OP5-Log-Analytics-2.x Documentation

Release latest

Oct 02, 2018

Contents

CHAPTER 1

About

OP5 Log Analytics User Guide

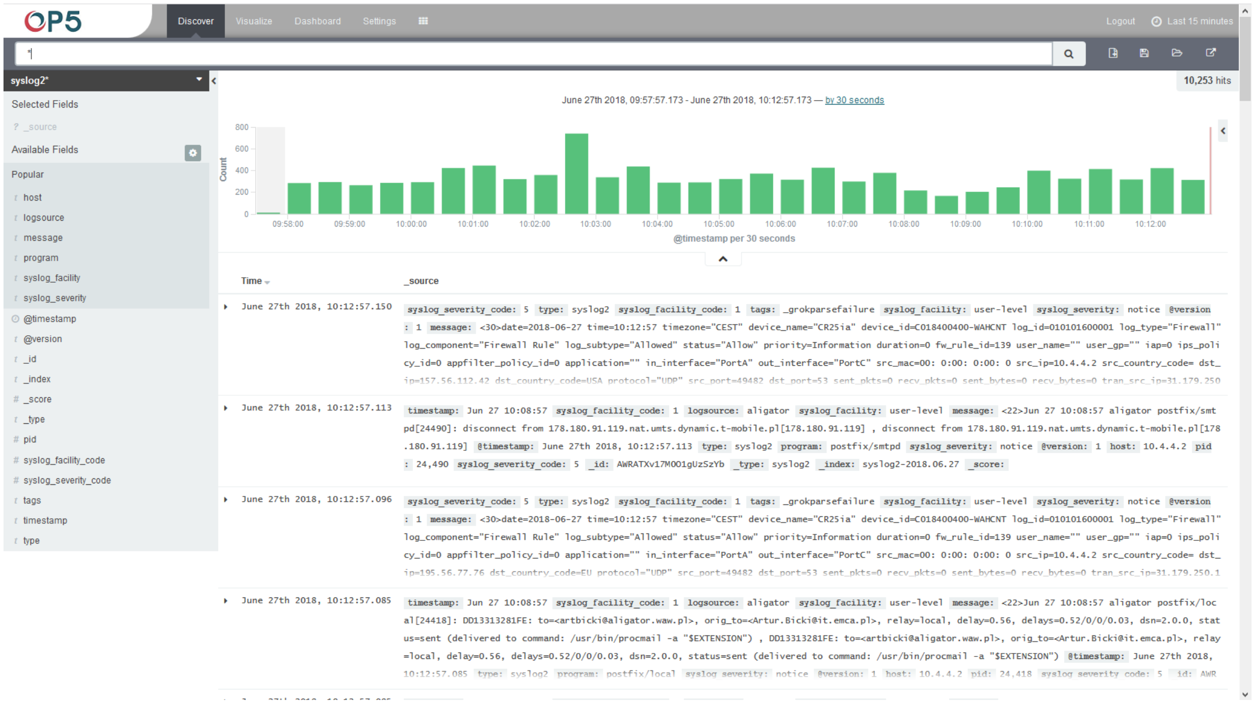
Software ver. 2.x

Document version. 0.8

CHAPTER 2

Introduction

OP5 Log Analytics is innovation solution allowing for centralize IT systems events. It allows for an immediately review, analyze and reporting of system logs - the amount of data does not matter. OP5 Log Analytics is a response to the huge demand for storage and analysis of the large amounts of data from IT systems. OP5 Log Analytics is innovation solution that responds to the need of effectively processing large amounts of data coming from IT environments of today's organizations. Based on the open-source project Elasticsearch valued on the marked, we have created an efficient solution with powerful data storage and searching capabilities. The System has been enriched of functionality that ensures the security of stored information, verification of users, data correlation and visualization, alerting and reporting.



```
June 27th 2018, 10:12:57.150  syslog_severity_code: 5 type: syslog2 syslog_facility_code: 1 tags: _grokparsefailure syslog_facility: user-level syslog_severity: notice @version : 1 message: <30>date=2018-06-27 time=10:12:57 timezone="CEST" device_name="CR25ia" device_id=C018400400-WAHCNT log_id=010101600001 log_type="Firewall" log_component="Firewall Rule" log_subtype="Allowed" status="Allow" priority=Information duration=0 fw_rule_id=139 user_name="" user_gp="" iap=0 ips_policy_id=0 appfilter_policy_id=0 application="" in_interface="PortA" out_interface="PortC" src_mac=00: 0:00: 0:00: 0 src_ip=10.4.4.2 src_country_code= dst_ip=157.56.112.42 dst_country_code=USA protocol="UDP" src_port=49482 dst_port=53 sent_pkts=0 recv_pkts=0 sent_bytes=0 recv_bytes=0 tran_src_ip=31.179.250

June 27th 2018, 10:12:57.113  timestamp: Jun 27 10:08:57 syslog_facility_code: 1 logsource: aligator syslog_facility: user-level message: <22>Jun 27 10:08:57 aligator postfix/smtpd[24490]: disconnect from 178.180.91.119.nat.umts.dynamic.t-mobile.pl[178.180.91.119] , disconnect from 178.180.91.119.nat.umts.dynamic.t-mobile.pl[178.180.91.119] @timestamp: June 27th 2018, 10:12:57.113 type: syslog2 program: postfix/smtpd syslog_severity: notice @version: 1 host: 10.4.4.2 pid : 24,490 syslog_severity_code: 5 _id: AWRATXv17MOO1gUzSzYb _type: syslog2 _index: syslog2-2018.06.27 _score:

June 27th 2018, 10:12:57.096  syslog_severity_code: 5 type: syslog2 syslog_facility_code: 1 tags: _grokparsefailure syslog_facility: user-level syslog_severity: notice @version : 1 message: <30>date=2018-06-27 time=10:12:57 timezone="CEST" device_name="CR25ia" device_id=C018400400-WAHCNT log_id=010101600001 log_type="Firewall" log_component="Firewall Rule" log_subtype="Allowed" status="Allow" priority=Information duration=0 fw_rule_id=139 user_name="" user_gp="" iap=0 ips_policy_id=0 appfilter_policy_id=0 application="" in_interface="PortA" out_interface="PortC" src_mac=00: 0:00: 0:00: 0 src_ip=10.4.4.2 src_country_code= dst_ip=195.56.77.76 dst_country_code=EU protocol="UDP" src_port=49482 dst_port=53 sent_pkts=0 recv_pkts=0 sent_bytes=0 recv_bytes=0 tran_src_ip=31.179.250.1

June 27th 2018, 10:12:57.085  timestamp: Jun 27 10:08:57 syslog_facility_code: 1 logsource: aligator syslog_facility: user-level message: <22>Jun 27 10:08:57 aligator postfix/local[24418]: DD13313281FE: to=<artbicki@aligator.waw.pl>, orig_to=<Artur.Bicki@it.emca.pl>, relay=local, delay=0.56, delays=0.52/0/0/0.03, dsn=2.0.0, status=sent (delivered to command: /usr/bin/procmail -a "$EXTENSION") , DD13313281FE: to=<artbicki@aligator.waw.pl>, orig_to=<Artur.Bicki@it.emca.pl>, relay=local, delay=0.56, delays=0.52/0/0/0.03, dsn=2.0.0, status=sent (delivered to command: /usr/bin/procmail -a "$EXTENSION") @timestamp: June 27th 2018, 10:12:57.085 type: syslog2 program: postfix/local syslog_severity: notice @version: 1 host: 10.4.4.2 pid: 24,418 syslog_severity_code: 5 _id: AWR
```

OP5 Log Analytics project was created to centralize events of all IT areas in the organization. We focused on creating a tool that functionality is most expected by IT departments. Because an effective licensing model has been applied, the solution can be implemented in the scope expected by the customer even with very large volume of data. At the same time, the innovation architecture allows for servicing a large portion of data, which cannot be dedicated to solution with limited scalability.

CHAPTER 3

Elasticsearch

Elasticsearch is a NoSQL database solution that is the heart of our system. Text information send to the system, application and system logs are processed by Logstash filters and directed to Elasticsearch. This storage environment creates, based on the received data, their respective layout in a binary form, called a data index. The Index is kept on Elasticsearch nodes, implementing the appropriate assumptions from the configuration, such as:

- Replication index between nodes,
- Distribution index between nodes.

The Elasticsearch environment consists of nodes:

- Data node - responsible for storing documents in indexes,
- Master node - responsible for the supervisions of nodes,
- Client node - responsible for cooperation with the client.

Data, Master and Client elements are found even in the smallest Elasticsearch installations, therefore often the environment is referred to as a cluster, regardless of the number of nodes configured. Within the cluster, Elasticsearch decides which data portions are held on a specific node.

Index layout, their name, set of fields is arbitrary and depends on the form of system usage. It is common practice to put data of a similar nature to the same type of index that has a permanent first part of the name. The second part of the name often remains the date the index was created, which in practice means that the new index is created every day. This practice, however, is conventional and every index can have its own rotation convention, name convention, construction scheme and its own set of other features. As a result of passing document through the Logstash engine, each entry receive a data field, which allow to work witch data in relations to time.

The Indexes are built with elementary part called shards. It is good practice to create Indexes with the number of shards that is the multiple of the Elasticsearch data nodes number.

CHAPTER 4

Kibana

Kibana lets you visualize your Elasticsearch data and navigate the Elastic Stack. Kibana gives you the freedom to select the way you give shape to your data. And you don't always have to know what you're looking for. Kibana core ships with the classics: histograms, line graphs, pie charts, sunbursts, and more. Plus, you can use Vega grammar to design your own visualizations. All leverage the full aggregation capabilities of Elasticsearch. Perform advanced time series analysis on your Elasticsearch data with our curated time series UIs. Describe queries, transformations, and visualizations with powerful, easy-to-learn expressions.

CHAPTER 5

Logstash

Logstash is an open source data collection engine with real-time pipelining capabilities. Logstash can dynamically unify data from disparate sources and normalize the data into destinations of your choice. Cleanse and democratize all your data for diverse advanced downstream analytics and visualization use cases.

While Logstash originally drove innovation in log collection, its capabilities extend well beyond that use case. Any type of event can be enriched and transformed with a broad array of input, filter, and output plugins, with many native codecs further simplifying the ingestion process. Logstash accelerates your insights by harnessing a greater volume and variety of data.

CHAPTER 6

ELK

"ELK" is the acronym for three open source projects: Elasticsearch, Logstash, and Kibana. Elasticsearch is a search and analytics engine. Logstash is a serverside data processing pipeline that ingests data from multiple sources simultaneously, transforms it, and then sends it to a "stash" like Elasticsearch. Kibana lets users visualize data with charts and graphs in Elasticsearch. The Elastic Stack is the next evolution of the ELK Stack.

CHAPTER 7

Where does the data come from?

OP5 Log Analytics is a solution allowing effective data processing from the IT environment that exists in the organization.

The Elsasticsearch engine allows building a database in witch large amounts of data are stored in ordered indexes. The Logstash module is responsible for load data into Indexes, whose function is to collect data on specific tcp/udp ports, filter them, normalize them and place them in the appropriate index. Additional plugins, that we can use in Logstash reinforce the work of the module, increase its efficiency, enabling the module to quick interpret data and parse it.

Below is an example of several of the many available Logstash plugins:

exec - receive output of the shell function as an event;

imap - read email from IMAP servers;

jdbc - create events based on JDC data;

jms - create events from Jms broker;

Both Elasticsearch and Logstash are free Open-Source solutions.

More information about Elasticsearch module can be find at:https://github.com/elastic/elasticsearch

List of available Logstash plugins:https://github.com/elastic/logstash-docs/tree/master/docs/plugins

CHAPTER 8

System services

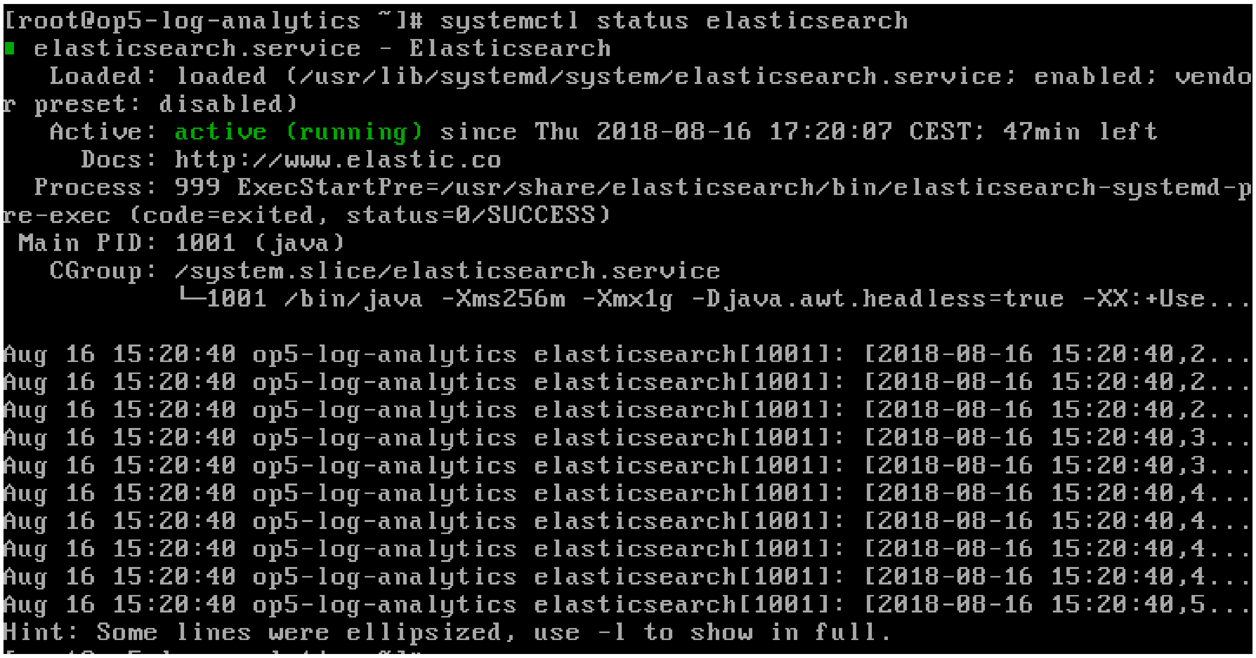
For proper operation OP5 Log Analytics requires starting the following system services:

- elasticsearch.service - we can run it with a command:

  `systemctl start elasticsearch.service`

  we can check its status with a command:

  `systemctl status elasticsearch.service`



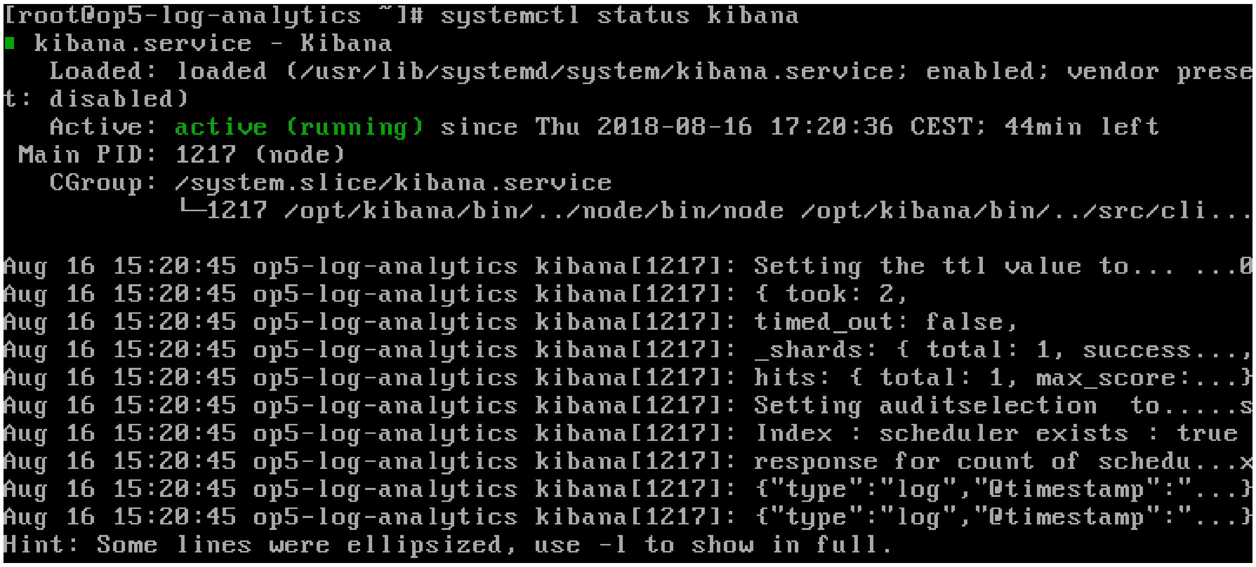
```
[root@op5-log-analytics ~]# systemctl status elasticsearch
■ elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendo
r preset: disabled)
   Active: active (running) since Thu 2018-08-16 17:20:07 CEST; 47min left
     Docs: http://www.elastic.co
  Process: 999 ExecStartPre=/usr/share/elasticsearch/bin/elasticsearch-systemd-p
re-exec (code=exited, status=0/SUCCESS)
 Main PID: 1001 (java)
   CGroup: /system.slice/elasticsearch.service
           └─1001 /bin/java -Xms256m -Xmx1g -Djava.awt.headless=true -XX:+Use...

Aug 16 15:20:40 op5-log-analytics elasticsearch[1001]: [2018-08-16 15:20:40,2...
Aug 16 15:20:40 op5-log-analytics elasticsearch[1001]: [2018-08-16 15:20:40,2...
Aug 16 15:20:40 op5-log-analytics elasticsearch[1001]: [2018-08-16 15:20:40,2...
Aug 16 15:20:40 op5-log-analytics elasticsearch[1001]: [2018-08-16 15:20:40,3...
Aug 16 15:20:40 op5-log-analytics elasticsearch[1001]: [2018-08-16 15:20:40,3...
Aug 16 15:20:40 op5-log-analytics elasticsearch[1001]: [2018-08-16 15:20:40,4...
Aug 16 15:20:40 op5-log-analytics elasticsearch[1001]: [2018-08-16 15:20:40,4...
Aug 16 15:20:40 op5-log-analytics elasticsearch[1001]: [2018-08-16 15:20:40,4...
Aug 16 15:20:40 op5-log-analytics elasticsearch[1001]: [2018-08-16 15:20:40,4...
Aug 16 15:20:40 op5-log-analytics elasticsearch[1001]: [2018-08-16 15:20:40,5...
Hint: Some lines were ellipsized, use -l to show in full.
```

- kibana.service - we can run it with a command:

  `systemctl start kibana.service`

  we can check its status with a command:

```
systemctl status kibana.service
```



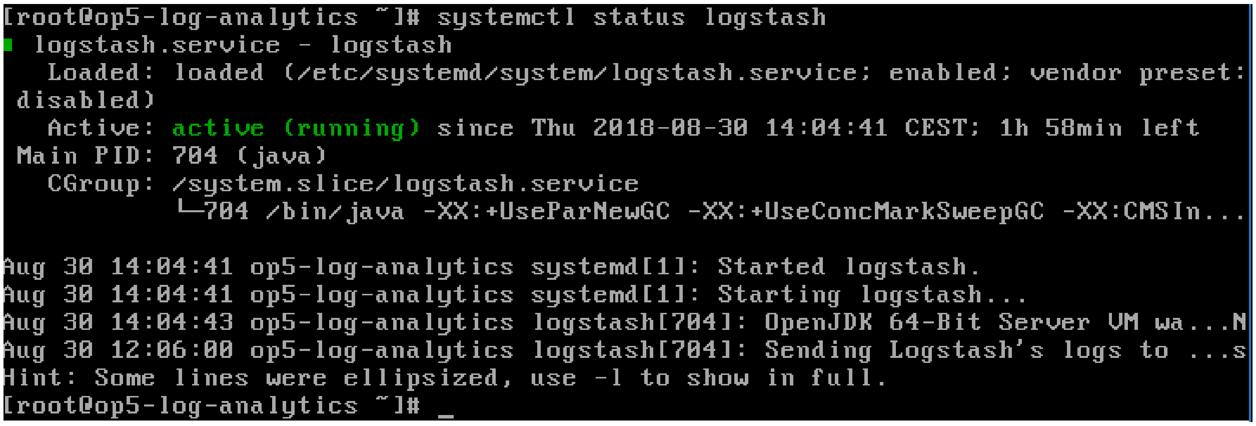
```
[root@op5-log-analytics ~]# systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/usr/lib/systemd/system/kibana.service; enabled; vendor prese
t: disabled)
   Active: active (running) since Thu 2018-08-16 17:20:36 CEST; 44min left
 Main PID: 1217 (node)
   CGroup: /system.slice/kibana.service
           └─1217 /opt/kibana/bin/../node/bin/node /opt/kibana/bin/../src/cli...

Aug 16 15:20:45 op5-log-analytics kibana[1217]: Setting the ttl value to... ...0
Aug 16 15:20:45 op5-log-analytics kibana[1217]: { took: 2,
Aug 16 15:20:45 op5-log-analytics kibana[1217]: timed_out: false,
Aug 16 15:20:45 op5-log-analytics kibana[1217]: _shards: { total: 1, success...,
Aug 16 15:20:45 op5-log-analytics kibana[1217]: hits: { total: 1, max_score:...}
Aug 16 15:20:45 op5-log-analytics kibana[1217]: Setting auditselection  to.....s
Aug 16 15:20:45 op5-log-analytics kibana[1217]: Index : scheduler exists : true
Aug 16 15:20:45 op5-log-analytics kibana[1217]: response for count of schedu...x
Aug 16 15:20:45 op5-log-analytics kibana[1217]: {"type":"log","@timestamp":"...}
Aug 16 15:20:45 op5-log-analytics kibana[1217]: {"type":"log","@timestamp":"...}
Hint: Some lines were ellipsized, use -l to show in full.
```

- logstash.service - we can run it with a command:

  ```
  systemctl start logstash.service
  ```

  we can check its status with a command:

  ```
  systemctl status logstash.service
  ```



```
[root@op5-log-analytics ~]# systemctl status logstash
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset:
 disabled)
   Active: active (running) since Thu 2018-08-30 14:04:41 CEST; 1h 58min left
 Main PID: 704 (java)
   CGroup: /system.slice/logstash.service
           └─704 /bin/java -XX:+UseParNewGC -XX:+UseConcMarkSweepGC -XX:CMSIn...

Aug 30 14:04:41 op5-log-analytics systemd[1]: Started logstash.
Aug 30 14:04:41 op5-log-analytics systemd[1]: Starting logstash...
Aug 30 14:04:43 op5-log-analytics logstash[704]: OpenJDK 64-Bit Server VM wa...N
Aug 30 12:06:00 op5-log-analytics logstash[704]: Sending Logstash's logs to ...s
Hint: Some lines were ellipsized, use -l to show in full.
[root@op5-log-analytics ~]# _
```

CHAPTER 9

First configuration steps

To install and configure OP5 Log Analytics on the CentOS Linux system you should:

- copy archive OP5 Log Analytics tar.bz2 to the hosted server;
- extract archive OP5 Log Analytics tar.bz2 contain application:

```
cd /root/
tar xvfj archive.tar.bz2
```

- go to the application directory and run installation script as a root user:

```
cd /roo/insatll/
./install.sh
```

During instalation you will be ask about following tasks:

- add firewall exeption on ports 22(ssh), 5044, 5514 (Logstash), 5601 (Kibana), 9200 (Elastisearch), 9300 (ES cross-JVM);
- installation of Java environment (Open-JDK), if you use your own Java environment - answer "N";
- connect to the OP5 CentOS repository, which provides Python libraries, and some fonts;
- installation of Logstash application;
- configuration of Logstash with custom OP5 Log Analytics configuration;
- installation of mail components for OP5 Log Analytics notification;
- installation of Kibana, the OP5 Log Analytics GUI;
- installation of data-node of Elasticsearch;
- configuration of Elasticsearch as Data Node;
- configuration of Elasticsearch as Master Node.

Optionally you can:

- install and configure the filebeat agent;

- install and configure the winlogbeat agent;
- configure op5 perf_data to integrated with the OP5 Monitor;
- configure naemonLogs to integrated with the Naemon;
- configure integration with Active Directory and SSO servers. You can find necessary information in 12-00-00-Integration_with_AD and 13-00-00-Windows-SSO;
- install and conigure monitoring with Marver:

```
    cd /usr/share/elasticsearch
    sudo bin/plugin install license
    sudo bin/plugin install marvel-agent
    systemctl restart elasticsearch
```

- enable predictive functionality in Intelligence module:

```
curl -XPOST 'http://localhost:9200/_aliases' -d '{
        "actions" : [
        { "add" : { "index" : "intelligence", "alias" : "predictive" } },
        { "add" : { "index" : "perfdata-linux", "alias" : "predictive" } }
        ]}'
```

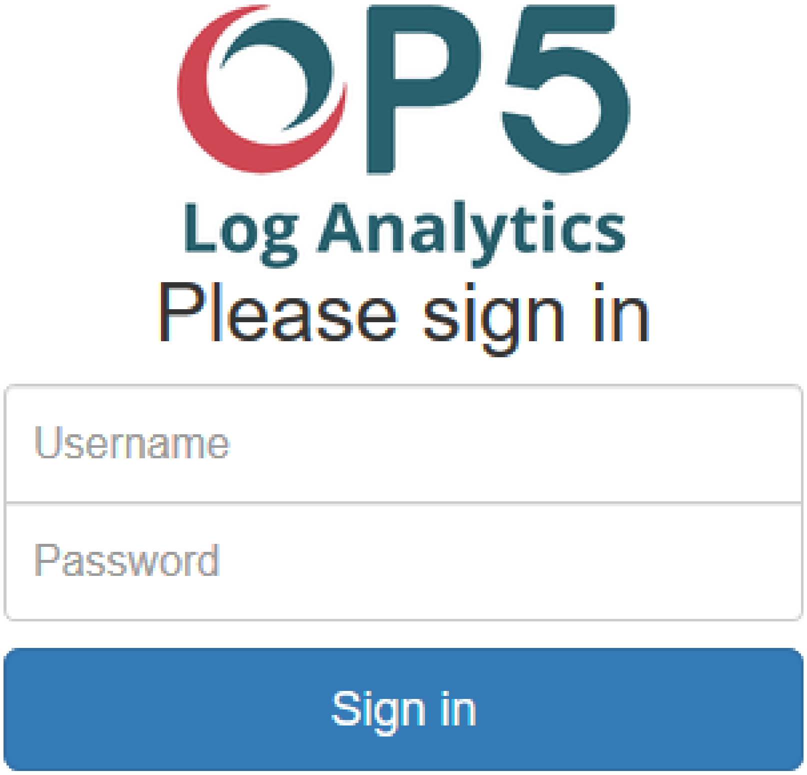
- generate writeback index for Alert service:

```
    /opt/alert/bin/elastalert-create-index --config /opt/alert/config.yaml
```

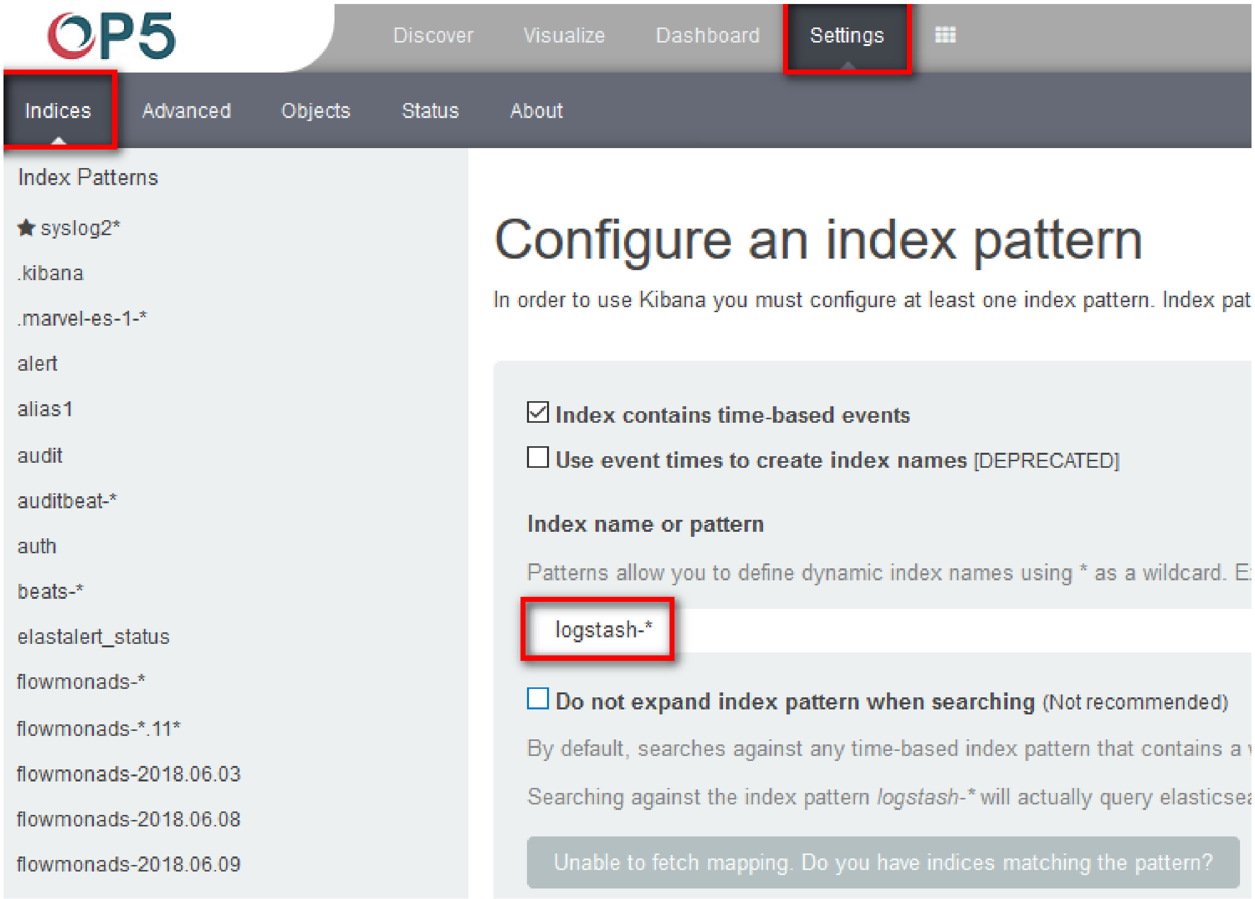
CHAPTER 10

First login

If you log in to OP5 Log Analytics for the first time, you must specify the Index to be searched. We have the option of entering the name of your index, indicate a specific index from a given day, or using the asterix (*) to indicate all of them matching a specific index pattern. Therefore, to start working with OP5 Log Analytics application, we log in to it (by default the user: logserver/password:logserver).



The application at the first login is set by default on the tab: **Settings-\Indices**



Configure an index pattern

In order to use Kibana you must configure at least one index pattern. Index pat

☑ Index contains time-based events

☐ Use event times to create index names [DEPRECATED]

Index name or pattern

Patterns allow you to define dynamic index names using * as a wildcard. E

logstash-*

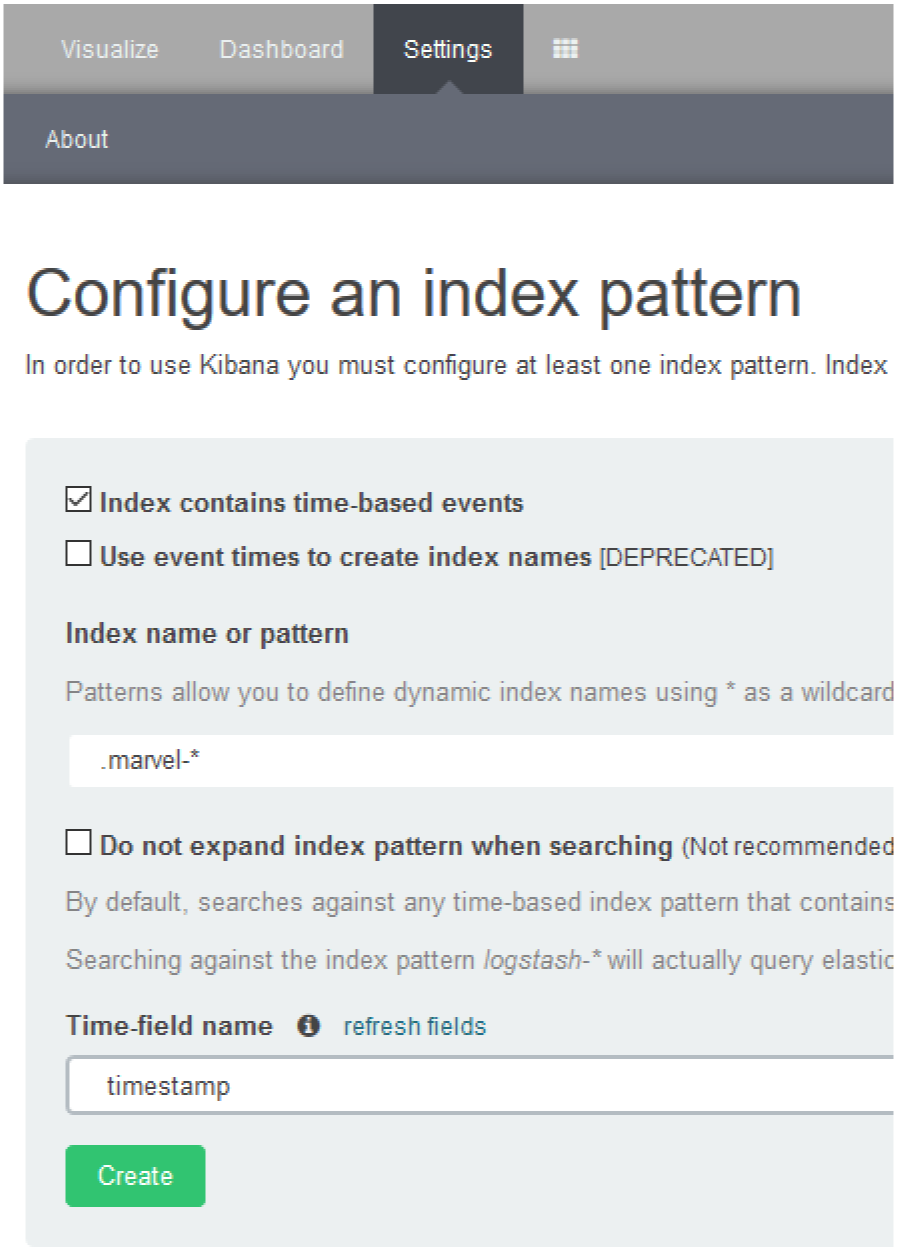
☐ Do not expand index pattern when searching (Not recommended)

By default, searches against any time-based index pattern that contains a v

Searching against the index pattern *logstash-** will actually query elasticsea

In the place where application by default sets name of the Logstash-* pattern, enter the name of the index or index pattern (after confirming that the index or sets of indexes exists).

In additional, the field name should be given, after witch individual event (events) should be sorter. By default the *timestamp* is set, which is the time of occurrence of the event, but depending of the preferences. It may also be the time of the indexing or other selected based on the fields indicate on the event.



Configure an index pattern

In order to use Kibana you must configure at least one index pattern. Index

☑ **Index contains time-based events**

□ **Use event times to create index names** [DEPRECATED]

Index name or pattern

Patterns allow you to define dynamic index names using * as a wildcard

.marvel-*

□ **Do not expand index pattern when searching** (Not recommended

By default, searches against any time-based index pattern that contains

Searching against the index pattern *logstash-** will actually query elastic

Time-field name

timestamp

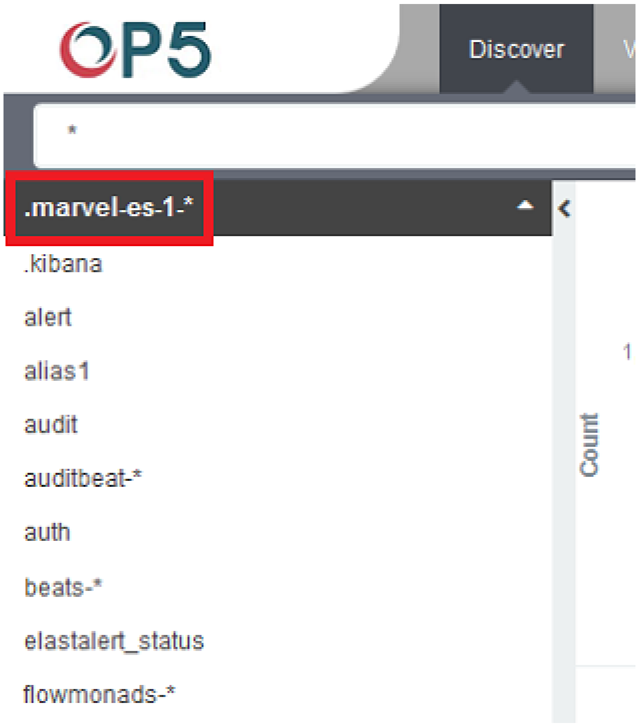
At any time, you can add more indexes or index patters by going to the main tab select „Settings” and next select „Indices”.

CHAPTER 11

Index selection

After login into OP5 Log Analytics you will going to „Discover" tab, where you can interactively explore your data. You have access to every document in every index that matches the selected index patterns.

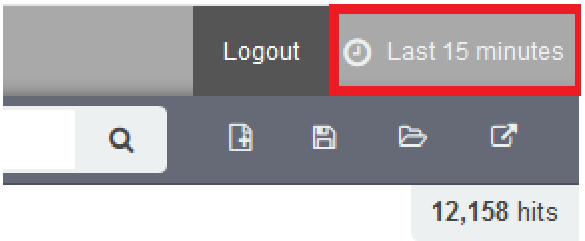
If you want to change selected index, click on the black field with the name of the current object in the left panel. Clicking on the object from the expanded list of previously create index patterns, will change the searched index.



CHAPTER 12

Time settings and refresh

In the upper right corner there is a section in which it defines the range of time that OP5 will search in terms of conditions contained in the search bar. The default value is the last 15 minutes.

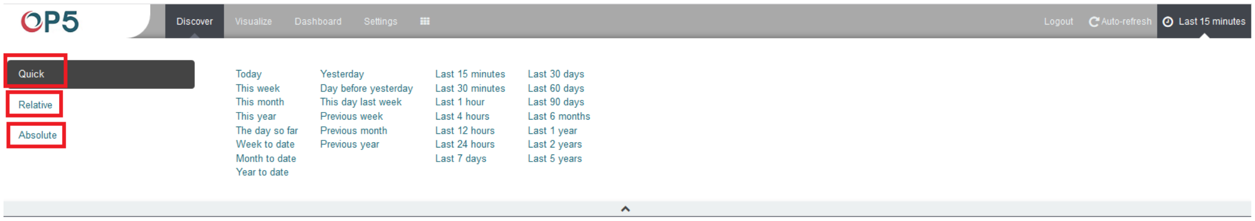


After clicking this selection, we can adjust the scope of search by selecting one of the three tabs in the drop-down window:

Quick: contain several predefined ranges that should be clicked.

Relative: in this windows specify the day from which OP5 Log Analytics should search for data.

Absolute: using two calendars we define the time range for which the search results are to be returned.

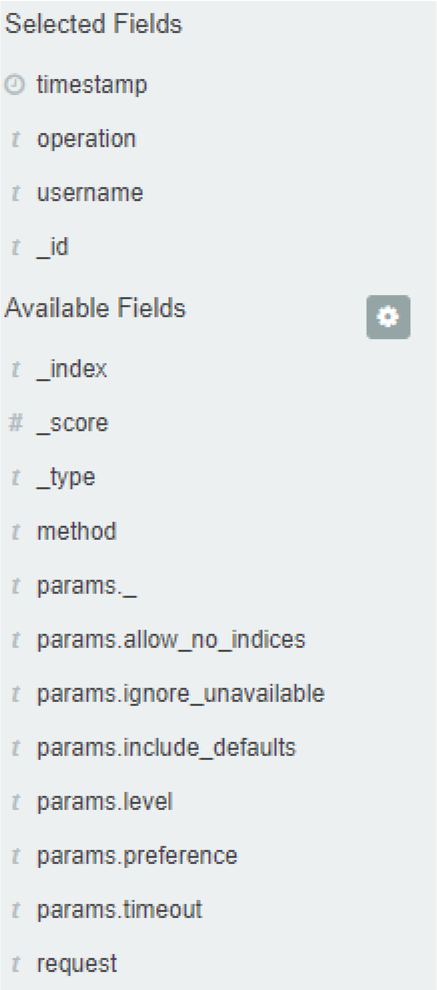


CHAPTER 13

Fields

OP5 Log Analytics in the body of searched events, it recognize fields that can be used to created more precision queries. The extracted fields are visible in the left panel. They are divided on three types: timestamp, marked on clock icon 🕒 timestamp ; text, marked with the letter "t" t params.level and digital, marked witch hashtag # _score .

Pointing to them and clicking on icon add, they are automatically transferred to the „Selected Fields" column and in the place of events a table with selected columns is created on regular basis. In the "Selected Fields" selection you can also delete specific fields from the table by clicking remove on the selected element.



