Documentation

Installation and Configuration Guide

IDM Audit Dashboard 2.5

for NetIQ Identity Manager (version 4 or higher)

Version:	2.5
created:	March 7, 2018
last modified:	January 9, 2020
File:	Audit_Dashboard_Installation_Manual_v2.5.docx

Contents

1. Legal Notice 4

2. Introduction 5
2.1 Components 5
2.2 Requirements 5

3. Installation 7
3.1 Check and install Oracle Java 7
3.1.1 Check Java installation for Linux 7
3.1.2 Check Java installation for Windows 7
3.1.3Official installation of Oracle Java 8
3.1.4 Global configuration of JAVA_HOME for Linux 8
3.1.5 Global configuration of JAVA_HOME for Windows 8
3.2 Install Elasticsearch 1.4.4 8
3.2.1 Configure file changes (Elasticsearch 1.4.4) 10
3.2.2 Start, stop, status of Elasticsearch 10
3.2.3 Check if your Elasticsearch 1.4.4 is running 11
3.3 Install Elasticsearch 6.2.4 12
3.3.1 Check if your Elasticsearch 6.2.4 is running 13
3.4 Install Kibana 6.2.4 14
3.4.1 Check if your Kibana 6.2.4 is running 15
3.5 Install the Audit Proxy 16
3.5.1Install the Audit Proxy for Linux 16
3.5.2Install the Audit Proxy for Windows 16
3.5.3Configure the Audit Proxy 17
3.6 Install and configure the Audit Server 18
3.6.1 Unpacking and manual start 18
3.6.2 Make runnable as a service for Linux 19
3.6.3 Make runnable as a process for Windows 20
3.6.4 First start of Audit Server 21
3.6.5 Check if your Audit Server is running 23
3.6.6 Configure the Audit Server 24
3.7 The Audit Driver 27
3.7.1 Create the driver 27
3.7.2 Test the driver 31
3.7.3 Update the driver 32

4.Install the Report Service 34
4.1 Extract and manual start 34
4.2 Make runnable as service for Linux 35
4.3 Make runnable as a service for Windows 36

4.4 Check the history 38

5 Install the Audit Export service 39
5.1. Extract and manual start 39
5.2 Make runnable as service for Linux 39
5.3 Make runnable as service for Windows 40
5.4 Check if your Audit Export service is running. 42
5.5 Configure the Audit Export 42

6 Dashboards 43
6.1 Sample dashboards 43
6.2 Dashboards on Kibana 3 (Elasticsearch 1.4.4) 43
6.2.1 Modify a Dashboard 43
6.2.2 Experience the IDM Audit Dashboard 45
6.2.3 Understand the IDM Audit Dashboard 46
6.2.4 Work with Panels 47
6.3 Dashboards on Kibana 6 (Elasticsearch 6.x) 52
6.3.1 Create new visualization. 52
6.3.2 Create new dashboard. 54
6.3.3. Using the dashboards 55

7 Report Editor 57
7.1 Actions in Report Editor 57
7.2 Report editing 58

8 Configuring LDAP authentication for Audit Server 65

Conclusion 69

Attachment 1 70

Attachment 2 73

Attachment 3 79

1. Legal Notice

SKyPRO AG makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose.
Further, SKyPRO AG reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.
Further, SKyPRO AG makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose.
Further, SKyPRO AG reserves the right to make changes to any and all parts of SKyPRO software, at any time, without any obligation to notify any person or entity of such changes.
Any products or technical information provided under this Agreement may be subject to the Swiss export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current Swiss export exclusion lists or to any embargoed or terrorist countries as specified in the Swiss export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. SKyPRO assumes no responsibility for your failure to obtain any necessary export approvals.

SKyPRO AG
Gewerbestrasse 7
CH-6330 Cham
SWITZERLAND

www.skypro.eu

About this document

This document explains the installation and configuration of the "IDM Audit & Compliance dashboard."

