

```
root@centos-tomcat:/home/vagrant 185x51
[root@centos-tomcat vagrant]# curl http://172.10.48.5:9200/_cat/indices
green open .kibana 1 YS00MwW2S6NvYBFZlFzlaw 1 0 23 1 73.4kb 73.4kb
green open .kibana_task_manager AYYyCj0sR568uaTjuyKTA 1 0 2 0 12.8kb 12.8kb
yellow open logstash-2019.07.08_000001 cqIXPcb7TRYkVlhlPiULLw 1 1 192 0 72.5kb 72.5kb
[root@centos-tomcat vagrant]#
```

Picture 1



```

root@centos-tomcat:/home/vagrant 185x1
Jul 08 19:28:50 centos-tomcat logstash[30453]: [2019-07-08T19:28:50.218] [INFO] [logstash.inputs.file] No sinedcb path set, generating one based on the "path" setting :{sinedcb path
["var/lib/logstash/plugins/inputs/file", sinedcb 6aed304b8e7cf2d2478d6e37e15a93f", :path="[/opt/apache-tomcat-8.5.42/logs/*.*.log"]}
Jul 08 19:28:50 centos-tomcat logstash[30453]: [2019-07-08T19:28:50.315] [INFO] [logstash.javapipeline] Pipeline started ("pipeline.id"=="main")
Jul 08 19:28:50 centos-tomcat logstash[30453]: [2019-07-08T19:28:50.511] [INFO] [logstash.agent] Pipelines running :{count=1, :running_pipelines=>[main], :non_running_pipeli
n
Jul 08 19:28:50 centos-tomcat logstash[30453]: [2019-07-08T19:28:50.530] [INFO] [filewatch.observtail] START, creating Discoverer, Watch with file and sinedcb collections
Jul 08 19:28:51 centos-tomcat logstash[30453]: [2019-07-08T19:28:51.308] [INFO] [logstash.agent] Successfully started Logstash API endpoint {:port=>9600}
[root@centos-tomcat vagrant]# systemctl status logstash -l
logstash.service - logstash
Loaded: loaded (/etc/systemd/system/logstash.service; vendor preset: disabled)
Active: active (running) since Mon 2019-07-08 19:28:23 UTC; 31s ago
Main PID: 30453 (java)
Group: /system.slice/logstash.service
CGroup: /system.slice/logstash.service
└─30453 /bin/java -Xmx1g -Xms1g -XX:UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75 -XX:+UseCMSInitiatingOccupancyOnly -Djava.awt.headless=true -Dfile.encoding=UTF-
8 -Druby.compat.invokedynamic=true -Drubyjit.threshold=0 -XX:+HeapDumpOnOutOfMemoryError -Djava.security.egd=file:/dev/urandom -c /usr/share/logstash/logstash-core/lib/jars/animal
sniffer-annotations-1.14.jar:/usr/share/logstash/logstash-core/lib/jars/commons-codec-1.11.jar:/usr/share/logstash/logstash-core/lib/jars/commons-compiler-3.0.11.jar:/usr/share/logstash
logstash-core/lib/jars/error_prone_annotations-2.0.18.jar:/usr/share/logstash/logstash-core/lib/jars/google-java-format-1.1.jar:/usr/share/logstash/logstash-core/lib/jars/gradle-licens
e-report-6.0.7-1.jar:/usr/share/logstash/logstash-core/lib/jars/guava-22.0.jar:/usr/share/logstash/logstash-core/lib/jars/j2objc-annotations-1.1.jar:/usr/share/logstash/logstash-core/lib/
jars/jackson-annotations-2.9.8.jar:/usr/share/logstash/logstash-core/lib/jars/jackson-core-2.9.8.jar:/usr/share/logstash/logstash-core/lib/jars/jackson-databind-2.9.8.jar:/usr/share/log
stash/logstash-core/lib/jars/jackson-dataformat-cbor-2.9.8.jar:/usr/share/logstash/logstash-core/lib/jars/janino-3.0.11.jar:/usr/share/logstash/logstash-core/lib/jars/javassist-3.24.0-G
A.jar:/usr/share/logstash/logstash-core/lib/jars/jruby-complete-9.2.7.6.jar:/usr/share/logstash/logstash-core/lib/jars/jsr305-1.3.9.jar:/usr/share/logstash/logstash-core/lib/jars/log4j-
1.7.0.jar:/usr/share/logstash/logstash-core/lib/jars/log4j-core-2.11.1.jar:/usr/share/logstash/logstash-core/lib/jars/log4j-slf4j-impl-2.11.1.jar:/usr/share/logstash/logstash-core/lib/
jars/logstash-core.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.core.commands-3.6.0.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.core.contenttype-3.4.100
.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.core.expressions-3.4.300.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.core.filesystem-1.3.100.jar:/usr/share/log