Selected Fields

- ◷ timestamp
- t operation
- t username
- t _id

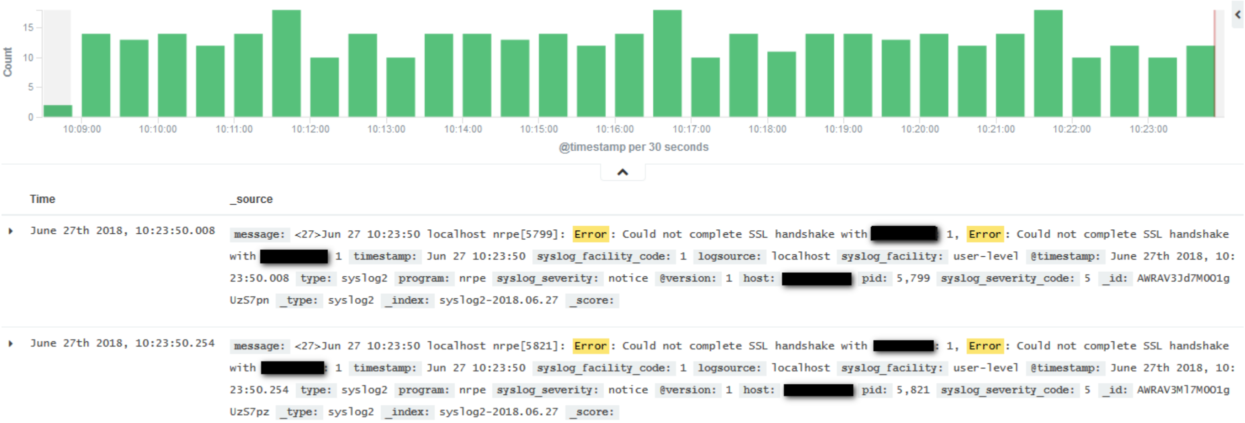
Available Fields ⚙

- t _index
- # _score
- t _type
- t method
- t params._
- t params.allow_no_indices
- t params.ignore_unavailable
- t params.include_defaults
- t params.level
- t params.preference
- t params.timeout
- t request

CHAPTER 14

Filtering and syntax building

We use the query bar to search interesting events. For example, after entering the word „error”, all events that contain the word will be displayed, additional highlighting them with an orange background.



```
June 27th 2018, 10:23:50.008  message: <27>Jun 27 10:23:50 localhost nrpe[5799]: Error: Could not complete SSL handshake with [redacted] 1, Error: Could not complete SSL handshake
                              with [redacted] 1 timestamp: Jun 27 10:23:50 syslog_facility_code: 1 logsource: localhost syslog_facility: user-level @timestamp: June 27th 2018, 10:
                              23:50.008 type: syslog2 program: nrpe syslog_severity: notice @version: 1 host: [redacted] pid: 5,799 syslog_severity_code: 5 _id: AWRAV3Jd7MO01g
                              UzS7pn _type: syslog2 _index: syslog2-2018.06.27 _score:

June 27th 2018, 10:23:50.254  message: <27>Jun 27 10:23:50 localhost nrpe[5821]: Error: Could not complete SSL handshake with [redacted]: 1, Error: Could not complete SSL handshake
                              with [redacted]: 1 timestamp: Jun 27 10:23:50 syslog_facility_code: 1 logsource: localhost syslog_facility: user-level @timestamp: June 27th 2018, 10:
                              23:50.254 type: syslog2 program: nrpe syslog_severity: notice @version: 1 host: [redacted] pid: 5,821 syslog_severity_code: 5 _id: AWRAV3Ml7MO01g
                              UzS7pz _type: syslog2 _index: syslog2-2018.06.27 _score:
```

Fields can be used in the similar way by defining conditions that interesting us. The syntax of such queries is:

`<fields_name:<fields_value>`

Example:

`status:500`

This query will display all events that contain the „status” fields with a value of 500.

The field value does not have to be a single, specific value. For digital fields we can specify range in the following scheme:

`<fields_name:[<range_from TO <range_to]`

Example:

`status:[500 TO 599]`

This query will return events with status fields that are in the range 500 to 599.

The search language used in OP5 allows to you use logical operators „AND", „OR" and „NOT", which are key and necessary to build more complex queries.

- **AND** is used to combined expressions, e.g. „error AND „access denied". If an event contain only one expression or the words error and denied but not the word access, then it will not be displayed.
- **OR** is used to search for the events that contain one OR other expression, e.g. „status:500" OR "denied". This query will display events that contain word „denied" or status field value of 500. OP5 uses this operator by default, so query „status:500" "denied" would return the same results.
- **NOT** is used to exclude the following expression e.g. „status:[500 TO 599] NOT status:505" will display all events that have a status fields, and the value of the field is between 500 and 599 but will eliminate from the result events whose status field value is exactly 505.
- **The above methods** can be combined with each other by building even more complex queries. Understanding how they work and joining it, is the basis for effective searching and full use of OP5 Log Analytics.

Example of query built from connected logical operations:

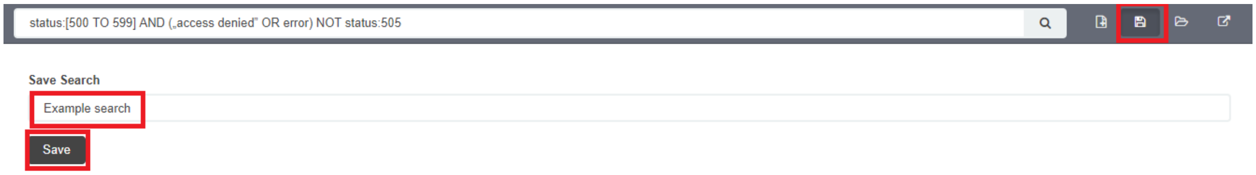
```
status:[500 TO 599] AND („access denied" OR error) NOT status:505
```

Returns in the results all events for which the value of status fields are in the range of 500 to 599, simultaneously contain the word „access denied" or „error", omitting those events for which the status field value is 505.

CHAPTER 15

Saving and deleting queries

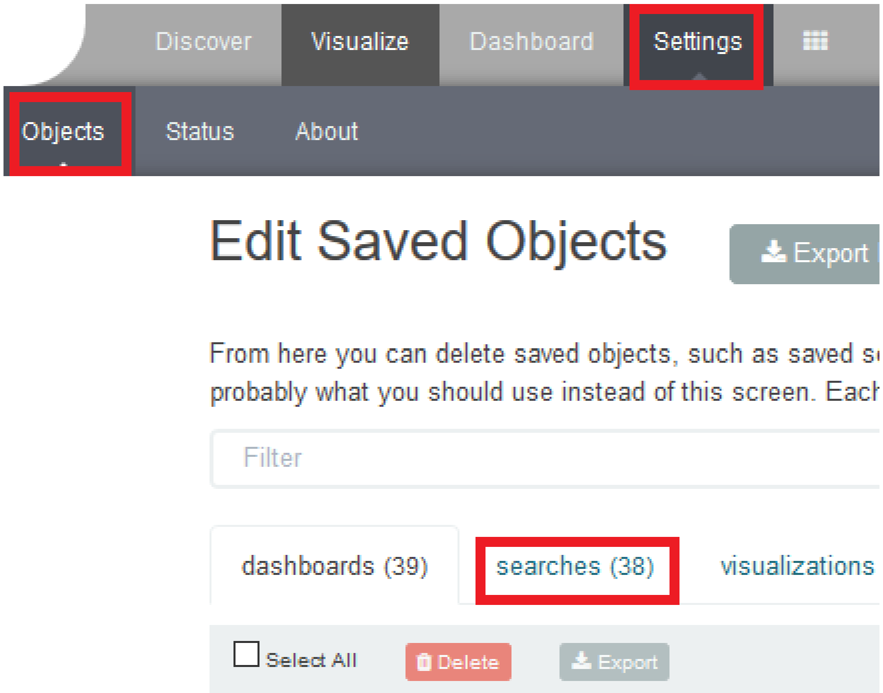
Saving queries enables you to reload and use them in the future. To do this, click on the icon 💾 to the right on the query bar. This will bring up a window in which we give the query a name and then click the button Save.



status:[500 TO 599] AND („access denied" OR error) NOT status:505

Example search

Saved queries can be opened by going to „Settings" from the main menu at the top of the page, then from the submenu select „Object" and finally the „Searches" tab.

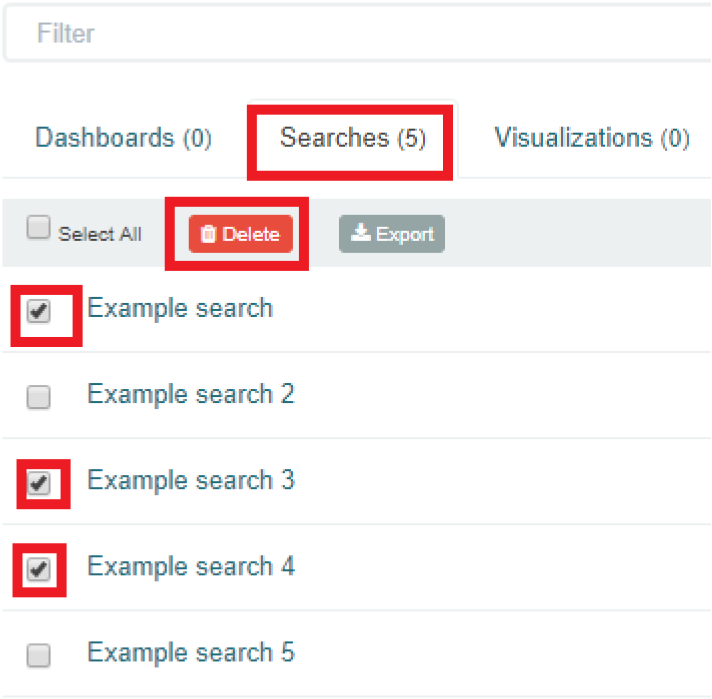


Edit Saved Objects

From here you can delete saved objects, such as saved s
probably what you should use instead of this screen. Each

To open a saved query in the search window, you can click on the icon 👁 to the right of the query you are interested in. After clicking on the icon ✎ or the name of the saved query, we will gain access to the advanced editing mode, so that we can change the query on at a lower level. It is a powerful tool designed for advanced users, designed to modify the query and the way it is presented by OP5 Log Analytics.

To delete a saved query, select it in the list (the icon □ to the left of the query name), and then click Delete. In this way, you can delete many saved queries simultaneously.



☑ Example search

□ Example search 2

☑ Example search 3

☑ Example search 4

□ Example search 5

From this level, you can also export saved queries in the same way. To do this, you need to click on Export and choose the save location. The file will be saved in .JSON format. If you then want to import such a file to OP5 Log Analytics, click on button Import, at the top of the page and select the desired file.

CHAPTER 16

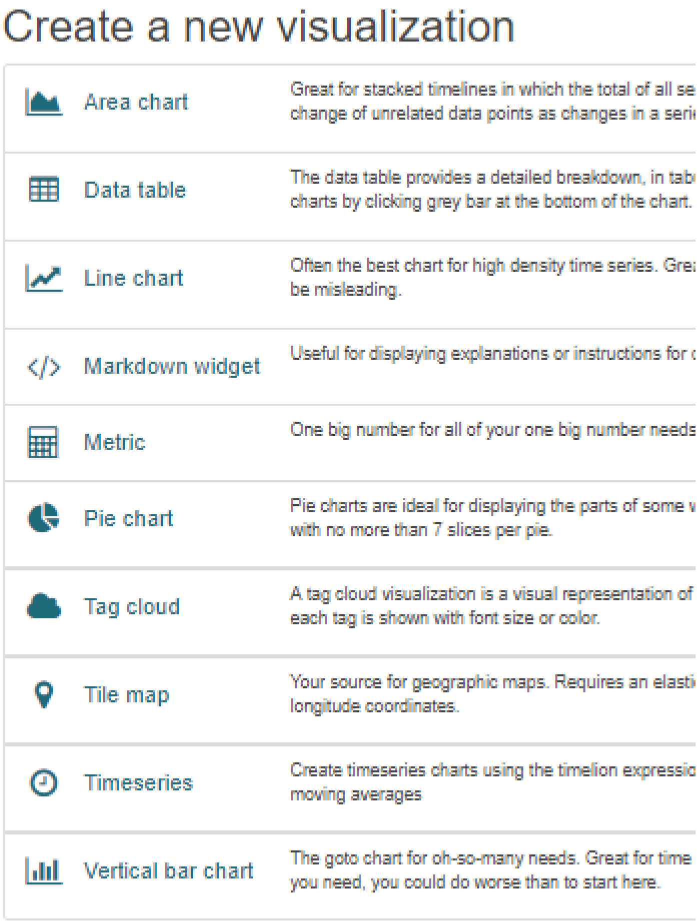
Visualizations

Visualize enables you to create visualizations of the data in your OP5 Log Analytics indices. You can then build dashboards that display related visualizations. Visualizations are based on OP5 Log Analytics queries. By using a series of OP5 Log Analytics aggregations to extract and process your data, you can create charts that show you the trends, spikes, and dips.

CHAPTER 17

Creating visualization

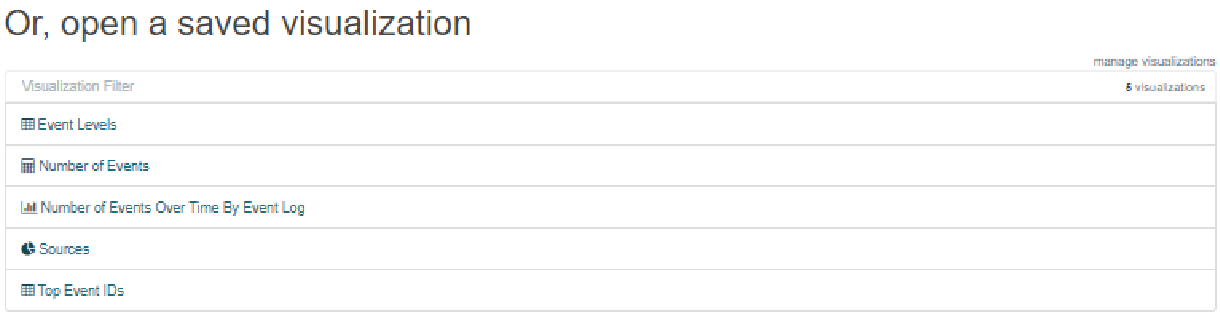
To create visualization, go to the „Visualize" tab from the main menu.



Create a new visualization

Area chart	Great for stacked timelines in which the total of all se change of unrelated data points as changes in a seri
Data table	The data table provides a detailed breakdown, in tab charts by clicking grey bar at the bottom of the chart.
Line chart	Often the best chart for high density time series. Gre be misleading.
Markdown widget	Useful for displaying explanations or instructions for
Metric	One big number for all of your one big number needs
Pie chart	Pie charts are ideal for displaying the parts of some v with no more than 7 slices per pie.
Tag cloud	A tag cloud visualization is a visual representation of each tag is shown with font size or color.
Tile map	Your source for geographic maps. Requires an elasti longitude coordinates.
Timeseries	Create timeseries charts using the timelion expressio moving averages
Vertical bar chart	The goto chart for oh-so-many needs. Great for time you need, you could do worse than to start here.

A new page will be appearing where you can create or load visualization. To load previously created and saved visualization, you must select it from the list.



Or, open a saved visualization

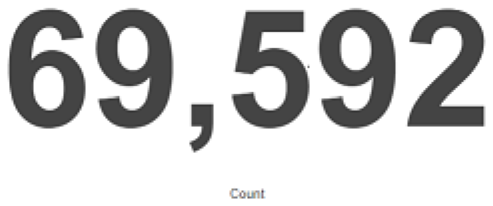
- Event Levels
- Number of Events
- Number of Events Over Time By Event Log
- Sources
- Top Event IDs

In order to create a new visualization, you should choose the preferred method of data presentation. Next, specify whether the created visualization will be based on a new or previously saved query. If on new one, select the index whose visualization should concern. If visualization is created from a saved query, you just need to select the appropriate query from the list, or (if there are many saved searches) search for them by name.

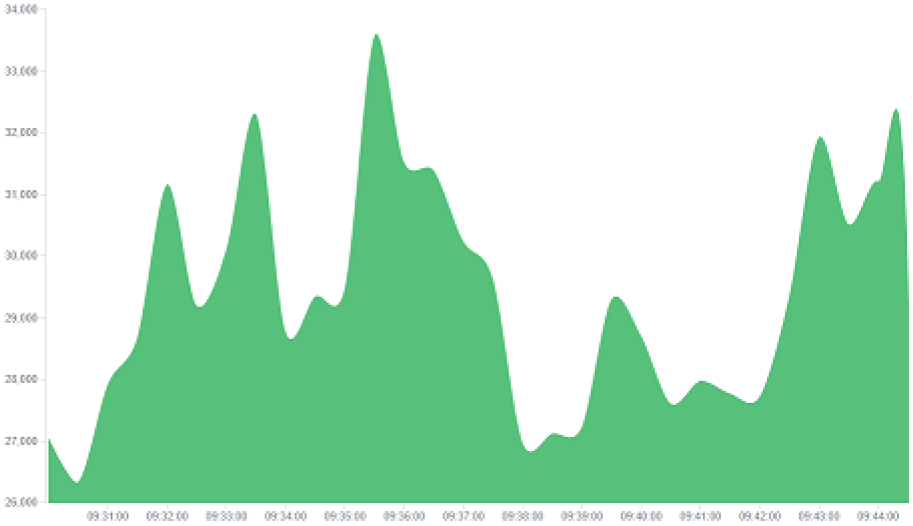
CHAPTER 18

Vizualization types

Before the data visualization will be created, first you have to choose the presentation method from an existing list. Currently there are 7 types of visualization. Each of them serves different purposes. If you want to see only the current number of products sold, it is best to choose „Metric”, which presents one value.



However, if we would like to see user activity trends on pages in different hour and days, a better choice will be „Area chart”, which displays a chart with time division.

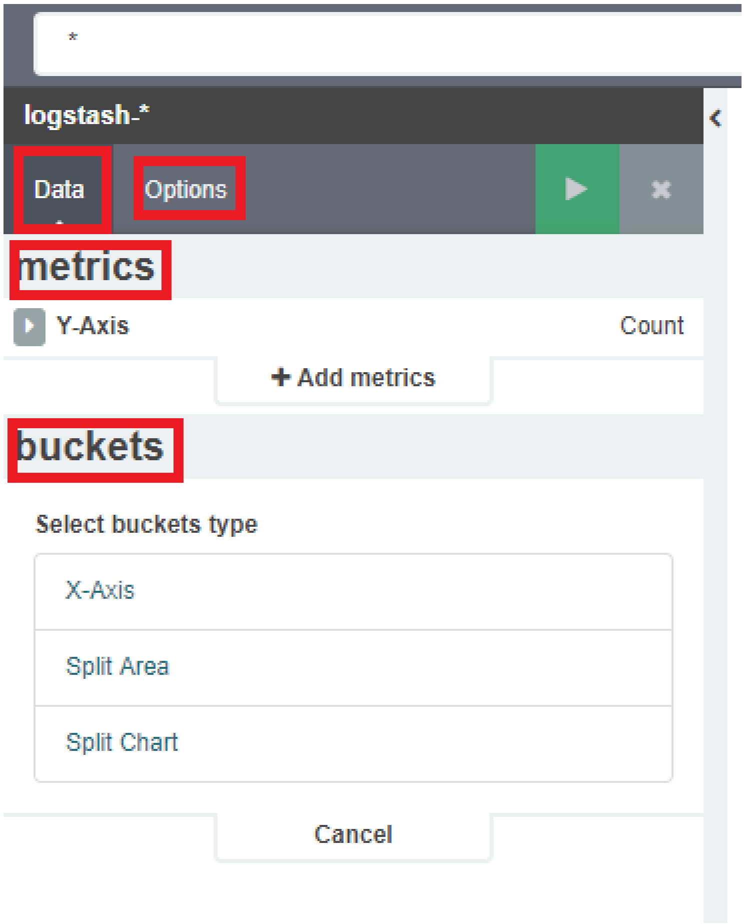


The „Markdown widget” views is used to place text e.g. information about the dashboard, explanations and instruction on how to navigate. Markdown language was used to format the text (the most popular use is GitHub). More information and instruction can be found at this link:https://help.github.com/categories/writing-on-github/

CHAPTER 19

Edit visualization and saving

Editing a saved visualization enables you to directly modify the object definition. You can change the object title, add a description, and modify the JSON that defines the object properties. After selecting the index and the method of data presentation, you can enter the editing mode. This will open a new window with empty visualization.

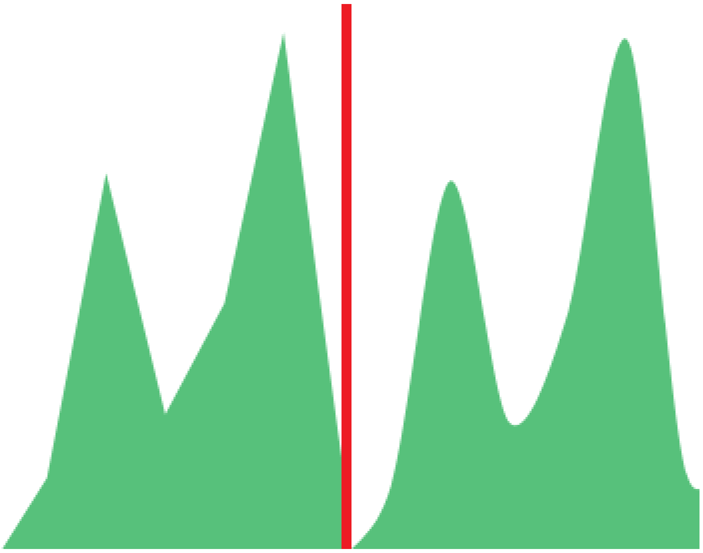


At the very top there is a bar of queries that cat be edited throughout the creation of the visualization. It work in the same way as in the "Discover" tab, which means searching the raw data, but instead of the data being displayed, the visualization will be edited. The following example will be based on the „Area chart". The visualization modification panel on the left is divided into two tabs: „Data" and „Options".

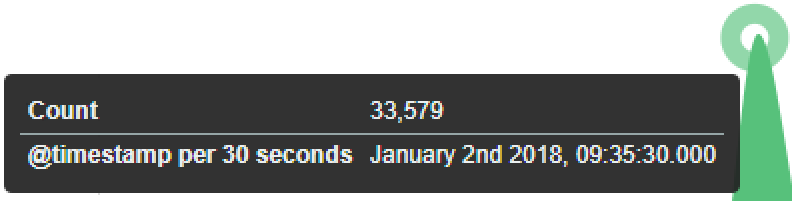
In the „Data" tab, you can modyfiy the elements responsible for which data and how should be presented. In this tab there are two sectors: "metrics", in which we set what data should be displayed, and „buckets" in which we specify how they should be presented. In the „Options" tab, there are settings relating mainly to visual aesthetics. Each type of visualization has separate options. To create the first graph in the char modification panel, in the „Data" tab we add X-Axis in the "buckets" sections. In „Aggregation" choose „Date Histogram", in „Field" should automatically be located "timestamp", and "interval": "Auto" (if not, this is how we set it). Click on the icon on the panel. Now our first graph should show up.

Some of the options for „Area Chart" are:

Smooth Lines - is used to smooth the graph line.



- **Current time marker** – places a vertical line on the graph that determines the current time.
- **Set Y-Axis Extents** – allows you to set minimum and maximum values for the Y axis, which increases the readability of the graphs. This is useful, if we know that the data will never be less then (the minimum value), or to indicate the goals the company (maximum value).
- **Show Tooltip** – option for displaying the information window under the mouse cursor, after pointing to the point on the graph.



Count	33,579
@timestamp per 30 seconds	January 2nd 2018, 09:35:30.000

To save the visualization, click the icon 💾 next to the query bar, give it a name and click the button Save. To load the visualization, go to the „Settings" tab from the main menu at the top of the page, then from the submenu select „Objects" and finally the "Visualizations" tab. From this place, we can also go into advanced editing mode, export and delete visualization.

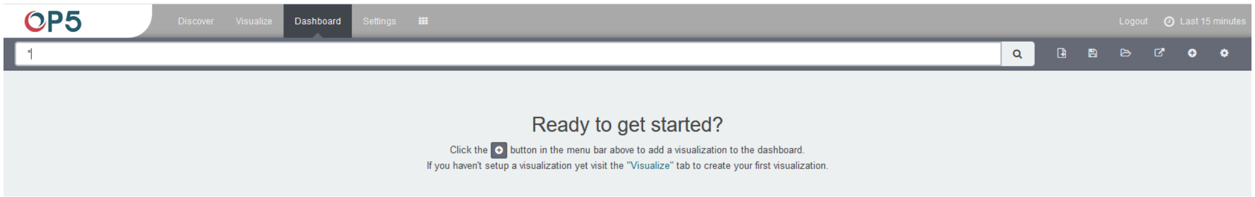
CHAPTER 20

Dashboards

Dashboard is a collection of several visualizations or searches. Depending on how it is build and what visualization it contains, it can be designed for different teams e.g.:

- SOC - which is responsible for detecting failures or threats in the company;
- business - which thanks to the listings can determine the popularity of products and define the strategy of future sales and promotions;
- managers and directors - who may immediately have access to information about the performance units or branches.

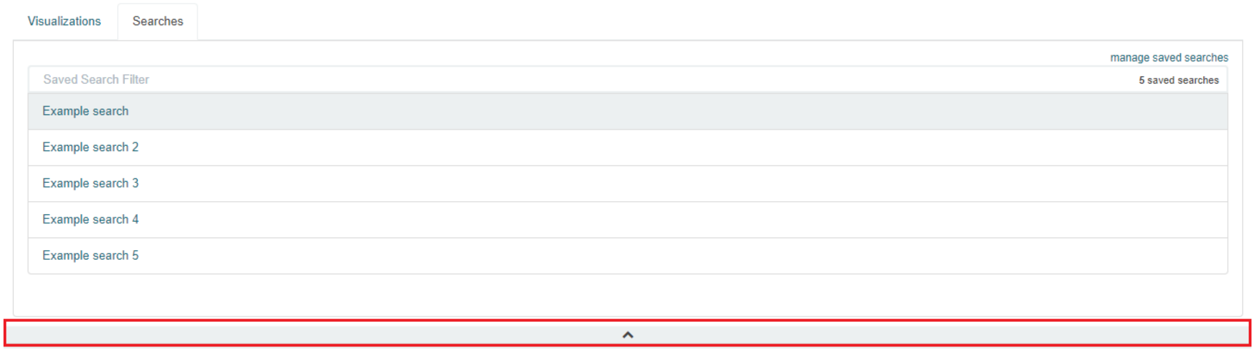
To create a dashboard from previously saved visualization and queries, go to the „Dashboard" tab in the main menu bar. When you open it, a new page will appear.



Ready to get started?

Click the ⊕ button in the menu bar above to add a visualization to the dashboard.
If you haven't setup a visualization yet visit the "Visualize" tab to create your first visualization.

Clicking on the icon ⊕ and selecting a saved query and / or visualization from the list will add them to the dashboard. If, there are a large number of saved objects, use the bar to search for them by name. To collapse the window for adding objects, click on the gray bar with icon ⌃ (the windows can be re-opened by clicking the icon ⊕ to the right of the query bar again).



Elements of the dashboard can be enlarged arbitrarily (by clicking on the right bottom corner of object and dragging the border) and moving (by clicking on the title bar of the object and moving it).

To save a dashboard, click on the icon 💾 to the right of the query bar and give it a name. To load the dashboard go to the "Settings" tab in the main menu at the top of the page, then "Object" from the submenu and finally in the "Dashboard" tab. Here you can also go into advanced editing mode, export and delete dashboard.

CHAPTER 21

Sharing

The dashboard can be share with other OP5 Log Analytics users as well as on any page - by placing a snippet of code. Provided that it cans retrieve information from OP5 Log Analytics.

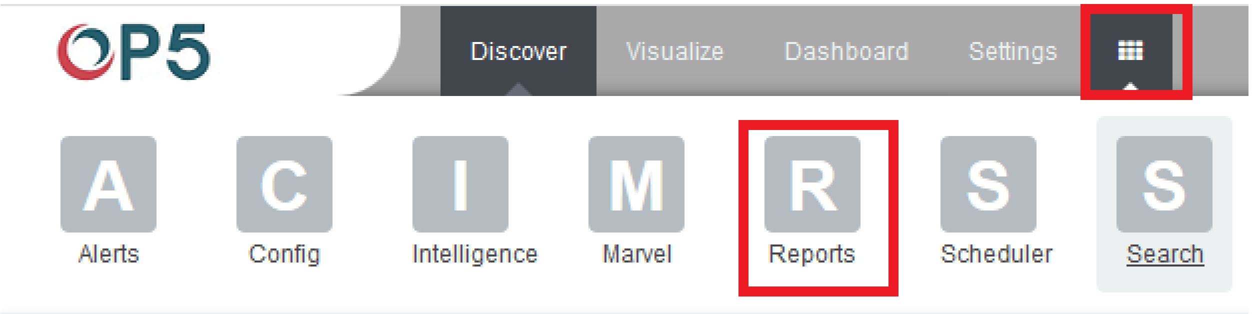
To do this, open the saved dashboard and click on the icon ↗ to the right of the query bar. A window will appear with two gray bars. The content of the first one is used to provide the dashboard in the page code, and the second is a link that can be passed on to another user. There are two icons next to them, the first is to shorten the length of the link, and second on copies to clipboard the contest of the given bar

CHAPTER 22

Reports

OP5 Log Analytics contains a module for creating reports that can be run cyclically and contain only interesting data, e.g. a weekly sales report.

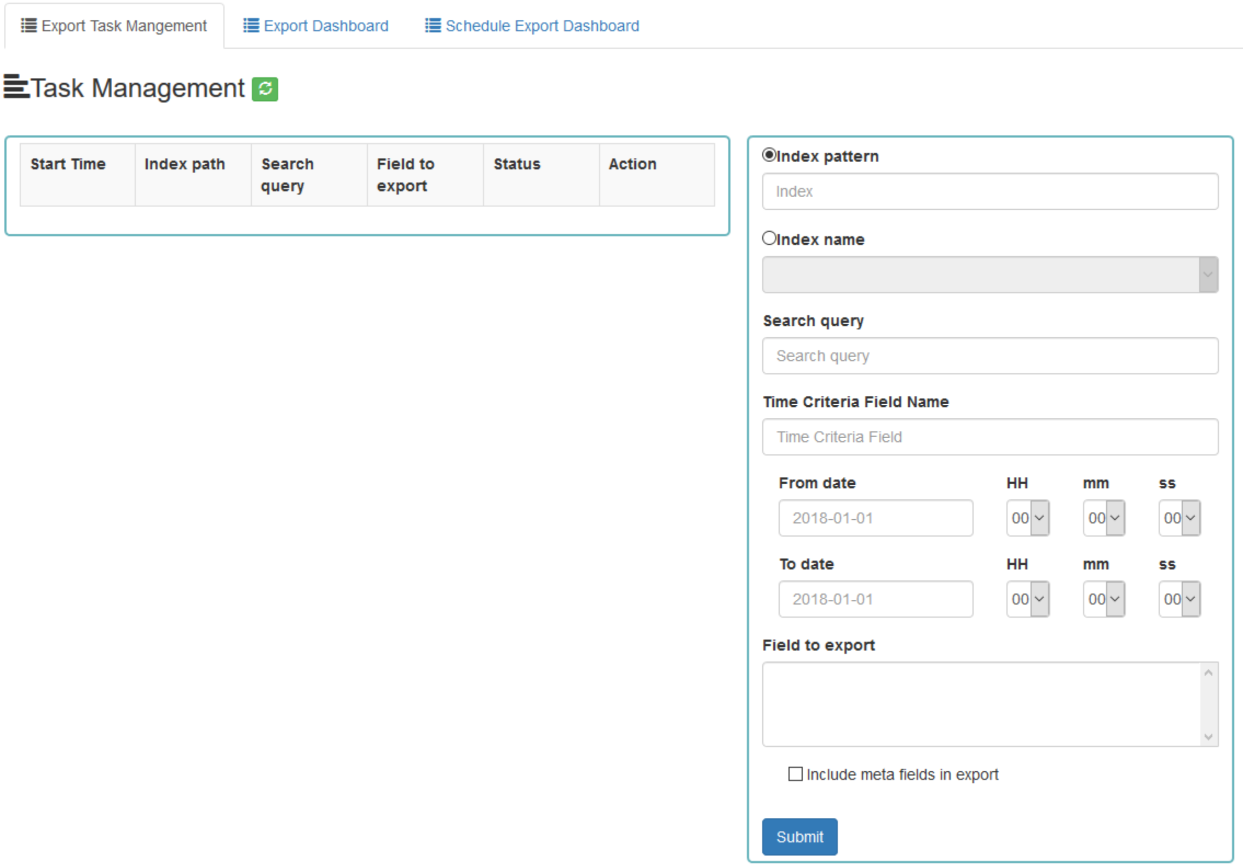
To go to the reports windows, select to tiles icon from the main menu bar, and then go to the „Reports" icon (To go back, go to the „Search" icon).



CHAPTER 23

CSV Report

To export data to CSV Report click the Reports icon, you immediately go to the first tab - Export Task Management.



Export Task Mangement | Export Dashboard | Schedule Export Dashboard

Task Management

Start Time	Index path	Search query	Field to export	Status	Action

● Index pattern

Index

○ Index name

Search query

Search query

Time Criteria Field Name

Time Criteria Field

From date: 2018-01-01 HH 00 mm 00 ss 00

To date: 2018-01-01 HH 00 mm 00 ss 00

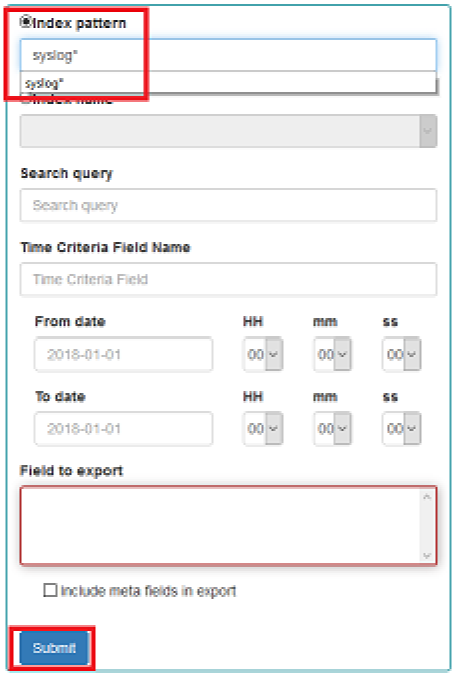
Field to export

□ Include meta fields in export

Submit

In this tab we have the opportunity to specify the source from which we want to do export. It can be an index pattern. After selecting it, we confirm the selection with the Submit button and a report is created at the moment. The symbol

🔄 can refresh the list of reports and see what its status is.



● Index pattern

syslog*

syslog*

○ Index name

Search query

Search query

Time Criteria Field Name

Time Criteria Field

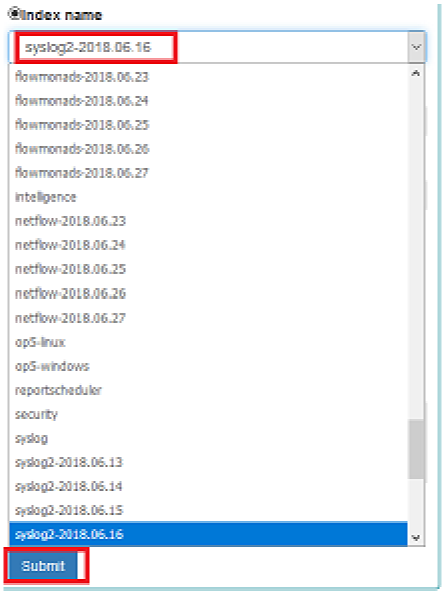
From date	HH	mm	ss
2018-01-01	00	00	00

To date	HH	mm	ss
2018-01-01	00	00	00

Field to export

☐ Include meta fields in export

We can also create a report by pointing to a specific index from the drop-down list of indexes.

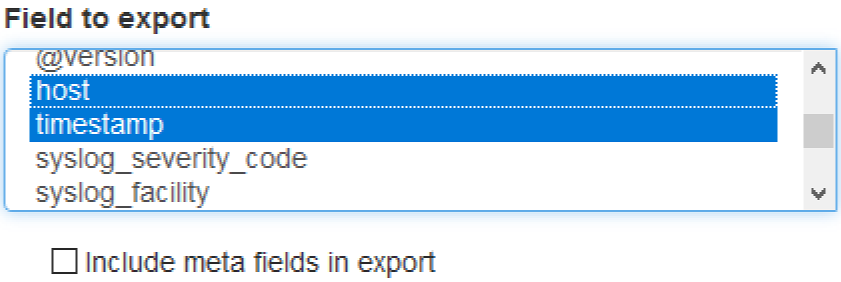


● Index name

syslog2-2018.06.16

flowmonads-2018.06.23
flowmonads-2018.06.24
flowmonads-2018.06.25
flowmonads-2018.06.26
flowmonads-2018.06.27
intelligence
netflow-2018.06.23
netflow-2018.06.24
netflow-2018.06.25
netflow-2018.06.26
netflow-2018.06.27
op5-linux
op5-windows
reportscheduler
security
syslog
syslog2-2018.06.13
syslog2-2018.06.14
syslog2-2018.06.15
syslog2-2018.06.16

We can also check which fields are to be included in the report. The selection is confirmed by the Submit button.

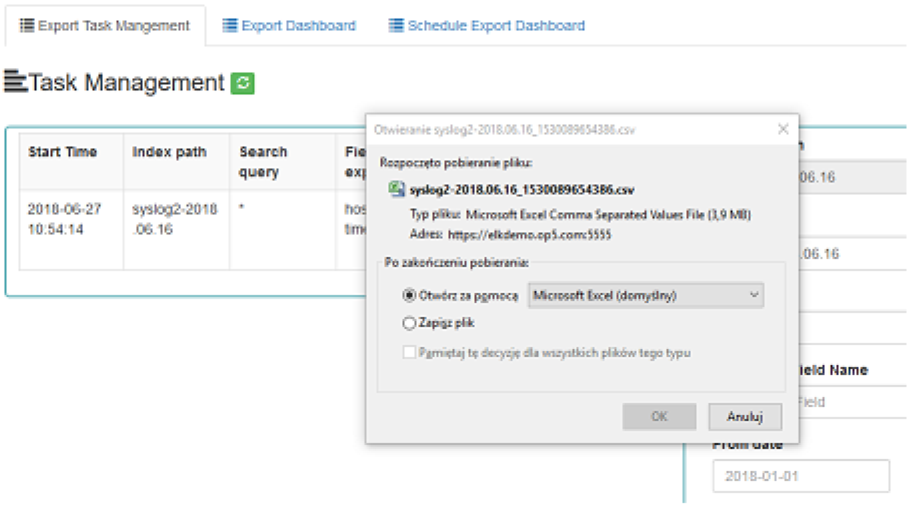


Field to export

- @version
- host
- timestamp
- syslog_severity_code
- syslog_facility

□ Include meta fields in export

When the process of generating the report (Status:Completed) is finished, we can download it (Download button) or delete (Delete button). The downloaded report in the form of *.csv file can be opened in the browser or saved to the disk.



Start Time	Index path	Search query	Fie exp
2018-06-27 10:54:14	syslog2-2018 .06.16	*	hos tim

Otwieranie syslog2-2018.06.16_1530089654386.csv

Rozpoczęto pobieranie pliku:

syslog2-2018.06.16_1530089654386.csv

Typ pliku: Microsoft Excel Comma Separated Values File (3,9 MB)

Adres: https://elkdemo.op5.com:5555

Po zakończeniu pobierania:

● Otwórz za pomocą Microsoft Excel (domyślny)

○ Zapisz plik

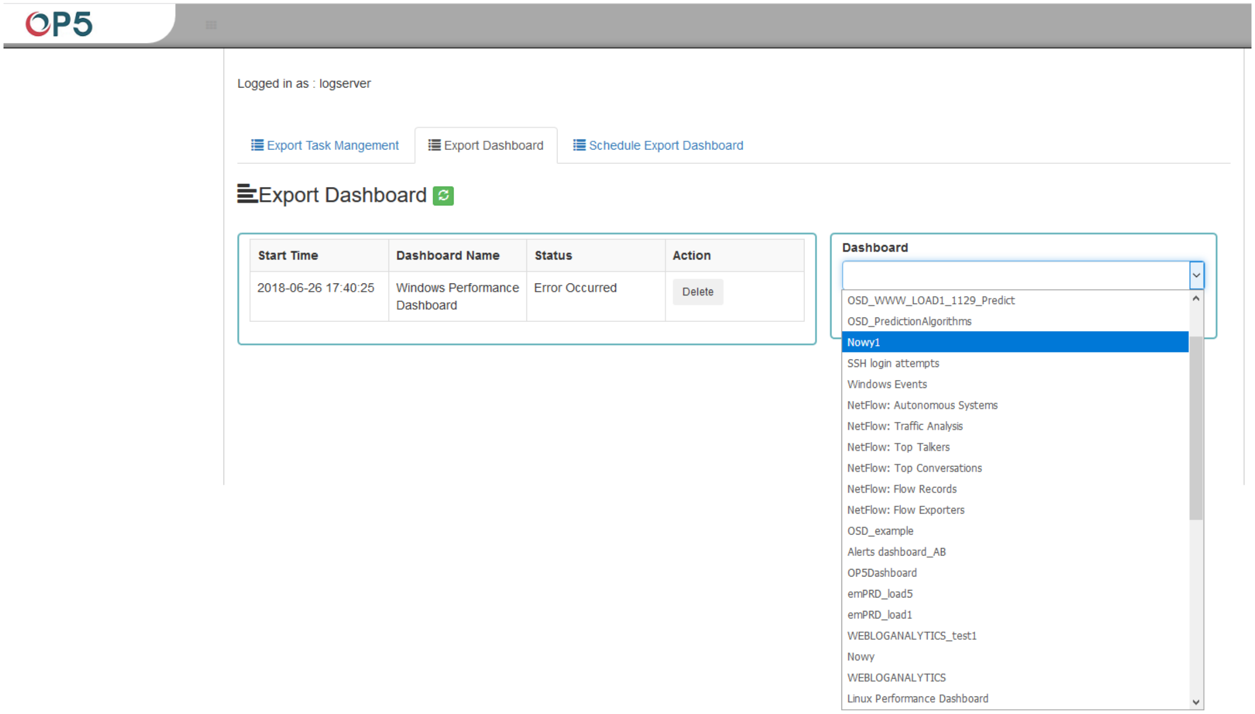
□ Pamiętaj tę decyzję dla wszystkich plików tego typu

In this tab, the downloaded data has a format that we can import into other systems for further analysis.

