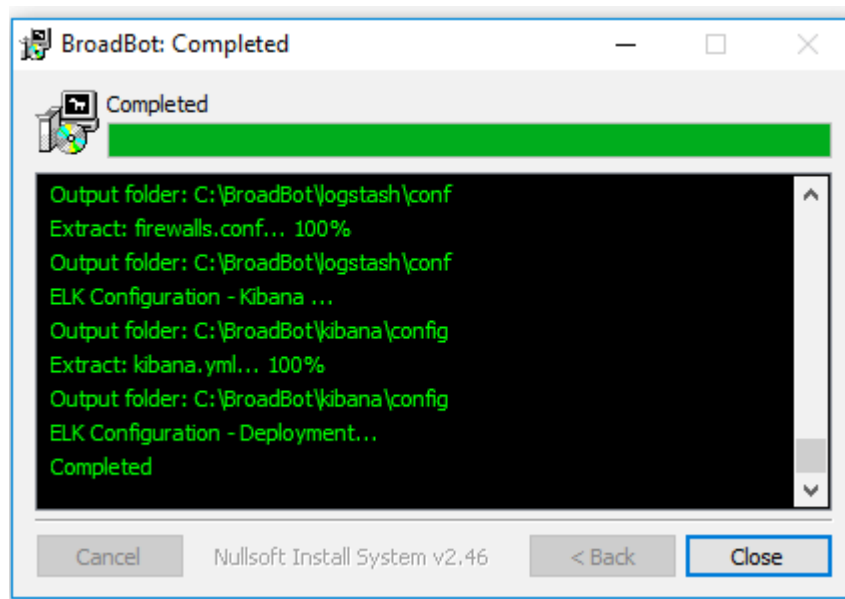


Next, select the Install Directory: take note of the paths where BroadBot will install the shared components (default is C:\BroadBot drive). Click Install to begin the installation.

Please note that the installation might take some time.

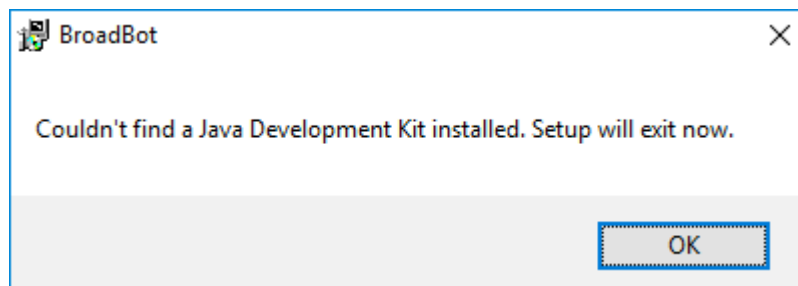


Once the installation is complete, the last version of BroadBot service will be available on the localhost.



Once completed, click on Close.