stash/logstash-core/lib/jars/org.eclipse.core.jobs-3.5.100.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.core.resources-3.7.100.jar:/usr/share/logstash/logstash-core/lib/j/
rs/org.eclipse.core.runtime-3.7.0.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.equinox.app-1.3.100.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.equinox.com
on-3.6.0.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.equinox.preferences-3.4.1.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.equinox.registry-3.5.101.jar:/us
r/share/logstash/logstash-core/lib/jars/org.eclipse.jdt.core-3.10.0.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.osgi-3.7.1.jar:/usr/share/logstash/logstash-core/lib/jars/or
g.eclipse.text-3.5.101.jar:/usr/share/logstash/logstash-core/lib/jars/slf4j-api-1.7.25.jar:/usr.logstash.logstash-core-elasticsearch-output-plugin-settings /etc/logstash
Jul 08 19:28:49 centos-tomcat logstash[30453]: [2019-07-08T19:28:49.436] [INFO] [logstash.outputs.elasticsearch] New Elasticsearch output :{class=>"LogStash::Outputs::ElasticSearch", :ho
sts=>["//172.10.48.5:9200"]}
Jul 08 19:28:49 centos-tomcat logstash[30453]: [2019-07-08T19:28:49.520] [WARN] [org.logstash.instrument.metrics.gauge.LazyDelegatingGauge] A gauge metric of an unknown type (org.jruby.R
ubyArray) has been create for key: cluster_uids. This may result in invalid serialization. It is recommended to log an issue to the responsible developer/development team.
Jul 08 19:28:49 centos-tomcat logstash[30453]: [2019-07-08T19:28:49.522] [INFO] [logstash.javapipeline] Starting pipeline :{pipeline_id=="main", "pipeline.workers">=2, "pipeline.batc
h.size">=125, "pipeline.batch.delay">=50, "pipeline.max_inflight">=250, :thread=>#<Thread:0x43ecd47d run>}
Jul 08 19:28:49 centos-tomcat logstash[30453]: [2019-07-08T19:28:49.611] [INFO] [logstash.outputs.elasticsearch] Using default mapping template
Jul 08 19:28:49 centos-tomcat logstash[30453]: [2019-07-08T19:28:49.751] [INFO] [logstash.outputs.elasticsearch] Attempting to install template :{manage_templates=>["index_patterns">="log
stash-*", "index.refresh_interval">=1, "number_of_shards">=1, "index.lifecycle.name">="logstash-policy", "index.lifecycle.rollout_alias">="logstash-
", "mappings">{"dynamic_templates">[{"message_field">{"path_match">="message", "match_mapping_type">="string", "mapping">{"type">="text", "norms">false}], "string_fields">{"match
">="*", "match_mapping_type">="string", "mapping">{"type">="text", "norms">false, "fields">{"keyword">{"type">="keyword", "ignore_above">=256}}}], "properties">{"@timestamp">{"ty
pe">="date", "version">{"type">="keyword", "geoip">{"dynamic">true, "properties">{"ip">{"type">="ip", "location">{"type">="geo_point", "latitude">{"type">="half_float", "lo
ngitude">{"type">="half_float"}}}}}}}}}}
Jul 08 19:28:50 centos-tomcat logstash[30453]: [2019-07-08T19:28:50.218] [INFO] [logstash.inputs.file] No sinedcb path set, generating one based on the "path" setting :{sinedcb path
["var/lib/logstash/plugins/inputs/file", sinedcb 6aed304b8e7cf2d2478d6e37e15a93f", :path="[/opt/apache-tomcat-8.5.42/logs/*.*.log"]}
Jul 08 19:28:50 centos-tomcat logstash[30453]: [2019-07-08T19:28:50.315] [INFO] [logstash.javapipeline] Pipeline started ("pipeline.id"=="main")
Jul 08 19:28:50 centos-tomcat logstash[30453]: [2019-07-08T19:28:50.511] [INFO] [logstash.agent] Pipelines running :{count=1, :running_pipelines=>[main], :non_running_pipeli
ness[1]}
Jul 08 19:28:50 centos-tomcat logstash[30453]: [2019-07-08T19:28:50.530] [INFO] [filewatch.observtail] START, creating Discoverer, Watch with file and sinedcb collections
Jul 08 19:28:51 centos-tomcat logstash[30453]: [2019-07-08T19:28:51.308] [INFO] [logstash.agent] Successfully started Logstash API endpoint {:port=>9600}
[root@centos-tomcat vagrant]#