CHAPTER 24

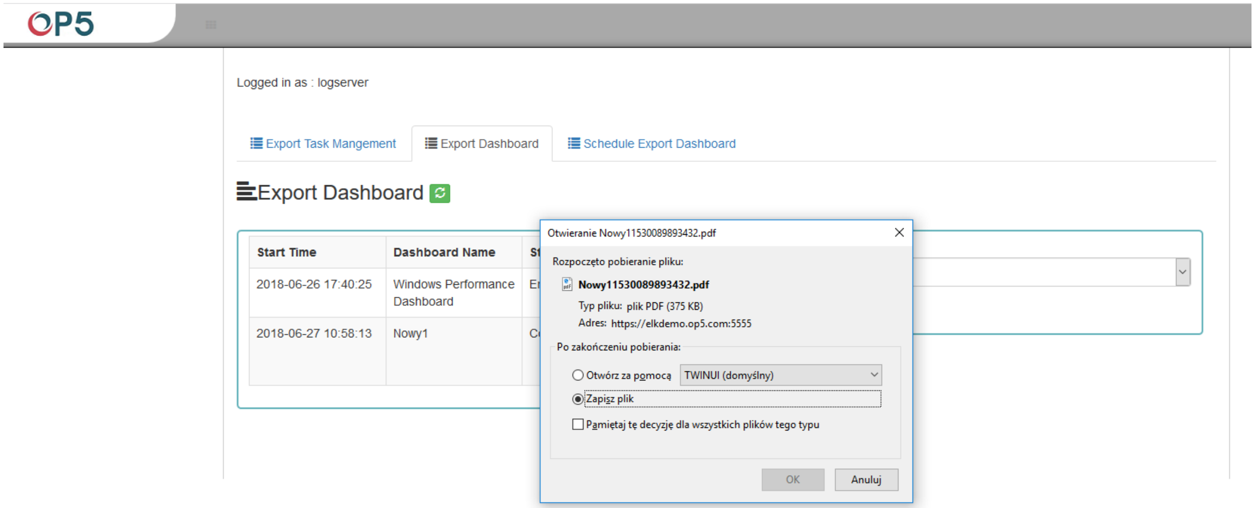
PDF Report

In the Export Dashboard tab we have the possibility to create graphic reports in PDF files. To create such a report, just from the drop-down list of previously created and saved Dashboards, indicate the one we are interested in, and then confirm the selection with the Submit button. A newly created export with the Processing status will appear on the list under Dashboard Name. When the processing is completed, the Status changes to Complete and it will be possible to download the report.



Start Time	Dashboard Name	Status	Action
2018-06-26 17:40:25	Windows Performance Dashboard	Error Occurred	Delete

By clicking the Download button, the report is downloaded to the disk or we can open it in the PDF file browser. There is also to option of deleting the report with the Delete button.



Logged in as : logserver

Export Dashboard

Start Time	Dashboard Name	St
2018-06-26 17:40:25	Windows Performance Dashboard	Er
2018-06-27 10:58:13	Nowy1	C

Otwieranie Nowy11530089893432.pdf

Rozpoczęto pobieranie pliku:

Nowy11530089893432.pdf

Typ pliku: plik PDF (375 KB)

Adres: https://elkdemo.op5.com:5555

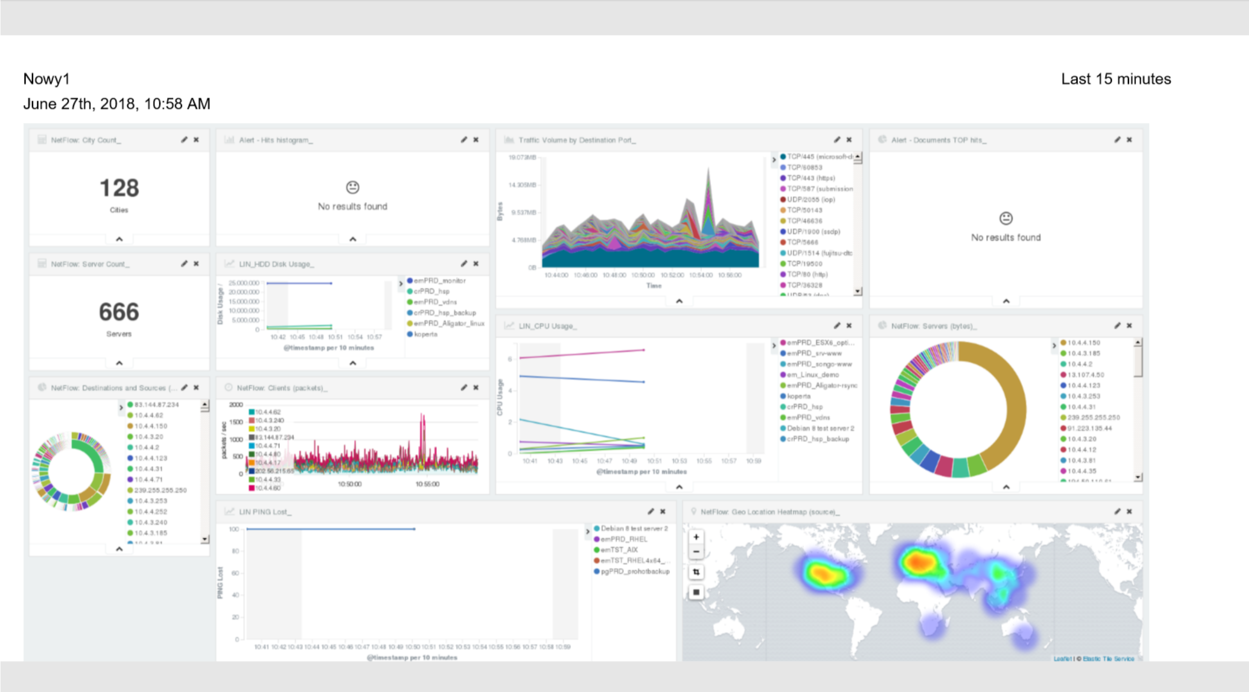
Po zakończeniu pobierania:

○ Otwórz za pomocą TWINUI (domyślny)

● Zapisz plik

□ Pamiętaj tę decyzję dla wszystkich plików tego typu

Below is an example report from the Dashboard template generated and downloaded as a PDF file.


NetFlow: City Count_
128
Cities
Alert - Hits histogram_
No results found
Traffic Volume by Destination Port_
Alert - Documents TOP hits_
No results found
NetFlow: Server Count_
666
Servers
LIN_HDD Disk Usage_
LIN_CPU Usage_
NetFlow: Servers (bytes)_
NetFlow: Destinations and Sources (...
NetFlow: Clients (packets)_
LIN PING Lost_
NetFlow: Geo Location Heatmap (source)_
@timestamp per 10 minutes
Leaflet | © Elastic Tile Service

Nowy1

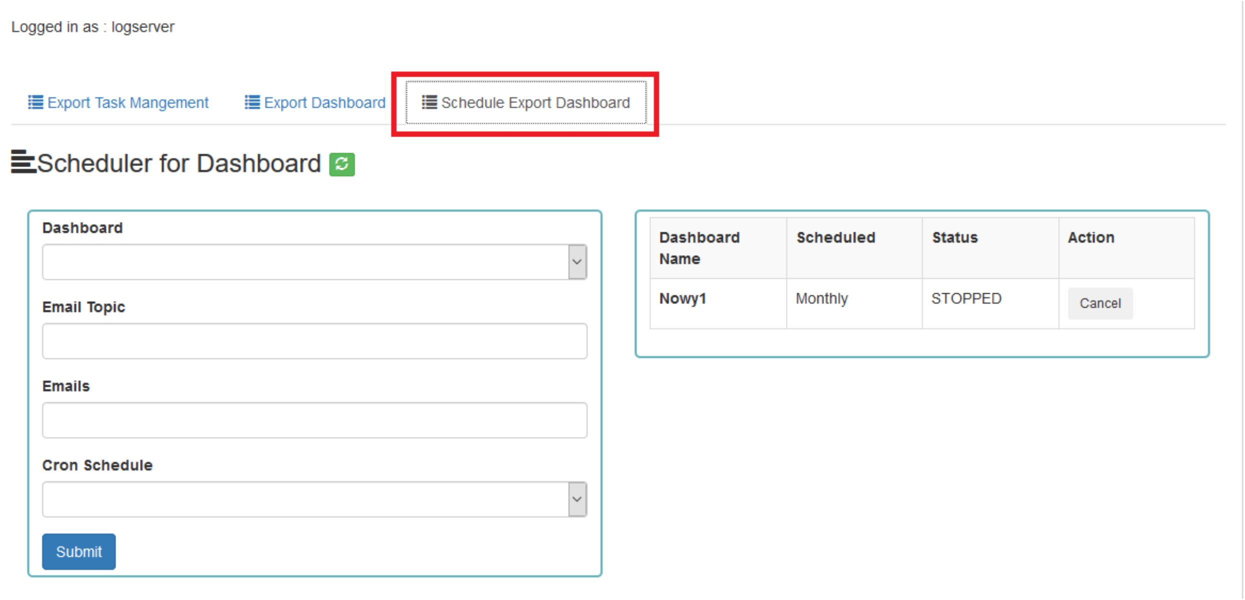
June 27th, 2018, 10:58 AM

Last 15 minutes

CHAPTER 25

Scheduler Report (Schedule Export Dashboard)

In the Report selection, we have the option of setting the Scheduler which from Dashboard template can generate a report at time intervals. To do this goes to the Schedule Export Dashboard tab.

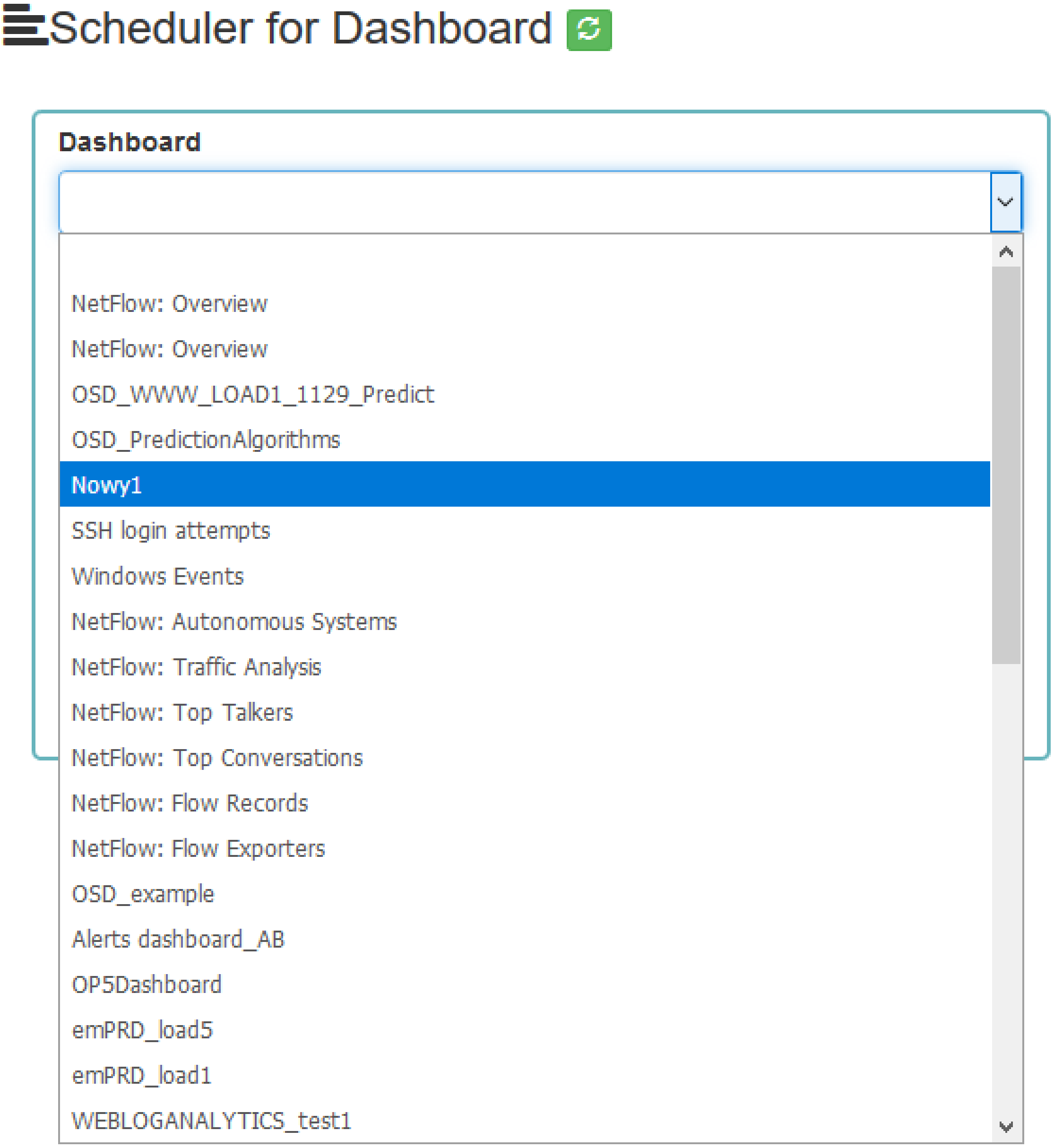


Logged in as : logserver

Scheduler for Dashboard

Dashboard Name	Scheduled	Status	Action
Nowy1	Monthly	STOPPED	Cancel

In this tab mark the saved Dashboard.

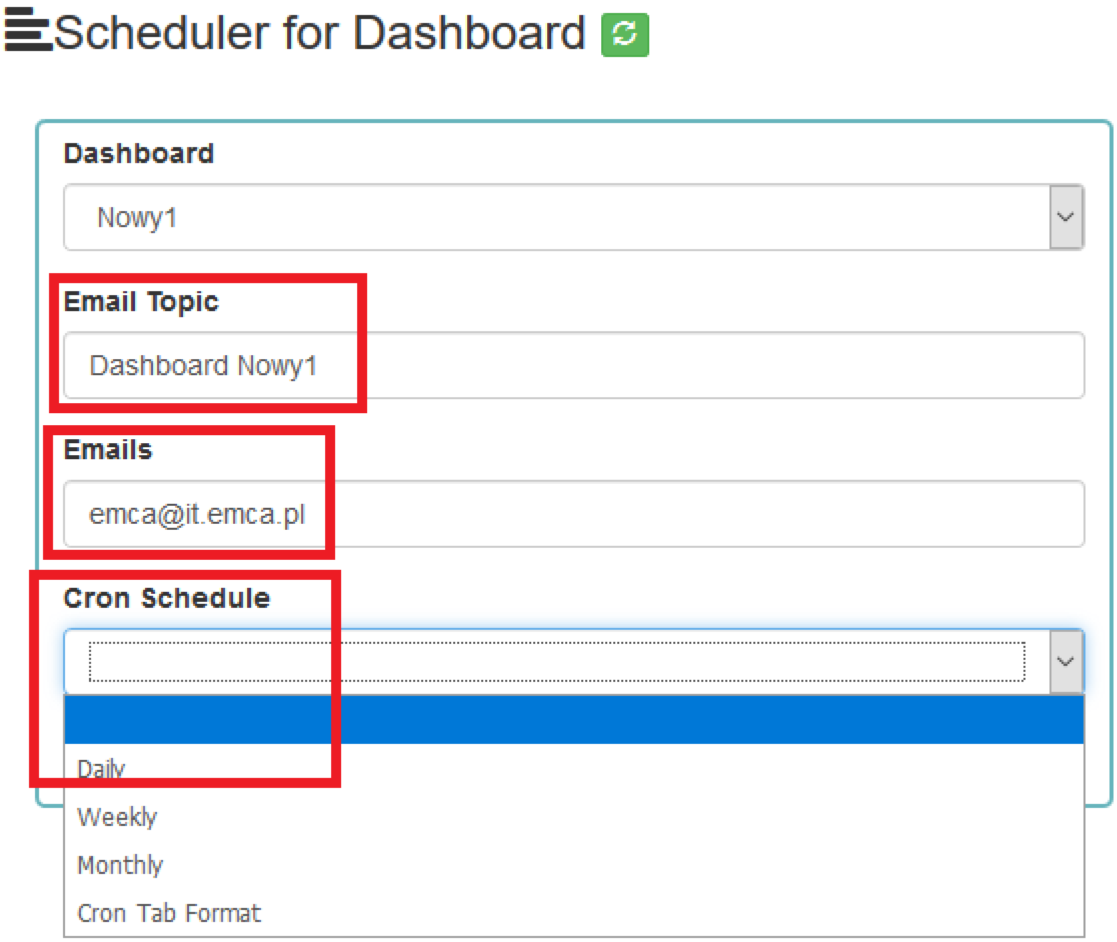


Scheduler for Dashboard

Dashboard

NetFlow: Overview
NetFlow: Overview
OSD_WWW_LOAD1_1129_Predict
OSD_PredictionAlgorithms
Nowy1
SSH login attempts
Windows Events
NetFlow: Autonomous Systems
NetFlow: Traffic Analysis
NetFlow: Top Talkers
NetFlow: Top Conversations
NetFlow: Flow Records
NetFlow: Flow Exporters
OSD_example
Alerts dashboard_AB
OP5Dashboard
emPRD_load5
emPRD_load1
WEBLOGANALYTICS_test1

In the Email Topic field, enter the Message title, in the Email field enter the email address to which the report should be sent. From drop-down list choose at what frequency you want the report to be generated and sent. The action configured in this way is confirmed with the Submit button.



Scheduler for Dashboard

Dashboard

Nowy1

Email Topic

Dashboard Nowy1

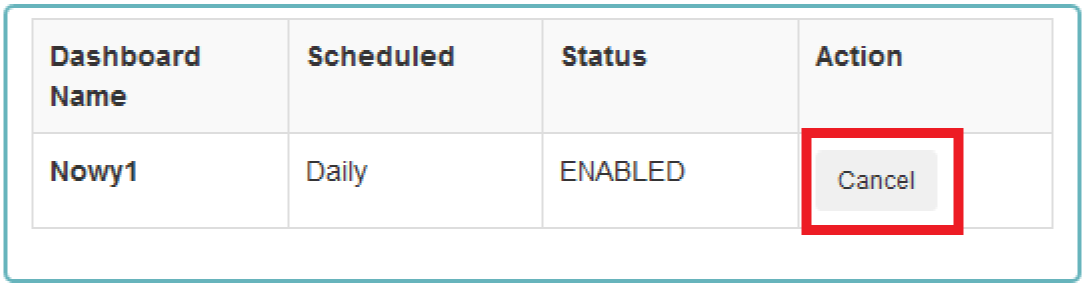
Emails

emca@it.emca.pl

Cron Schedule

Daily
Weekly
Monthly
Cron Tab Format

The defined action goes to the list and will generate a report to the e-mail address, with the cycle we set, until we cannot cancel it with the Cancel button.

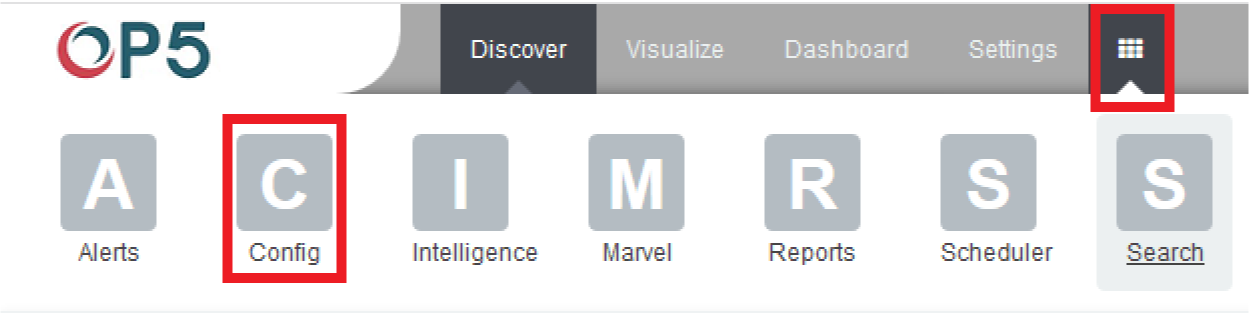


Dashboard Name	Scheduled	Status	Action
Nowy1	Daily	ENABLED	Cancel

CHAPTER 26

Users, roles and settings

OP5 Log Analytics allows to you manage users and permission for indexes and methods used by them. To go to the management window, select the tile icon from the main menu bar and then go to the „Config" icon (To go back, go to the „Search" icon).



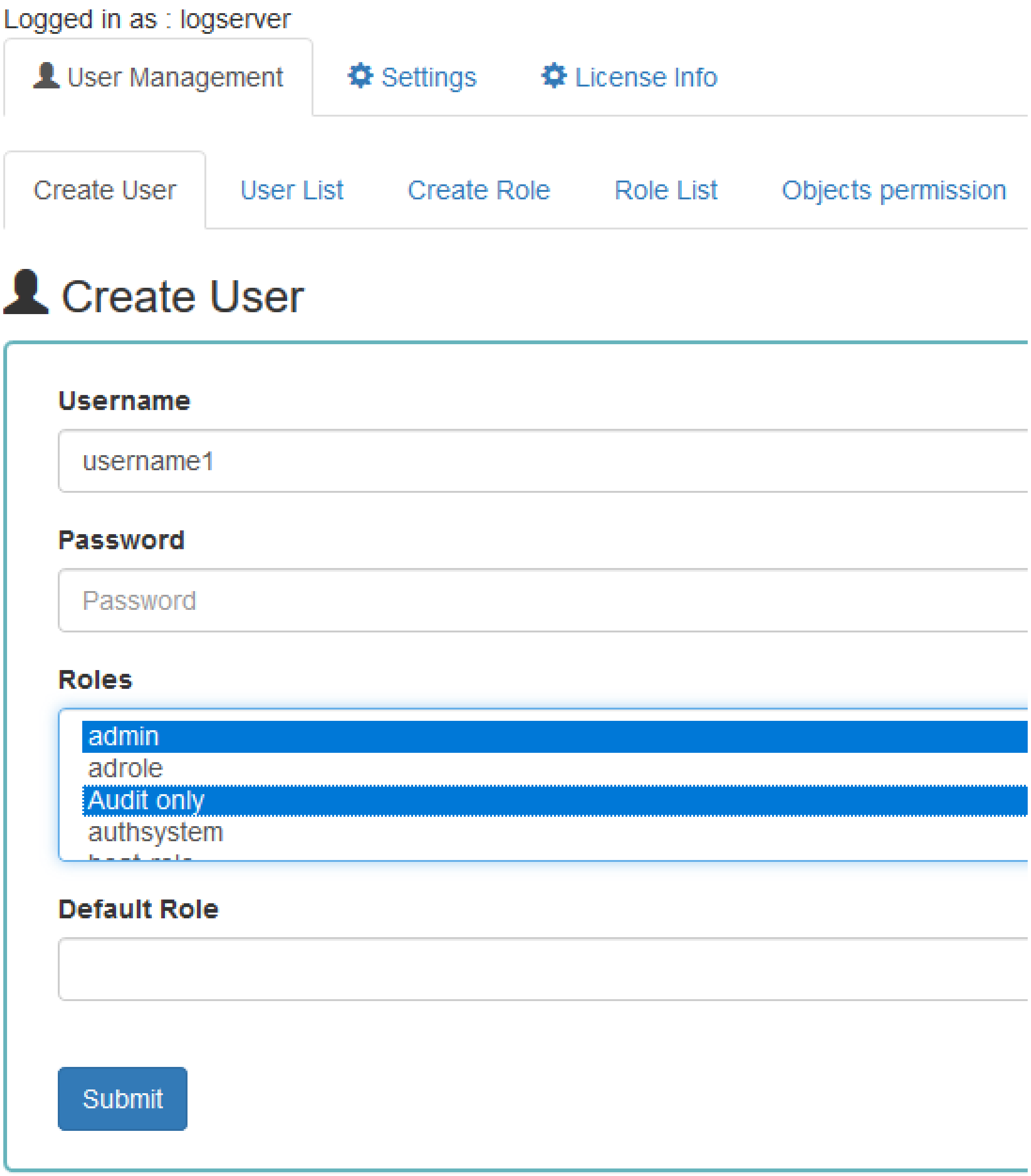
A new window will appear with three main tabs: „User Management", „Settings" and „License Info".

From the „User Management" level we have access to the following possibilities: Creating a user in „Create User", displaying users in „User List", creating new roles in „Create roles" and displaying existing roles in „List Role".

CHAPTER 27

Creating a User (Create User)

To create a new user click on the Config icon and you immediately enter the administration panel, where the first tab is to create a new user (**Create User**).



Logged in as : logserver

Create User

Username: username1

Password: Password

Roles: admin, adrole, Audit only, authsystem

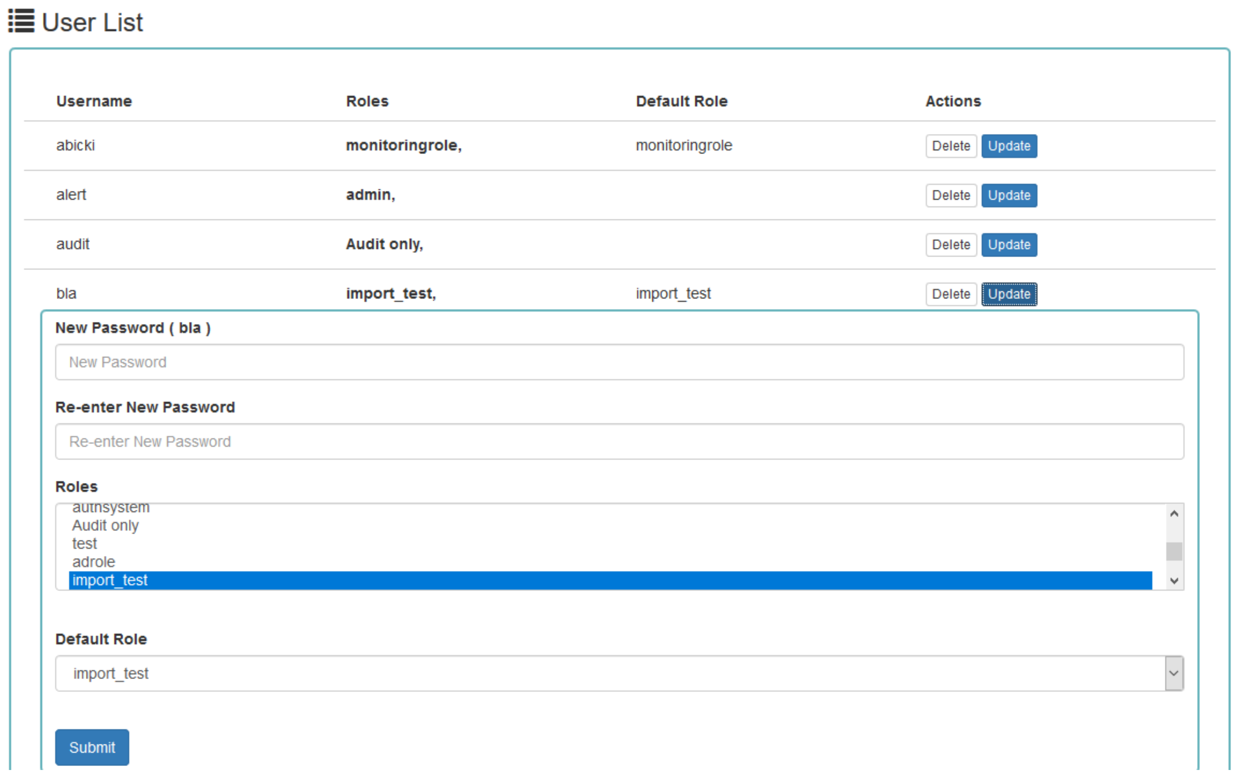
Default Role:

In the wizard that opens, we enter a unique username (Username field), password for the user (field Password) and assign a role (field Role). In this field we have the option of assigning more than one role. Until we select role in the Roles field, the Default Role field remains empty. When we mark several roles, these roles appear in the Default Role field. In this field we have the opportunity to indicate which role for a new user will be the default role with which the user will be associated in the first place when logging in. The default role field has one more important task - it binds all users with the field / role set in one group. When one of the users of this group create Visualization or Dashboard it will be available to other users from this role(group). Creating the account is confirmed with the Submit button.

CHAPTER 28

User’s modification and deletion, (User List)

Once we have created users, we can display their list. We do it in next tab (**User List**).



User List

Username	Roles	Default Role	Actions
abicki	**monitoringrole,**	monitoringrole	Delete Update
alert	**admin,**		Delete Update
audit	**Audit only,**		Delete Update
bla	**import_test,**	import_test	Delete Update

New Password (bla)

New Password

Re-enter New Password

Re-enter New Password

Roles

authsystem
Audit only
test
adrole
import_test

Default Role

import_test

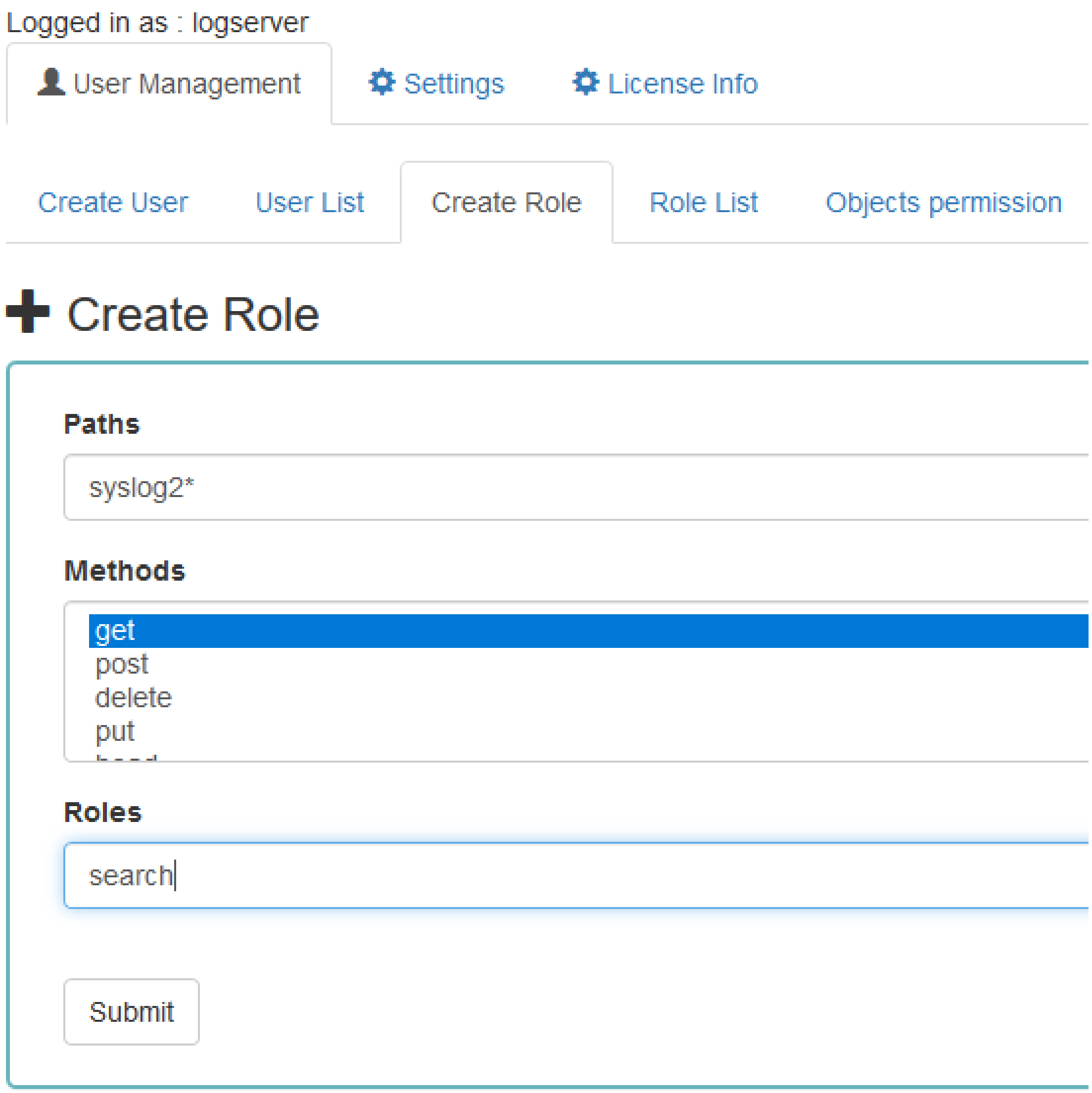
In this view, we get a list of user account with assigned roles and we have two buttons: Delete and Update. The first of these is ability to delete a user account. Under the Update button is a drop-down menu in which we can change the previous password to a new one (New password), change the password (Re-enter Ne Password), change the previously assigned roles (Roles), to other (we can take the role assigned earlier and give a new one, extend user permissions with new roles). The introduced changes are confirmed with the Submit button.

We can also see current user setting and clicking the Update button collapses the previously expanded menu.

CHAPTER 29

Create, modify and delete a role (Create Role), (Role List)

In the Create Role tab we can define a new role with permissions that we assign to a pattern or several index patterns.



Paths: syslog2*

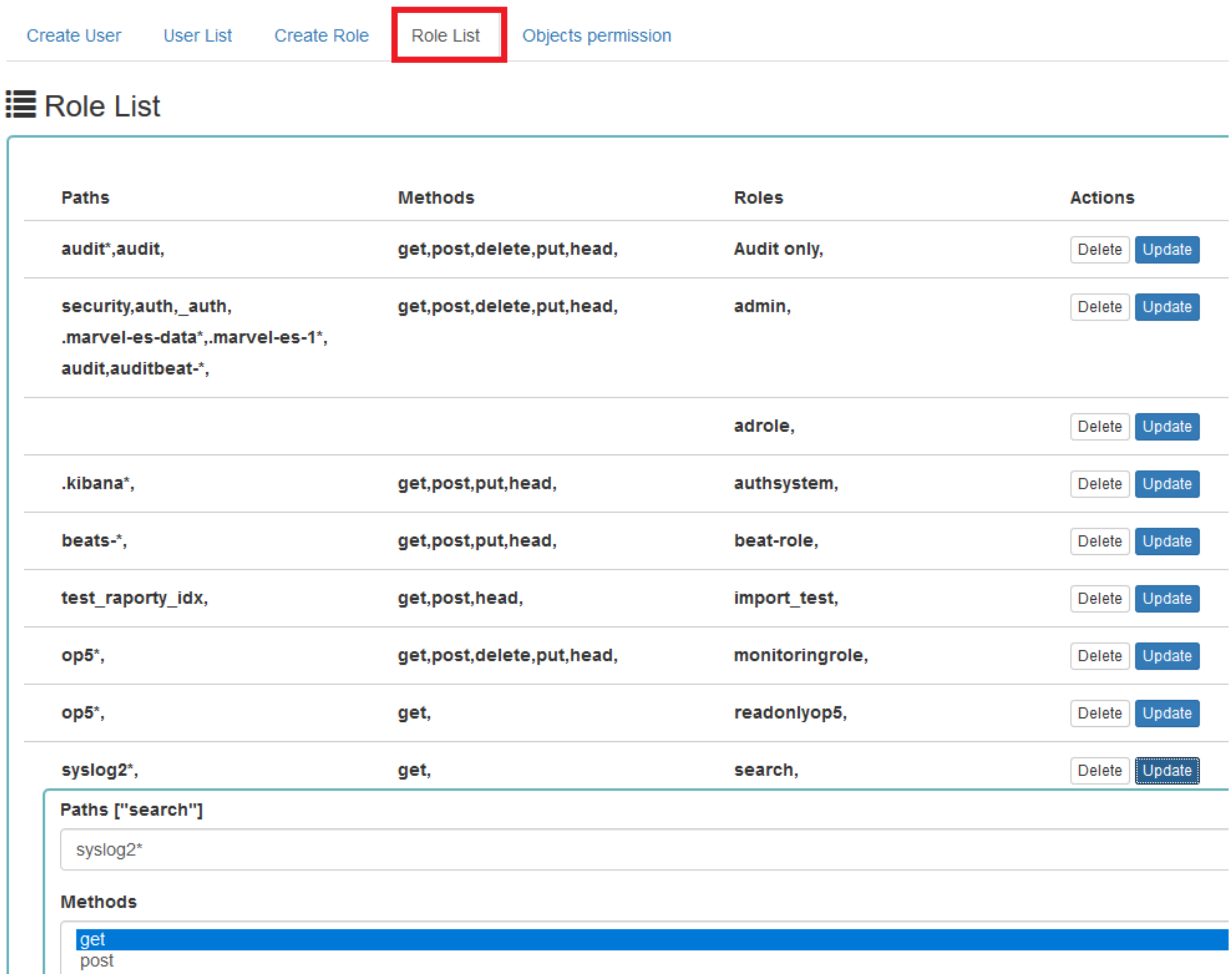
Methods: get (selected), post, delete, put

Roles: search

In example, we use the syslog2* index pattern. We give this name in the Paths field. We can provide one or more index patterns, their names should be separated by a comma. In the next Methods field, we select one or many methods that will be assigned to the role. Available methods:

- PUT - sends data to the server
- POST - sends a request to the server for a change
- DELETE - deletes the index / document
- GET - gets information about the index /document
- HEAD - is used to check if the index /document exists

In the role field, enter the unique name of the role. We confirm addition of a new role with the Submit button. To see if a new role has been added, go to the net Role List tab.



Role List

Paths	Methods	Roles	Actions
audit*,audit,	get,post,delete,put,head,	Audit only,	Delete Update
security,auth,_auth, .marvel-es-data*,.marvel-es-1*, audit,auditbeat-*,	get,post,delete,put,head,	admin,	Delete Update
		adrole,	Delete Update
.kibana*,	get,post,put,head,	authsystem,	Delete Update
beats-*,	get,post,put,head,	beat-role,	Delete Update
test_raporty_idx,	get,post,head,	import_test,	Delete Update
op5*,	get,post,delete,put,head,	monitoringrole,	Delete Update
op5*,	get,	readonlyop5,	Delete Update
syslog2*,	get,	search,	Delete Update

Paths ["search"]

syslog2*

Methods

get
post

As we can see, the new role has been added to the list. With the Delete button we have the option of deleting it, while under the Update button we have a drop-down menu thanks to which we can add or remove an index pattern and add or remove a method. When we want to confirm the changes, we choose the Submit button. Pressing the Update button again will close the menu.