Audience

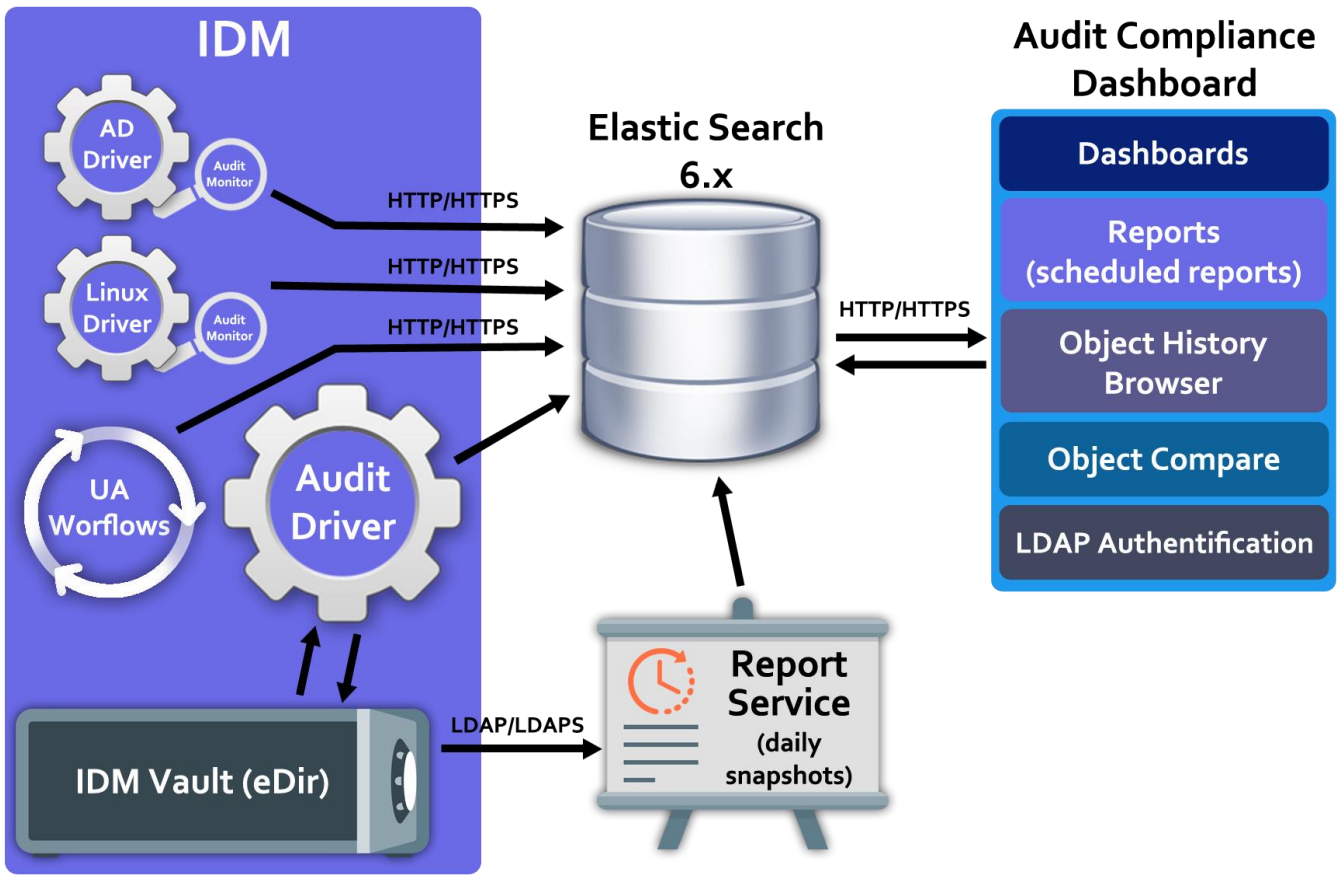
This guide is intended for administrators maintaining existing NetIQ Identity Manager environments. You should have an understanding of drivers, workflows, eDirectory, and the IDM Designer tool.