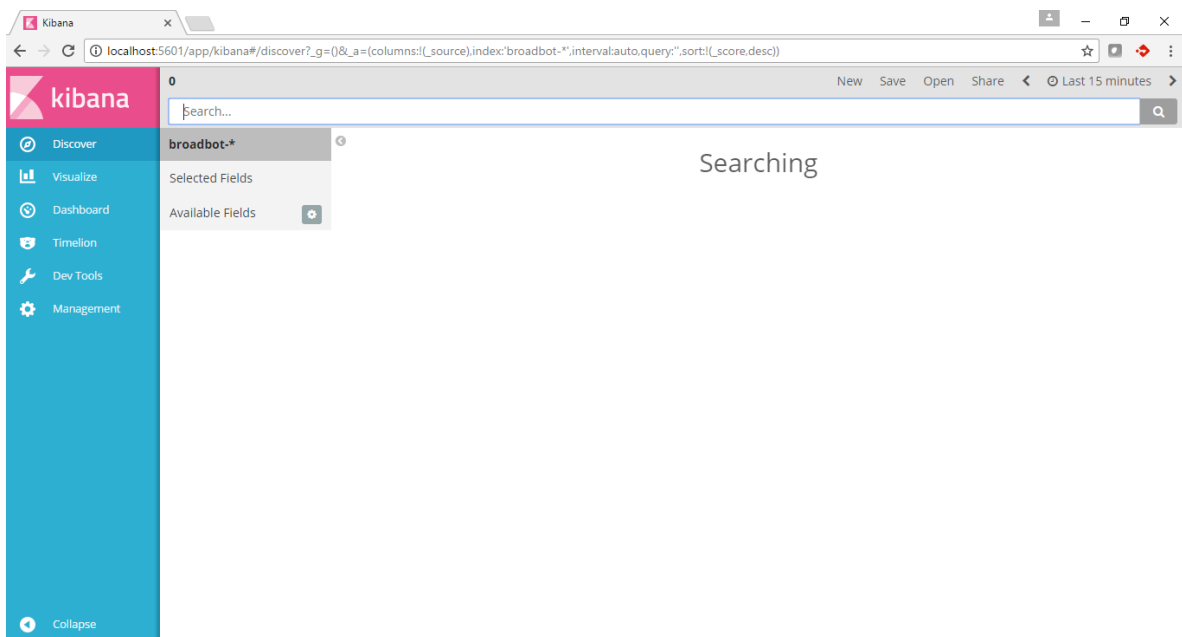
If you receive an error related to the Java Development Kit not installed, check the [pre-requisites](#) section.



4. Post-installation.

Once the installation process is completed, make sure that BroadBot is running successfully.

Open a browser window, and go to: <http://localhost:5601/>



If the page fails, BroadBot might not be running. In that case, please check the following services are running:

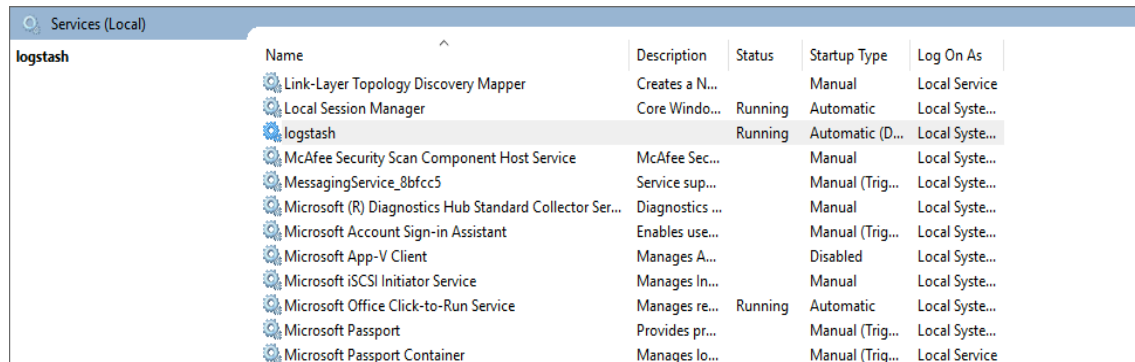
- **Elasticsearch 5.3.2:**

Services (Local)					
Elasticsearch 5.3.2 (elasticsearch-service-x64)					
Description: Elasticsearch 5.3.2 Windows Service - https://elastic.co					
Name	Description	Status	Startup Type	Log On As	
Elasticsearch 5.3.2 (elasticsearch-service-x64)	Elasticsearch...	Running	Automatic (D...	Local Syste...	
Embedded Mode	The Embed...		Manual (Trig...	Local Syste...	
Encrypting File System (EFS)	Provides th...		Manual (Trig...	Local Syste...	
Enterprise App Management Service	Enables ent...		Manual	Local Syste...	
Extensible Authentication Protocol	The Extensi...		Manual	Local Syste...	
Fax	Enables you...		Manual	Network S...	
File History Service	Protects use...		Manual (Trig...	Local Syste...	
Function Discovery Provider Host	The FDPHO...	Running	Manual	Local Service	
Function Discovery Resource Publication	Publishes th...		Manual	Local Service	