```

Picture 2

← → 🔒 Not secure | 172.10.48.3:8080/manager/html/upload?org.apache.catalina.filters.CSRF\_NONCE=D87251D75422B867E6D2737E2CC06058



### Tomcat Web Application Manager

Message: OK

**Manager**  
List ApplicationsHTML Manager HelpManager HelpServer Status

**Applications**

Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	None specified	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/sample	None specified	Hello, World Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes



**Deploy**  
Deploy directory or WAR file located on server

Context Path (required):  
XML Configuration file URL:  
WAR or Directory URL:  
Deploy

**WAR file to deploy**

Picture 3

← → 🔒 Not secure | 172.10.48.5:5601/app/kibana#/management/kibana/index\_patterns/afa00350-a1b6-11e9-a02c-b1ba64f9bc3f?\_g=()&\_a=(tab:indexedFields)



Management / Index patterns / logstash-2019.07.08-000001

**Elasticsearch**  
Index Management  
Index Lifecycle Policies  
Rollup Jobs  
Cross-Cluster Replication  
Remote Clusters  
Snapshot Repositories  
License Management  
8.0 Upgrade Assistant

**Kibana**  
Index Patterns  
Saved Objects  
Spaces  
Reporting  
Advanced Settings

### logstash-2019.07.08-000001

Time Filter field name: @timestamp

This page lists every field in the **logstash-2019.07.08-000001** index and the field's associated core type as recorded by Elasticsearch. To change a field type, use the Elasticsearch [Mapping API](#).

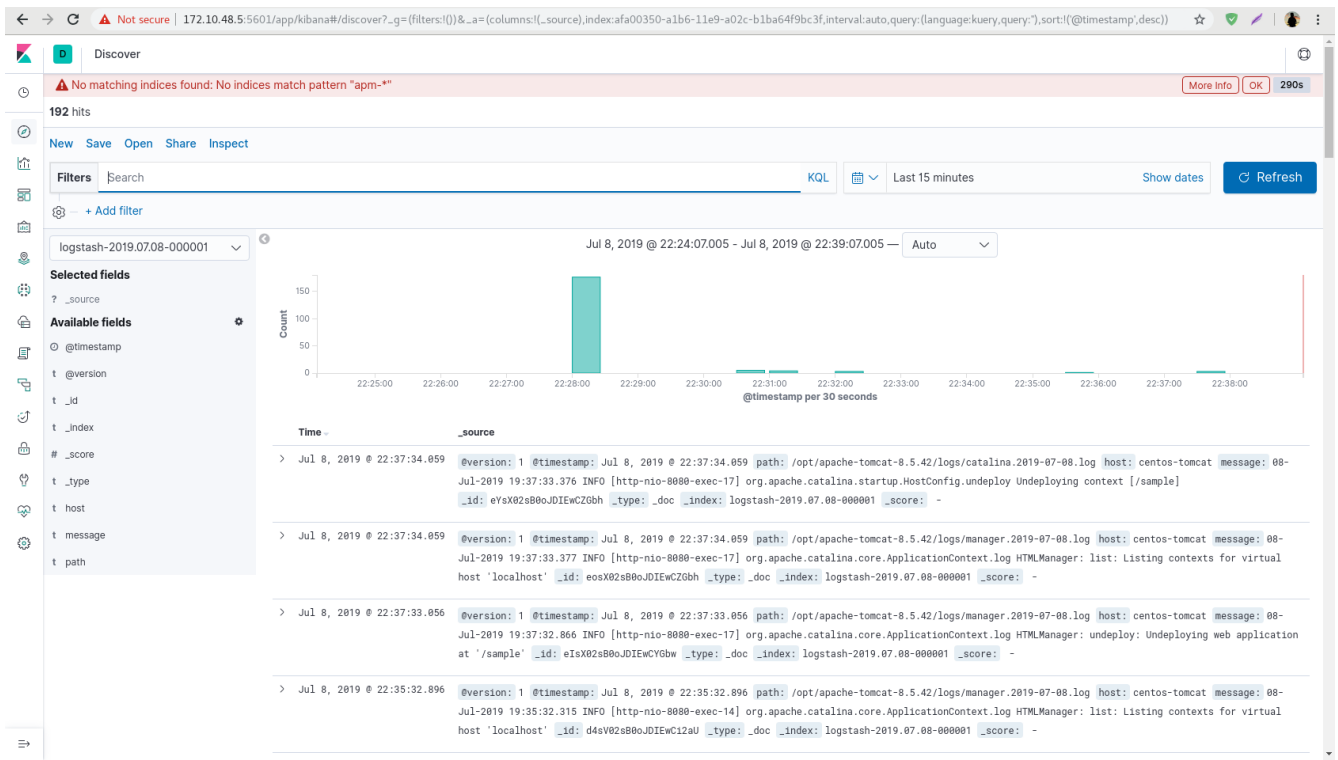
Fields (16)Scripted fields (0)Source filters (0)