Feedback

We appreciate your comments and suggestions about our products and documentation. If you have any suggestions, comments, or feature requests please contact us via info@skypro.ch or in our Live Chat https://www.skypro.eu/en/services/support/#

2. Introduction

2.1 Components



2.2 Requirements

Due to the fact that as of April 2015 Oracle no longer releases public updates for Java 7, we recommend you to use the latest available version of Java 8. Make sure that your system meets the system requirements necessary for the normal functioning of the IDM Audit Dashboard server and components.
Official supporting platforms for Java 8:

Linux	Oracle Linux 6.x (64-bit) 2 Oracle Linux 7.x (64-bit) 2 (8u20 or later) Red Hat Enterprise Linux 6.x (64-bit) 2 Red Hat Enterprise Linux 7.x (64-bit) 2 (8u20 or later) Centos 6, 7 Suse Linux Enterprise Server 10 SP2 +, 11.x Suse Linux Enterprise Server 12.x (64-bit) 2 (8u31 or later) Ubuntu Linux 12.04 LTS, 13.x Ubuntu Linux 14.x (8u25 or later) Ubuntu Linux 16.x

Mac OS X	Mac with Intel processor under Mac OS X 10.8.3+, 10.9+ running
Windows	Windows 10 (8u51 or later) Windows 8.x (Desktop version) Windows 7 with service pack 1 (SP1) Windows Vista SP2 (x64 version) Windows Server 2008 R2 with service pack 1 (SP1) (x64 version) Windows Server 2012 and 2012 R2, 2013, 2014, 2015, 2016 (x64 version)

Hardware requirements for Audit Dashboard components:

Audit Server	Processor: Not less than 2266 MHz Ram: Not less than 2GB Disk space: Not less than 500 MB Processor architecture: x64
Audit Report service	Processor: Not less than 2266 MHz RAM: Not less than 1GB Disk space: Not less than 200 MB Processor architecture: x64
Audit Export service	Processor: Not less than 2266 MHz RAM: Not less than 2GB Disk space: Not less than 1000 MB Processor architecture: x64
Audit Driver	Identity Manager official requirements https://www.netiq.com/documentation/idm402/
Elasticsearch 1.4	Elasticsearch official requirements https://www.elastic.co/guide/en/elasticsearch/guide/1.x/hardware.html
Elasticsearch 6.x	Elasticsearch official requirements https://www.elastic.co/guide/en/elasticsearch/reference/6.2/index.html
AuditProxy	Processor: Not less than 2266 MHz RAM: Not less than 1GB Disk space: Not less than 100 MB Processor architecture: x64

Choose from the following platform:

- Java: Version 8 or higher http://java.com/en/download/help/sysreq.xml
- NetIQ Identity Manager (version 4 or higher) https://www.netiq.com/documentation/idm402/

3. Installation

To install the IDM Audit Dashboard, go to our web site https://www.skypro.eu/en/products/idm-audit-dashboard/ and download the complete installation file *AuditDashboard_v2.x.zip*. (where 2.x is currently available version for download).
This file contains all the needed components. After downloading, please unpack it. You will see the following packages:

- AuditDriver.zip
- AuditServer.zip
- AuditProxy.zip
- Elasticsearch-1.4.4.zip
- elasticsearch-6.X.X.zip
- kibana-6.X.X-linux-x86_64.zip
- kibana-6.X.X-windows-x86_64.zip
- AuditReport.zip
- AuditExport.zip

3.1 Check and install Oracle Java

IDM Audit Dashboard components require Oracle Java to be installed. We recommend using Java 8.
Java installation varies by platform. To check if Java is needed to be installed, please follow the next steps depending on your platform:

3.1.1 Check Java installation for Linux

To check if Java is installed, please run the following commands in your Terminal:

whereis java
YOUR_JAVA_LOCATION/java -version
echo $JAVA_HOME

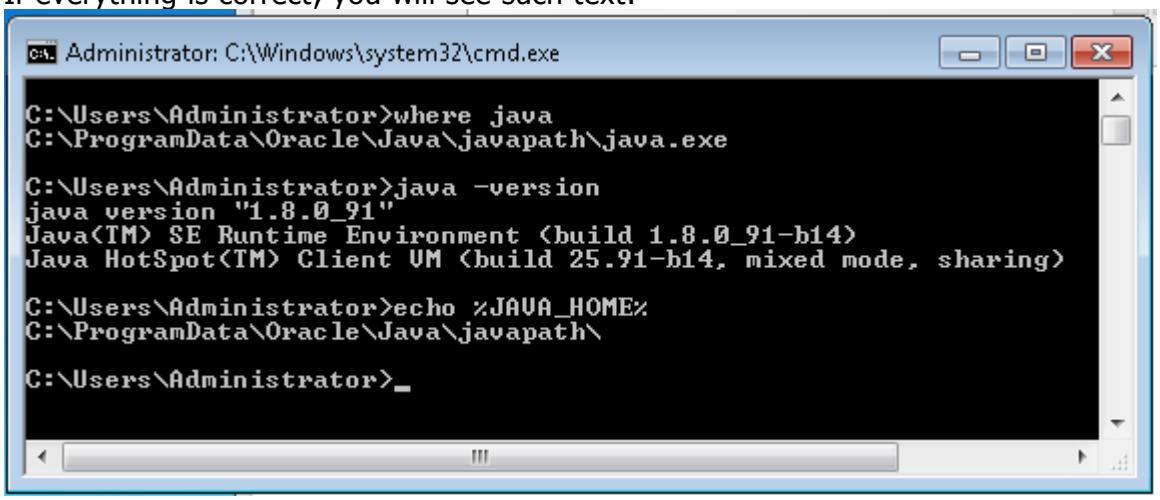
If all is correct, you will see the text like this:

3.1.2 Check Java installation for Windows

To check if Java is installed, please run the following commands in Windows Command Processor (cmd.exe):

where java
YOUR_JAVA_LOCATION/java -version
echo %JAVA_HOME%

If everything is correct, you will see such text:



3.1.3 Official installation of Oracle Java

If no Java 8 is installed, please follow the official installation instructions from Oracle: http://www.java.com/en/download/manual.jsp
If you have already installed Java 8 but JAVA_HOME or JAVA_PATH are not defined, you can manually define them for each service or make it globally.

3.1.4 Global configuration of JAVA_HOME for Linux

To define JAVA_HOME global for Linux, please follow these steps:

1. Create file "jdk_home.sh" in the "/etc/profile.d" folder
2. Add the following commands to this file:

   export JAVA_HOME=PATH_OF_YOUR_JAVA

   export PATH=$JAVA_HOME/bin:$PATH
3. Save this file.
4. Restart your server or terminal.

3.1.5 Global configuration of JAVA_HOME for Windows

If no Java 8 is installed, please follow the official installation instructions from Oracle: http://www.java.com/en/download/manual.jsp
If you have already installed Java 8 but JAVA_HOME or JAVA_PATH are not defined, you can manually define them for each service or make it globally.
To define JAVA_HOME global in Windows, please follow official instruction https://www.java.com/en/download/help/path.xml

3.2 Install Elasticsearch 1.4.4

If you plan to use Elasticsearch 1.4.4 with Kibana 3.x, please follow the instructions below. If you plan to use Elasticsearch 6.X with Kibana 6.x skip this chapter and go to the chapter 3.3.