Fresh installation of the application have sewn solid roles which granting user special rights:

- admin - this role gives unlimited permissions to administer / manage the application
- alert - a role for users who want to see the Alert module
- kibana - a role for users who want to see the application GUI
- Intelligence - a role for users who are to see the Intelligence module

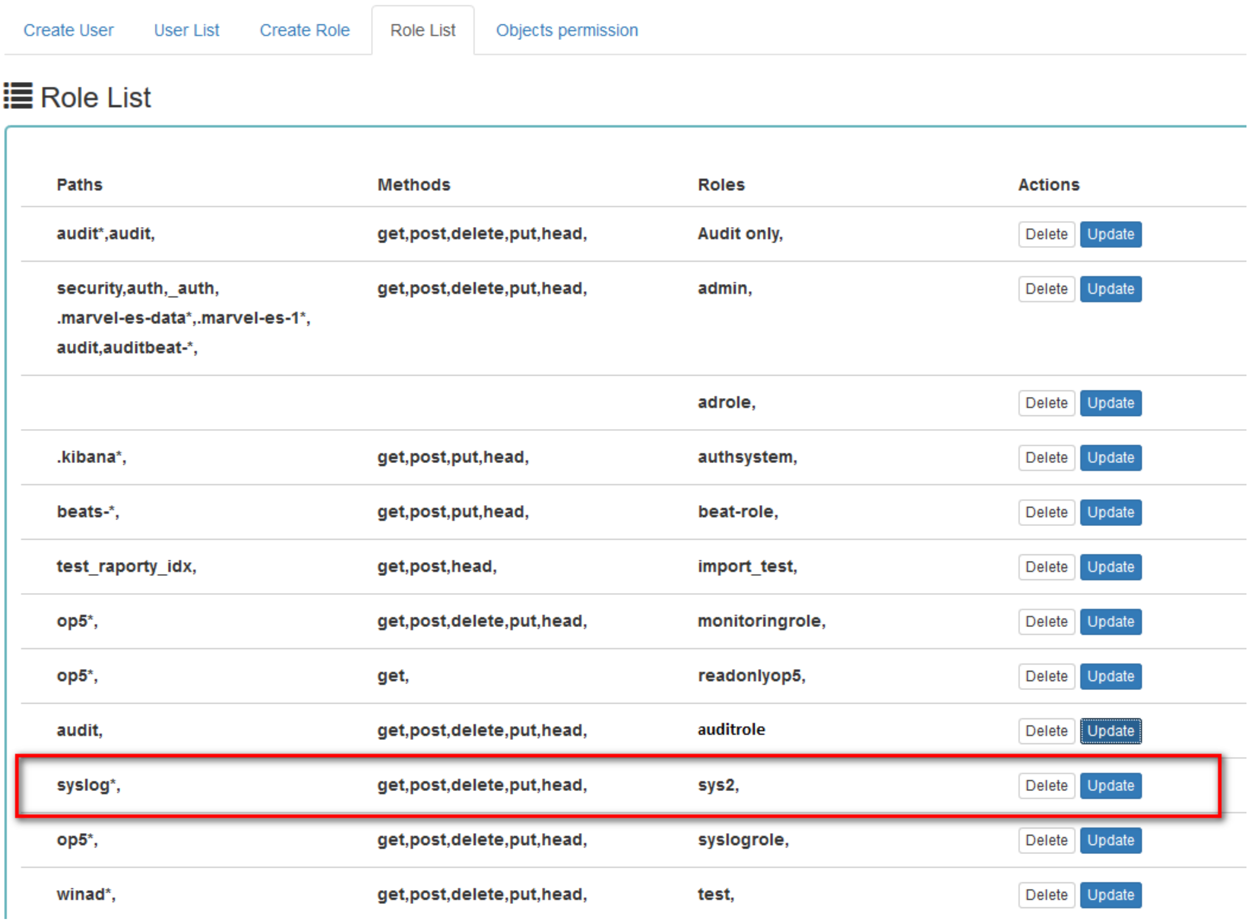
CHAPTER 30

Object access permissions (Objects permissions)

In the User Manager tab we can parameterize access to the newly created role as well as existing roles. In this tab we can indicate to which object in the application the role has access.

Example:

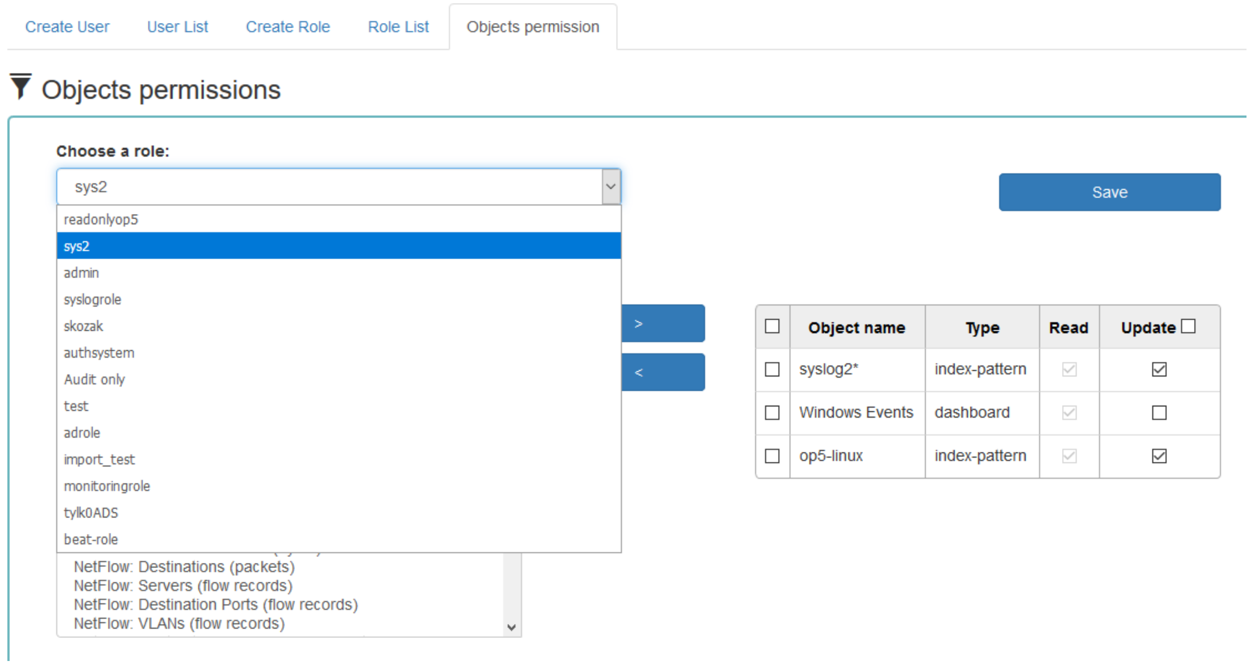
In the Role List tab we have a role called **sys2**, it refers to all index patterns beginning with syslog* and the methods get, post, delete, put and head are assigned.



Role List

Paths	Methods	Roles	Actions
audit*,audit,	get,post,delete,put,head,	Audit only,	Delete Update
security,auth,_auth, .marvel-es-data*,.marvel-es-1*, audit,auditbeat-*,	get,post,delete,put,head,	admin,	Delete Update
		adrole,	Delete Update
.kibana*,	get,post,put,head,	authsystem,	Delete Update
beats-*,	get,post,put,head,	beat-role,	Delete Update
test_raporty_idx,	get,post,head,	import_test,	Delete Update
op5*,	get,post,delete,put,head,	monitoringrole,	Delete Update
op5*,	get,	readonlyop5,	Delete Update
audit,	get,post,delete,put,head,	auditrole	Delete Update
syslog*,	get,post,delete,put,head,	sys2,	Delete Update
op5*,	get,post,delete,put,head,	syslogrole,	Delete Update
winad*,	get,post,delete,put,head,	test,	Delete Update

When we go to the Object permission tab, we have the option to choose the sys2 role in the drop-down list choose a role:



Objects permissions

Choose a role:

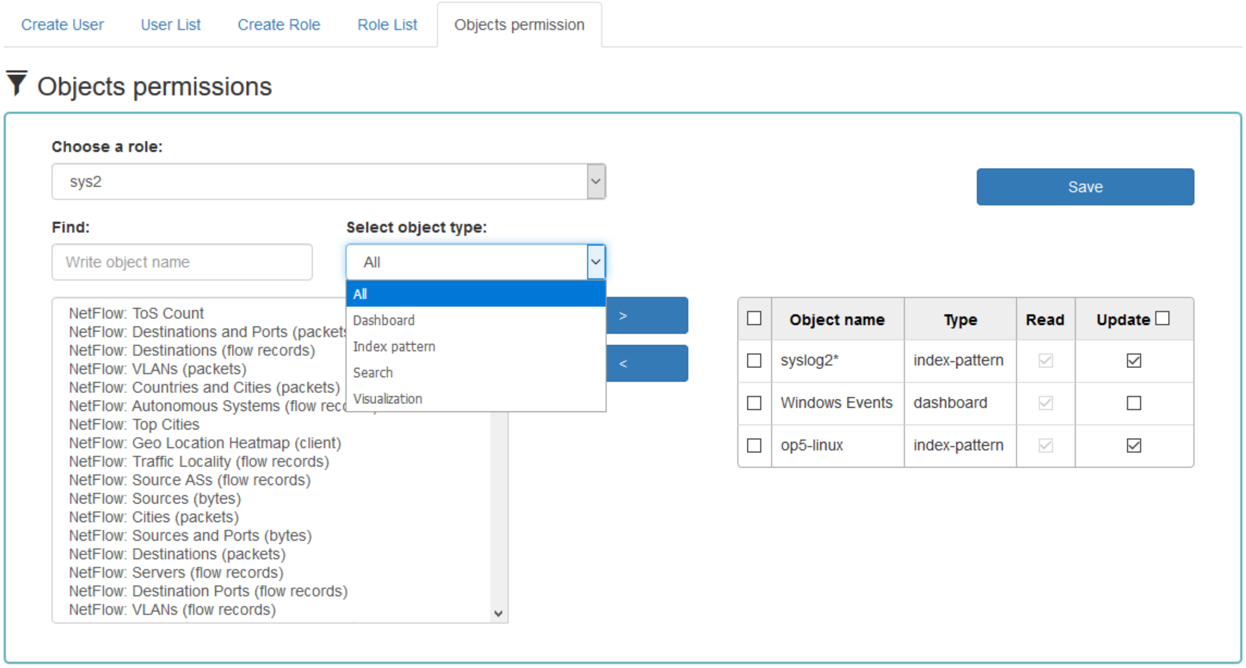
sys2

readonlyop5
sys2
admin
syslogrole
skozak
authsystem
Audit only
test
adrole
import_test
monitoringrole
tylk0ADS
beat-role

NetFlow: Destinations (packets)
NetFlow: Servers (flow records)
NetFlow: Destination Ports (flow records)
NetFlow: VLANs (flow records)

☐	Object name	Type	Read	Update ☐
☐	syslog2*	index-pattern	☑	☑
☐	Windows Events	dashboard	☑	☐
☐	op5-linux	index-pattern	☑	☑

After selecting, we can see that we already have access to the objects: two index patterns syslog2* and op5-* and on dashboard Windows Events. There are also appropriate read or updates permissions.



Objects permissions

Choose a role: sys2

Find: Write object name

Select object type: All

NetFlow: ToS Count
NetFlow: Destinations and Ports (packets
NetFlow: Destinations (flow records)
NetFlow: VLANs (packets)
NetFlow: Countries and Cities (packets)
NetFlow: Autonomous Systems (flow rec
NetFlow: Top Cities
NetFlow: Geo Location Heatmap (client)
NetFlow: Traffic Locality (flow records)
NetFlow: Source ASs (flow records)
NetFlow: Sources (bytes)
NetFlow: Cities (packets)
NetFlow: Sources and Ports (bytes)
NetFlow: Destinations (packets)
NetFlow: Servers (flow records)
NetFlow: Destination Ports (flow records)
NetFlow: VLANs (flow records)

□	Object name	Type	Read	Update □
□	syslog2*	index-pattern	☑	☑
□	Windows Events	dashboard	☑	□
□	op5-linux	index-pattern	☑	☑

From the list we have the opportunity to choose another object that we can add to the role. We have the ability to quickly find this object in the search engine (Find) and narrowing the object class in the drop-down field "Select object type". The object type are associated with saved previously documents in the sections Dashboard, Index pattern, Search and Visualization. By buttons > < we have the ability to add or remove or object, and Save button to save the selection.

CHAPTER 31

Default user and passwords

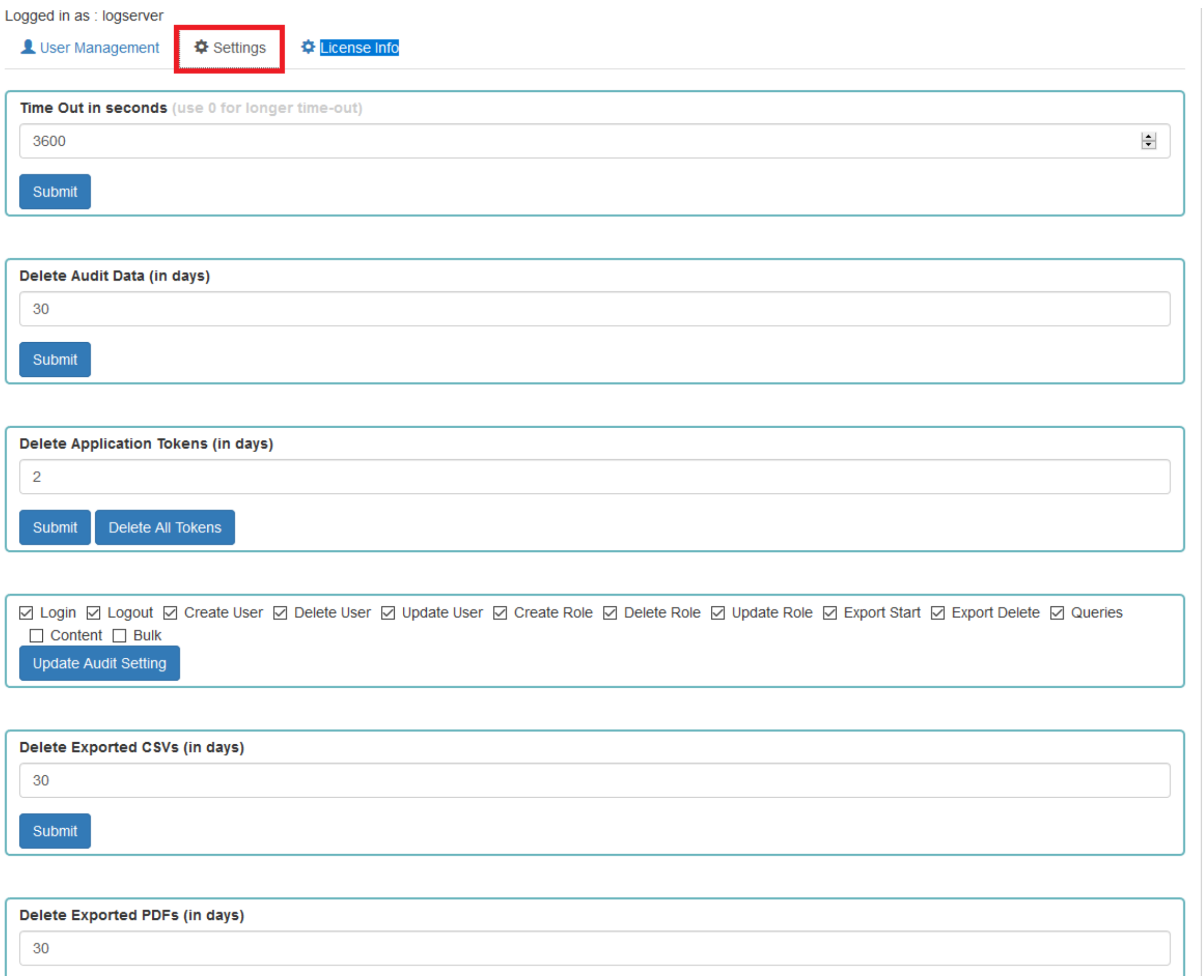
The table below contains built-in user accounts and default passwords:

```
|Addres                 |User           |Password       |Description                  ␣
↪                       |Usage          |
|-----------------------|---------------|---------------|-----------------------------
↪----------------------|---------------|
|https://localhost:5601 |logserver      |logserver      |A built-in *superuser*␣
↪account                     |               |
|                       |alert          |alert          |A built-in account for the␣
↪Alert module            |               |
|                       |intelligence   |intelligece    |A built-in account for the␣
↪Intelligence module     | usage for authorizing communication with elasticsearch␣
↪server, for put and get the data from indexes  |
|                       |scheduler      |scheduler      |A built-in account for the␣
↪Scheduler module        |               |
```

CHAPTER 32

Settings

The Settings tab is used to set the audit on different activates or events and consists of several fields:



Logged in as : logserver

Time Out in seconds (use 0 for longer time-out)

3600

Delete Audit Data (in days)

30

Delete Application Tokens (in days)

2

☑ Login ☑ Logout ☑ Create User ☑ Delete User ☑ Update User ☑ Create Role ☑ Delete Role ☑ Update Role ☑ Export Start ☑ Export Delete ☑ Queries
□ Content □ Bulk

Delete Exported CSVs (in days)

30

Delete Exported PDFs (in days)

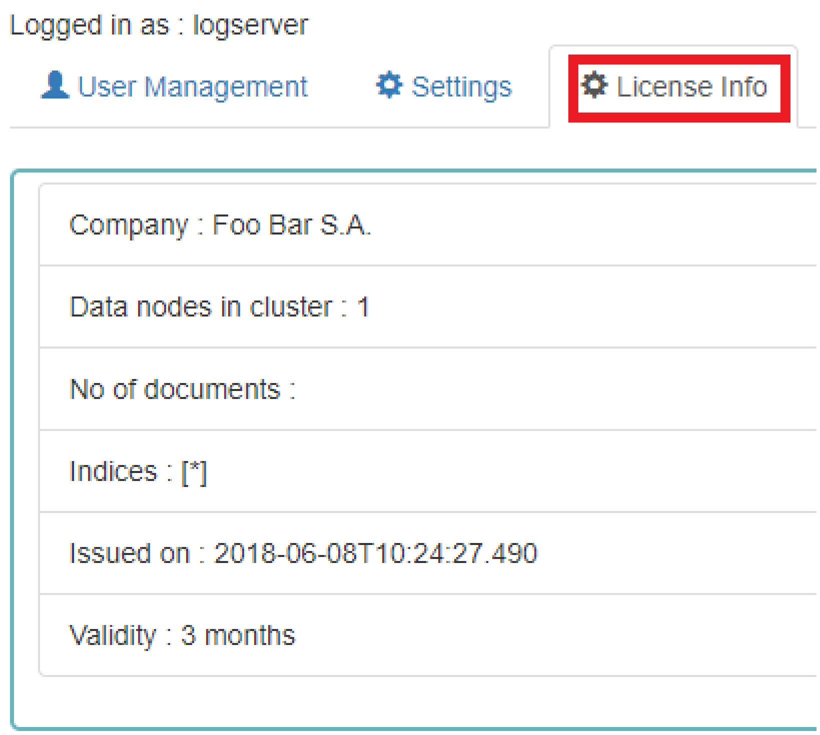
30

- Time Out in seconds field - this field defines the time after how many minutes the application will automatically log you off
- Delete Audit Data (in days) field - in this field we specify after what time the data from the audit should be deleted
- Delete Application Tokens (in days) - in this field we specify after what time the data from the audit should be deleted
- Next field are checkboxes in which we specify what kind of events are to be logged (saved) in the audit index. The events that can be monitored are: logging (Login), logging out (Logout), creating a user (Create User), deleting a user (Delete User), updating user (Update User), creating a role (Create Role), deleting a role (Delete Role), update of the role (Update Role), start of export (Export Start), delete of export (Export Delete), queries (Queries), result of the query (Content), if attempt was made to perform a series of operation (Bulk)
- Delete Exported CSVs (in days) field - in this field we specify after which time exported file with CSV extension have to be removed
- Delete Exported PDFs (in days) field - in this field we specify after which time exported file with PDF extension have to be removed
- To each field is assigned button thanks to which we can confirm the changes.

CHAPTER 33

License (License Info)

The License Information tab consists of several non-editable information fields.



Company : Foo Bar S.A.

Data nodes in cluster : 1

No of documents :

Indices : [*]

Issued on : 2018-06-08T10:24:27.490

Validity : 3 months

These fields contain information:

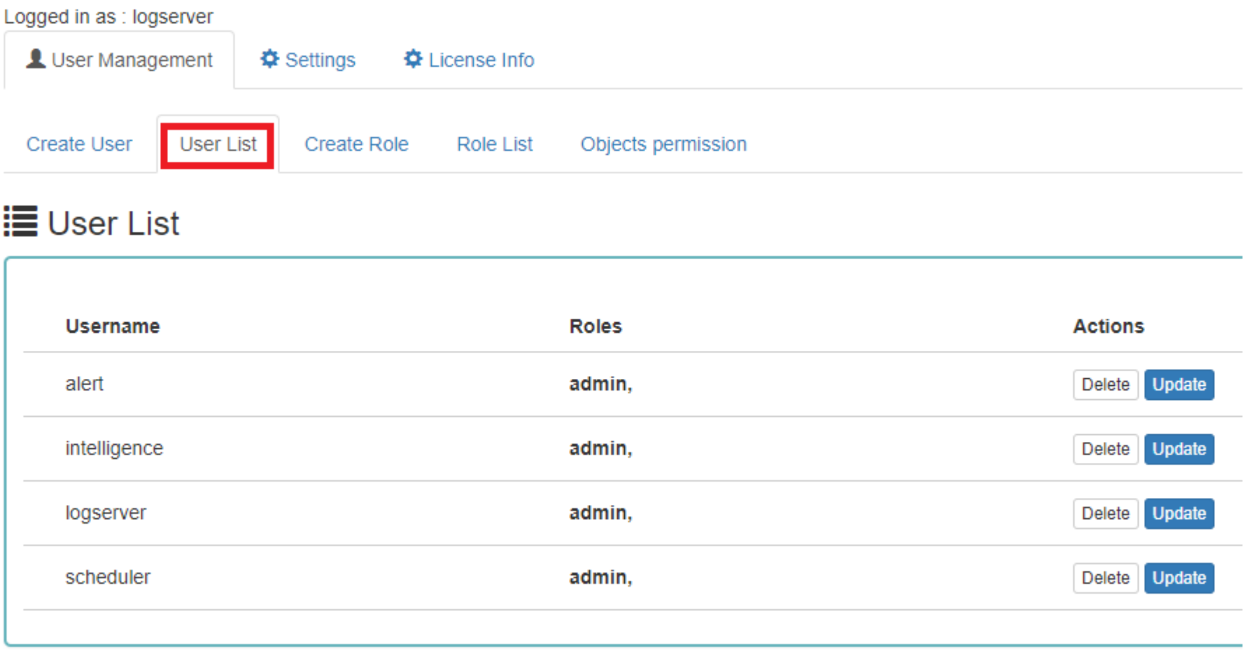
- Company field, who owns the license - in this case EMCA S.A.
- Data nodes in cluster field - how many nodes we can put in one cluster - in this case 100
- No of documents field - empty field

- Indices field - number of indexes, symbol[*] means that we can create any number of indices
- Issued on field - date of issue
- Validity field - validity, in this case for 360000 months

CHAPTER 34

Special accounts

At the first installation of the OP5 Log Analytics application, apart from the administrative account (logserver), special applications are created in the application: alert, intelligence and scheduler.



Username	Roles	Actions
alert	admin,	Delete Update
intelligence	admin,	Delete Update
logserver	admin,	Delete Update
scheduler	admin,	Delete Update

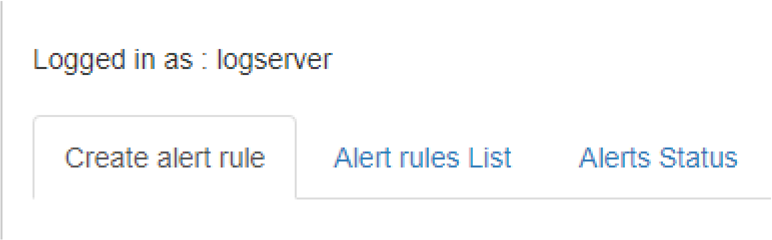
- **Alert Account** - this account is connected to the Alert Module which is designed to track events written to the index for the previously defined parameters. If these are met the information action is started (more on the action in the Alert section)
- **Intelligence Account** - with this account is related to the module of artificial intelligence which is designed to track events and learn the network based on previously defined rules artificial intelligence based on one of the available algorithms (more on operation in the Intelligence chapter)

- **Scheduler Account** - the scheduler module is associated with this account, which corresponds to, among others for generating reports

CHAPTER 35

Alert Module

OP5 Log Analytics allows you to create alerts, i.e. monitoring queries. These are constant queries that run in the background and when the conditions specified in the alert are met, the specify action is taken.



Logged in as : logserver

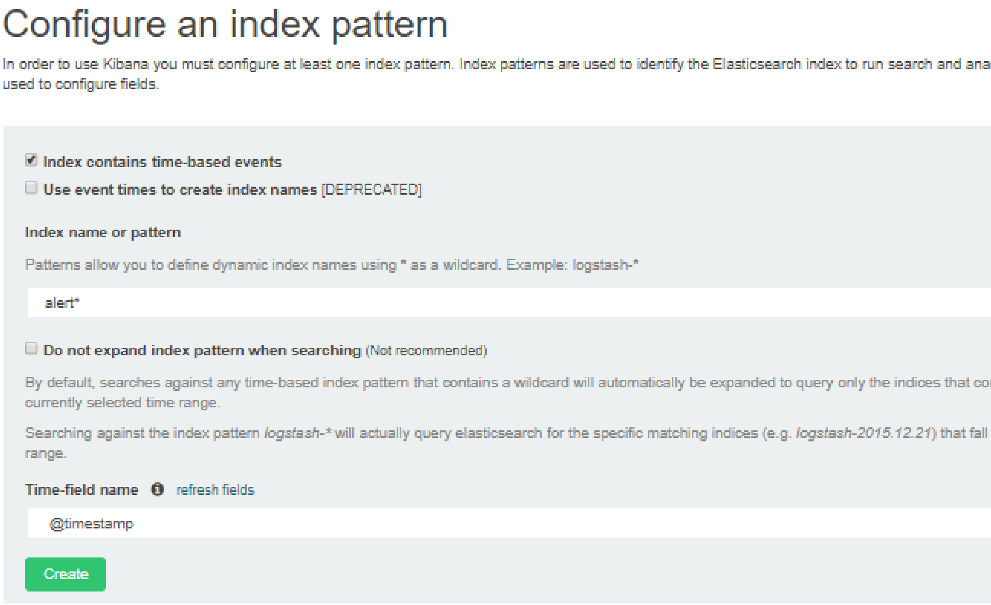
For example, if you want to know when more than 20 „status:500" responscode from on our homepage appear within an one hour, then we create an alert that check the number of occurrences of the „status:500" query for a specific index every 5 minutes. If the condition we are interested in is met, we send an action in the form of sending a message to our e-mail address. In the action, you can also set the launch of any script.

CHAPTER 36

Enabling the Alert Module

To enabling the alert module you should:

- generate writeback index for Alert service`/opt/alert/bin/elastalert-create-index --config /opt/alert/config.yaml`



Configure an index pattern

In order to use Kibana you must configure at least one index pattern. Index patterns are used to identify the Elasticsearch index to run search and ana
used to configure fields.

☑ Index contains time-based events

☐ Use event times to create index names [DEPRECATED]

Index name or pattern

Patterns allow you to define dynamic index names using * as a wildcard. Example: logstash-*

alert*

☐ Do not expand index pattern when searching (Not recommended)

By default, searches against any time-based index pattern that contains a wildcard will automatically be expanded to query only the indices that co
currently selected time range.

Searching against the index pattern *logstash-** will actually query elasticsearch for the specific matching indices (e.g. *logstash-2015.12.21*) that fall
range.

Time-field name refresh fields

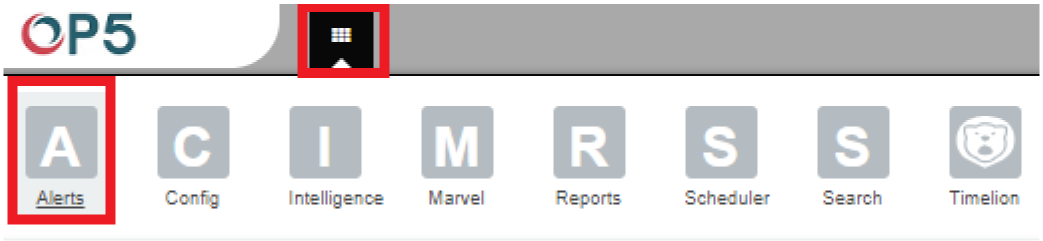
@timestamp

- configure the index pattern for alert*
- start Alert service`systemctl start alert`

CHAPTER 37

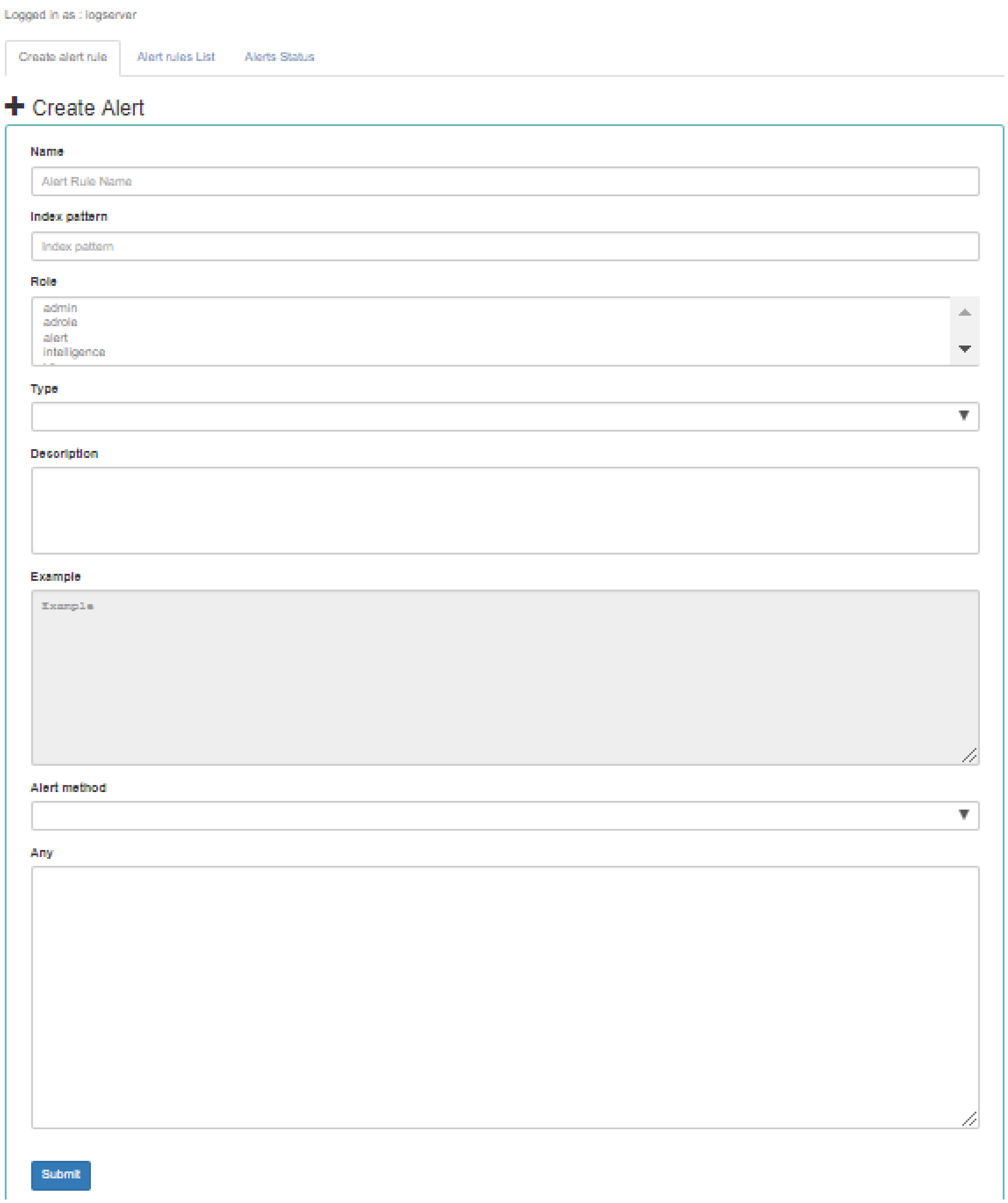
Creating Alerts

To create the alert, select the tile icon from the main menu bar and then go to the „Alerts" icon (To go back, go to the „Search" icon).



We will display a page with tree tabs: Create new alerts in „Create alert rule", manage alerts in „Alert rules List" and check alert status „Alert Status".

In the alert creation windows we have an alert creation form:



- Name - the name of the alert, after which we will recognize and search for it.
- Index pattern - a pattern of indexes after which the alert will be searched.
- Role - the role of the user for whom an alert will be available
- Type - type of alert
- Description - description of the alert.
- Example - an example of using a given type of alert. Descriptive field
- Alert method - the action the alert will take if the conditions are met (sending an email message or executing a

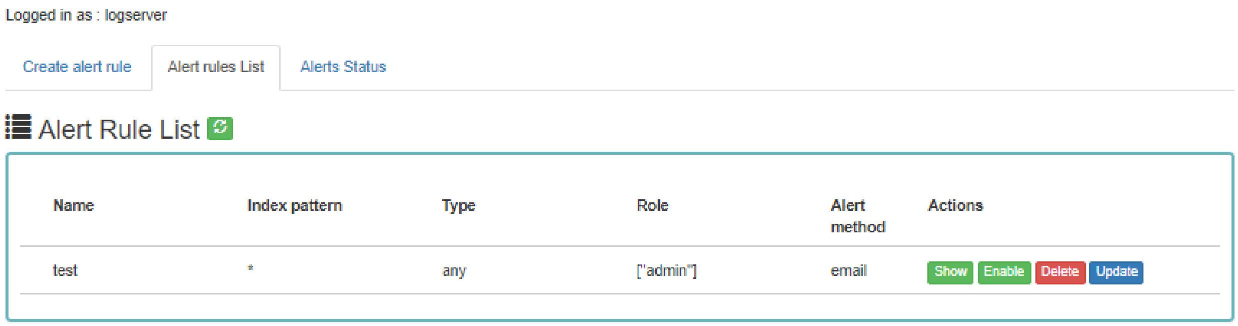
command)

- Any - additional descriptive field.

CHAPTER 38

List of Alert rules

The "Alert Rule List" tab contain complete list of previously created alert rules:



Logged in as : logserver

Alert Rule List

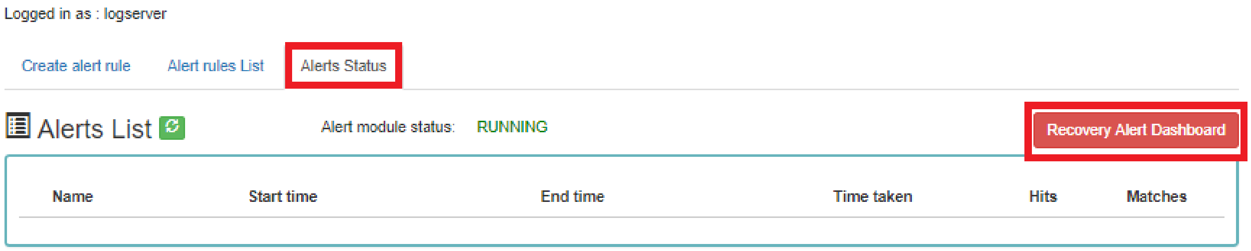
Name	Index pattern	Type	Role	Alert method	Actions
test	*	any	["admin"]	email	Show Enable Delete Update

In this winsow, you can activate / deactivate, delete and update alerts by clicking on the selected icon with the given alert. Enable Delete Update.

CHAPTER 39

Alerts status

In the “Alert status” tab, you can check the current alert status: if it activated, when it started and when it ended, how long it lasted, how many event sit found and how many times it worked.



Logged in as : logserver

Alert module status: RUNNING

Name	Start time	End time	Time taken	Hits	Matches

Also, on this tab, you can recover the alert dashboard, by clicking the “Recovery Alert Dashboard” button.

CHAPTER 40

Type of the Alert module rules

The various RuleType classes, defined in OP5-Log-Aalytics. An instance is held in memory for each rule, passed all of the data returned by querying Elasticsearch with a given filter, and generates matches based on that data.

- ***Any*** - The any rule will match everything. Every hit that the query returns will generate an alert.
- ***Blacklist*** - The blacklist rule will check a certain field against a blacklist, and match if it is in the blacklist.
- ***Whitelist*** - Similar to blacklist, this rule will compare a certain field to a whitelist, and match if the list does not contain the term.
- ***Change*** - This rule will monitor a certain field and match if that field changes.
- ***Frequency*** - his rule matches when there are at least a certain number of events in a given time frame.
- ***Spike*** - This rule matches when the volume of events during a given time period is spike_height times larger or smaller than during the previous time period.
- ***Flatline*** - This rule matches when the total number of events is under a given threshold for a time period.
- ***New Term*** - This rule matches when a new value appears in a field that has never been seen before.
- ***Cardinality*** - This rule matches when a the total number of unique values for a certain field within a time frame is higher or lower than a threshold.
- ***Metric Aggregation*** - This rule matches when the value of a metric within the calculation window is higher or lower than a threshold.
- ***Percentage Match*** - This rule matches when the percentage of document in the match bucket within a calculation window is higher or lower than a threshold.

CHAPTER 41

Example of rules

CHAPTER 42

Example of rules

42.1 Unix - Authentication Fail

- index pattern:

```
syslog-*
```

- Type:

```
Frequency
```

- Alert Method:

```
Email
```

- Any:

```
num_events: 4
timeframe:
  minutes: 5

filter:
- query_string:
    query: "program: (ssh OR sshd OR su OR sudo) AND message: \"Failed password\""
```

42.2 Windows - Firewall disable or modify

- index pattern:

```
beats-*
```

- Type:

```
Any
```

- Alert Method:

```
Email
```

- Any:

filter:

```
    - query_string:
            query: "event_id:(4947 OR 4948 OR 4946 OR 4949 OR 4954 OR 4956 OR 5025)"
```

CHAPTER 43

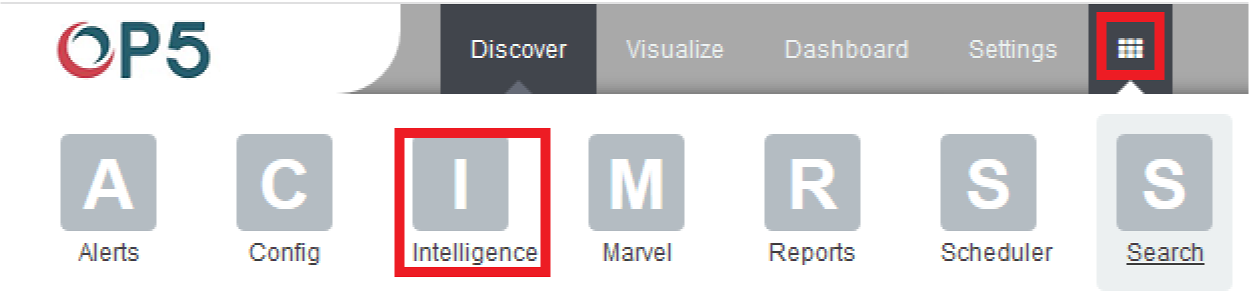
Intelligence Module

A dedicated artificial intelligence module has been built in the OP5 Log Analytics system that allows prediction of parameter values relevant to the maintenance of infrastructure and IT systems. Such parameters include:

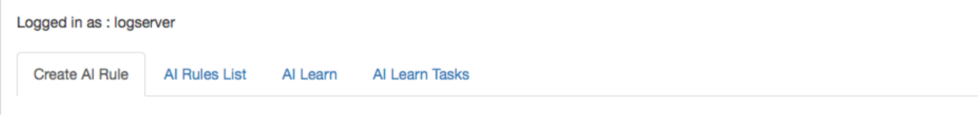
- use of disk resources,
- use of network resources,
- using the power of processors
- detection of known incorrect behavior of IT systems In the future, it is planned to launch algorithms that enable automatic detection of anomalies, e.g. non-standard network traffic, which may suggest hacking attempts.

(A detailed description of the implemented algorithms can be found in a separate document)

To access of the Intelligence module, click the tile icon from the main meu bar and then go to the „Intelligence" icon (To go back, click to the „Search" icon).



There are 4 screens available in the module:



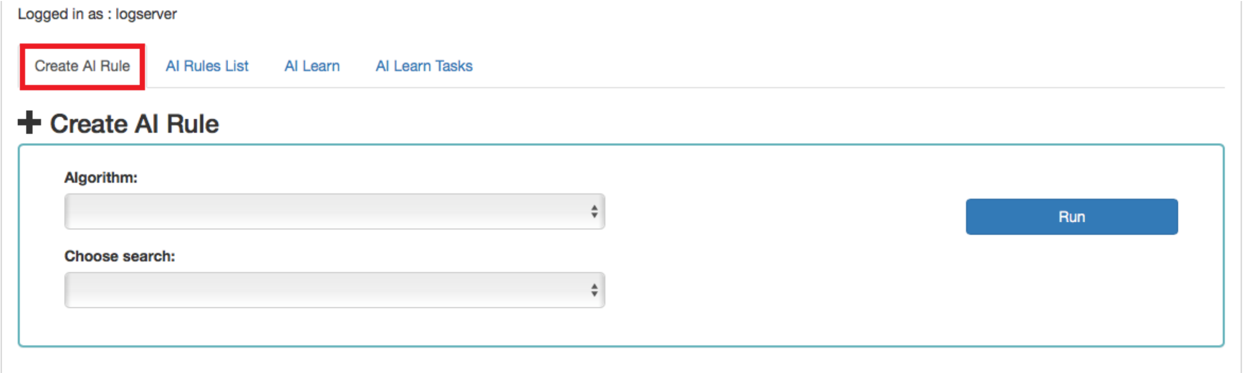
- **Create AI Rule** - the screen allows you to create artificial intelligence rules and run them in scheduler mode or immediately

- **AI Rules List** - the screen presents a list of created artificial intelligence rules with the option of editing, previewing and deleting them
- **AI Learn** - the screen allows to define the conditions for teaching the MLP neural network
- **AI Learn Tasks** - a screen on which the initiated and completed learning processes of neural networks with the ability to preview learning results are presented.