- **Kibana:**

Services (Local)					
kibana					
Name	Description	Status	Startup Type	Log On As	
Kaspersky Anti-Virus Service 17.0.0	Provides co...	Running	Automatic	Local Syste...	
Kaspersky Secure Connection Service 1.0.0	Protects co...	Running	Automatic (D...	Local Syste...	
kibana		Running	Automatic (D...	Local Syste...	
klvssbrigde64			Manual	Local Syste...	
KtmRm for Distributed Transaction Coordinator	Coordinates...		Manual (Trig...	Network S...	
Link-Layer Topology Discovery Mapper	Creates a N...		Manual	Local Service	
Local Session Manager	Core Windo...	Running	Automatic	Local Syste...	
logstash		Running	Automatic (D...	Local Syste...	
McAfee Security Scan Component Host Service	McAfee Sec...		Manual	Local Syste...	
MessagingService_8bfcc5	Service sup...		Manual (Trig...	Local Syste...	

Logstash:



The screenshot shows the Windows Services console with the 'logstash' service selected. The service is running and has an automatic startup type.

Name	Description	Status	Startup Type	Log On As
Link-Layer Topology Discovery Mapper	Creates a N...		Manual	Local Service
Local Session Manager	Core Windo...	Running	Automatic	Local Syste...
logstash		Running	Automatic (D...	Local Syste...
McAfee Security Scan Component Host Service	McAfee Sec...		Manual	Local Syste...
MessagingService_8bfcc5	Service sup...		Manual (Trig...	Local Syste...
Microsoft (R) Diagnostics Hub Standard Collector Ser...	Diagnostics ...		Manual	Local Syste...
Microsoft Account Sign-in Assistant	Enables use...		Manual (Trig...	Local Syste...
Microsoft App-V Client	Manages A...		Disabled	Local Syste...
Microsoft iSCSI Initiator Service	Manages In...		Manual	Local Syste...
Microsoft Office Click-to-Run Service	Manages re...	Running	Automatic	Local Syste...
Microsoft Passport	Provides pr...		Manual (Trig...	Local Syste...
Microsoft Passport Container	Manages lo...		Manual (Trig...	Local Service

5. Uninstall or Roll-back.

If you no longer need to use BroadBot, or would like to re-install it or change feature, follow the steps below to uninstall BroadBot from your system.