The first step is to install Elasticsearch 1.4.4:

1. Extract the archive

Extract content of the "Elasticsearch-1.4.4.zip" file

- For Linux use the following command:

  unzip Elasticsearch-1.4.4.zip

- For Windows please use Windows Explorer option "Extract All"

  After extraction you will get the following packages:
  ZIP – for Windows
  DEB – for Debian-based distributives (Ubuntu, Debian, etc.)
  RPM – for RPM-based distributives (CentOS, SLES, etc.)
  TAR – for Linux manual installation

2. Install Elasticsearch depending on your system.

(Please make sure that you have permission to install packages).

a. For Debian-based distributives please use this command:

sudo dpkg -i elasticsearch-1.4.4.deb

b. For RPM-based distributives please use this command:

rpm -i elasticsearch-1.4.4.noarch.rpm

c. Manual installation for Linux

1. Extract TAR GZIP archive by command:

tar -zxf elasticsearch-1.4.4.tar.gz

(After extraction, "elasticsearch-1.4.4" folder will be created automatically)

2. Move the extracted folder to the location you want.

e.g., "/opt/elasticsearch-1.4.4"

mv elasticsearch-1.4.4 /opt

(You can delete the tar.gz file afterwards)

3. To make Elasticsearch runnable as a service, please follow the official instructions:

https://www.elastic.co/guide/en/elasticsearch/reference/1.4/setup-service.html

d. Manual installation for Windows

1. Extract elasticsearch-1.4.4.zip archive by using Windows Explorer option "Extract All" (after extraction "elasticsearch-1.4.4" folder will be created automatically).

2. Move the extracted folder to the location you want.

e.g., "\Programs\elasticsearch-1.4.4"

(You can delete the zip file afterwards)

3. To make Elasticsearch runnable as a service, please follow the official instructions:

https://www.elastic.co/guide/en/elasticsearch/reference/1.4/setup-service-win.html

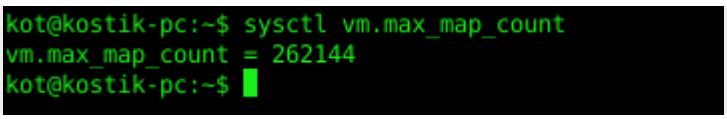
3.2.1 Configure file changes (Elasticsearch 1.4.4)

Configure Elasticsearch stored in "elasticsearch.yml" file which is located in "config" folders for manual installation or in "/etc/elasticsearch" for Linux DEB and RPM distributives. To make changes, you need to edit this file in text editor:

1. Change the cluster name.
   Uncomment line "cluster.name: xxxxxxxxx" and rename your cluster name.
2. Increase Boolean operator's amount.
   Add the following line to the end of the file: "index.query.bool.max_clause_count: 16536"
3. Max opened files adjustments. If you have installed Elasticsearch manually, you need to increase the limit of max_file_descriptors with command:

sysctl -w vm.max_map_count=262144

If you installed Elasticsearch from RPM or DEB, this variable will be defined automatically; to check this run the command:
sysctl vm.max_map_count



4. Restart Elasticsearch.

3.2.2 Start, stop, status of Elasticsearch

For normal work of Audit Dashboard, make sure that Elasticsearch is running.
You can run it manually from the Elasticsearch folder:

- on Linux bin/elasticsearch
- on Windows bin/elasticsearch.bat

For a production environment we recommend making Elasticsearch runnable as a service with each system start.

For Linux, use the following commands to control your Elasticsearch server (from users which have permissions to do this):

- Check status **service elasticsearch status**
- Start service **service elasticsearch start**
- Stop service **service elasticsearch stop**