CHAPTER 44

Create AI Rule

To create the AI Rule, click on the tile icon from the main menu bar, go to the „Intelligence" icon and select "Create AI Rule" tab. The screen allows to defining the rules of artificial intelligence based on one of the available algorithms (a detailed description of the available algorithms is available in a separate document).



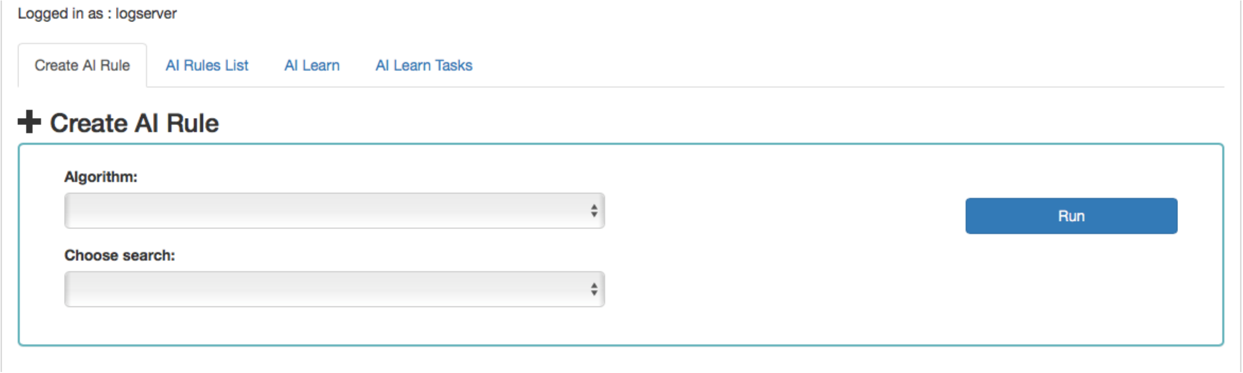
Description of the controls available on the fixed part of screen:

- **Algorithm** - the name of the algorithm that forms the basis of the artificial intelligence rule
- **Choose search** - search defined in the OP5 Log Analytics system, which is used to select a set of data on which the artificial intelligence rule will operate
- **Run** - a button that allows running the defined AI rule or saving it to the scheduler and run as planned

The rest of the screen will depend on the chosen artificial intelligence algorithm.

CHAPTER 45

The fixed part of the screen

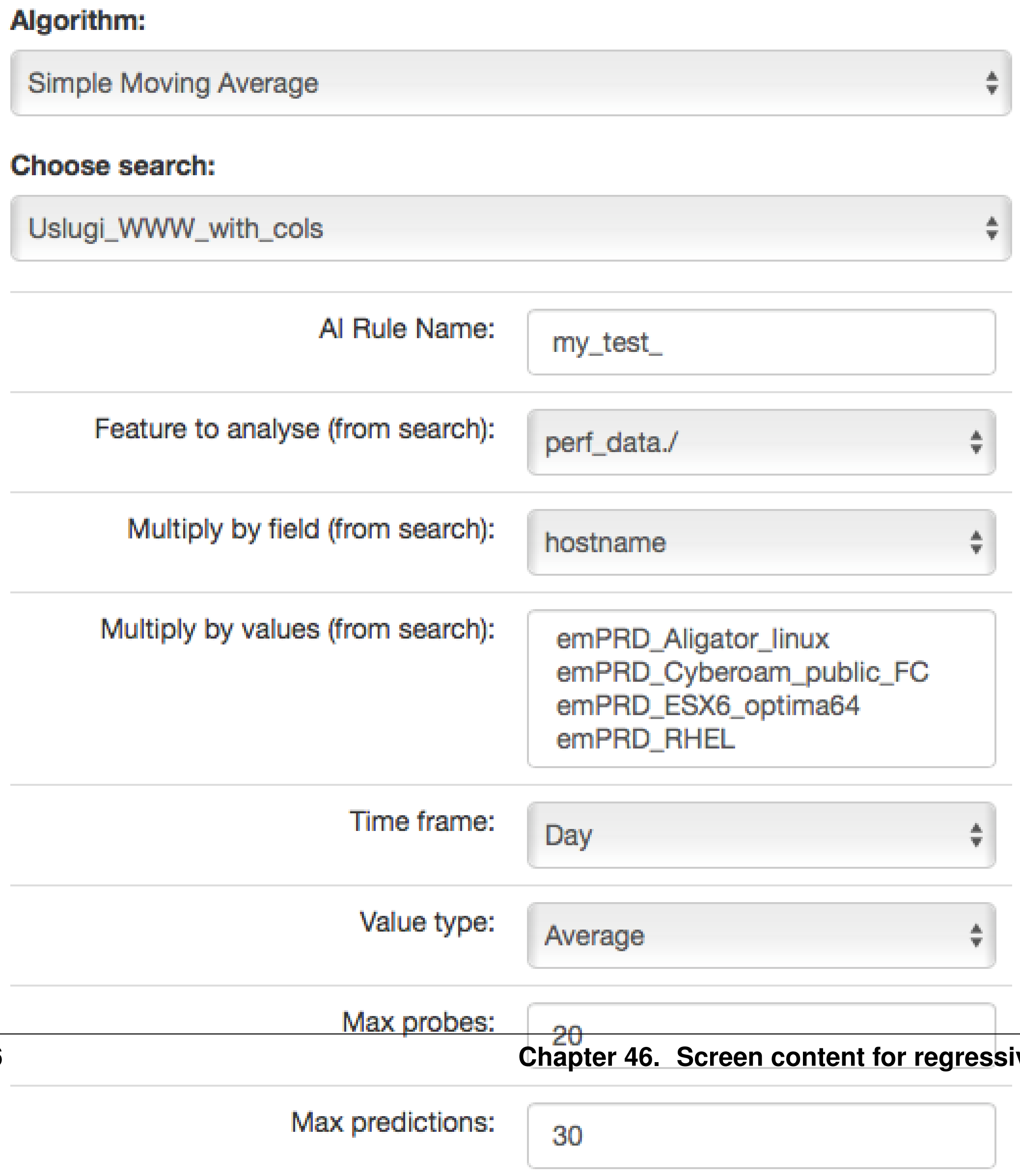


Description of the controls available on the fixed part of screen:

Algorithm - the name of the algorithm that forms the basis of the artificial intelligence rule Choose search - search defined in the OP5 Log Analytics system, which is used to select a set of data on which the artificial intelligence rule will operate Run - a button that allows running the defined AI rule or saving it to the scheduler and run as planned The rest of the screen will depend on the chosen artificial intelligence algorithm.

CHAPTER 46

Screen content for regressive algorithms



Algorithm: Simple Moving Average

Choose search: Uslugi_WWW_with_cols

AI Rule Name: my_test_

Feature to analyse (from search): perf_data./

Multiply by field (from search): hostname

Multiply by values (from search):
emPRD_Aligator_linux
emPRD_Cyberoam_public_FC
emPRD_ESX6_optima64
emPRD_RHEL

Time frame: Day

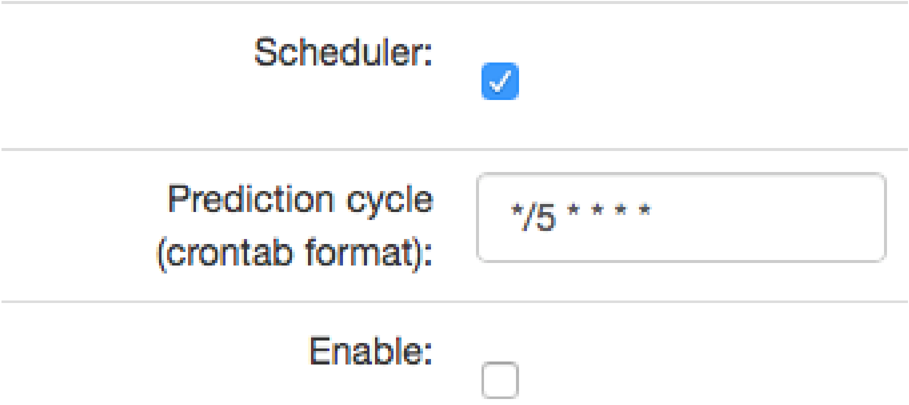
Value type: Average

Max probes: 20

Max predictions: 30

Description of controls:

- **feature to analyze from search** - analyzed feature (dictated)
- **multiply by field** - enable multiplication of algorithms after unique values of the feature indicated here. Multiplication allows you to run the AI rule one for e.g. all servers. The value "none" in this field means no multiplication.
- **multiply by values** - if a trait is indicated in the „multiply by field", then unique values of this trait will appear in this field. Multiplications will be made for the selected values. If at least one of value is not selected, the „Run" buttons will be inactive.'
- **time frame** - feature aggregation method (1 minute, 5 minute, 15 minute, 30 minute, hourly, weekly, monthly, 6 months, 12 months)
- **max probes** - how many samples back will be taken into account for analysis. A single sample is an aggregated data according to the aggregation method.
- **value type** - which values to take into account when aggregating for a given time frame (e.g. maximum from time frame, minimum, average)
- **max predictions** - how many estimates we make for ahead (we take time frame)
- **data limit** - limits the amount of date downloaded from the source. It speeds up processing but reduces its quality
- **start date** - you can set a date earlier than the current date in order to verify how the selected algorithm would work on historical data
- **Scheduler** - a tag if the rule should be run according to the plan for the scheduler. If selected, additional fields will appear;



Scheduler: ☑

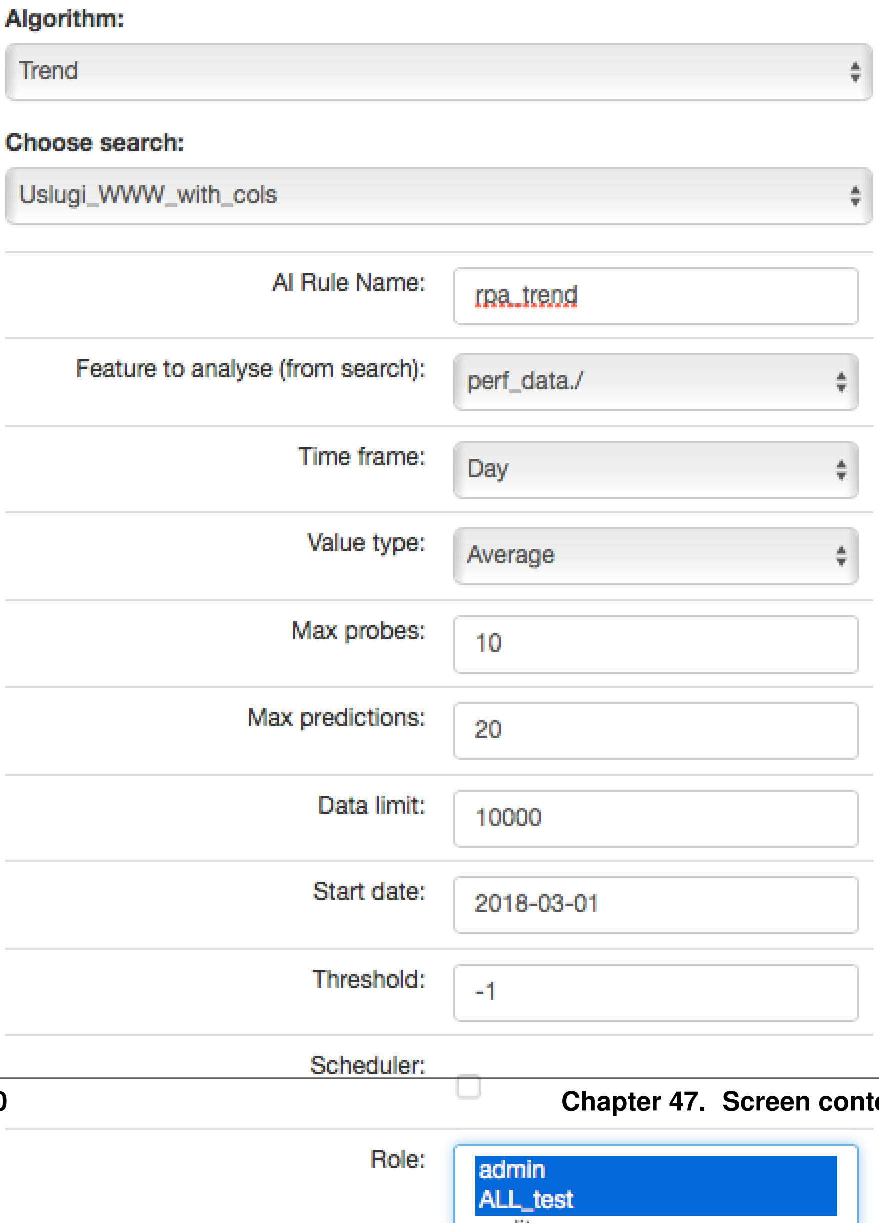
Prediction cycle (crontab format): */5 * * * *

Enable: □

- **Prediction cycle** - plan definition for the scheduler, i.e. the cycle in which the prediction rule is run (e.g. once a day, every hour, once a week). In the field, enter the command that complies with the cron standard. Enable – whether to immediately launch the scheduler plan or save only the definition
- **Role** - only users with the roles selected here and the administrator will be able to run the defend AI rules The selected „time frame" also affects the prediction period. If we choose "time frame = monthly", we will be able to predict a one month ahead from the moment of prediction (according to the "prediction cycle" value)

CHAPTER 47

Screen content for the Trend algorithm



Algorithm:

Trend

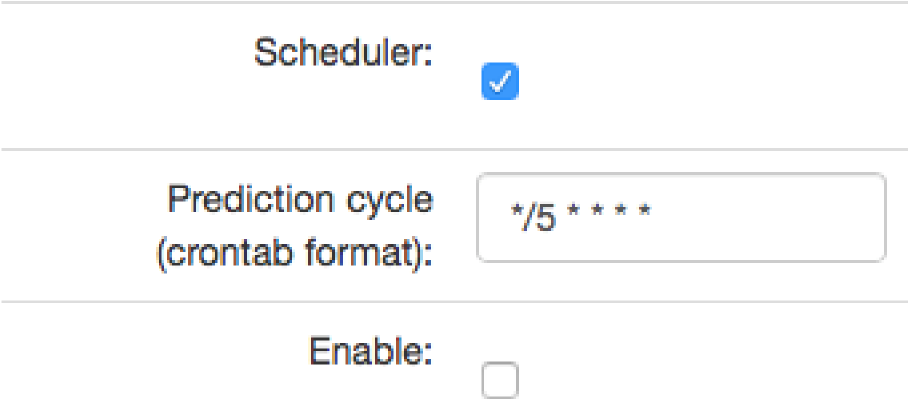
Choose search:

Uslugi_WWW_with_cols

AI Rule Name:	rpa_trend
Feature to analyse (from search):	perf_data./
Time frame:	Day
Value type:	Average
Max probes:	10
Max predictions:	20
Data limit:	10000
Start date:	2018-03-01
Threshold:	-1
Scheduler:	☐
Role:	admin ALL_test

Description of controls:

- **feature to analyze from search** - analyzed feature (dictated)
- **multiply by field** - enable multiplication of algorithms after unique values of the feature indicated here. Multiplication allows you to run the AI rule one for e.g. all servers. The value "none" in this field means no multiplication.
- **multiply by values** - if a trait is indicated in the „multiply by field", then unique values of this trait will appear in this field. Multiplications will be made for the selected values. If at least one of value is not selected, the „Run" buttons will be inactive.'
- **time frame** - feature aggregation method (1 minute, 5 minute, 15 minute, 30 minute, hourly, weekly, monthly, 6 months, 12 months)
- **max probes** - how many samples back will be taken into account for analysis. A single sample is an aggregated data according to the aggregation method.
- **value type** - which values to take into account when aggregating for a given time frame (e.g. maximum from time frame, minimum, average)
- **max predictions** - how many estimates we make for ahead (we take time frame)
- **data limit** - limits the amount of date downloaded from the source. It speeds up processing but reduces its quality
- **start date** - you can set a date earlier than the current date in order to verify how the selected algorithm would work on historical data
- **Scheduler** - a tag if the rule should be run according to the plan for the scheduler. If selected, additional fields will appear;



Scheduler: ☑

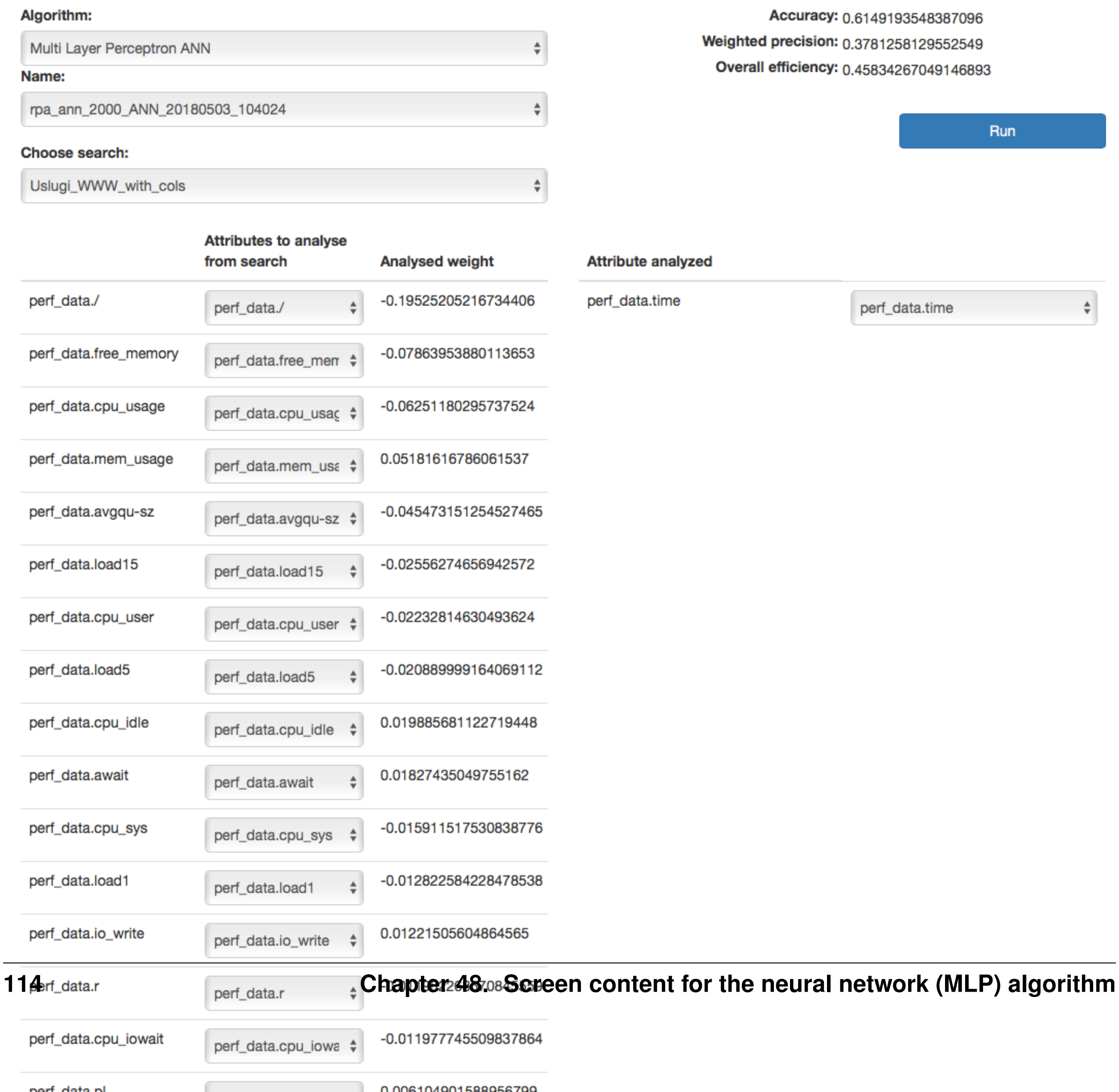
Prediction cycle (crontab format): */5 * * * *

Enable: □

- **Prediction cycle** - plan definition for the scheduler, i.e. the cycle in which the prediction rule is run (e.g. once a day, every hour, once a week). In the field, enter the command that complies with the cron standard. Enable – whether to immediately launch the scheduler plan or save only the definition
- **Role** - only users with the roles selected here and the administrator will be able to run the defend AI rules The selected „time frame" also affects the prediction period. If we choose "time frame = monthly", we will be able to predict a one month ahead from the moment of prediction (according to the "prediction cycle" value)
- **Threshold** - default values -1 (do not search). Specifies the algorithm what level of exceeding the value of the feature „feature to analyze from cheese" is to look for. The parameter currently used only by the "Trend" algorithm.

CHAPTER 48

Screen content for the neural network (MLP) algorithm



Algorithm: Multi Layer Perceptron ANN

Name: rpa_ann_2000_ANN_20180503_104024

Choose search: Uslugi_WWW_with_cols

Accuracy: 0.6149193548387096

Weighted precision: 0.3781258129552549

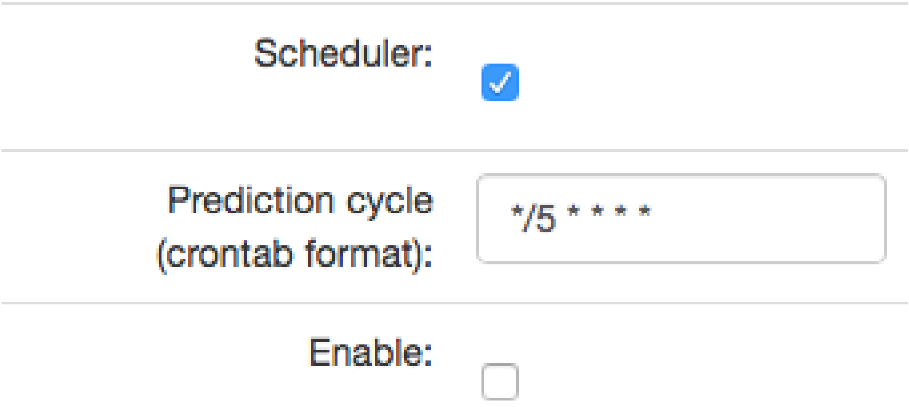
Overall efficiency: 0.45834267049146893

	Attributes to analyse from search	Analysed weight
perf_data./	perf_data./	-0.19525205216734406
perf_data.free_memory	perf_data.free_mem	-0.07863953880113653
perf_data.cpu_usage	perf_data.cpu_usag	-0.06251180295737524
perf_data.mem_usage	perf_data.mem_usa	0.05181616786061537
perf_data.avgqu-sz	perf_data.avgqu-sz	-0.045473151254527465
perf_data.load15	perf_data.load15	-0.02556274656942572
perf_data.cpu_user	perf_data.cpu_user	-0.02232814630493624
perf_data.load5	perf_data.load5	-0.020889999164069112
perf_data.cpu_idle	perf_data.cpu_idle	0.019885681122719448
perf_data.await	perf_data.await	0.01827435049755162
perf_data.cpu_sys	perf_data.cpu_sys	-0.015911517530838776
perf_data.load1	perf_data.load1	-0.012822584228478538
perf_data.io_write	perf_data.io_write	0.01221505604864565
perf_data.r	perf_data.r	[illegible]
perf_data.cpu_iowait	perf_data.cpu_iowa	-0.011977745509837864
perf_data.pl		0.006104901588956799

Attribute analyzed	
perf_data.time	perf_data.time

Descriptions of controls:

- **Name** - name of the learned neural network
- **Choose search** - search defined in OP5 Log Analytics, which is used to select a set of data on which the rule of artificial intelligence will work
- **Below**, on the left, a list of attributes and their weights based on teaching ANN will be defined during the teaching. The user for each attribute will be able to indicate the field from the above mentioned search, which contain the values of the attribute and which will be analyzed in the algorithm. The presented list (for input and output attributes) will have a static and dynamic part. Static creation by presenting key with the highest weights. The key will be presented in the original form, i.e. perf_data./ The second part is a DropDown type list that will serve as a key update according to the user's naming. On the right side, the attribute will be examined in a given rule / pattern. Here also the user must indicate a specific field from the search. In both cases, the input and output are narrowed based on the search fields indicated in Choose search.
- **Data limit** - limits the amount of data downloaded from the source. It speeds up the processing, but reduces its quality.
- **Scheduler** - a tag if the rule should be run according to the plan or the scheduler. If selected, additional fields will appear:



Scheduler: ☑

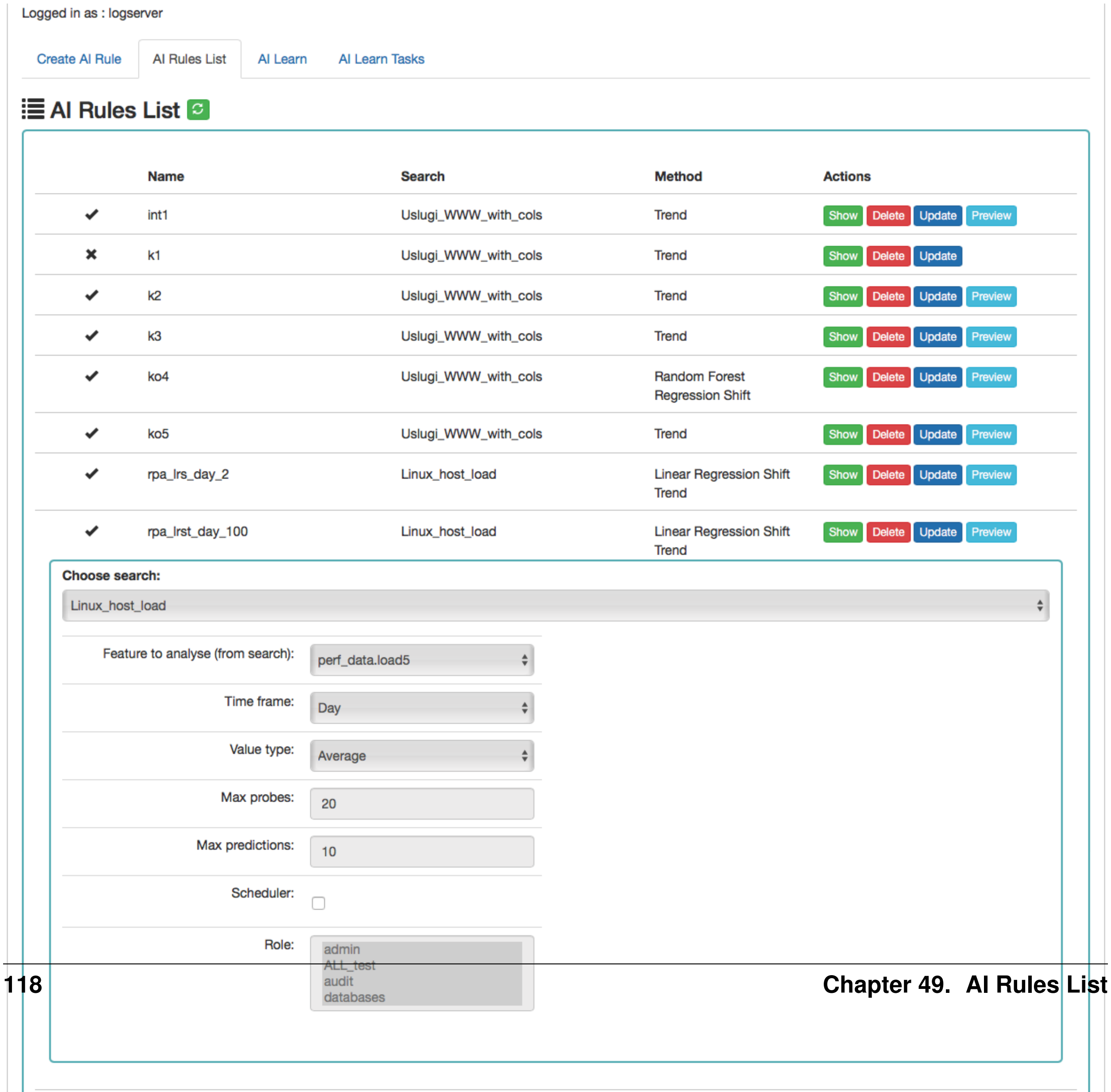
Prediction cycle (crontab format): */5 * * * *

Enable: □

- **Prediction cycle** - plan definition for the scheduler, i.e. the cycle in which the prediction rule is run (e.g. once a day, every hour, once a week). In the field, enter the command that complies with the *cron* standard
- **Enable** - whether to immediately launch the scheduler plan or save only the definition
- **Role** - only users with the roles selected here and the administrator will be able to run the defined AI rules

CHAPTER 49

AI Rules List



Logged in as : logserver

AI Rules List

	Name	Search	Method	Actions
✓	int1	Uslugi_WWW_with_cols	Trend	Show Delete Update Preview
✗	k1	Uslugi_WWW_with_cols	Trend	Show Delete Update
✓	k2	Uslugi_WWW_with_cols	Trend	Show Delete Update Preview
✓	k3	Uslugi_WWW_with_cols	Trend	Show Delete Update Preview
✓	ko4	Uslugi_WWW_with_cols	Random Forest Regression Shift	Show Delete Update Preview
✓	ko5	Uslugi_WWW_with_cols	Trend	Show Delete Update Preview
✓	rpa_lrs_day_2	Linux_host_load	Linear Regression Shift Trend	Show Delete Update Preview
✓	rpa_lrst_day_100	Linux_host_load	Linear Regression Shift Trend	Show Delete Update Preview

Choose search: Linux_host_load

Feature to analyse (from search): perf_data.load5

Time frame: Day

Value type: Average

Max probes: 20

Max predictions: 10

Scheduler: □

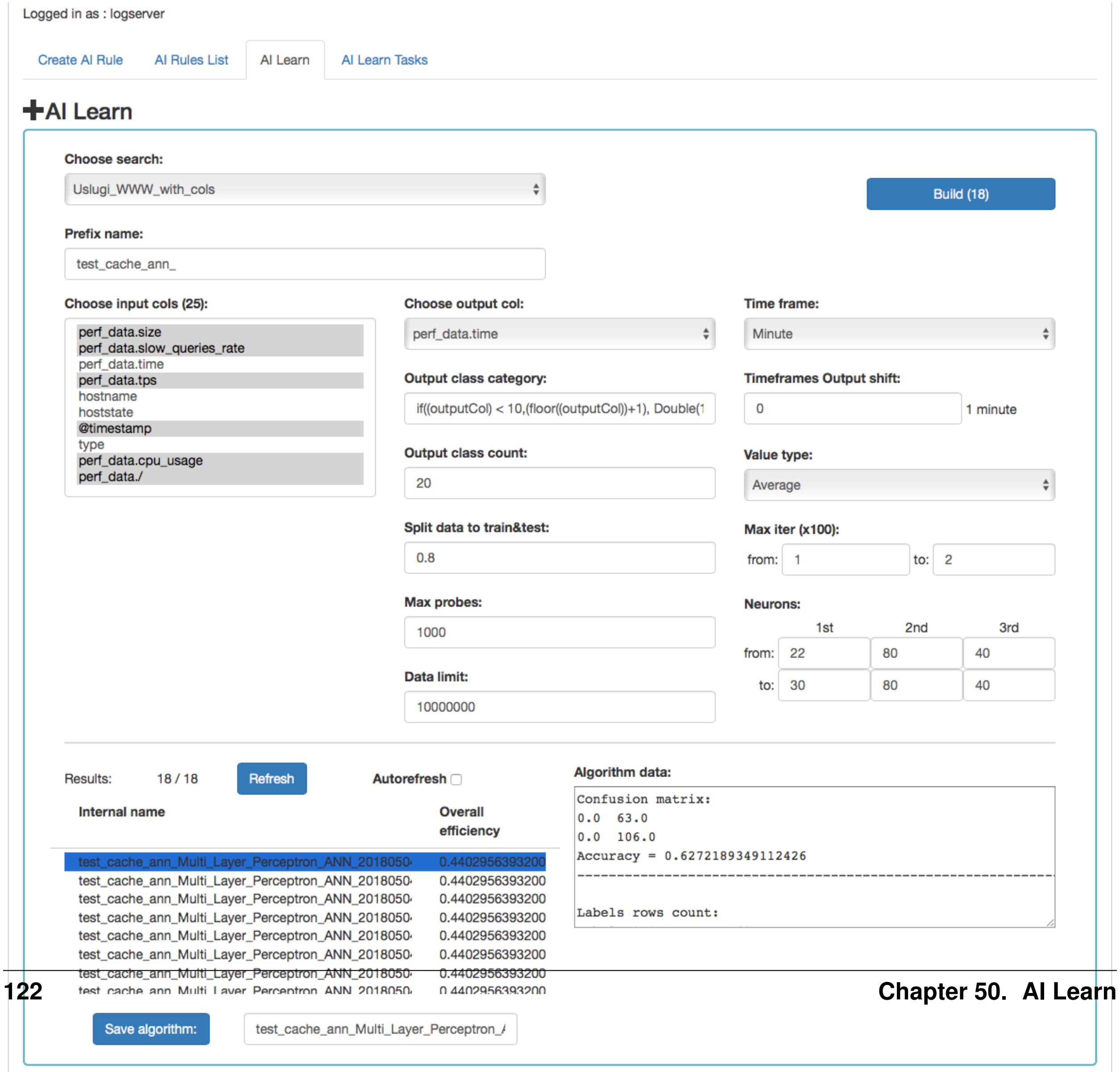
Role: admin, ALL_test, audit, databases

Column description:

- **Status**:
  - ◷ - the process is being processed (the pid of the process is in brackets)
  - ✔ - process completed correctly
  - ✖ - the process ended with an error
- **Name** - the name of the rule
- **Search** - the search on which the rule was run
- **Method** - an algorithm used in the AI rule
- **Actions** - allowed actions:
  - **Show** - preview of the rule definition
  - **Enable/Disable** - rule activation /deactivation
  - **Delete** - deleting the rule
  - **Update** - update of the rule definition
  - **Preview** - preview of the prediction results (the action is available after the processing has been completed correctly).

CHAPTER 50

AI Learn



Logged in as : logserver

✚AI Learn

Choose search: Uslugi_WWW_with_cols

Prefix name: test_cache_ann_

Choose input cols (25):

perf_data.size
perf_data.slow_queries_rate
perf_data.time
perf_data.tps
hostname
hoststate
@timestamp
type
perf_data.cpu_usage
perf_data./

Choose output col: perf_data.time

Output class category: if((outputCol) < 10,(floor((outputCol))+1), Double(1

Output class count: 20

Split data to train&test: 0.8

Max probes: 1000

Data limit: 10000000

Time frame: Minute

Timeframes Output shift: 0 1 minute

Value type: Average

Max iter (x100): from: 1 to: 2

Neurons:

	1st	2nd	3rd
from:	22	80	40
to:	30	80	40

Results: 18 / 18

Internal name	Overall efficiency
test_cache_ann_Multi_Layer_Perceptron_ANN_2018050	0.4402956393200
test_cache_ann_Multi_Layer_Perceptron_ANN_2018050	0.4402956393200
test_cache_ann_Multi_Layer_Perceptron_ANN_2018050	0.4402956393200
test_cache_ann_Multi_Layer_Perceptron_ANN_2018050	0.4402956393200
test_cache_ann_Multi_Layer_Perceptron_ANN_2018050	0.4402956393200
test_cache_ann_Multi_Layer_Perceptron_ANN_2018050	0.4402956393200
test_cache_ann_Multi_Layer_Perceptron_ANN_2018050	0.4402956393200
test_cache_ann_Multi_Layer_Perceptron_ANN_2018050	0.4402956393200

Algorithm data:

```
Confusion matrix:
0.0  63.0
0.0  106.0
Accuracy = 0.6272189349112426
------------------------------------------------------------

Labels rows count:
```

test_cache_ann_Multi_Layer_Perceptron_A

Description of controls:

- **Search** - a source of data for teaching the network
- **prefix name** - a prefix added to the id of the learned model that allows the user to recognize the model
- **Input cols** - list of fields that are analyzed / input features. Here, the column that will be selected in the output col should not be indicated. Only those columns that are related to processing should be selected. **
- **Output col** - result field, the recognition of which is learned by the network. **This field should exist in the learning and testing data, but in the production data is unnecessary and should not occur. This field cannot be on the list of selected fields in "input col".**
- **Output class category** - here you can enter a condition in SQL format to limit the number of output categories e.g. `if((outputCol) \< 10,(floor((outputCol))+1), Double(10))`. This condition limits the number of output categories to 10. **Such conditions are necessary for fields selected in "output col" that have continuous values. They must necessarily by divided into categories. In the Condition, use your own outputCol name instead of the field name from the index that points to the value of the "output col" attribute.**
- **Time frame** - a method of aggregation of features to improve their quality (e.g. 1 minute, 5 minutes, 15 minutes, 30 minutes, 1 hour, 1 daily).
- **Time frames output shift** - indicates how many time frame units to move the output category. This allows teaching the network with current attributes, but for categories for the future.
- **Value type** - which values to take into account when aggregating for a given time frame (e.g. maximum from time frame, minimum, average)
- **Output class count**- the expected number of result classes. **If during learning the network identifies more classes than the user entered, the process will be interrupted with an error, therefore it is better to set up more classes than less, but you have to keep in mind that this number affects the learning time.**
- **Neurons in first hidden layer (from, to)** - the number of neurons in the first hidden layer. Must have a value > 0. Jump every 1.
- **Neurons in second hidden layer (from, to)** - the number of neurons in second hidden layer. If = 0, then this layer is missing. Jump every 1.
- **Neurons in third hidden layer (from, to)** - the number of neurons in third hidden layer. If = 0 then this layer is missing. Jump every 1.
- **Max iter** (from, to) - maximum number of network teaching repetitions (the same data is used for learning many times in internal processes of the neural network). The slower it is. Jump every 100. The maximum value is 10, the default is 1.
- **Split data to train&test** - for example, the entered value of 0.8 means that the input data for the network will be divided in the ratio 0.8 to learning, 0.2 for the tests of the network learned.
- **Data limit** - limits the amount of data downloaded from the source. It speeds up the processing, but reduces its quality.
- **Max probes** - limits the number of samples taken to learn the network. Samples are already aggregated according to the selected "Time frame" parameter. It speed up teaching but reduces its quality.
- **Build** - a button to start teaching the network. The button contains the number of required teaching curses. You should be careful and avoid one-time learning for more than 1000 courses. It is better to divide them into several smaller ones. One pass after a full data load take about 1-3 minutes on a 4 core 2.4.GHz server. **The module has implemented the best practices related to the number of neurons in individual hidden layers. The values suggested by the system are optimal from the point of view of these practices, but the user can decide on these values himself.**

Under the parameters for learning the network there is an area in which teaching results will appear.

After pressing the “Refresh” button, the list of the resulting models will be refreshed.

Autorefresh - selecting the field automatically refreshes the list of learning results every 10s.

The following information will be available in the table on the left:

- **Internal name** - the model name given by the system, including the user - specified prefix
- **Overall efficiency** - the network adjustment indicator - allow to see at a glance whether it is worth dealing with the model. The grater the value, the better.

After clicking on the table row, detailed data collected during the learning of the given model will be displayed. This data will be visible in the box on the right.

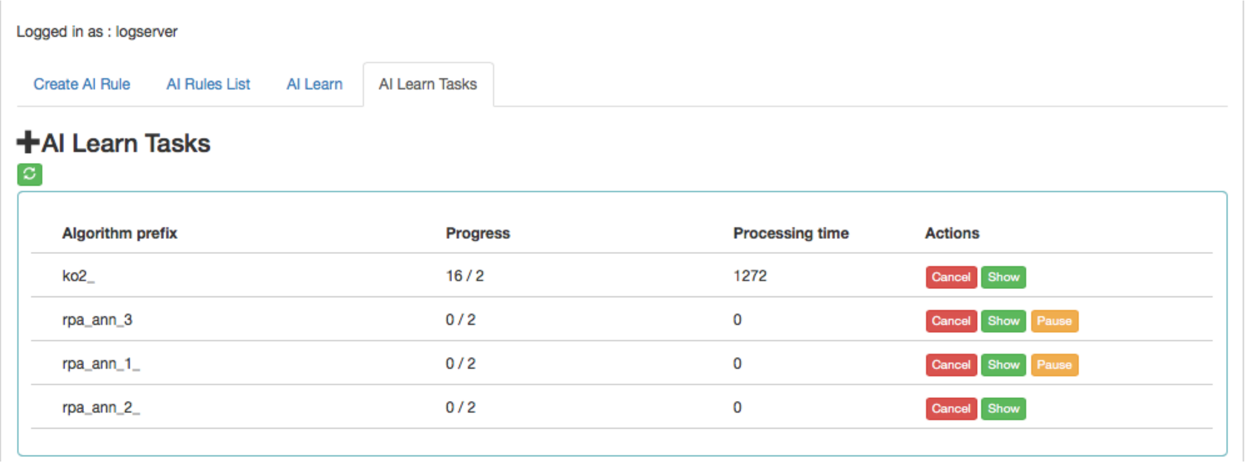
The selected model can be saved under its own name using the “Save algorithm” button. This saved algorithm will be available in the “Choose AI Rule” list when creating the rule (see Create AI Rule).