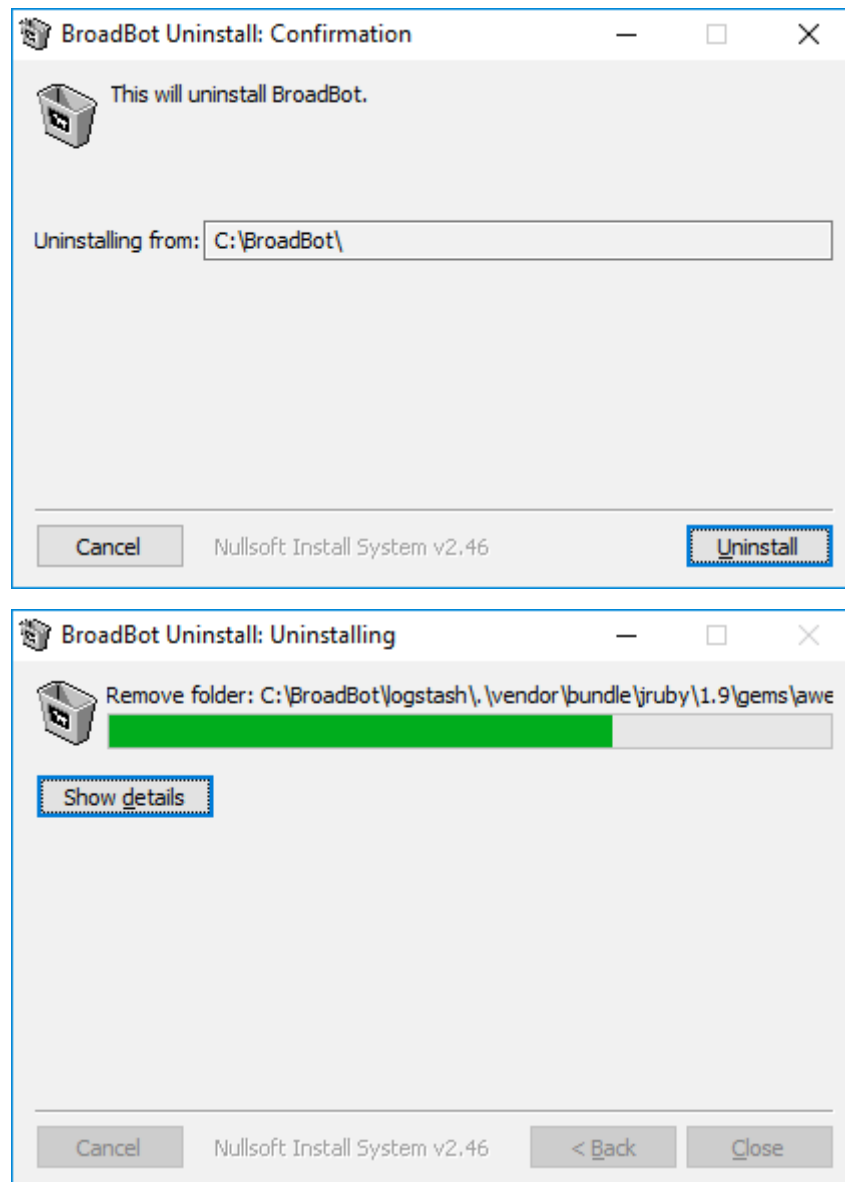
- Go to Windows Control Panel -> Programs and Features. Sort program list by name.
- Look for BroadBot, and select Uninstall.

Uninstall or change a program

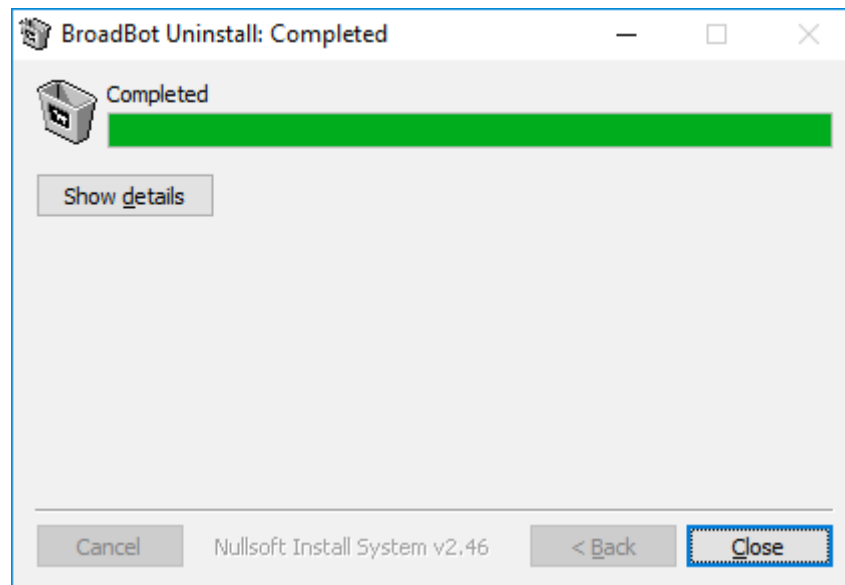
To uninstall a program, select it from the list and then click Uninstall, Change or Repair.

Name	Publisher	Installed On	Size	Version
Adobe Acrobat Reader DC - Español	Adobe Systems Incorporated	15/04/2017	413 MB	17.009.20044
ALPS GlidePoint Driver	Alps Electric	31/03/2017	43.0 MB	10.1201.1717.104
Aqua Data Studio 17.0 - 64bit	AquaFold, Inc.	25/01/2017	456 MB	17.0
<input checked="" type="checkbox"/> BroadBot (remove only)		27/04/2017		
Cisco WebEx Meetings	Cisco WebEx LLC	03/02/2017		

- BroadBot will gather the information it needs to perform the uninstall. Click on Uninstall. This will take some time.