FilterAll field types

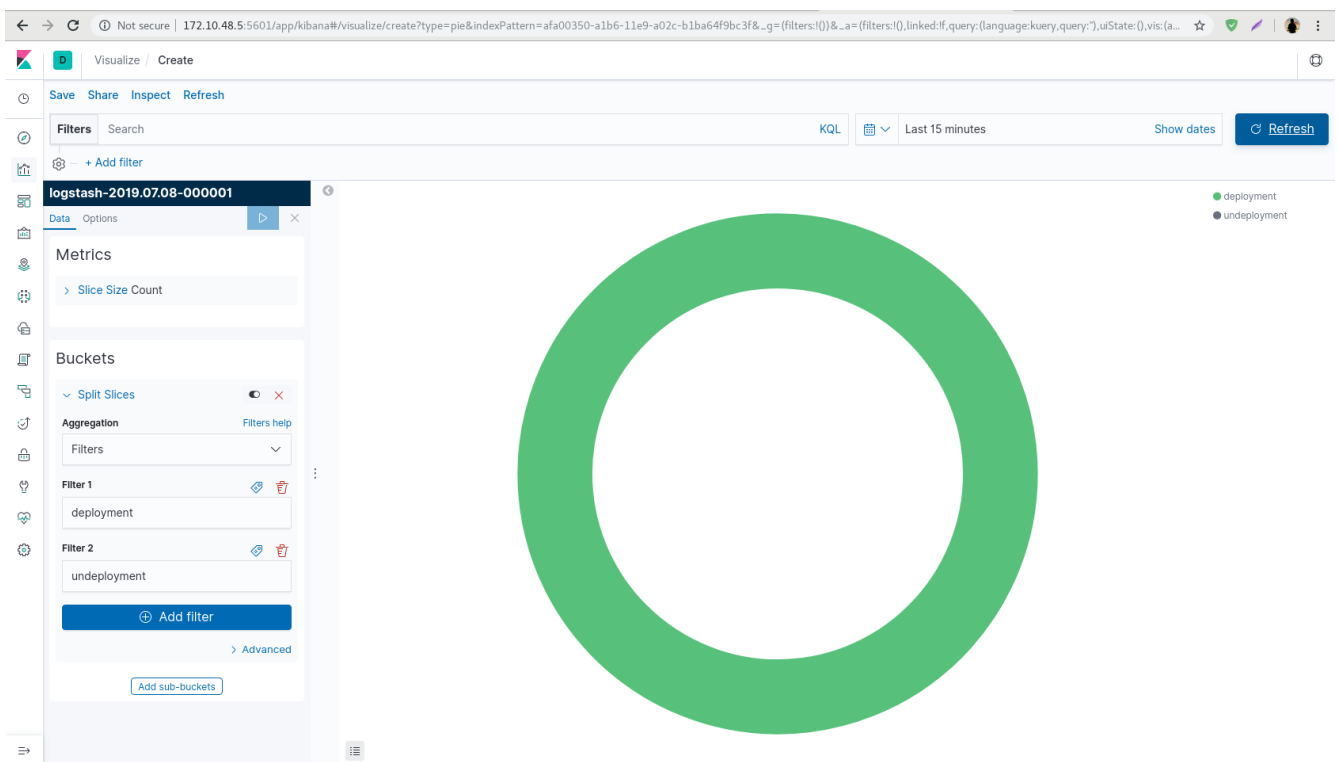
Name	Type	Format	Searchable	Aggregatable	Excluded
@timestamp	date		•	•	✎
@version	string		•	•	✎
_id	string		•	•	✎
_index	string		•	•	✎
_score	number				✎
_source	_source				✎
_type	string		•	•	✎
geoip.ip	ip		•	•	✎
geoip.latitude	number		•	•	✎
geoip.location	geo_point		•	•	✎

Rows per page: 10 < 1 2 >

Picture 4



Picture 5



Picture 6