CHAPTER 51

AI Learn Tasks

The "AI Learn Task" tab shows the list of processes initiated teaching the ANN network with the possibility of managing processes.

Each user can see only the process they run. The user in the role of Intelligence sees all running processes.



Logged in as : logserver

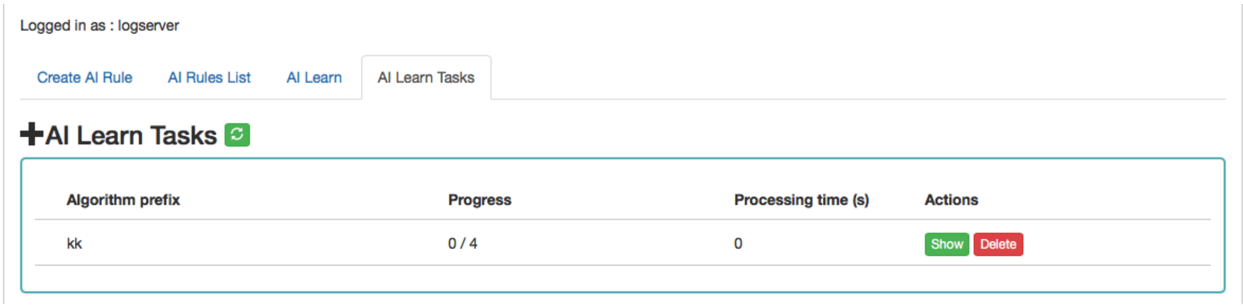
✚AI Learn Tasks

Algorithm prefix	Progress	Processing time	Actions
ko2_	16 / 2	1272	Cancel Show
rpa_ann_3	0 / 2	0	Cancel Show Pause
rpa_ann_1_	0 / 2	0	Cancel Show Pause
rpa_ann_2_	0 / 2	0	Cancel Show

Description of controls:

- **Algorithm prefix** - this is the value set by the user on the AI Learn screen in the Prefix name field
- **Progress** - here is the number of algorithms generated / the number of all to be generated
- **Processing time** - duration of algorithm generation in seconds (or maybe minutes or hours)
- **Actions**:
  - **Cancel** - deletes the algorithm generation task (user require confirmation of operation)
  - **Pause / Release** - pause / resume algorithm generation process.

AI Learn tab contain the Show in the preview mode of the ANN hyperparameters After completing the learning activity or after the user has interrupted it, the "Delete" button appears in "Action" field. This button allows you to permanently delete the learning results of a specific network.


Logged in as : logserver

✚AI Learn Tasks

Algorithm prefix	Progress	Processing time (s)	Actions
kk	0 / 4	0	Show Delete

CHAPTER 52

Scenarios of using algorithms implemented in the Intelligence module

1. Teaching MLP networks and choosing the algorithm to use:

   a. Go to the AI Learn tab,b. We introduce the network teaching parameters,c. Enter your own prefix for the names of the algorithms you have learned,d. Press Build,e. We observe the learned networks on the list (we can also stop the observation at any moment and go to other functions of the system. We will return to the learning results by going to the AI Learn Tasks tab and clicking the show action),f. We choose the best model from our point of view and save it under our own name,g. From this moment the algorithm is visible in the Create AI Rule tab.

2. Starting the MLP network algorithm:

   a. Go to the Create AI Rule tab and create rules,b. Select the previously saved model of the learned network,c. Specify parameters visible on the screen (specific to MLP),d. Press the Run button.

3. Starting regression algorithm:

   a. Go to the Create AI Rule tab and create rules,b. We choose AI Rule, e.g. Simple Moving Average, Linear Regression or Random Forest Regression, etc.,c. Enter your own rule name (specific to regression),d. Set the parameters of the rule (specific to regression),e. Press the Run button.

4. Management of available rules:

   a. Go to the AI Rules List tab,b. A list of AI rules available for our role is displayed,c. We can perform the actions available on the right for each rule.\

CHAPTER 53

Results of algorithms

The results of the “AI algorithms” are saved to the index „intelligence” specially created for this purpose. The index with the prediction result. These following fields are available in the index (where xxx is the name of the attribute being analyzed):

- **xxx_pre** - estimate value
- **xxx_cur** - current value at the moment of estimation
- **method_name** - name of the algorithm used
- **rmse** - avarage square error for the analysis in which _cur values were available. **The smaller the value, the better.**
- **rmse_normalized** - mean square error for the analysis in which _cur values were available, normalized with _pre values. **The smaller the value, the better.**
- **overall_efficiency** - efficiency of the model. **The greater the value, the better. A value less than 0 may indicate too little data to correctly calculate the indicator**
- **linear_function_a** - directional coefficient of the linear function y = ax + b. **Only for the Trend and Linear Regression Trend algorithm**
- **linear_function_b** - the intersection of the line with the Y axis for the linear function y = ax + b. **Only for the Trend and Linear Regression Trend algorithm.**

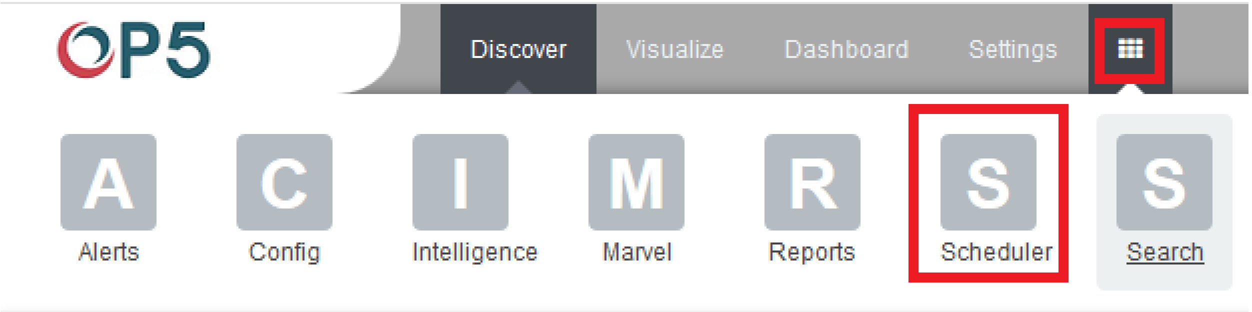
Visualization and signals related to the results of data analysis should be created from this index. The index should be available to users of the Intelligence module.

CHAPTER 54

Scheduler Module

OP5 Log Analytics has a built-in task schedule. In this module, we can define a command or a list of commands whose execution we instruct the application in the form of tasks. We can determine the time and frequency of tasks. Tasks can contain a simple syntax, but they can also be associated with modules, e.g. with Intelligence module.

To go to the Scheduler window, select the tile icon from the main menu bar and then go to the „Scheduler" icon (To go back, go to the „Search" icon)



The page with three tabs will be displayed: Creating new tasks in the „Create Scheduler Job", managing tasks in the „Job List" and checking the status of tasks in „Jobs Status"

In the window for creating new tasks we have a form consisting of fields:

- **Name** - in which we enter the name of the task
- **Cron Pattern** - a field in which in cron notation we define the time and frequency of the task
- **Command** - we give the syntax of the command that will be executed in this task. These can be simple system commands, but also complex commands related to the Intelligence module. In the task management window, we can activate /deactivate, delete and update the task by clicking on the selected icon for a given task Enable Delete Update

In the task status windows you can check the current status of the task: if it activated, when it started and when it ended, how long it took. This window is not editable and indicates historical data.

CHAPTER 55

Permission

Permission have been implemented in the following way:

- Only the user in the admin role can create / update rules.
- When creating rules, the roles that will be able to enables / disengage / view the rules will be indicated.

We assume that the Learn process works as an administrator.

We assume that the visibility of Search in AI Learn is preceded by receiving the search permission in the module object permission.

The role of “Intelligence” launches the appropriate tabs.

An ordinary user only sees his models. The administrator sees all models.

CHAPTER 56

Verification of Elasticsearch service

To verify of Elasticsearch service you can use following command:

- Control of the Elastisearch system service via **systemd**: `# sysetmctl status elasticsearch` output:

```
  `elasticsearch.service - Elasticsearch`
  `Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor␣
↪preset: disabled)`
  `Active: active (running) since Fri 2017-09-01 10:36:52 CEST; 3h 7min ago`
   `Docs: http://www.elastic.co`
  `Main PID: 8362 (java)`
  `CGroup: /system.slice/elasticsearch.service`
         `└─8362 /bin/java -Xms256m -Xmx1g -Djava.awt.headless=true`
```

- Control of Elasticsearch instance via **tcp port**:

`# curl -XGET '127.0.0.1:9200/'`

output:

```
`{`
`  "name" : "Henry Peter Gyrich",`
 ` "cluster_name" : "elasticsearch",`
  `"version" : {`
   ` "number" : "2.3.5",`
    `"build_hash" : "90f439ff60a3c0f497f91663701e64ccd01edbb4",`
    `"build_timestamp" : "2016-07-27T10:36:52Z",`
    `"build_snapshot" : false,`
    `"lucene_version" : "5.5.0"`
  `},`
  `"tagline" : "You Know, for Search"`
`}`
```

- Control of Elasticsearch instance via **log file**:

  `# tail -f /var/log/elasticsearch/elasticsearch.log`

- other control commands via ***curl* application**:

```
`curl -xGET "http://localhost:9200/_cat/health?v"`
`curl -XGET "http://localhost:9200/_cat/nodes?v"`
`curl -XGET "http://localhost:9200/_cat/indicates"`
```

CHAPTER 57

Verification of Logstash service

To verify of Logstash service you can use following command:

- control Logstash service via **systemd**:

```
# systemctl status logstash
```

output:

```
`logstash.service - logstash`
   `Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset:␣
↪disabled)`
   `Active: active (running) since Wed 2017-07-12 10:30:55 CEST; 1 months 23 days ago`
 `Main PID: 87818 (java)`
   `CGroup: /system.slice/logstash.service`
          `└─87818 /usr/bin/java -XX:+UseParNewGC -XX:+UseConcMarkSweepGC`
```

- control Logstash service via **port tcp**:

```
# curl -XGET '127.0.0.1:9600'
```

output:

```
`{`
   `"host": "skywalker",`
   `"version": "4.5.3",`
   `"http_address": "127.0.0.1:9600"`
`}`
```

- control Logstash service via **log file**:

```
# tail -f /var/log/logstash/logstash-plain.log
```

Debuging:

- dynamically update logging levels through the logging API (service restart not needed):

```
        curl -XPUT 'localhost:9600/_node/logging?pretty' -H 'Content-Type:␣
↪application/json' -d'
        {
            "logger.logstash.outputs.elasticsearch" : "DEBUG"
        }
```

- permanent change of logging level (service need to be restarted):
- edit file */etc/logstash/logstash.yml* and set the following parameter:

```
    *`log.level: debug`*
```

  – restart `logstash` service:

    systemctl restart logstash

- checking correct syntax of configuration files:

  /usr/share/logstash/bin/logstash -tf /etc/logstash/conf.d

- get information about load of the Logstash:

  # curl -XGET '127.0.0.1:9600/_node/jvm?pretty=true'

output:

```
    {
       "host" : "iosssmes1",
       "version" : "5.4.3",
       "http_address" : "100.127.111.14:9600",
       "id" : "defdfe2f-2f5a-4c7e-ae03-e163e550bdb0",
       "name" : "iosssmes1",
       "jvm" : {
         "pid" : 3535,
         "version" : "1.8.0_131",
         "vm_name" : "OpenJDK 64-Bit Server VM",
         "vm_version" : "1.8.0_131",
         "vm_vendor" : "Oracle Corporation",
         "start_time_in_millis" : 1503057722599,
         "mem" : {
           "heap_init_in_bytes" : 268435456,
           "heap_max_in_bytes" : 1038876672,
           "non_heap_init_in_bytes" : 2555904,
           "non_heap_max_in_bytes" : 0
         },
         "gc_collectors" : [ "ParNew", "ConcurrentMarkSweep" ]
       }
```

CHAPTER 58

Verificatoin of OP5 Log Analytics GUI service

To verify of OP5 Log Analytics GUI service you can use following command:

- control the OP5 Log Analytics GUI service via **systemd**:

```
  `# systemctl status kibana`
```

output:

```
`kibana.service - no description given`
   `Loaded: loaded (/usr/lib/systemd/system/kibana.service; enabled; vendor preset:␣
↪disabled)`
   `Active: active (running) since Fri 2017-09-01 10:39:46 CEST; 2 days ago`
   `Main PID: 8527 (node)`
   `CGroup: /system.slice/kibana.service`
           `└─8527 /opt/kibana/bin/../node/bin/node /opt/kibana/bin/../src/cl`
```

- control the OP5 Log Analytics GUI via **port tcp**:

```
  `# curl -XGET '127.0.0.1:5601/'`
```

output:

```
  `<script>var hashRoute = '/app/kibana';`
  `var defaultRoute = '/app/kibana';`
  `var hash = window.location.hash;`
  `if (hash.length) {`
  `  window.location = hashRoute + hash;`
  `} else {`
  `  window.location = defaultRoute;`
  `}</script>`
```

- Control the OP5 Log Analytics GUI via **log file**:

```
  `# tail -f /var/log/messages`
```

CHAPTER 59

Node roles

Every instance of Elasticsearch server is called a *node*. A collection of connected nodes is called a *cluster*. All nodes know about all the other nodes in the cluster and can forward client requests to the appropriate node. Besides that, each node serves one or more purpose:

- Master-eligible node - A node that has node.master set to true (default), which makes it eligible to be elected as the master node, which controls the cluster
- Data node - A node that has node.data set to true (default). Data nodes hold data and perform data related operations such as CRUD, search, and aggregations
- Client node - A client node has both node.master and node.data set to false. It can neither hold data nor become the master node. It behaves as a "smart router" and is used to forward cluster-level requests to the master node and data-related requests (such as search) to the appropriate data nodes
- Tribe node - A tribe node, configured via the tribe.* settings, is a special type of client node that can connect to multiple clusters and perform search and other operations across all connected clusters.

CHAPTER 60

Naming convention

Elasticsearch require litte configuration before before goint into work. The following settings must be considered before going to production:

- **path.data** and **path.logs** - default locations of these files are:

  `/var/lib/elasticsearch` and `/var/log/elasticsearch`.

- **cluster.name** - A node can only join a cluster when it shares its `cluster.name` with all the other nodes in the cluster. The default name is "elasticsearch", but you should change it to an appropriate name which describes the purpose of the cluster. You can do this in `/etc/elasticsearch/elasticsearch.yml` file.
- **node.name** - By default, Elasticsearch will use the first seven characters of the randomly generated UUID as the node id. Node id is persisted and does not change when a node restarts. It is worth configuring a more human readable name: `node.name:  prod-data-2` in file `/etc/elstaicsearch/elasticsearch.yml`
- **network.host** - parametr specifying network interfaces to which Elasticsearch can bind. Default is `network.host:  ["_local_","_site_"]`.
- **discovery** - Elasticsearch uses a custom discovery implementation called "Zen Discovery". There are two important settings:
  - `discovery.zen.ping.unicast.hosts` - specify list of other nodes in the cluster that are likely to be live and contactable;
  - `discovery.zen.minimum_master_nodes` - to prevent data loss, you can configure this setting so that each master-eligible node knows the minimum number of master-eligible nodes that must be visible in order to form a cluster.
- **heap size** - By default, Elasticsearch tells the JVM to use a heap with a minimum (Xms) and maximum (Xmx) size of 1 GB. When moving to production, it is important to configure heap size to ensure that Elasticsearch has enough heap available

CHAPTER 61

Config files

To configure the Elstaicsearch cluster you must sprecify some parameters in the following configuration files on every node that will be connceted to the cluster:

- `/etc/elsticsearch/elasticserach.yml`:

  ```
  - `cluster.name:name_of_the_cluster` - same for every node;
  - `node.name:name_of_the_node` - uniq for every node;
  - `node.master:true_or_false`
  - `node.data:true_or_false`
  - `network.host:["_local_","_site_"]`
  - `discovery.zen.ping.multicast.enabled`
  - `discovery.zen.ping.unicast.hosts`
  - `index.number_of_shards`
  ```

  - `index.number_of_replicas`

- `/etc/elsticsearch/logging.yml`:

  `logger: action: DEBUG` - for easier debuging.

CHAPTER 62

Example setup

Example of the Elasticsearch cluster configuration:

- file `/etc/elasticsearch/elasticsearch.yml`:

  cluster.name: tm-lab node.name: “elk01” node.master: true‘*node.data: true network.host: 127.0.0.1,10.0.0.4 http.port: 9200 discovery.zen.ping.multicast.enabled: false discovery.zen.ping.unicast.hosts: [“10.0.0.4:9300”,”10.0.0.5:9300”,”10.0.0.6:9300”] index.number_of_shards: 3 index.number_of_replicas: 1

- to start the Elasticsearch cluster execute command:

```
# systemctl restart elasticsearch`
```

- to check status of the Elstaicsearch cluster execute command:

  - check of the Elasticsearch cluster nodes status via tcp port:

```
 # curl -XGET '127.0.0.1:9200/_cat/nodes?v'
 host              ip           heap.percent ram.percent load node.role␣
↪master name
 10.0.0.4     10.0.0.4     18           91          0.00 -         -     ␣
↪elk01
 10.0.0.5     10.0.0.5     66           91          0.00 d         *    ␣
↪elk02
 10.0.0.6     10.0.0.6     43           86              0.65 d         m     ␣
↪elk03
 10.0.0.7     10.0.0.7     45           77              0.26 d         m     ␣
↪elk04
```

  - check status of the Elasticsearch cluster via log file:\

```
tail -f /var/log/elasticsearch/tm-lab.log (cluster.name)
```

CHAPTER 63

Integration with AD

You can configure the OP5 Log Analytics to communicate with Active Directory to authenticate users. To integrate with Active Directory, you configure an Active Directory realm and assign Active Directory users and groups to the OP5 Log Analytics roles in the role mapping file.

To protect passwords, communications between the OP5 Log Analytics and the LDAP server should be encrypted using SSL/TLS. Clients and nodes that connect via SSL/TLS to the LDAP server need to have the LDAP server's certificate or the server's root CA certificate installed in their keystore or truststore.

CHAPTER 64

AD configuration

The AD configuration should be done in the `/etc/elasticsearch/elasticsearch.yml` file.

Below is a list of settings to be made in the elasticsearch.yml file (the commented section in the file in order for the AD settings to start working, this fragment should be uncommented):

```
|**Direcitve**                                          | **Description**                                   ␣
↪                          |
| -------------------------------------------------------|------------------------------
↪----------------------------------------------------------|
| # LDAP                                                |                                                   ␣
↪                          |
| #ldaps:                                               |                                                   ␣
↪                          |
| # - name: \"example.com\"                             |# domain that is configured                        ␣
↪                          |
| # host: \"127.0.0.1,127.0.0.2\"                       |# list of server for this domain                   ␣
↪                          |
| # port: 389                                           |# optional, default 389 for␣
↪unencrypted session or 636 for encrypted sessions      |
|# ssl\_enabled: false                                  |# optional, default true                           ␣
↪                          |
|# ssl\_trust\_all\_certs: true                         |# optional, default false                          ␣
↪                          |
|# ssl.keystore.file: \"path\"                          |# path to the truststore store                     ␣
↪                          |
|# ssl.keystore.password: \"path\"                      |# password to the trusted␣
↪certificate store                      |
|# bind\_dn: [[admin\@example.com]                      |# account name administrator                       ␣
↪                          |
|# bind\_password: \"password\"                         |# password for the administrator␣
↪account                       |
|# search\_user\_base\_DN: \"OU=lab,DC=example,DC=com\" |# search for the DN user␣
↪tree database                          |
|# user\_id\_attribute: \"uid                           |# search for a user attribute␣
↪optional, by default \"uid\"                              |
```

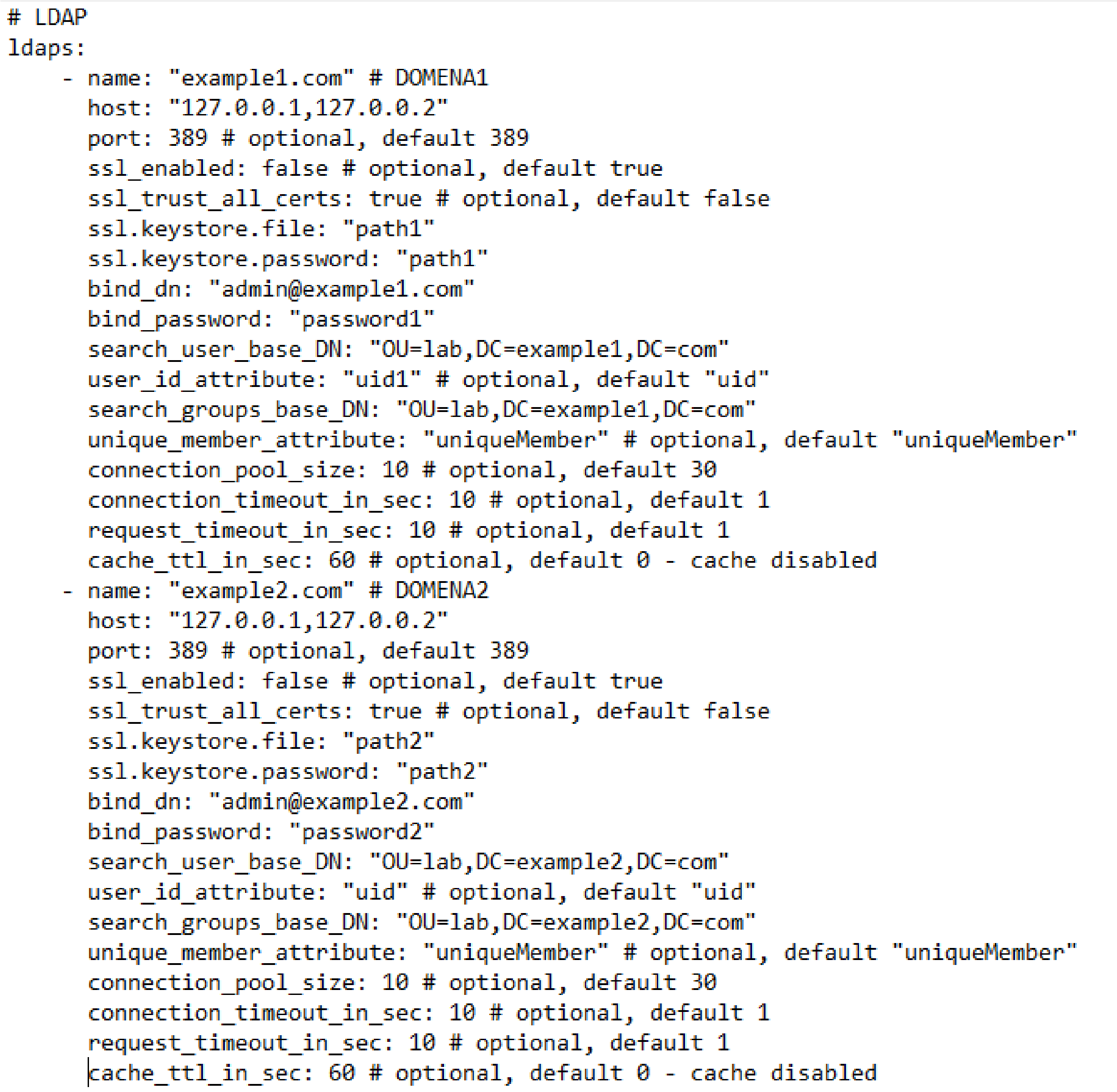
(continues on next page)

(continued from previous page)

```
|# search\_groups\_base\_DN:\"OU=lab,DC=example,DC=com\"|# group database search.␣
↪This is a catalog main, after which the groups will be sought.|
|# unique\_member\_attribute: \"uniqueMember\"      |# optional, default\
↪"uniqueMember\"                                  |
|# connection\_pool\_size: 10                      |# optional, default 30        ␣
↪                     |
|# connection\_timeout\_in\_sec: 10                    |# optional, default 1       ␣
↪                         |
|# request\_timeout\_in\_sec: 10                       |# optional, default 1       ␣
↪                         |
|# cache\_ttl\_in\_sec: 60                             |# optional, default 0 -␣
↪cache disabled                         |
```

If we want to configure multiple domains, then in this configuration file we copy the # LDAP section below and configure it for the next domain.

Below is an example of how an entry for 2 domains should look like. (It is important to take the interpreter to read these values correctly).



```
# LDAP
ldaps:
    - name: "example1.com" # DOMENA1
      host: "127.0.0.1,127.0.0.2"
      port: 389 # optional, default 389
      ssl_enabled: false # optional, default true
      ssl_trust_all_certs: true # optional, default false
      ssl.keystore.file: "path1"
      ssl.keystore.password: "path1"
      bind_dn: "admin@example1.com"
      bind_password: "password1"
      search_user_base_DN: "OU=lab,DC=example1,DC=com"
      user_id_attribute: "uid1" # optional, default "uid"
      search_groups_base_DN: "OU=lab,DC=example1,DC=com"
      unique_member_attribute: "uniqueMember" # optional, default "uniqueMember"
      connection_pool_size: 10 # optional, default 30
      connection_timeout_in_sec: 10 # optional, default 1
      request_timeout_in_sec: 10 # optional, default 1
      cache_ttl_in_sec: 60 # optional, default 0 - cache disabled
    - name: "example2.com" # DOMENA2
      host: "127.0.0.1,127.0.0.2"
      port: 389 # optional, default 389
      ssl_enabled: false # optional, default true
      ssl_trust_all_certs: true # optional, default false
      ssl.keystore.file: "path2"
      ssl.keystore.password: "path2"
      bind_dn: "admin@example2.com"
      bind_password: "password2"
      search_user_base_DN: "OU=lab,DC=example2,DC=com"
      user_id_attribute: "uid" # optional, default "uid"
      search_groups_base_DN: "OU=lab,DC=example2,DC=com"
      unique_member_attribute: "uniqueMember" # optional, default "uniqueMember"
      connection_pool_size: 10 # optional, default 30
      connection_timeout_in_sec: 10 # optional, default 1
      request_timeout_in_sec: 10 # optional, default 1
      cache_ttl_in_sec: 60 # optional, default 0 - cache disabled
```

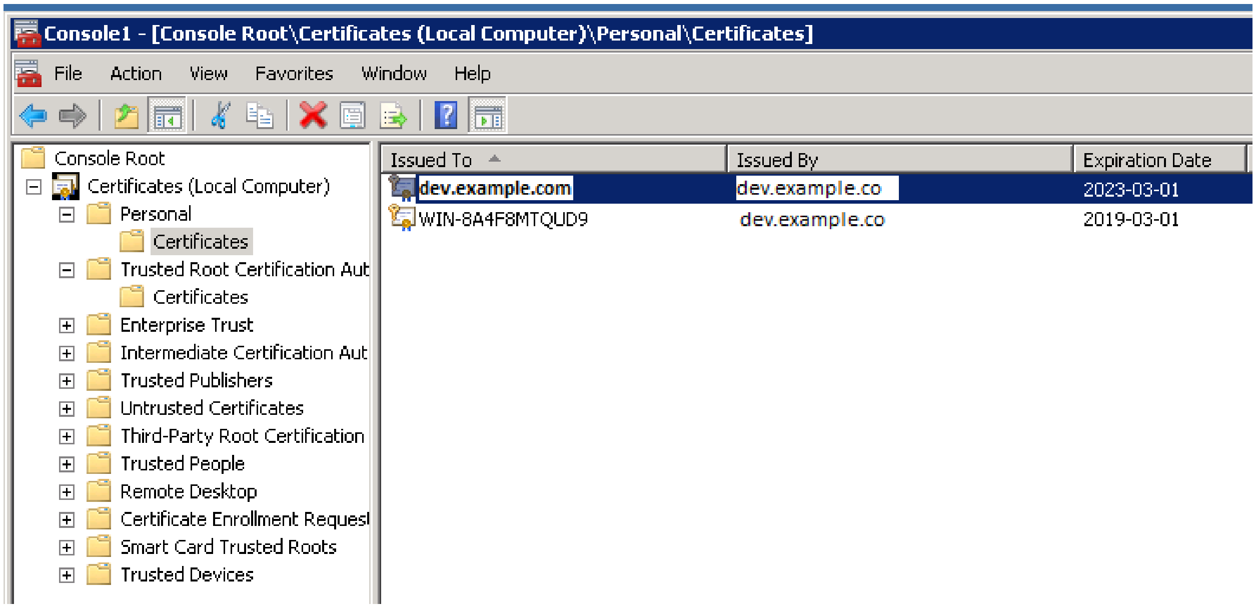
After completing the LDAP section entry in the `elasticsearch.yml` file, save the changes and restart the service with the command:

```
# systemctl restart elasticsearch
```

CHAPTER 65

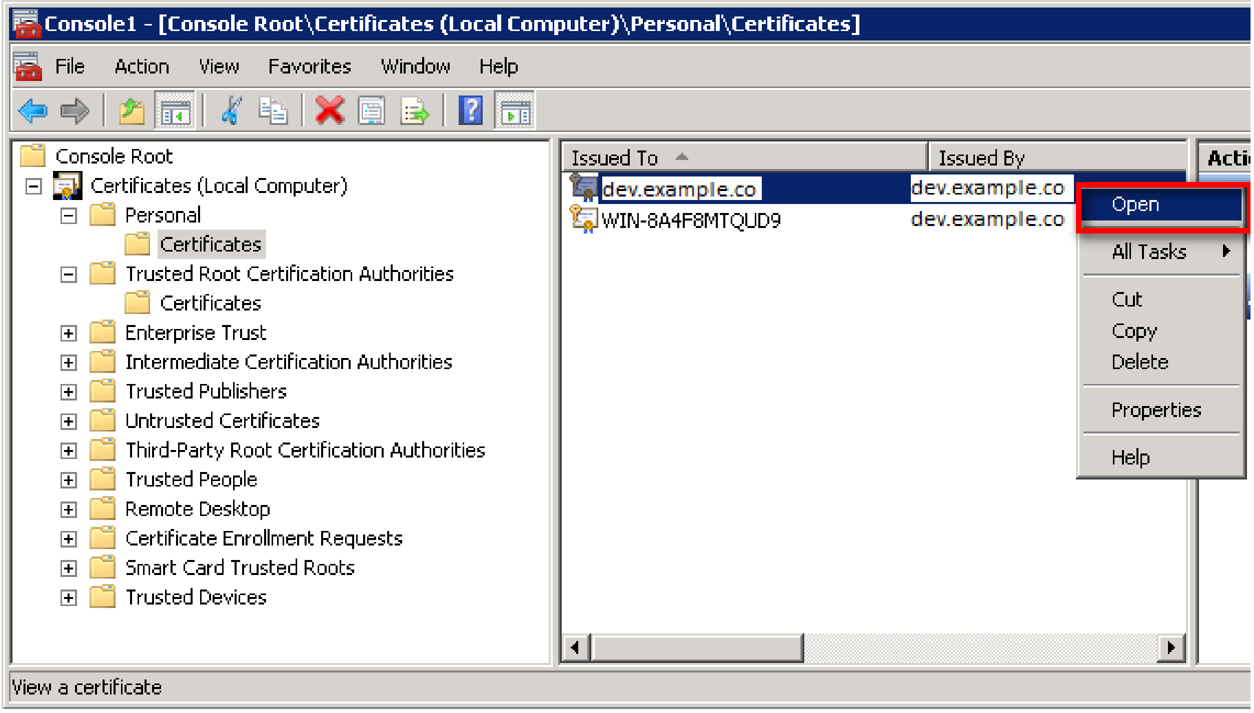
Configure SSL suport for AD authentication.

1. Open the certificate manager on the AD server.


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Aut
Certificates
Enterprise Trust
Intermediate Certification Aut
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification
Trusted People
Remote Desktop
Certificate Enrollment Request
Smart Card Trusted Roots
Trusted Devices

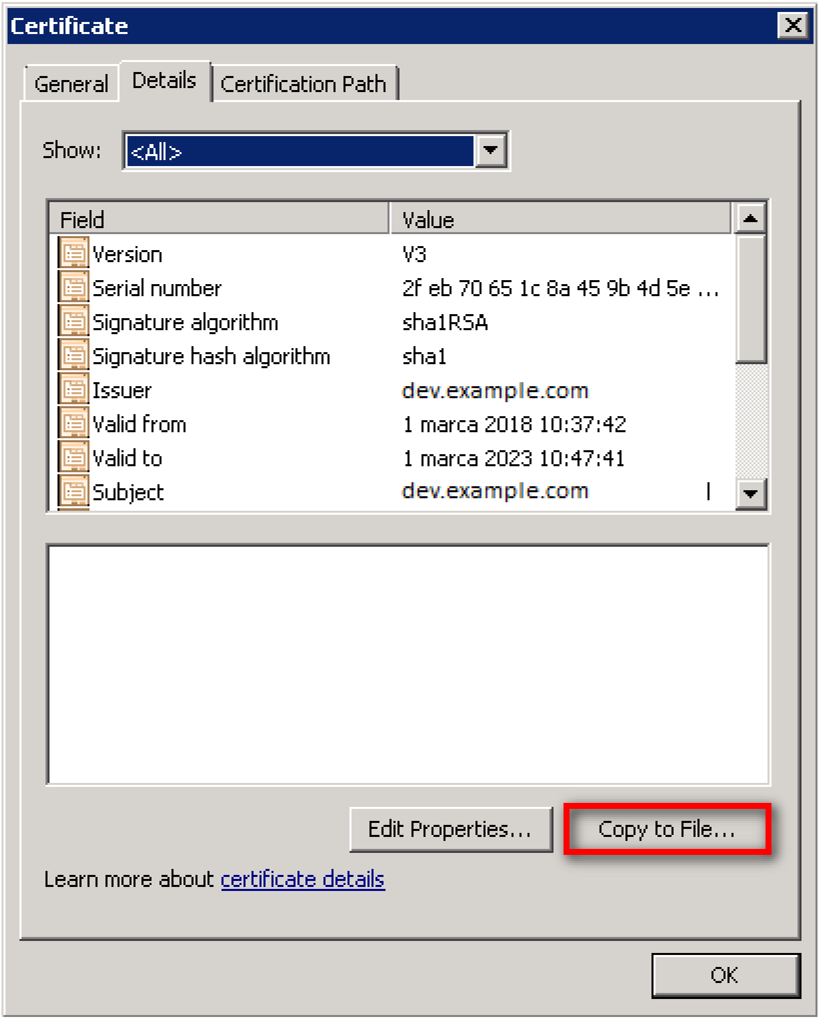
Issued To	Issued By	Expiration Date
dev.example.com	dev.example.co	2023-03-01
WIN-8A4F8MTQUD9	dev.example.co	2019-03-01

1. Select the certificate and open it



Issued To	Issued By
dev.example.co	dev.example.co
WIN-8A4F8MTQUD9	dev.example.co

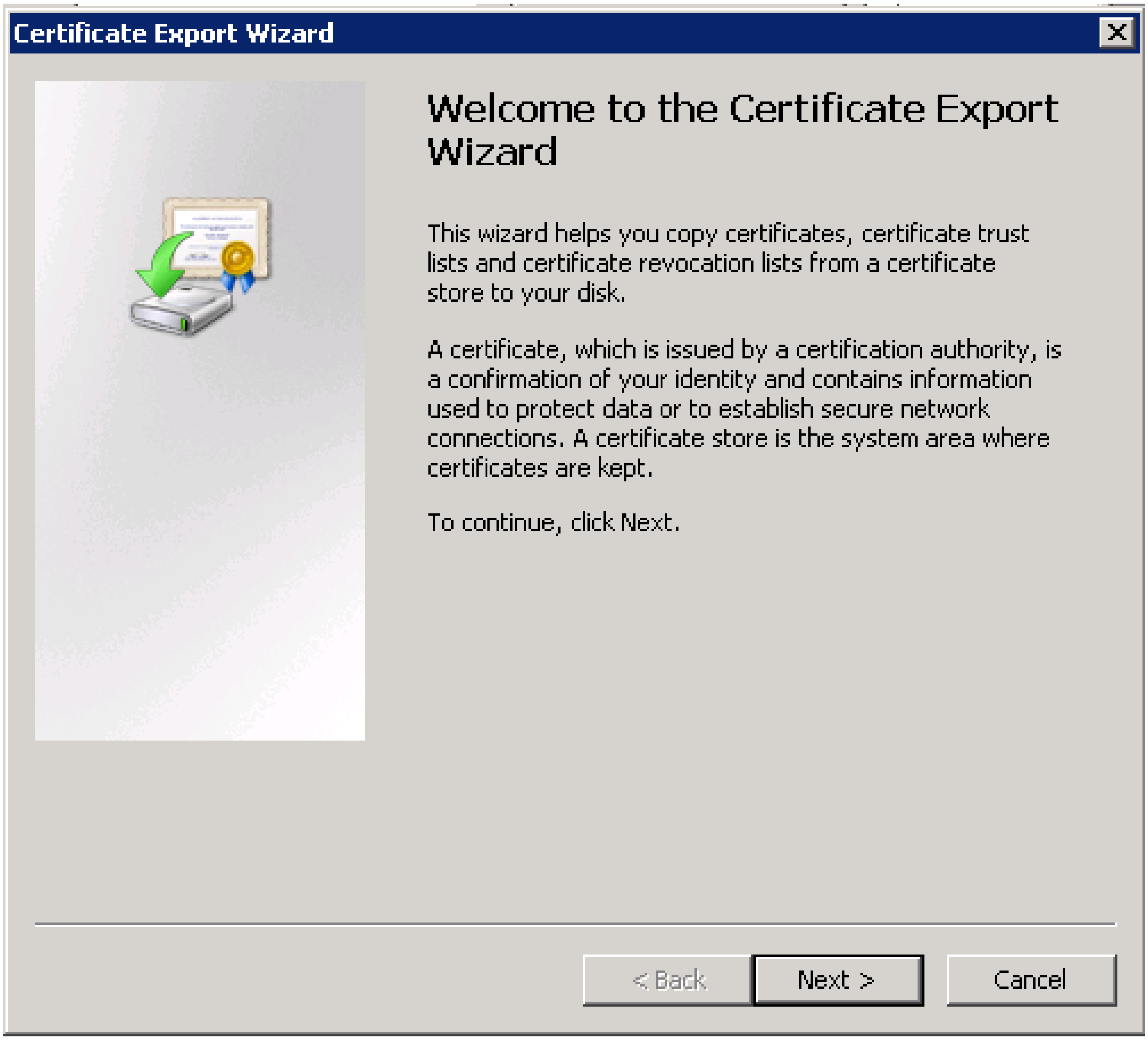
1. Select the option of copying to a file in the Details tab



Field	Value
Version	V3
Serial number	2f eb 70 65 1c 8a 45 9b 4d 5e …
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	dev.example.com
Valid from	1 marca 2018 10:37:42
Valid to	1 marca 2023 10:47:41
Subject	dev.example.com

Learn more about certificate details

1. Click the Next button



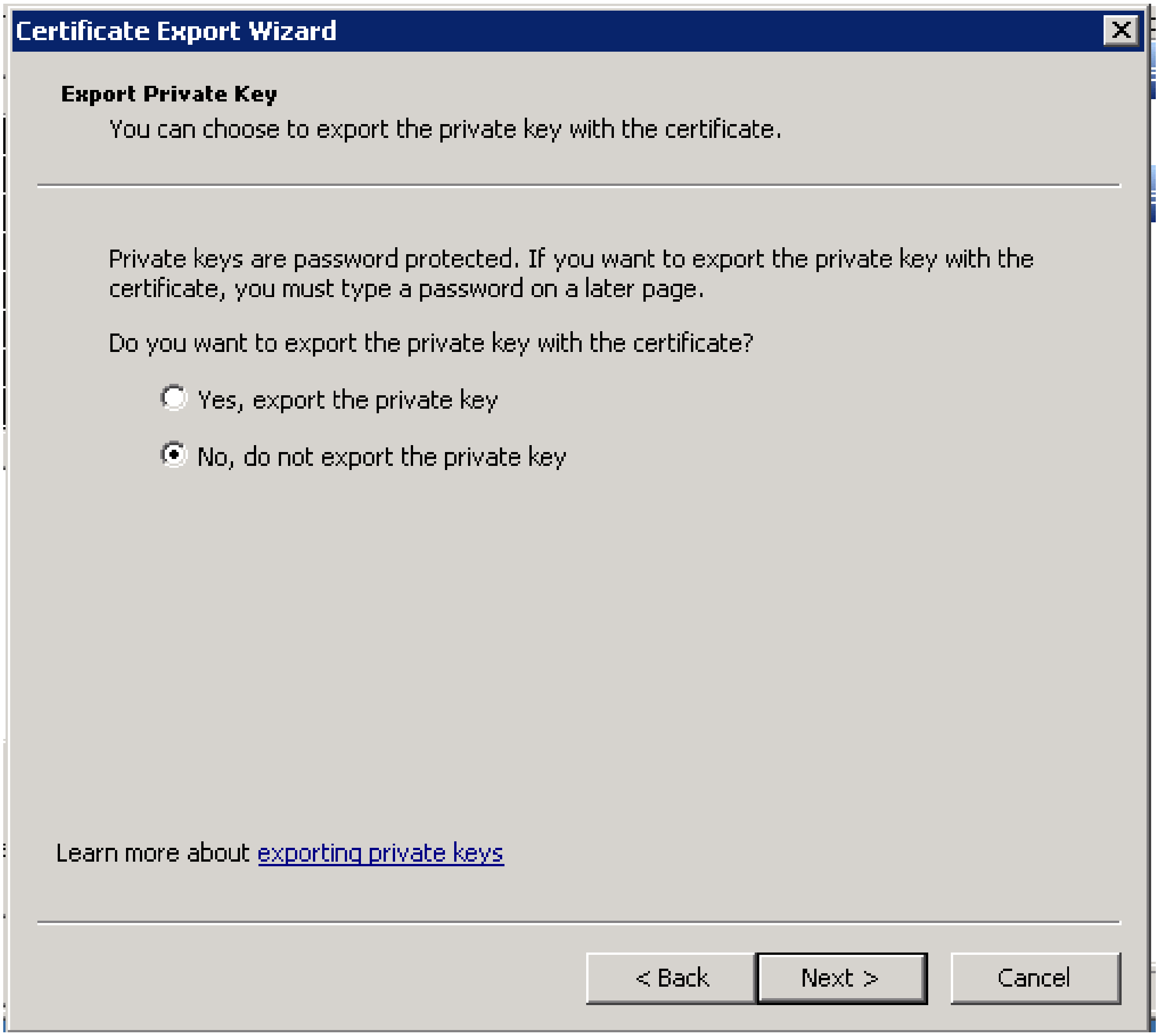
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

1. Keep the setting as shown below and click Next



Certificate Export Wizard

Export Private Key

You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

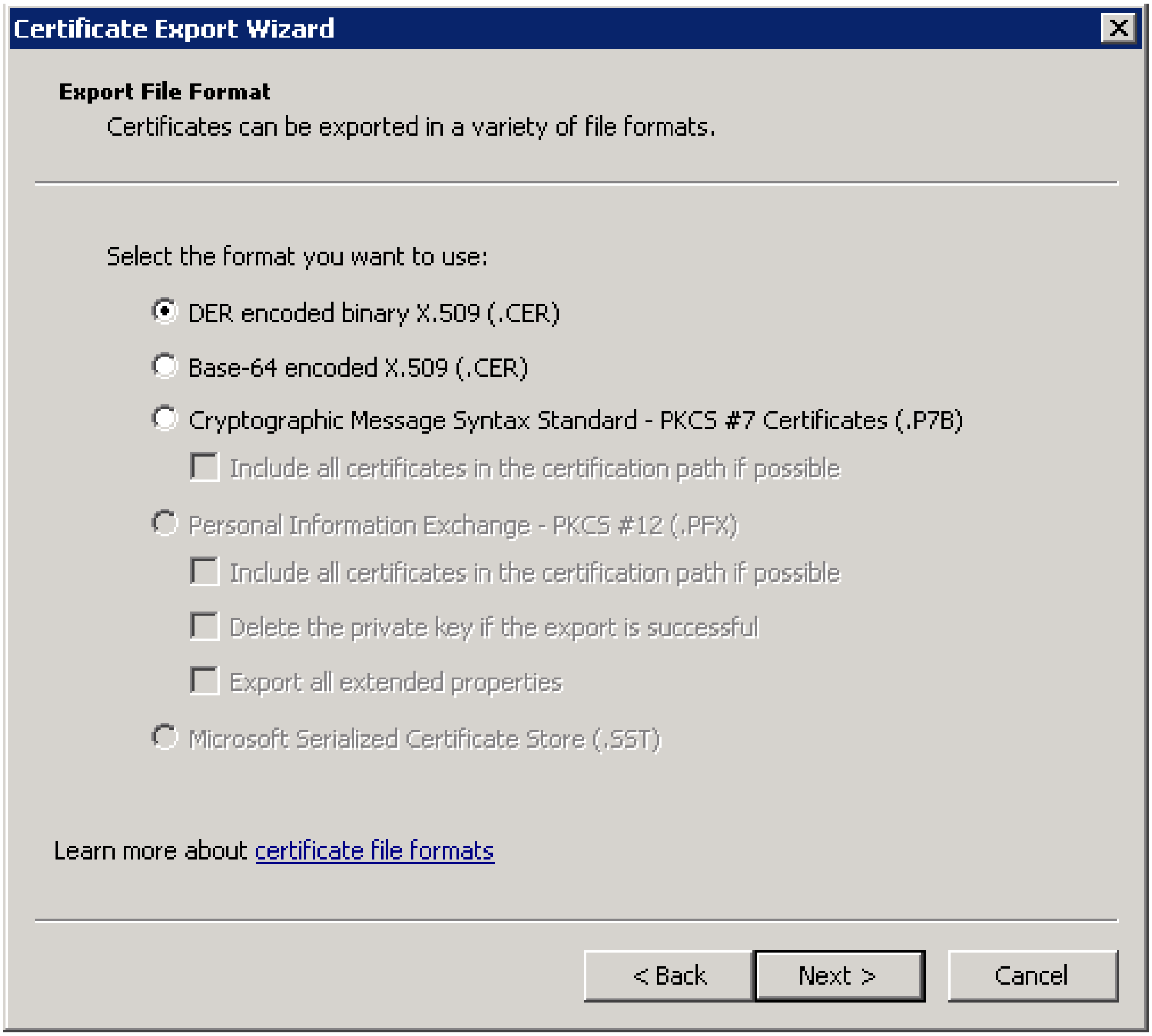
Do you want to export the private key with the certificate?