- Once finished, BroadBot is removed. Click on Close.



- Perform a quick check to make sure BroadBot was removed (Windows Control Panel -> Programs and Features).

6. Installation Procedure for Centos/Debian:

`curl --silent https://gitlab.deeprecce.net/invinsec/Elk-Installer/raw/master/BB-Unix.tar.gz | tar xvz && bash BB-Unix-Install.sh`

That's pretty much it! To start using the included dashboards, point your browser to `http://x.x.x.x:5601` or `http://hostname:5601` (as instructed at the end of the installer).

BroadBot ships with one 'Firewall' Dashboard, which is what you are greeted with upon accessing the above URL.

The installer also ships with a predefined configuration that is expecting firewalls logs in `/var/log/firewalltype.log`. This can be changed if required from `/etc/logstash/firewalls.conf`

```
#inputs for files or tcp
input{
  file {
    path => "/var/log/iptables.log"
    type => "iptables"
  }
}
```

Also included in the configuration is an option to receive such logs via syslog. This is 100% configurable. You may assign any port or protocol that you wish. Any TCP port specified can also support TLS encryption, however certificate generation is not in scope of this release. This is also configurable from from `/etc/logstash/firewalls.conf`. Simple uncomment the port stanzas and comment the file stanzas.

```
#tcp {
  #port => 5141
  #type => "iptables"
#}
```

Any changes made to this file require a restart of logstash:

systemctl restart logstash or service logstash restart for older systems.

7. Points to Note:

IPTables

If you are using IPTables on the BroadBot host itself, or shipping logs from another host, the message within the IPTables log for any block filter must contain the word 'Dropped'. Otherwise, BroadBot will mark these packets with a 'pass' action.

Example of a block action:

```
Apr 23 07:42:55 Server kernel: IPTables-Inbound-Dropped: IN=eth0 OUT=
MAC=04:01:e7:93:12:01:5c:45:27:79:03:30:08:00 SRC=1.2.3.4 DST=5.6.7.8 LEN=44 TOS=0x00
PREC=0x00 TTL=56 ID=63836 PROTO=TCP SPT=43517 DPT=81 WINDOW=22997 RES=0x00 SYN
URGP=0
```

Examples of a pass action:

```
Apr 24 07:09:50 Server kernel: IPTables-Outbound: IN= OUT=tun0 SRC=1.2.3.4 DST=5.6.7.8 LEN=60
TOS=0x00 PREC=0x00 TTL=64 ID=22977 DF PROTO=TCP SPT=56620 DPT=5141 WINDOW=29200
RES=0x00 SYN URG=0
```

```
Apr 24 07:09:54 Server kernel: IPTables-Inbound: IN=tun0 OUT= MAC= SRC=1.2.3.4 DST=5.6.7.8
LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=120 DF PROTO=TCP SPT=34616 DPT=10050
WINDOW=29200 RES=0x00 SYN URG=0
```

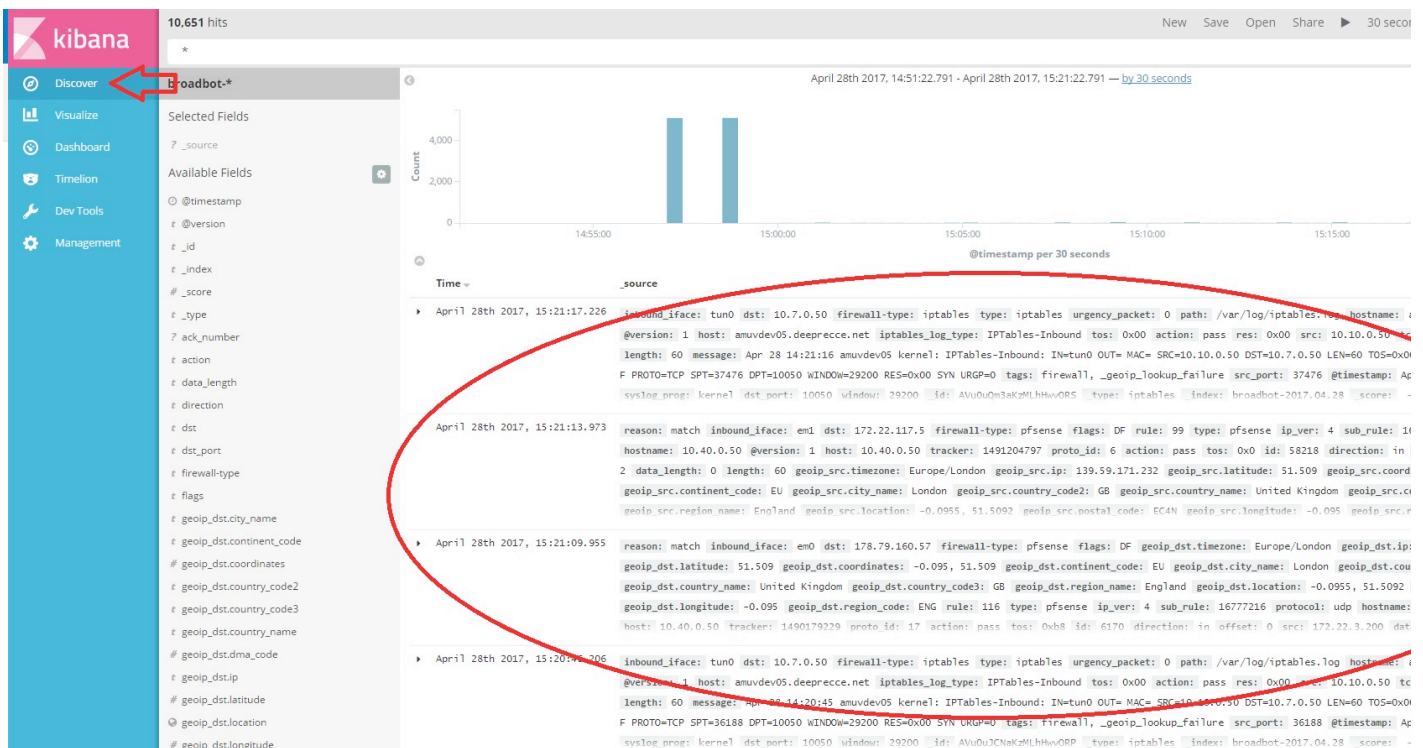
8. Troubleshooting:

My Dashboard is Blank!

First and foremost, make sure you are sending some logs! Confirm you have logs in the predefined directories, or that your syslog devices are indeed sending logs.