○ Yes, export the private key

● No, do not export the private key

Learn more about exporting private keys

1. Keep the setting as shown below and click Next.



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

● DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

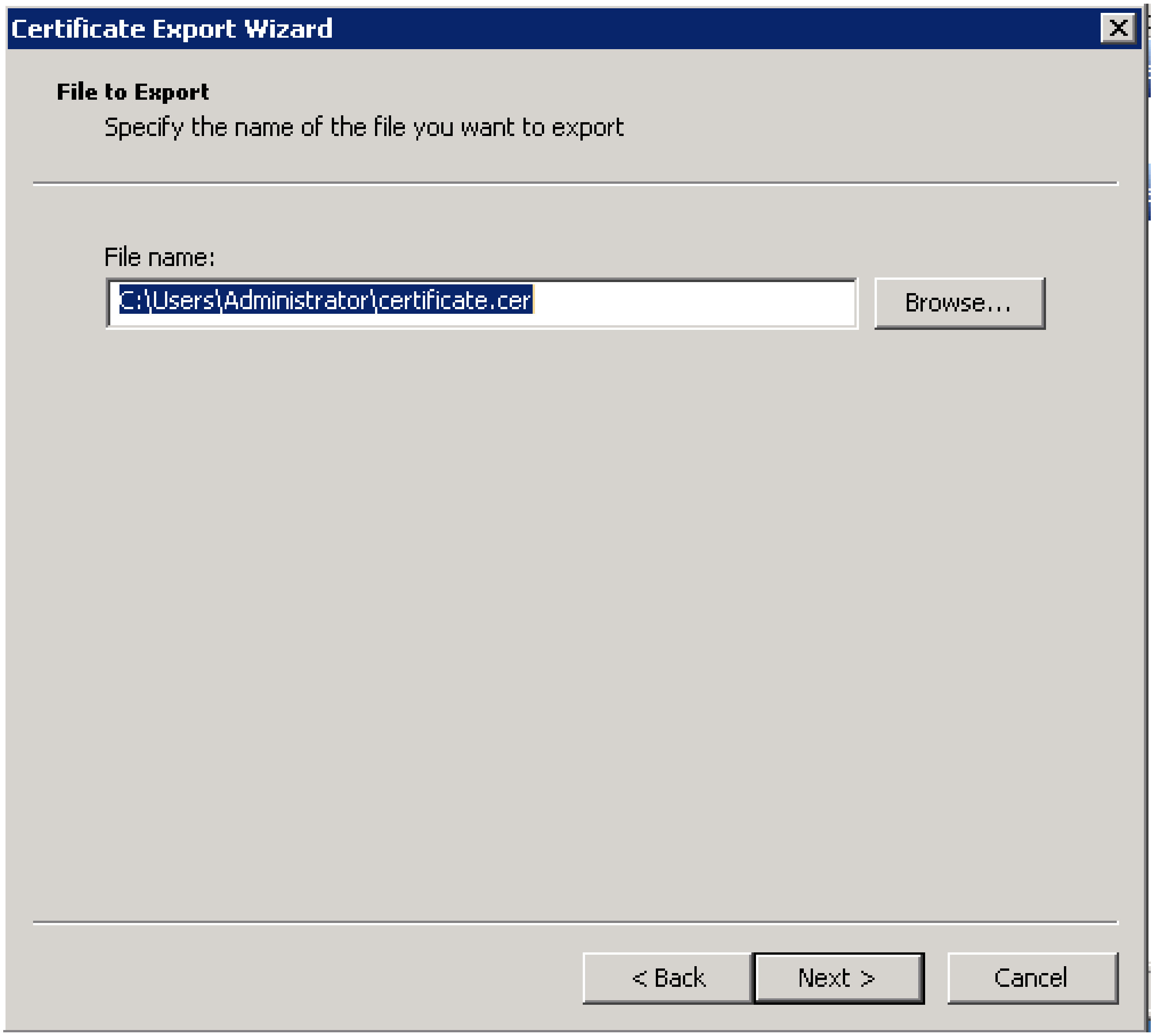
□ Delete the private key if the export is successful

□ Export all extended properties

○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

1. Give the name a certificate


Certificate Export Wizard
File to Export
Specify the name of the file you want to export
File name:
Browse...
< Back
Next >
Cancel

C:\Users\Administrator\certificate.cer

After the certificate is exported, this certificate should be imported into a trusted certificate file that will be used by the Elasticsearch plugin.

To import a certificate into a trusted certificate file, a tool called „keytool.exe" is located in the JDK installation directory.

Use the following command to import a certificate file:

```
keytool -import -alias adding_certificate_keystore -file certificate.cer
-keystore certificatestore
```

The values for RED should be changed accordingly.

By doing this, he will ask you to set a password for the trusted certificate store. Remember this password, because it must be set in the configuration of the elasticsearch plugin. The following settings must be set in the `elasticsearch.yml` configuration for SSL:`ssl.keystore.file: "<path to the trust certificate store>"`

`ssl.keystore.password: "< password to the trust certificate store>"`

CHAPTER 66

Role mapping.

In the /etc/elasticsearch/elasticsearch.yml configuration file you can find a section for configuring role mapping:

```
# LDAP ROLE MAPPING FILE
# rolemapping.file.path: /etc/elasticsearch/role-mappings.yml
```

This variable points to the file /etc/elasticsearch/role-mappings.yml Below is the sample content for this file:

admin:

- "CN=Admins,OU=lab,DC=dev,DC=it,DC=example,DC=com"

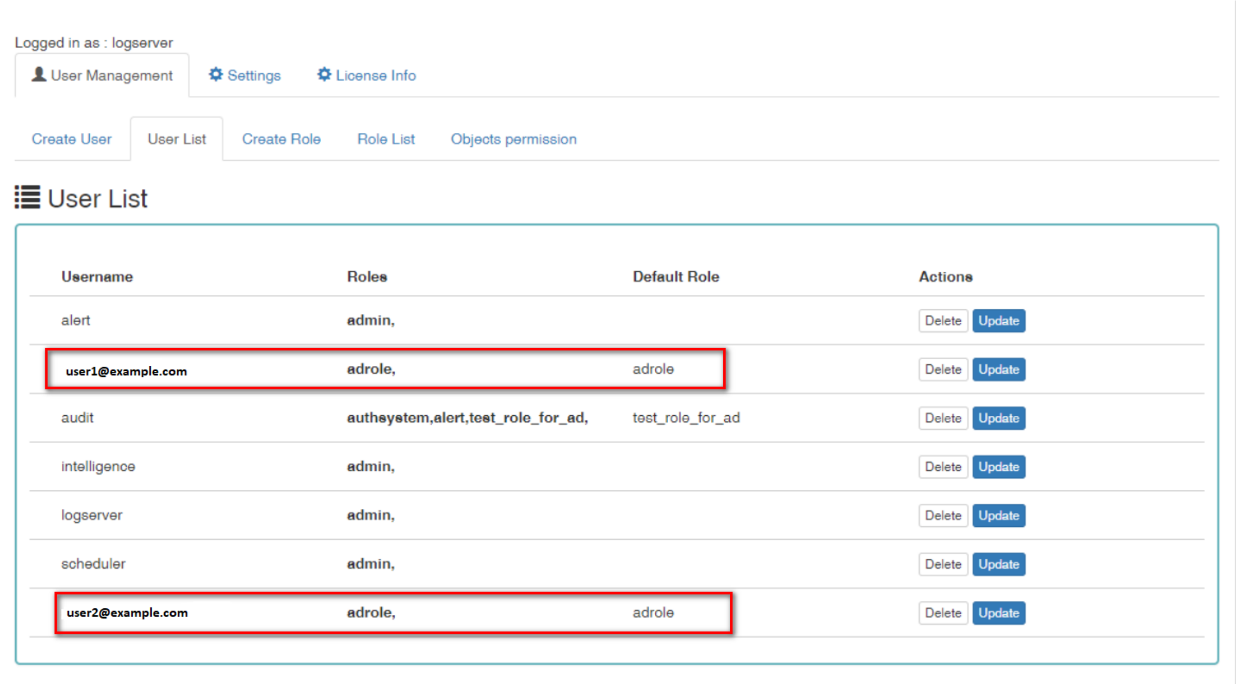
bank:

- "CN=security,OU=lab,DC=dev,DC=it,DC=example,DC=com"

The mapping mechanism works in this way: An AD user log in to OP5 Log Analytics. In the application there is a admin role, which through the file role-mapping .yml binds to the name of the admin role to which the Admins container from AD is assigned. It is enough for the user from the AD account to log in to the application with the privileges that are assigned to admin role in the OP5 Log Analytics. At the same time, if it is the first login in the OP5 Log Analytics, an account is created with an entry that informs the application administrator that is was created by logging in with AD.

Similar, the mechanism will work if we have a role with an arbitrary name created in OP5 Logistics and connected to the name of the role-mappings.yml and existing in AD any container.

Below a screenshot of the console on which are marked accounts that were created by uesrs logging in from AD



User List

Username	Roles	Default Role	Actions
alert	admin,		Delete Update
user1@example.com	adrole,	adrole	Delete Update
audit	authsystem,alert,test_role_for_ad,	test_role_for_ad	Delete Update
intelligence	admin,		Delete Update
logserver	admin,		Delete Update
scheduler	admin,		Delete Update
user2@example.com	adrole,	adrole	Delete Update

If you map roles with from several domains, for example dev.examloe1.com, dev.example2.com then in User List we will see which user from which domain with which role logged in OP5 Log Analytics.

CHAPTER 67

Configuring Single Sign On (SSO)

In order to configure SSO, the system should be accessible by domain name URL, not IP address nor localhost.

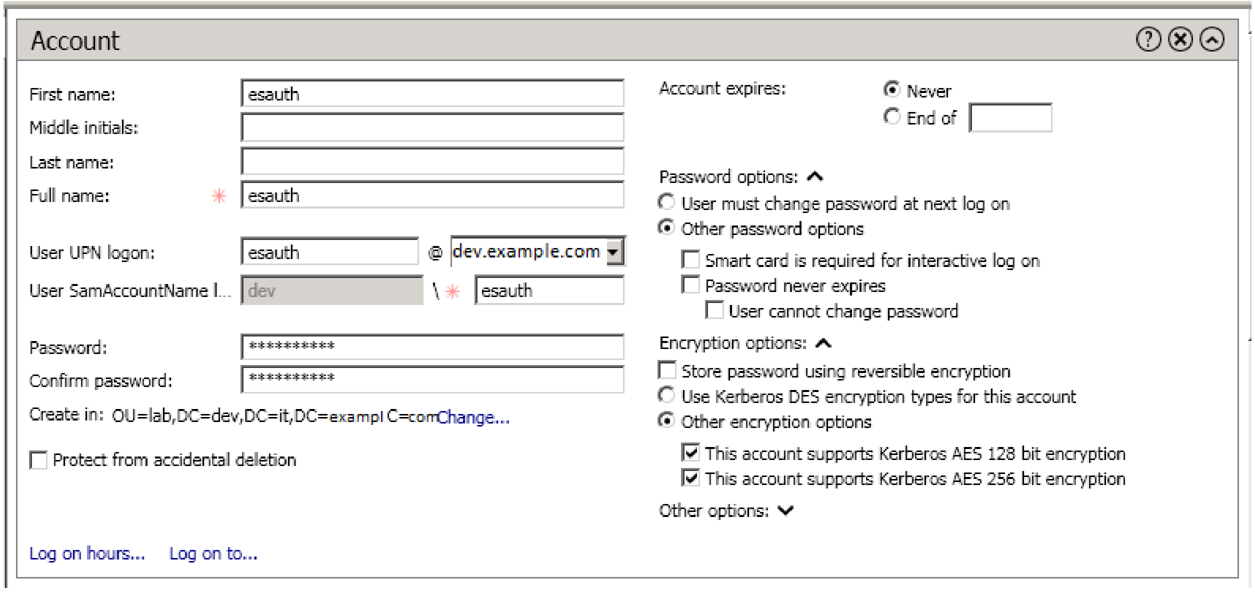
Ok :`https://loggui.com:5601/login`. **Wrong :** `https://localhost:5601/login`, `https://10.0.10.120:5601/login`

In order to enable SSO on your system follow below steps. The configuration is made for AD: `dev.example.com`, GUI URL: `loggui.com`

67.1 Create an User Account for Elasticsearch auth plugin

In this step, a Kerberos Principal representing Elasticsearch auth plugin is created on the Active Directory. The principal name would be `name@DEV.EXAMPLE.COM`, while the `DEV.EXAMPLE.COM` is the administrative name of the realm. In our case, the principal name will be `esauth@DEV.EXAMPLE.COM`.

Create User in AD. Set "Password never expires" and "Other encryption options" as shown below:



Account

First name:	esauth
Middle initials:	
Last name:	
Full name: *	esauth
User UPN logon:	esauth @ dev.example.com
User SamAccountName l...	dev \ * esauth
Password:	***********
Confirm password:	***********

Create in: OU=lab,DC=dev,DC=it,DC=exampl C=comChange...

□ Protect from accidental deletion

Log on hours... Log on to...

Account expires: ● Never ○ End of

Password options:

○ User must change password at next log on
● Other password options
□ Smart card is required for interactive log on
□ Password never expires
□ User cannot change password

Encryption options:

□ Store password using reversible encryption
○ Use Kerberos DES encryption types for this account
● Other encryption options
☑ This account supports Kerberos AES 128 bit encryption
☑ This account supports Kerberos AES 256 bit encryption

Other options:

67.2 Define Service Principal Name (SPN) and Create a Keytab file for it

Use the following command to create the keytab file and SPN:

> C:> ktpass -out c:\Users\Administrator\esauth.keytab -princ **HTTP/loggui.com@DEV.EXAMPLE.COM** -mapUser **esauth** -mapOp set -pass '**Sprint$123**' -crypto ALL -pType KRB5_NT_PRINCIPAL

Values highlighted in bold should be adjusted for your system. The `esauth.keytab` file should be placed on your elasticsearch node - preferably `/etc/elasticsearch/` with read permissions for elasticsearch user: `chmod 640 /etc/elasticsearch/esauth.keytab` `chown elasticsearch: /etc/elasticsearch/esauth.keytab`

67.3 Create a file named *krb5Login.conf*:

```
com.sun.security.jgss.initiate{
    com.sun.security.auth.module.Krb5LoginModule required
    principal="esauth@DEV.EXAMPLE.COM" useKeyTab=true
    keyTab=/etc/elasticsearch/esauth.keytab storeKey=true debug=true;
    };
com.sun.security.jgss.krb5.accept {
    com.sun.security.auth.module.Krb5LoginModule required
    principal="esauth@DEV.EXAMPLE.COM" useKeyTab=true
    keyTab=/etc/elasticsearch/esauth.keytab storeKey=true debug=true;
    };
```

Principal user and keyTab location should be changed as per the values created in the step 2. Make sure the domain is in UPPERCASE as shown above. The `krb5Login.conf` file should be placed on your elasticsearch node, for instance `/etc/elasticsearch/` with read permissions for elasticsearch user:

```
sudo chmod 640 /etc/elasticsearch/krb5Login.conf
sudo chown elasticsearch: /etc/elasticsearch/krb5Login.conf
```

67.4 Append the following JVM arguments (on Elasticsearch node in */etc/sysconfig/elasticsearch*):

> -Dsun.security.krb5.debug=true -Djava.security.krb5.realm=**DEV.EXAMPLE.COM** -Djava.security.krb5.kdc=**AD_HOST_IP_ADDRESS** -Djava.security.auth.login.config=**/etc/elasticsearch/krb5Login.conf** -Djavax.security.auth.useSubjectCredsOnly=false

Change the appropriate values in the bold. This JVM arguments has to be set for Elasticsearch server.

67.5 Add the following additional (sso.domain, service_principal_name, service_principal_name_password) settings for ldap in elasticsearch.yml or properties.yml file wherever the ldap settings are configured:

```
sso.domain: "dev.example.com"
ldaps:
- name: "dev.example.com"
    host: "IP_address"
    port: 389                                                 # optional, default 389
    ssl_enabled: false                                        # optional, default  ␣
↪true
    ssl_trust_all_certs: false                                 # optional, default␣
↪false
    bind_dn: "Administrator@dev.example.com"                     # optional, skip for␣
↪anonymous bind
    bind_password: "administrator_password"                                 #␣
↪optional, skip for anonymous bind
    search_user_base_DN: "OU=lab,DC=dev,DC=it,DC=example,DC=com"
    user_id_attribute: "uid"                                  # optional, default "uid
↪"
    search_groups_base_DN: "OU=lab,DC=dev,DC=it,DC=example,DC=com"
    unique_member_attribute: "uniqueMember"                   # optional, default
↪"uniqueMember"
    service_principal_name: "esauth@DEV.EXAMPLE.COM"
    service_principal_name_password : "Sprint$123"
```

Note: At this moment, SSO works for only single domain. So you have to mention for what domain SSO should work in the above property `sso.domain`

67.6 To apply the changes restart Elasticsearch service

```
sudo systemctl restart elasticsearch.service
```

67.7 Enable SSO feature in `kibana.yml` file:

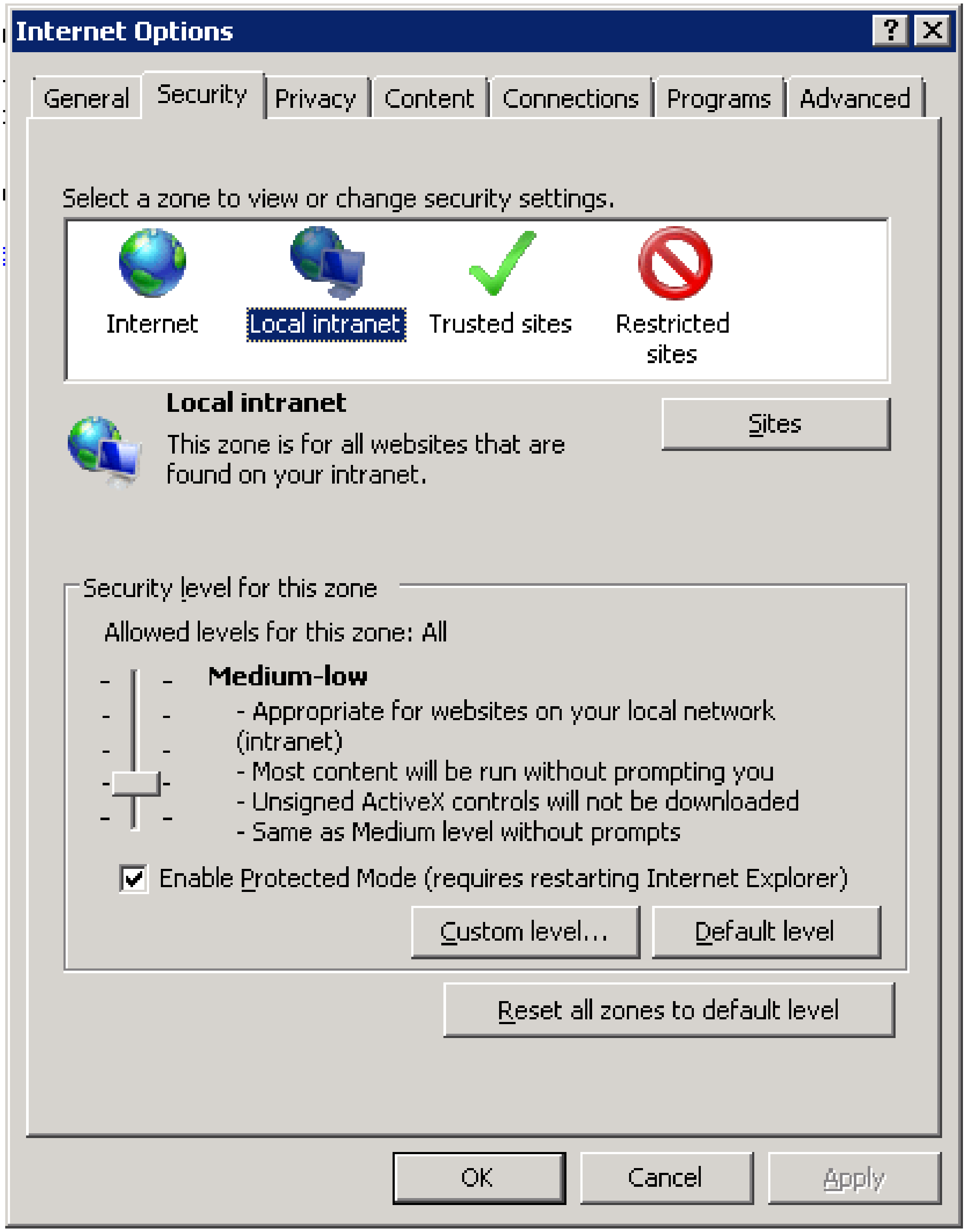
`kibana.sso_enabled: true` After that Kibana has to be restarted: `sudo systemctl restart kibana.service`

CHAPTER 68

Client (Browser) Configuration

68.1 Internet Explorer configuration

1. Goto `Internet Options` from `Tools` menu and click on `Security` Tab:



Select a zone to view or change security settings.

Local intranet

This zone is for all websites that are found on your intranet.

Security level for this zone

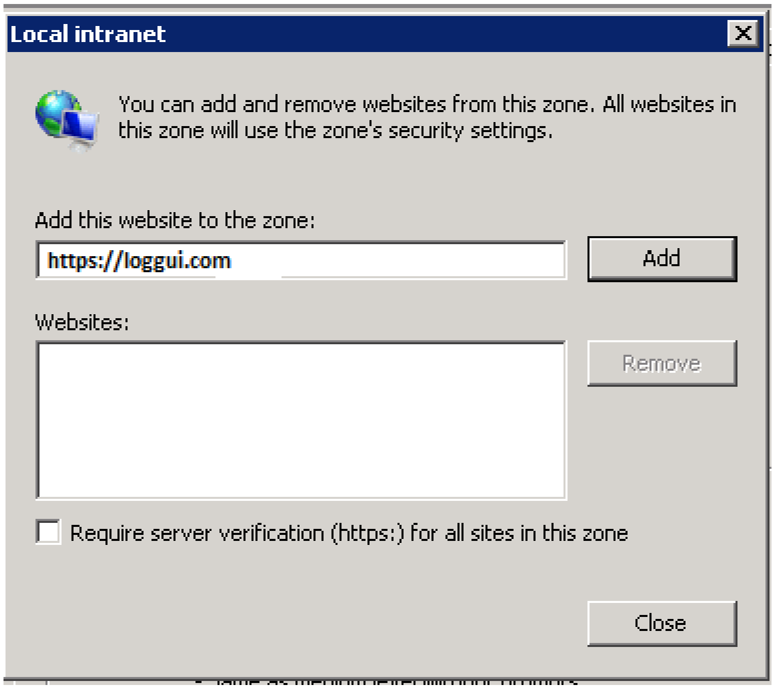
Allowed levels for this zone: All

Medium-low

- Appropriate for websites on your local network (intranet)
- Most content will be run without prompting you
- Unsigned ActiveX controls will not be downloaded
- Same as Medium level without prompts

☑ Enable Protected Mode (requires restarting Internet Explorer)

1. Select `Local intranet`, click on `Site` -> `Advanced` -> `Add` the url:



Local intranet

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:

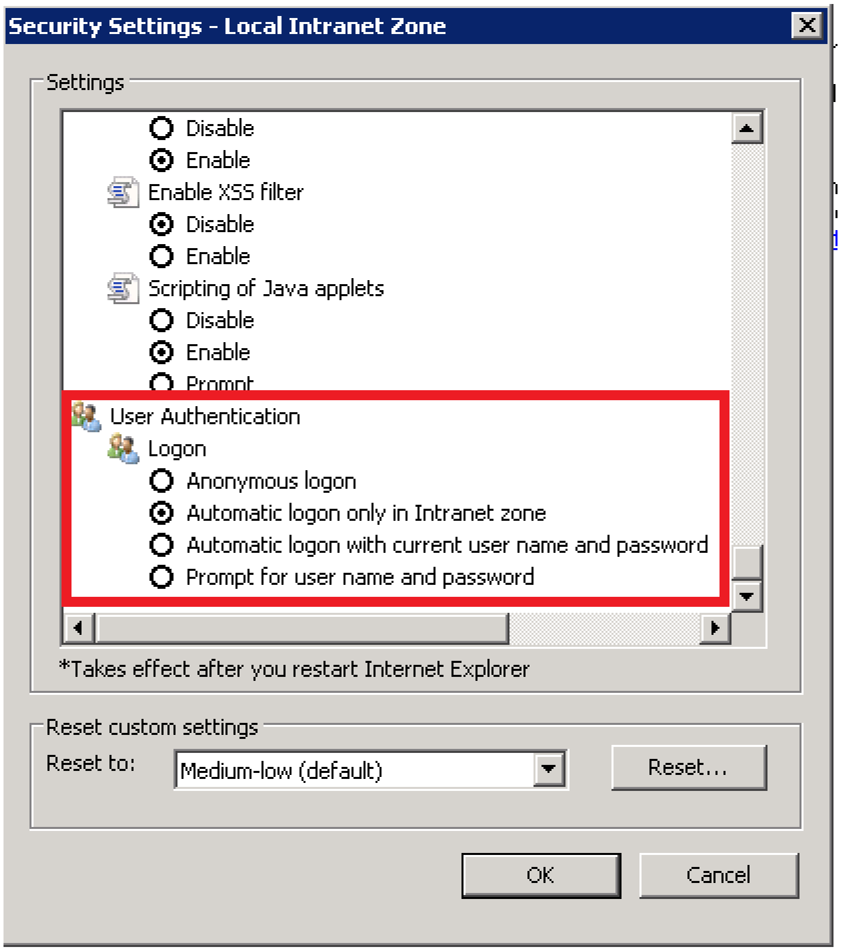
https://loggui.com

Websites:

□ Require server verification (https:) for all sites in this zone

After adding the site click close.

1. Click on custom level and select the option as shown below:



○ Disable
● Enable
Enable XSS filter
● Disable
○ Enable
Scripting of Java applets
○ Disable
● Enable
○ Prompt
User Authentication
Logon
○ Anonymous logon
● Automatic logon only in Intranet zone
○ Automatic logon with current user name and password
○ Prompt for user name and password

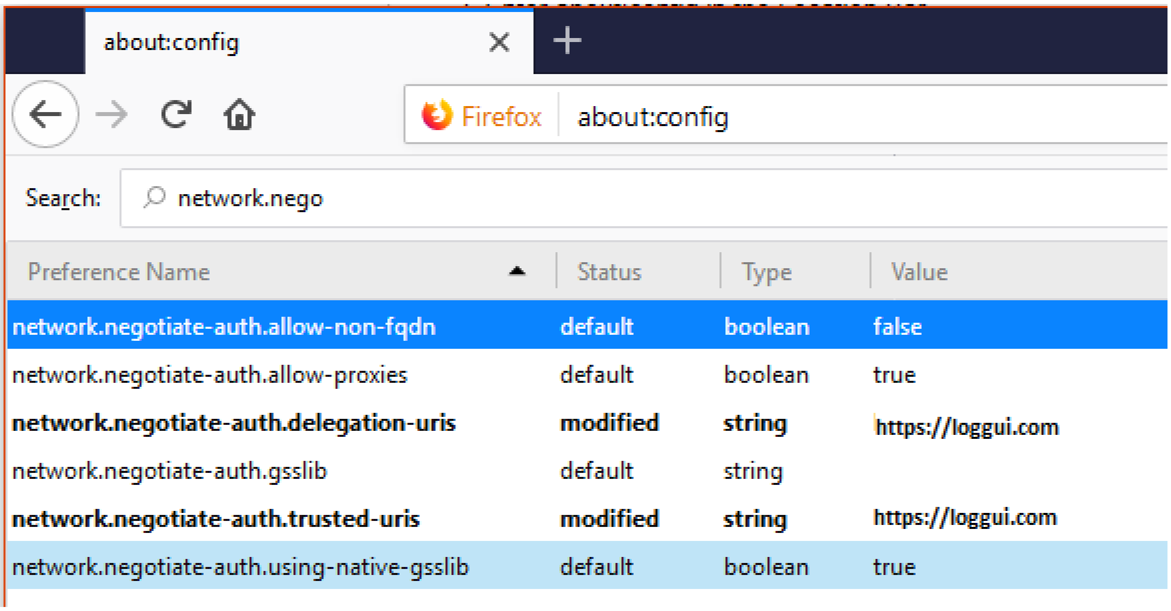
*Takes effect after you restart Internet Explorer

68.2 Chrome configuration

For Chrome, the settings are taken from IE browser.

68.3 Firefox configuration

Update the following config:



about:config

network.nego

Preference Name	Status	Type	Value
network.negotiate-auth.allow-non-fqdn	default	boolean	false
network.negotiate-auth.allow-proxies	default	boolean	true
network.negotiate-auth.delegation-uris	**modified**	**string**	**https://loggui.com**
network.negotiate-auth.gsslib	default	string	
network.negotiate-auth.trusted-uris	**modified**	**string**	**https://loggui.com**
network.negotiate-auth.using-native-gsslib	default	boolean	true

CHAPTER 69

Configure email delivery for sending PDF reports in Scheduler.

The default e-mail client that installs with the Linux CentOS system, which is used by OP5 Log Analytics to send reports (Section 5.3 of the Reports chapter), is ***postfix***.

CHAPTER 70

Configuration file for **postfix** mail client

The *postfix* configuration directory for CentOS is */etc/postfix*. It contains files:

main.cf - the main configuration file for the program specifying the basics parameters

Some of its directives:

```
|**Directive**             |       **Description**                                                    ␣
↪                                                    |
| -------------------------| ------------------------------------------------------------------------
↪--------------------------------------------------|
|queue\_directory          |       The postfix queue location.
|command\_directory        |      The location of Postfix commands.
|daemon\_directory         |       Location of Postfix daemons.
|mail\_owner               |       The owner of Postfix domain name of the server
|myhostname                |       The fully qualified domain name of the server.
|mydomain                  |       Server domain
|myorigin                  |       Host or domain to be displayed as origin on email␣
↪leaving the server.
|inet\_interfaces          |       Network interface to be used for incoming email.
|mydestination             |       Domains from which the server accepts mail.
|mynetworks                |       The IP address of trusted networks.
|relayhost                 |       Host or other mail server through which mail will␣
↪be sent. This server will act as an outbound gateway.
|alias\_maps               |       Database of asliases used by the local delivery␣
↪agent.
|alias\_database           |       Alias database generated by the new aliases␣
↪command.
|mail\_spool\_directory    |       The location where user boxes will be stored.
```

master.cf - defines the configuration settings for the master daemon and the way it should work with other agents to deliver mail. For each service installed in the master.cf file there are seven columns that define how the service should be used.

```
|Column            |     Description
|----------------- | -----------------------------------------------------------------
↪---------------------------
```

(continues on next page)

(continued from previous page)

```
|service           |    The name of the service
|type              |    The transport mechanism to be user.
|private           |    Is the service only for user by Postfix.
|unpriv            |    Can the service be run by ordinary users
|chroot            |    Whether the service is to change the main directory (chroot)␣
↪for the mail. Queue.
|wakeup            |    Wake up interval for the service.
|maxproc           |    The maximum number of processes on which the service can be␣
↪forked (to divide in branches)
|command + args    |   A command associated with the service plus any argument
```

access - can be used to control access based on e-mail address, host address, domain or network address.

Examples of entries in the file

```
|Description                                       | Example
|------------------------------------------------|--------------------
|To allow access for specific IP address:         | 192.168.122.20 OK
|To allow access for a specific domain:           | example.com OK
|To deny access from the 192.168.3.0/24 network:  | 192.168.3 REJECT
```

After making changes to the access file, you must convert its contents to the access.db database with the postmap command:

```
    # postmap /etc/postfix/access
    # ll /etc/postfix/access*

    -rw-r\--r\--. 1 root root 20876 Jan 26 2014 /etc/postfix/access
    -rw-r\--r\--. 1 root root 12288 Feb 12 07:47 /etc/postfix/access.db
```

canonical - mapping incoming e-mails to local users.

Examples of entries in the file:

To forward emails to user1 to the [[user1@yahoo.com] mailbox:

```
user1 user1\@yahoo.com
```

To forward all emails for example.org to another example.com domain:

```
@example.org @example.com
```

After making changes to the canonical file, you must convert its contents to the canonical.db database with the postmap command:

```
# postmap /etc/postfix/canonical
# ll /etc/postfix/canonical*

-rw-r\--r\--. 1 root root 11681 2014-06-10 /etc/postfix/canonical
-rw-r\--r\--. 1 root root 12288 07-31 20:56 /etc/postfix/canonical.db
```

generic - mapping of outgoing e-mails to local users. The syntax is the same as a canonical file. After you make change to this file, you must also run the postmap command.

```
# postmap /etc/postfix/generic
# ll /etc/postfix/generic*
```

(continues on next page)

(continued from previous page)

```
-rw-r\--r\--. 1 root root 9904 2014-06-10 /etc/postfix/generic
-rw-r\--r\--. 1 root root 12288 07-31 21:15 /etc/postfix/generic.db
```

reloceted – information about users who have been transferred. The syntax of the file is the same as canonical and generic files.

Assuming tha user1 was moved from example.com to example.net, you can forward all emails received on the old address to the new address:

Example of an entry in the file:

```
user1@example.com user1@example.net
```

After you make change to this file, you must also run the postmap command.

```
# postmap /etc/postfix/relocated
# ll /etc/postfix/relocated*

-rw-r\--r\--. 1 root root 6816 2014-06-10 /etc/postfix/relocated
-rw-r\--r\--. 1 root root 12288 07-31 21:26 /etc/postfix/relocated.d
```

transport – mapping between e-mail addresses and server through which these e-mails are to be sent (next hops) int the transport format: nexthop.

Example of an entry in the file:

```
user1@example.com smtp:host1.example.com
```

After you make changes to this file, you must also run the postmap command.

```
# postmap /etc/postfix/transport
[root@server1 postfix]# ll /etc/postfix/transport*

-rw-r\--r\--. 1 root root 12549 2014-06-10 /etc/postfix/transport
-rw-r\--r\--. 1 root root 12288 07-31 21:32 /etc/postfix/transport.db
```

virtual - user to redirect e-mails intended for a certain user to the account of another user or multiple users. It can also be used to implement the domain alias mechanism.

Examples of the entry in the file:

Redirecting email for user1, to root users and user3:

```
user1 root, user3
```

Redirecting email for user 1 in the example.com domain to the root user:

```
user1@example.com root
```

After you make change to this file, you must also run the postmap command:

```
# postmap /etc/postfix/virtual
# ll /etc/postfix/virtual

-rw-r\--r\--. 1 root root 12494 2014-06-10 /etc/postfix/virtual
-rw-r\--r\--. 1 root root 12288 07-31 21:58 /etc/postfix/virtual.db
```

CHAPTER 71

Basic postfix configuration

Base configuration of *postfix* application you can make in `/etc/postfix/main.cfg` configuration file, which must complete with the following entry:

- section *# RECEIVING MAIL*

  ```
  `inet\_interfaces = all`
  `inet\_protocols = ipv4`
  ```

- section *# INTERNET OR INTRANET*

  `relayhost = \[IP mail server\]:25 (port number)`

I the netxt step you must complete the canonical file of *postfix*

At the end you should restart the *postfix*:

```
`systemctl restart postfix`
```

CHAPTER 72

Example of postfix configuration with SSL encryption enabled

To configure email delivery with SSL encryption you need to make the following changes in the *postfix* configuration files:

- **`/etc/postfix/main.cf`** - file should contain the following entries in addition to standard (unchecked entries):
    - *`mydestination = $myhostname, localhost.$mydomain, localhost`*
    - *`myhostname = example.com`*
    - *`relayhost = [smtp.example.com]:587`*
    - *`smtp_sasl_auth_enable = yes`*
    - *`smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd`*
    - *`smtp_sasl_security_options = noanonymous`*
    - *`smtp_tls_CAfile = /root/certs/cacert.cer`*
    - *`smtp_use_tls = yes`*
    - *`smtp_sasl_mechanism_filter = plain, login`*
    - *`smtp_sasl_tls_security_options = noanonymous`*
    - *`canonical_maps = hash:/etc/postfix/canonical`*
    - *`smtp_generic_maps = hash:/etc/postfix/generic`*
    - *`smtpd_recipient_restrictions = permit_sasl_authenticated`*
- **`/etc/postfix/sasl/passwd`** - file should define the data for authorized

```
*`[smtp.example.com\]:587 [[USER@example.com:PASS]](mailto:USER@example.
↪com:PASS)`*
```

You need to give appropriate permissions:

```
*`chmod 400 /etc/postfix/sasl_passwd`*
```

and map configuration to database:

```
*`postmap /etc/postfix/sasl_passwd`*
```

next you need to generate a ca cert file:

```
*`cat /etc/ssl/certs/Example\_Server\_CA.pem | tee -a etc/postfix/cacert.pem`*
```

And finally, you need to restart postfix

```
*`/etc/init.d/postfix restart`*
```

CHAPTER 73

Elasticsearch API

The Elasticsearch has a typical REST API and data is received in JSON format after the HTTP protocol. By default the tcp/9200 port is used to communicate with the Elasticsearch API. For purposes of examples, communication with the Elasticsearch API will be carried out using the *curl* application.

Program syntax:

```
*`  # curl -X<metoda> -u login:password '<adres_ip_elasticsearch>:<port>'*\
*`  # curl -XGET -u login:password '127.0.0.1:9200'`*
```

Available methods:

- PUT - sends data to the server;
- POST - sends a request to the server for a change;
- DELETE - deletes the index / document;
- GET - gets information about the index /document;
- HEAD - is used to check if the index / document exists.

Avilable APIs by roles:

- Index API - manages indexes;
- Document API - manges documnets;
- Cluster API - manage the cluster;
- Search API - is userd to search for data.

CHAPTER 74

Elasticsearch Index API

The indices APIs are used to manage individual indices, index settings, aliases, mappings, and index templates.

CHAPTER 75

Elsaticsearch Index API - Adding Index

Adding Index - autormatic method:

```
*`# curl -XPUT -u login:password '127.0.0.1:9200/twitter/tweet/1?pretty=true' -d'{`*\
    *`"user" : "elk01",`*\
    *`"post_date" : "2017-09-05T10:00:00",`*\
    *`"message" : "tests auto index generation"`*\
   *`}'`*
```

You should see the output:

```
*`{`*\
*`"_index" : "twitter",`*\
  *`"_type" : "tweet",`*\
  *`"_id" : "1",`*\
  *`"_version" : 1,`*\
  *`"_shards" : {`*\
    *`"total" : 2,`*\
    *`"successful" : 1,`*\
    *`"failed" : 0`*\
  *`},`*\
  *`"created" : true`*\
*`}`*
```

The parameter `action.auto_create_index` must be set on `true`.

Adding Index – manual method:

- settings the number of shards and replicas:

  ```
  # curl -XPUT -u login:password '127.0.0.1:9200/twitter2?pretty=true'
  -d'{"settings" :  {"number_of_shards" :  1,"number_of_replicas" :  1}}’‘*
  ```

You should see the output:

```
*`{`*\
  *`"acknowledged" : true`*\
*`}`*
```

- command for manual index generation:

  ```
  # curl -XPUT -u login:password '127.0.0.1:9200/twitter2/tweet/1?
  pretty=true' -d'{"user" :  "elk01","post_date" :  "2017-09-05T10:00:00",
  "message" :  "tests manual index generation"}'
  ```

You should see the output:

```
*`{`*\
  *`"_index" : "twitter2",`*\
  *`"_type" : "tweet",`*\
  *`"_id" : "1",`*\
  *`"_version" : 1,`*\
  *`"_shards" : {`*\
    *`"total" : 2,`*\
     *`"successful" : 1,`*\
     *`"failed" : 0`*\
  *`},`*\
  *`"created" : true`*\
*`}`*
```

CHAPTER 76

Elasticsearch Index API

Delete Index - to delete *twitter* index you need use the following command:

```
# curl -XDELETE -u login:password '127.0.0.1:9200/twitter?pretty=true'
```

The delete index API can also be applied to more than one index, by either using a comma separated list, or on all indice by using _all or * as index:

```
# curl -XDELETE -u login:password '127.0.0.1:9200/twitter*?pretty=true'
```

To allowing to delete indices via wildcards set `action.destructive_requires_name` setting in the config to `false`.

CHAPTER 77

Elasticsearch Index_API useful commands.

- get information about Replicas and Shards:

```
# curl -XGET -u login:password '127.0.0.1:9200/twitter/_settings?pretty=true'#
curl -XGET -u login:password '127.0.0.1:9200/twitter2/_settings?pretty=true'
```

- get information about mapping and alias in the index:\

```
# curl -XGET -u login:password '127.0.0.1:9200/twitter/_mappings?pretty=true'#
curl -XGET -u login:password '127.0.0.1:9200/twitter/_aliases?pretty=true'
```

- get all information about the index:\

```
# curl -XGET -u login:password '127.0.0.1:9200/twitter?pretty=true'
```

- checking does the index exist:\

```
# curl -XGET -u login:password '127.0.0.1:9200/twitter?pretty=true'
```

- close the index:\

```
# curl -XGET -u login:password '127.0.0.1:9200/twitter/_close?pretty=true'
```

- open the index:\

```
# curl -XGET -u login:password '127.0.0.1:9200/twitter/_open?pretty=true'
```

- get the status of all indexes:\

```
# curl -XGET -u login:password '127.0.0.1:9200/_cat/indices?v'
```

- get the status of one specific index:\

```
# curl -XGET -u login:password '127.0.0.1:9200/_cat/indices/twitter?v'
```

- display how much memory is used by the indexes:\

```
# curl -XGET -u login:password '127.0.0.1:9200/_cat/indices?v&h=i,
tm&s=tm:desc'
```

- display details of the shards:\

```
# curl -XGET -u login:password '127.0.0.1:9200/_cat/shards?v'
```

CHAPTER 78

Elasticsearch Document API

CHAPTER 79

Elasticsearch Document API - Create_Document

- create a document with a specify ID:

```
# curl -XPUT -u login:password '127.0.0.1:9200/twitter/tweet/1?
pretty=true' -d'{"user" :  "lab1","post_date" :  "2017-08-25T10:00:00",
"message" :  "testuje Elasticsearch"}'
```

You should see the output:

```
*`{`*\
  *`"_index" : "twitter",`*\
  *`"_type" : "tweet",`*\
  *`"_id" : "1",`*\
  *`"_version" : 1,`*\
  *`"_shards" : {`*\
    *`"total" : 2,`*\
    *`"successful" : 1,`*\
    *`"failed" : 0`*\
  *`},`*\
  *`"created" : true`*\
*`}`*
```

- creating a document with an automatically generated ID: (note: PUT-> POST):\

```
  *`# curl -XPOST -u login:password '127.0.0.1:9200/twitter/tweet?pretty=true' -d'
↪{`*\
      *`"user" : "lab1",`*\
      *`"post_date" : "2017-08-25T10:10:00",`*\
      *`"message" : "testuje automatyczne generowanie ID"`*\
      *`}'`*
```

You should see the output:\

```
*`{`*\
  *`"_index" : "twitter",`*\
  *`"_type" : "tweet",`*\
```

(continues on next page)

(continued from previous page)

```
  *`"_id" : "AV49sTlM8NzerkV9qJfh",`*\
  *`"_version" : 1,`*\
  *`"_shards" : {`*\
    *`"total" : 2,`*\
    *`"successful" : 1,`*\
    *`"failed" : 0`*\
  *`},`*\
  *`"created" : true`*\
*`}`*
```

CHAPTER 80

Elasticsearch Document API - Delete Document

- delte a document by ID:\

```
# curl -XDELETE -u login:password '127.0.0.1:9200/twitter/tweet/1?
pretty=true'# curl -XDELETE -u login:password '127.0.0.1:9200/twitter/tweet/
AV49sTlM8NzerkV9qJfh?pretty=true'
```

- delete a document using a wildcard:\

```
# curl -XDELETE -u login:password '127.0.0.1:9200/twitter/tweet/1*?
pretty=true'\
```

(parametr: action.destructive_requires_name must be set to false)

CHAPTER 81

Elasticsearch Document API - useful commdnds

- get information about the document:\

```
# curl -XGET -u login:password '127.0.0.1:9200/twitter/tweet/1?pretty=true'
```

You should see the output:\

```
*`{`*\
  *`"_index" : "twitter",`*\
  *`"_type" : "tweet",`*\
  *`"_id" : "1",`*\
  *`"_version" : 1,`*\
  *`"found" : true,`*\
  *`"_source" : {`*\
    *`"user" : "lab1",`*\
    *`"post_date" : "2017-08-25T10:00:00",`*\
    *`"message" : "testuje Elasticsearch"`*\
  *`}`*\
```

}

- get the source of the document:\

```
# curl -XGET -u login:password '127.0.0.1:9200/twitter/tweet/1/_source?pretty=true'
```

You should see the output:\

```
*`{`*\
  *`"user" : "lab1",`*\
  *`"post_date" : "2017-08-25T10:00:00",`*\
  *`"message" : "testuje Elasticsearch"`*\
```

}\

- get information about all documents in the index:\

```
# curl -XGET -u login:password '127.0.0.1:9200/twitter*/_search?
q=*&pretty=true'
```

You should see the output:

```
`*{`*\
  `*"took" : 7,`*\
  `*"timed_out" : false,`*\
  `*"_shards" : {`*\
    `*"total" : 10,`*\
    `*"successful" : 10,`*\
    `*"failed" : 0`*\
  `*},`*\
  `*"hits" : {`*\
    `*"total" : 3,`*\
    `*"max_score" : 1.0,`*\
    `*"hits" : [ {`*\
      `*"_index" : "twitter",`*\
      `*"_type" : "tweet",`*\
      `*"_id" : "AV49sTlM8NzerkV9qJfh",`*\
      `*"_score" : 1.0,`*\
      `*"_source" : {`*\
        `*"user" : "lab1",`*\
        `*"post_date" : "2017-08-25T10:10:00",`*\
        `*"message" : "auto generated ID"`*\
      `*}`*\
    `*}, {`*\
      `*"_index" : "twitter",`*\
      `*"_type" : "tweet",`*\
      `*"_id" : "1",`*\
      `*"_score" : 1.0,`*\
      `*"_source" : {`*\
        `*"user" : "lab1",`*\
        `*"post_date" : "2017-08-25T10:00:00",`*\
        `*"message" : "Elasticsearch test"`*\
      `*}`*\
    `*}, {`*\
      `*"_index" : "twitter2",`*\
      `*"_type" : "tweet",`*\
      `*"_id" : "1",`*\
      `*"_score" : 1.0,`*\
      `*"_source" : {`*\
        `*"user" : "elk01",`*\
        `*"post_date" : "2017-09-05T10:00:00",`*\
        `*"message" : "manual index created test"`*\
      `*}`*\
    `*} ]`*\
  `*}`*\
`*}`*
```

- the sum of all documents in a specified index:\

```
# curl -XGET -u login:password '127.0.0.1:9200/_cat/count/twitter?v'
```

You should see the output:\

```
*`epoch              timestamp count`*\
*`1504281400    17:56:40     2`*
```

- the sum of all document in Elasticsearch database:\

```
# curl -XGET -u login:password '127.0.0.1:9200/_cat/count?v'
```

You should see the output:\

```
*`epoch             timestamp count`*\
*`1504281518    17:58:38    493658`*
```

CHAPTER 82

Elasticsearch Cluster API

Example of use:

- information about the cluster state:\

```
# curl -XGET -u login:password '127.0.0.1:9200/_cluster/health?pretty=true'
```

- information about the role and load of nodes in the cluster:\

```
# curl -XGET -u login:password '127.0.0.1:9200/_cat/nodes?v'
```

- information about the available and used place on the cluster nodes:\

```
# curl -XGET -u login:password '127.0.0.1:9200/_cat/allocation?v'
```

- information which node is currently in the master role:\

```
# curl -XGET -u login:password '127.0.0.1:9200/_cat/master?v'
```

- information abut currently performed operations by the cluster:\

```
# curl -XGET -u login:password '127.0.0.1:9200/_cat/pending_tasks?v'
```

- information on revoceries / transferred indices:\

```
# curl -XGET -u login:password '127.0.0.1:9200/_cat/recovery?v'
```

- information about shards in a cluster:\

```
# curl -XGET -u login:password '127.0.0.1:9200/_cat/shards?v'
```

- detailed inforamtion about the cluster:\

```
# curl -XGET -u login:password '127.0.0.1:9200/_cluster/stats?human&pretty'
```

- detailed information about the nodes:\

```
# curl -XGET -u login:password '127.0.0.1:9200/_nodes/stats?human&pretty'
```

CHAPTER 83

Elasticsearch Search API

- searching for documents by the string:\

```
 *`# curl -XPOST -u login:password '127.0.0.1:9200/twitter*/tweet/_search?
↪pretty=true' -d '{`*\
                 *`"query": {`*\
                         *`"bool" : {`*\
                                 *`"must" : {`*\
                                     *`"query_string" : {`*\
                                             *`"query" : "test"`*\
                                     *`}`*\
                                 *`}`*\
                 *`}`*\
              *`}`*\
         *`}'`*
```

- searching for document by the string and filtering:\

```
 *`# curl -XPOST -u login:password '127.0.0.1:9200/twitter*/tweet/_search?
↪pretty=true' -d'{`*\
                 *`"query": {`*\
                         *`"bool" : {`*\
                                 *`"must" : {`*\
                                     *`"query_string" : {`*\
                                             *`"query" : "testuje"`*\
                                         *`}`*\
                                     *`},`*\
                                 *`"filter" : {`*\
                                     *`"term" : { "user" : "lab1" }`*\
                                 *`}`*\
                         *`}`*\
                 *`}`*\
         *`}'`*
```

- simple search in a specific field (in this case user) uri query:\

```
# curl -XGET -u login:password '127.0.0.1:9200/twitter*/_search?
q=user:lab1&pretty=true'
```

- simple search in a specific field:\

```
*`# curl -XPOST -u login:password '127.0.0.1:9200/twitter*/_search?pretty=true'␣
↪-d '{`*\
              *`"query" : {`*\
                      *`"term" : { "user" : "lab1" }`*\
             *`}`*\
         *`}'`*
```

CHAPTER 84

Mapping, Fielddata and Templates

Mapping is a collection of fields along with a specific data type Fielddata is the field in which the data is stored (requires a specific type - string, float) Template is a template based on which fielddata will be created in a given index.

- Information on all set mappings:\

```
# curl -XGET -u login:password '127.0.0.1:9200/_mapping?pretty=true'
```

- Information about all mappings set in the index:\

```
# curl -XGET -u login:password '127.0.0.1:9200/twitter/_mapping/*?pretty=true'
```

- Information about the type of a specific field:\

```
# curl -XGET -u login:password '127.0.0.1:9200/twitter/_mapping/field/
message*?pretty=true'
```

- Information on all set templates:\

```
# curl -XGET -u login:password '127.0.0.1:9200/_template/*?pretty=true'
```

- Create - Mapping / Fielddata - It creates index twitter-float and the tweet message field sets to float:

```
   *`# curl -XPUT -u login:password '127.0.0.1:9200/twitter-float?pretty=true' -d
↪'{`*\
     *`"mappings": {`*\
       *`"tweet": {`*\
         *`"properties": {`*\
           *`"message": {`*\
             *`"type": "float"`*\
           *`}`*\
         *`}`*\
       *`}`*\
     *`}`*\
   *`}'`*
```

```
# curl -XGET -u login:password '127.0.0.1:9200/twitter-float/_mapping/
field/message?pretty=true'
```

- Create Template:\

  # curl -XPUT -u login:password '127.0.0.1:9200/_template/template_1' -d'{"template" : "twitter4","order" : 0,"settings" : {"number_of_shards" : 2}}'

# curl -XPOST -u login:password '127.0.0.1:9200/twitter4/tweet?pretty=true' -d'{\

```
*`"user" : "lab1",`*\
*`"post_date" : "2017-08-25T10:10:00",`*\
*`"message" : "test of ID generation"`*\
*`}'`*
```

# curl -XGET -u login:password '127.0.0.1:9200/twitter4/_settings?pretty=true'

– Create Template2 - Sets the mapping template for all new indexes specifying that the tweet data, in the field called message, should be of the “string” type:\

```
*`# curl -XPUT -u login:password '127.0.0.1:9200/_template/template_2' -d'{`*\
  *`"template" : "*",`*\
  *`"mappings": {`*\
    *`"tweet": {`*\
      *`"properties": {`*\
        *`"message": {`*\
          *`"type": "string"`*\
        *`}`*\
      *`}`*\
    *`}`*\
  *`}`*\
*`}'`*
```

- Delete Mapping - Deleting a specific index mapping (no possibility to delete - you need to index):\

# curl -XDELETE -u login:password '127.0.0.1:9200/twitter2'

- Delete Template:\

# curl -XDELETE -u login:password '127.0.0.1:9200/_template/template_1?pretty=true'

CHAPTER 85

Logstash

The OP5 Log Analytics use Logstash service to dynamically unify data from disparate sources and normalize the data into destynation of your choise. A Logstash pipeline has two required elements, *input* and *output*, and one optional elemnet *filter*. The input plugins consume data from a source, the filter plugins modify teh data as you specify, and the output plugins writethe data to a destynation. The default location of the Logstash plugin files is: */etc/logstash/conf.d/*. This location contain following OP5 Log Analytics default plugins:

- `01-input-beats.conf`
- `01-input-syslog.conf`
- `020-filter-beats-syslog.conf`
- `020-filter-network.conf`
- `099-filter-geoip.conf`
- `100-output-elasticsearch.conf`
- `naemon_beat.example`
- `perflogs.example`

CHAPTER 86

Logstash - Input “beats”

This plugin wait for reciving data from remote beats services. It use tcp /5044 port for communicaton:

```
            input {
                    beats {
                            port => 5044
                    }
            }
```

CHAPTER 87

Logstash - Input “network”

This plugin read events over a TCP or UDP socket assigns the appropriate tags:

```
input {
        tcp {
                port => 5514
                type => "network"

                tags => [ "LAN", "TCP" ]
        }

        udp {
                port => 5514
                type => "network"

                tags => [ "LAN", "UDP" ]
        }
}
```

CHAPTER 88

Logstash - Filter “beats syslog”

This filter prosessing an event data with syslog type:

```
    filter {

     if [type] == "syslog" {
            grok {
                    match => {
                      "message" => [
                    # auth: ssh|sudo|su

                      "%{SYSLOGTIMESTAMP:[system][auth][timestamp]} %
↪{SYSLOGHOST:[system][auth][hostname]} sshd(?:\[%{POSINT:[system][auth][pid]}\])?: %
↪{DATA:[system][auth][ssh][event]} %{DATA:[system][auth][ssh][method]} for (invalid␣
↪user )?%{DATA:[system][auth][user]} from %{IPORHOST:[system][auth][ssh][ip]} port %
↪{NUMBER:[system][auth][ssh][port]} ssh2(: %
↪{GREEDYDATA:[system][auth][ssh][signature]})?",

                              "%{SYSLOGTIMESTAMP:[system][auth][timestamp]} %
↪{SYSLOGHOST:[system][auth][hostname]} sshd(?:\[%{POSINT:[system][auth][pid]}\])?: %
↪{DATA:[system][auth][ssh][event]} user %{DATA:[system][auth][user]} from %
↪{IPORHOST:[system][auth][ssh][ip]}",

                              "%{SYSLOGTIMESTAMP:[system][auth][timestamp]} %
↪{SYSLOGHOST:[system][auth][hostname]} sshd(?:\[%{POSINT:[system][auth][pid]}\])?:␣
↪Did not receive identification string from %{IPORHOST:[system][auth][ssh][dropped_
↪ip]}",

                              "%{SYSLOGTIMESTAMP:[system][auth][timestamp]} %
↪{SYSLOGHOST:[system][auth][hostname]} sudo(?:\[%{POSINT:[system][auth][pid]}\])?:␣
↪\s*%{DATA:[system][auth][user]} :( %{DATA:[system][auth][sudo][error]} ;)? TTY=%
↪{DATA:[system][auth][sudo][tty]} ; PWD=%{DATA:[system][auth][sudo][pwd]} ; USER=%
↪{DATA:[system][auth][sudo][user]} ; COMMAND=%
↪{GREEDYDATA:[system][auth][sudo][command]}",
```

(continues on next page)

(continued from previous page)

```
                              "%{SYSLOGTIMESTAMP:[system][auth][timestamp]} %
↪{SYSLOGHOST:[system][auth][hostname]} %{DATA:[system][auth][program]}(?:\[%
↪{POSINT:[system][auth][pid]}\])?: %{GREEDYMULTILINE:[system][auth][message]}",

                    # add/remove user or group
                              "%{SYSLOGTIMESTAMP:[system][auth][timestamp]} %
↪{SYSLOGHOST:[system][auth][hostname]} groupadd(?:\[%{POSINT:[system][auth][pid]}\])?
↪: new group: name=%{DATA:system.auth.groupadd.name}, GID=%{NUMBER:system.auth.
↪groupadd.gid}",

                      "%{SYSLOGTIMESTAMP:[system][auth][timestamp]} %
↪{SYSLOGHOST:[system][auth][hostname]} userdel(?:\[%{POSINT:[system][auth][pid]}\])?
↪: removed group '%{DATA:[system][auth][groupdel][name]}' owned by '%
↪{DATA:[system][auth][group][owner]}'",

                              "%{SYSLOGTIMESTAMP:[system][auth][timestamp]} %
↪{SYSLOGHOST:[system][auth][hostname]} useradd(?:\[%{POSINT:[system][auth][pid]}\])?
↪: new user: name=%{DATA:[system][auth][user][add][name]}, UID=%
↪{NUMBER:[system][auth][user][add][uid]}, GID=%
↪{NUMBER:[system][auth][user][add][gid]}, home=%
↪{DATA:[system][auth][user][add][home]}, shell=%
↪{DATA:[system][auth][user][add][shell]}$",

                       "%{SYSLOGTIMESTAMP:[system][auth][timestamp]} %
↪{SYSLOGHOST:[system][auth][hostname]} userdel(?:\[%{POSINT:[system][auth][pid]}\])?
↪: delete user '%{WORD:[system][auth][user][del][name]}'$",

                       "%{SYSLOGTIMESTAMP:[system][auth][timestamp]} %
↪{SYSLOGHOST:[system][auth][hostname]} usermod(?:\[%{POSINT:[system][auth][pid]}\])?
↪: add '%{WORD:[system][auth][user][name]}' to group '%
↪{WORD:[system][auth][user][memberof]}'",

                       # yum install/erase/update package
                       "%{SYSLOGTIMESTAMP:[system][auth][timestamp]} %
↪{DATA:[system][package][action]}: %{NOTSPACE:[system][package][name]}"
                    ]

                }

                    pattern_definitions => {
                      "GREEDYMULTILINE"=> "(.|\n)*"
                    }
                  }

                date {
                        match => [ "[system][auth][timestamp]",
                        "MMM  d HH:mm:ss",
                    "MMM dd HH:mm:ss"
                    ]
                    target => "[system][auth][timestamp]"
                }

                mutate {
                  convert => { "[system][auth][pid]" => "integer" }
                  convert => { "[system][auth][groupadd][gid]" => "integer" }
                  convert => { "[system][auth][user][add][uid]" => "integer" }
                  convert => { "[system][auth][user][add][gid]" => "integer" }
```

(continues on next page)

(continued from previous page)

```
                }
      }
    }
```

CHAPTER 89

Logstash Filter “network”

This filter processing an event data with network type:

```
filter {
 if [type] == "network" {
     grok {
        named_captures_only => true
        match => {
            "message" => [

            # Cisco Firewall
            "%{SYSLOG5424PRI}%{NUMBER:log_sequence#}:%{SPACE}%{IPORHOST:device_ip}: (?
↪:.)?%{CISCOTIMESTAMP:log_data} CET: %%{CISCO_REASON:facility}-%{INT:severity_level}-
↪%{CISCO_REASON:facility_mnemonic}:%{SPACE}%{GREEDYDATA:event_message}",

            # Cisco Routers
            "%{SYSLOG5424PRI}%{NUMBER:log_sequence#}:%{SPACE}%{IPORHOST:device_ip}: (?
↪:.)?%{CISCOTIMESTAMP:log_data} CET: %%{CISCO_REASON:facility}-%{INT:severity_level}-
↪%{CISCO_REASON:facility_mnemonic}:%{SPACE}%{GREEDYDATA:event_message}",

            # Cisco Switches
            "%{SYSLOG5424PRI}%{NUMBER:log_sequence#}:%{SPACE}%{IPORHOST:device_ip}: (?
↪:.)?%{CISCOTIMESTAMP:log_data} CET: %%{CISCO_REASON:facility}-%{INT:severity_level}-
↪%{CISCO_REASON:facility_mnemonic}:%{SPACE}%{GREEDYDATA:event_message}",
            "%{SYSLOG5424PRI}%{NUMBER:log_sequence#}:%{SPACE}(?:.)?%
↪{CISCOTIMESTAMP:log_data} CET: %%{CISCO_REASON:facility}-%{INT:severity_level}-%
↪{CISCO_REASON:facility_mnemonic}:%{SPACE}%{GREEDYDATA:event_message}",

            # urzadzenia HP switches
            "%{SYSLOG5424PRI}%{SPACE}%{CISCOTIMESTAMP:log_data} %{IPORHOST:device_ip}
↪%{CISCO_REASON:facility}:%{SPACE}%{GREEDYDATA:event_message}"
            ]

        }
    }
```

(continues on next page)

(continued from previous page)

```
    syslog_pri { }

    if [severity_level] {

      translate {
        dictionary_path => "/etc/logstash/dictionaries/cisco_syslog_severity.yml"
        field => "severity_level"
        destination => "severity_level_descr"
      }

    }

    if [facility] {

      translate {
        dictionary_path => "/etc/logstash/dictionaries/cisco_syslog_facility.yml"
        field => "facility"
        destination => "facility_full_descr"
      }

    }

     # okreslamy locality dla adresow IP na listach ACL
     if [event_message] =~ /(\d+.\d+.\d+.\d+)/ {
      grok {
        match => {
        "event_message" => [
            "list %{NOTSPACE:[acl][name]} %{WORD:[acl][action]} %{WORD:[acl][proto]} %
↪{IP:[src][ip]}.*%{IP:[dst][ip]}",
            "list %{NOTSPACE:[acl][name]} %{WORD:[acl][action]} %{IP:[src][ip]}",
            "^list %{NOTSPACE:[acl][name]} %{WORD:[acl][action]} %{WORD:[acl][proto]}
↪%{IP:[src][ip]}.*%{IP:[dst][ip]}"
            ]
        }
      }
    }

    if [src][ip] {

        cidr {
           address => [ "%{[src][ip]}" ]
           network => [ "0.0.0.0/32", "10.0.0.0/8", "172.16.0.0/12", "192.168.0.0/16",
↪ "fc00::/7", "127.0.0.0/8", "::1/128", "169.254.0.0/16", "fe80::/10","224.0.0.0/4",
↪"ff00::/8","255.255.255.255/32"  ]
           add_field => { "[src][locality]" => "private" }
        }

        if ![src][locality] {
           mutate {
              add_field => { "[src][locality]" => "public" }
           }
        }
    }


    if [dst][ip] {
```

(continues on next page)

(continued from previous page)

```
        cidr {
           address => [ "%{[dst][ip]}" ]
           network => [ "0.0.0.0/32", "10.0.0.0/8", "172.16.0.0/12", "192.168.0.0/16",
↪ "fc00::/7", "127.0.0.0/8", "::1/128",
                "169.254.0.0/16", "fe80::/10","224.0.0.0/4", "ff00::/8","255.255.255.
↪255/32" ]
           add_field => { "[dst][locality]" => "private" }
        }

        if ![dst][locality] {
           mutate {
              add_field => { "[dst][locality]" => "public" }
           }
        }
    }

    # date format
    date {
      match => [ "log_data",
        "MMM dd HH:mm:ss",
        "MMM  dd HH:mm:ss",
        "MMM dd HH:mm:ss.SSS",
        "MMM  dd HH:mm:ss.SSS",
        "ISO8601"
      ]
      target => "log_data"
    }

 }
}
```

CHAPTER 90

Logstash - Filter “geoip”

This filter processing an events data with IP address and check localization:

```
filter {
     if [src][locality] == "public" {

        geoip {
            source => "[src][ip]"
            target => "[src][geoip]"
            database => "/etc/logstash/geoipdb/GeoLite2-City.mmdb"
            fields => [ "city_name", "country_name", "continent_code", "country_code2
↪", "location" ]
            remove_field => [ "[src][geoip][ip]" ]
        }

        geoip {
            source => "[src][ip]"
            target => "[src][geoip]"
            database => "/etc/logstash/geoipdb/GeoLite2-ASN.mmdb"
            remove_field => [ "[src][geoip][ip]" ]
        }

     }

     if [dst][locality] == "public" {

        geoip {
            source => "[dst][ip]"
            target => "[dst][geoip]"
            database => "/etc/logstash/geoipdb/GeoLite2-City.mmdb"
            fields => [ "city_name", "country_name", "continent_code", "country_code2
↪", "location" ]
            remove_field =>  [ "[dst][geoip][ip]" ]
        }
```

(continues on next page)

(continued from previous page)

```
        geoip {
            source => "[dst][ip]"
            target => "[dst][geoip]"
            database => "/etc/logstash/geoipdb/GeoLite2-ASN.mmdb"
            remove_field => [ "[dst][geoip][ip]" ]
        }
     }

}
```

CHAPTER 91

Logstash - Output to Elasticsearch

This output plugin sends all data to the local Elasticsearch instance and create indexes:

```
output {
    elasticsearch {
       hosts => [ "127.0.0.1:9200" ]
       #http_compression => true
       #sniffing => true

       index => "%{type}-%{+YYYY.MM.dd}"

       user => "logserver"
       password => "logserver"
    }
}
```

CHAPTER 92

Logstash pluging for “naemon beat”

This Logstash plugin has example of complete configuration for integration with naemon application:

```
input {
    beats {
        port => FILEBEAT_PORT
        type => "naemon"
    }
}

filter {
    if [type] == "naemon" {
        grok {
            patterns_dir => [ "/etc/logstash/patterns" ]
            match => { "message" => "%{NAEMONLOGLINE}" }
            remove_field => [ "message" ]
        }
        date {
            match => [ "naemon_epoch", "UNIX" ]
            target => "@timestamp"
            remove_field => [ "naemon_epoch" ]
        }
    }
}

output {
    # Single index
#    if [type] == "naemon" {
#        elasticsearch {
#            hosts => ["ELASTICSEARCH_HOST:ES_PORT"]
#            index => "naemon-%{+YYYY.MM.dd}"
#        }
#    }

    # Separate indexes
```

(continues on next page)

(continued from previous page)

```
    if [type] == "naemon" {
        if "_grokparsefailure" in [tags] {
            elasticsearch {
                hosts => ["ELASTICSEARCH_HOST:ES_PORT"]
                index => "naemongrokfailure"
            }
        }
        else {
            elasticsearch {
                hosts => ["ELASTICSEARCH_HOST:ES_PORT"]
                index => "naemon-%{+YYYY.MM.dd}"
            }
        }
    }
}
```

CHAPTER 93

Logstash pluging for “perflog”

This Logstash plugin has example of complete configuration for integration with perflog:

```
input {
  tcp {
    port => 6868
    host => "0.0.0.0"
    type => "perflogs"
  }
}

filter {
  if [type] == "perflogs" {
    grok {
      break_on_match => "true"
      match => {
        "message" => [
          "DATATYPE::%{WORD:datatype}\tTIMET::%{NUMBER:timestamp}\tHOSTNAME::%
↪{DATA:hostname}\tSERVICEDESC::%{DATA:servicedescription}\tSERVICEPERFDATA::%
↪{DATA:performance}\tSERVICECHECKCOMMAND::.*?HOSTSTATE::%{WORD:hoststate}
↪\tHOSTSTATETYPE::.*?SERVICESTATE::%{WORD:servicestate}\tSERVICESTATETYPE::%
↪{WORD:servicestatetype}",
          "DATATYPE::%{WORD:datatype}\tTIMET::%{NUMBER:timestamp}\tHOSTNAME::%
↪{DATA:hostname}\tHOSTPERFDATA::%{DATA:performance}\tHOSTCHECKCOMMAND::.*?HOSTSTATE::
↪%{WORD:hoststate}\tHOSTSTATETYPE::%{WORD:hoststatetype}"
          ]
        }
      remove_field => [ "message" ]
    }
    kv {
      source => "performance"
      field_split => "\t"
      remove_char_key => "\.\'"
      trim_key => " "
      target => "perf_data"
```

(continues on next page)

(continued from previous page)

```
      remove_field => [ "performance" ]
      allow_duplicate_values => "false"
      transform_key => "lowercase"
    }
    date {
      match => [ "timestamp", "UNIX" ]
      target => "@timestamp"
      remove_field => [ "timestamp" ]
    }
  }
}

output {
  if [type] == "perflogs" {
    elasticsearch {
      hosts => ["127.0.0.1:9200"]
      index => "perflogs-%{+YYYY.MM.dd}"
    }
  }
}
```

CHAPTER 94

CHANGELOG

CHAPTER 95

2.1.17

95.1 Added

- Export Dashboard to PDF

95.2 Changed

- bugfix dashboard generation using phantomjs

CHAPTER 96

2.1.24

96.1 Added

- Report generation time added to the PDF

96.2 Changed

- bugfix export Dashboard relative paths
- bugfix bigger dashboards
- bugfix relative path bug fix
- bugfix Export to CSV

CHAPTER 97

2.1.26

97.1 Added

- Kibana Reporting plugin

97.2 Changed

- bugfix for report generation date on PDF
- bugfix elastalert auth jar
- bugfix reports validation

CHAPTER 98

2.1.27

98.1 Added

- Password Change function
- Deleting old CSV/PDF function

CHAPTER 99

2.1.28

99.1 Added

- CSV Reports moved to reports tab

99.2 Changed

- bugfix ES Auth Plugin Jar
- bugfix Kibana
- bugfix for scheduler index

CHAPTER 100

2.1.29

100.1 Added

- Basic Auth function

CHAPTER 101

2.1.30

101.1 Changed

- bugfix From and To date on CSV CSV Task Export

CHAPTER 102

2.1.31

102.1 Changed

- bugfix auth-local-cookie.js change url to css file to relative
- bugfix fter submit command on ‘export dashboard’ page, Dashboard field shines in red
- bugfix server should not allow GET (even if user manually change request) server side verification
- bugfix In Export Task Managment tab use Search query “*” i Time Criteria Field Name as “@timestamp” by default

CHAPTER 103

2.1.32

103.1 Added

- Introduction of CSRF Tokens for each action. The CSRF Token can be generated once at login and appended to all GET / POST actions.

CHAPTER 104

2.1.33

104.1 Added

- Changing your password require you to enter your current password.
- Password change form require you to enter a new password twice.
- Cookies new flags: expires, secure, domain.

104.2 Changed

- bugfix Password Change function

CHAPTER 105

2.1.34

105.1 Added

- Auto create user elastalert by kibana with random password (like logserver user)
- Change Admin tab to Config
- Deleting a user or role should require confirmation that the user is sure about this action.

105.2 Changed

- bugfix: Marvel plugin problem with auth plugin enabled.
- bugfix: Public directory https://127.0.0.0.1:5601/bundles/

CHAPTER 106

2.1.35

106.1 Added

- In audit.log should not appear _bulk (default off)
- In audit.log should not appear password update/create request.
- In audit.log query output on/off (default on)
- Userlist and Rolelist alphabeticaly
- Add username in Password change page info about role on change page

CHAPTER 107

2.1.37

107.1 Added

- Non logged user which clicks on the link to the dashboard is redirected to the login page, and after successfully logging user is redirected to Discovery section rnot to the dashboard from the link

CHAPTER 108

2.2.1

108.1 Added

- Introduction to Licensing module

CHAPTER 109

2.2.2

109.1 Added

- Licensing module

CHAPTER 110

2.2.3

110.1 Added

- Code Documentation

110.2 Changed

- bugfix: in User/Role Update

CHAPTER 111

2.3.0

111.1 Added

- Object Management Elastafilter (kibana)
- Active Directory AD Integration (elasticsearch-auth)

111.2 Changed

- bugfix: in Alerts module (kibana)

CHAPTER 112

2.3.3

112.1 Added

- AD config moved to elasticsearch.yml (elasticsearch-auth)

112.2 Changed

- bugfix: Dashboards elastafilter (kibana)

CHAPTER 113

2.3.4

113.1 Added

- In Config-> settings: Miliseconds to seconds change
- Ldap/AD auth as optional

113.2 Changed

- bugfix Userlist problem no roles selected after Update action
- bugfix elasticsearch logging

CHAPTER 114

2.3.5

114.1 Added

- Timepicker on task export changed from 2015-05-19 to 2018-01-01*
- Object permission selector set/unset all
- Java jdk1.8.0_161 added to git
- Phantomjs added as kibana dependency
- Marvel added to git

114.2 Changed

- bugfix: If admin create role with /* pattern causes elasticsearch and kibana (no connection to elasticsearch) crash in loop. . . .
- bugfix: Default config settings with elastafilter problem with timeout 0/token expire etc
- bugfix: In Alert -> Flatline bad example
- bugfix: In Alert -> Alert writeback index based on the configuration file.

CHAPTER 115

2.3.6

115.1 Added

- LDAP/AD SSL Support
- Title and Logos change to Logserver

115.2 Changed

- bugfix: no Rules directory for alert
- bugfix: Example LDAP settings change

CHAPTER 116

2.3.7

116.1 Added

- Logserver/Energy tab changed to Search tab in Kibana
- Show license details in Kibana
- Added default system settings for services [sysctl,limits.d]
- Java dir changed => jdk-1.8.0_161.tar.bz2
- New default users: logserver, alert, scheduler, intelligence

116.2 Changed

- bugfix: Exception in thread "Timer-1"
- bugfix: Default elastalert password changed

CHAPTER 117

2.3.8

117.1 Added

- Intelligence plugin
- Schedule plugin
- Added kibana/elasticsearch PayLoad settings to config files.

117.2 Changed

- bugfix: All shards failed in Discovery Tab => (elastafilter limits)
- bugfix: LDAP settings format

CHAPTER 118

2.3.9

118.1 Added

- Intelligence plugin upgrade
- Schedule plugin upgrade
- Alerts upgrade
- Java upgrade to 1.8_171
- Added index-rotation.sh script for audit & alert index

118.2 Changed

- bugfix: All shards failed in Discovery Tab => (elastafilter limits)
- bugfix: Max clause limit => 10240

CHAPTER 119

2.4.0

119.1 Added

- Preview & Status in Intelligence section
- Role-Mapping for AD
- Default Users Role
- Added scripts\ldap-alias-create.sh for AD User Alias
- Example Alert Dashboard

119.2 Changed

- bugfix: Intelligence Trend

CHAPTER 120

2.4.1

120.1 Changed

- bugfixes: Intelligence Scheduler Login Filter
- bugfixes: elasticsearch-auth plugin

CHAPTER 121

2.4.2

121.1 Added

- Timelion
- More detailed logs Kibana
- More detailed logs Intelligence
- PDF/CSV reports for AD users
- Alerts preview for Users
- New Alert SAVE button

121.2 Changed

- bugfix: audit index: @timestamp
- bugfix: Intelligence Trend Threshold fix
- bugfix: Intelligence (SPARK_LOCAL_IP)
- bugfix: Mangement typo in Reports
- bugfix: Objects import
- bugfix: Recovery Alert Dashboard fix
- bugfix: Password update/change disabled for AD users

CHAPTER 122

2.4.3

122.1 Added

- Kibana role for GUI users
- Alert role for Alert Module users
- Intelligence role for A/I Module users
- Intelligence temporary directory
- Intelligence Preview update

CHAPTER 123

2.4.4

123.1 Added

- SSO single sign on implementation
- Improved installation process
- OpenJDK Support
- Removed all unnecessary dependencies
- Removed python libraries (pip)
- Logstash configuration examples
- OVF changed to OVA

123.2 Changed

- bugfix: Conflict during system upgrade (yum update)
- bugfix: journald.conf conflict
- bugfix: Defaultrole AD users
- bugfix: start_date Intelligence module

CHAPTER 124

2.4.5

124.1 Added

- New Login Page with SSO support
- Alert module update

124.2 Changed

- bugfix: metric_aggregation, new term, percentage_match