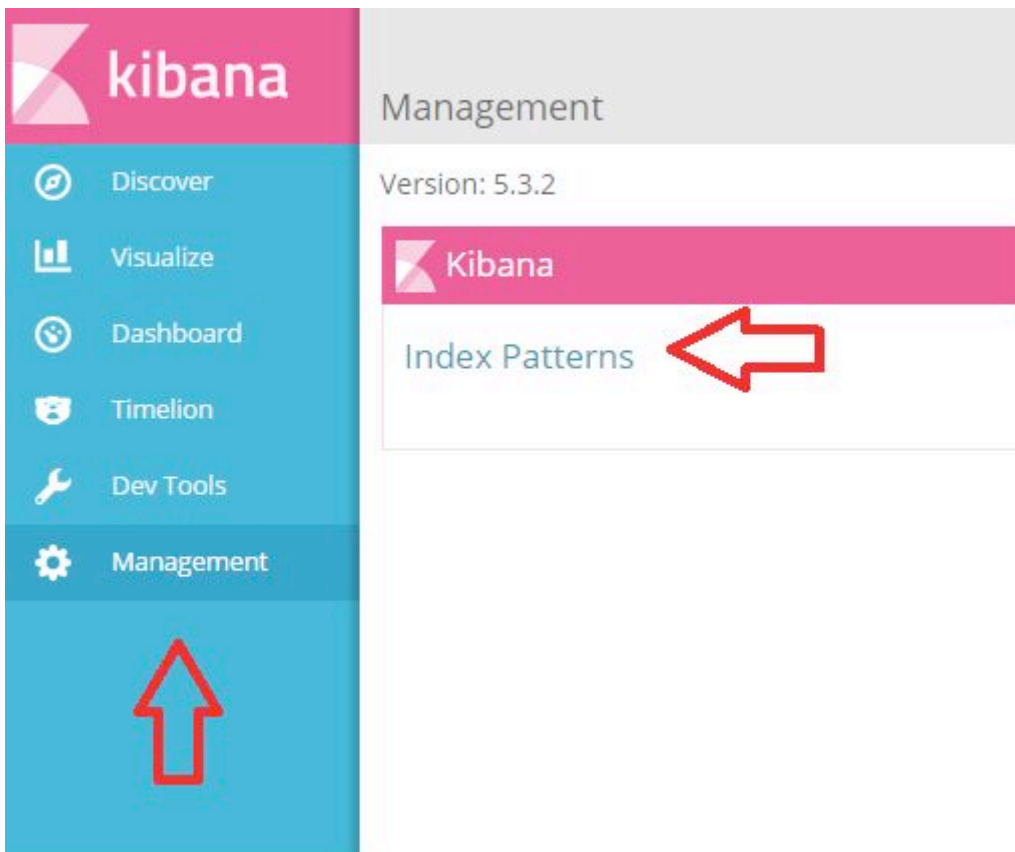
If you've confirmed this, and your dashboard is still blank - we need to confirm that logs are being ingested correctly.

Navigate to the 'Discover' tab - this will display log messages in a textual and tabular form.

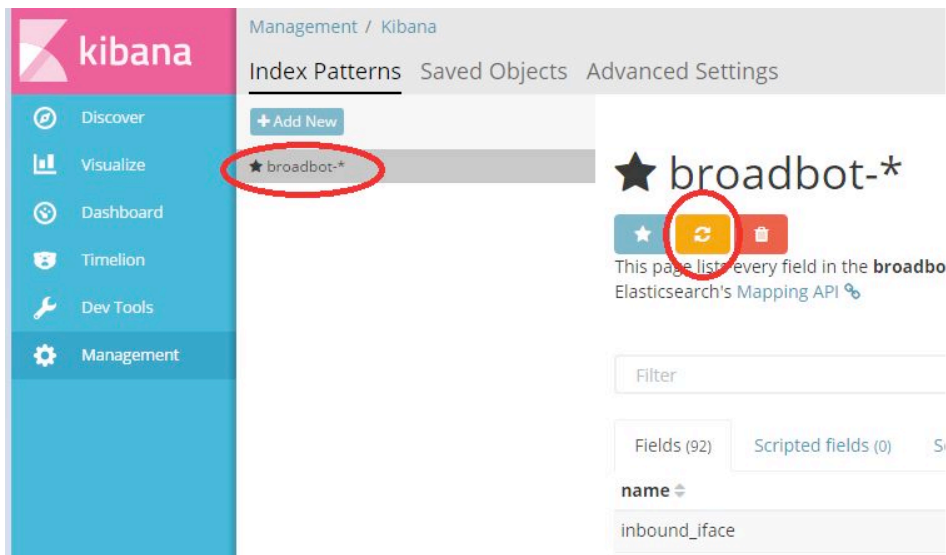


If you see that there are indeed log messages, then we may need to refresh the field lists. Since BroadBot is built on elasticsearch, a predefined set of fields is needed for it to work. When new data flows in, elasticsearch needs to be made aware that these fields are now available.

Navigate to the 'Management' tab and click on 'Index Patterns'



Select the 'BroadBot-*' index pattern and click on the 'refresh feilds' button as show below:



Head back to your Dashboard and hit the search button on the top right. Your dashboard should now be populated.