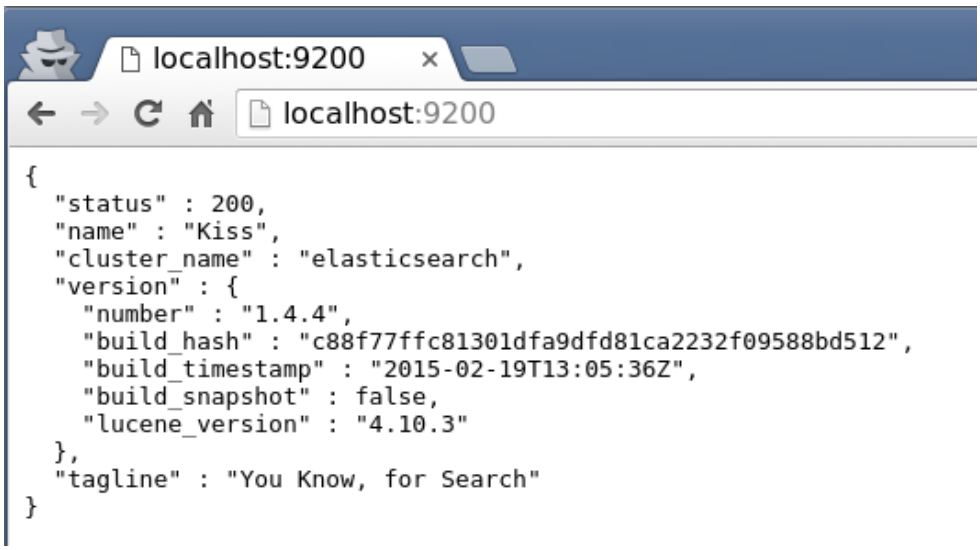
For Windows, use "service.bat" commands to control your Elasticsearch service (located in "bin" folder):

- Install as a service **service.bat install**
- Remove service **service.bat remove**
- Start service **service.bat start**
- Stop service **service.bat stop**
- Start GUI manager **service.bat manager**

For more details, please read official instructions:
https://www.elastic.co/guide/en/Elasticsearch/reference/1.4/setup-service-win.html

3.2.3 Check if your Elasticsearch 1.4.4 is running

After your Elasticsearch server is started, please make sure that it is working correctly.
To check if Elasticsearch is running:
Open the following URL in a browser: http://HOST:9200
(HOST is name or IP address of the server where Elasticsearch is installed. e.g., http://127.0.0.1:9200)



If everything is successful, you will see JSON data with the current status of the Elasticsearch server.
Use CURL command (you should have installed CURL):
curl -XGET 'http://HOST:9200'
If everything is successful, you will see JSON data with the current status of the Elasticsearch server.

Now you can go to the next step.
For more details, please follow the official instructions for installation of Elasticsearch: https://www.elastic.co/guide/en/elasticsearch/reference/1.4/_installation.html
If you deploy Elasticsearch for production, please follow the official deploying user guide: https://www.elastic.co/guide/en/elasticsearch/guide/1.x/deploy.html

3.3 Install Elasticsearch 6.2.4

If you plan to use Elasticsearch 1.4.4 with Kibana 3.x, please skip this chapter.

The first step is to install Elasticsearch 6.2.4:

1. Extract the archive

   Extract content of the "elasticsearch-6.2.4.zip" file

   - For Linux use the following command:

   unzip elasticsearch-6.2.4.zip

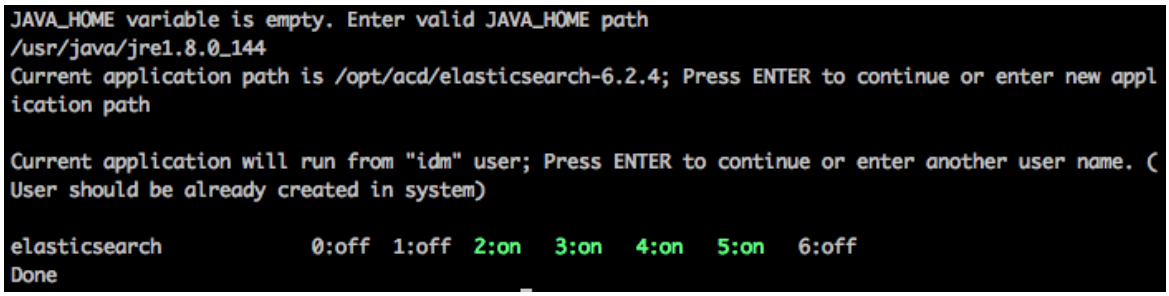
   - For Windows please use Windows Explorer option "Extract All"

   (After extraction "elasticsearch-6.2.4" folder will be created automatically.)

2. Install Elasticsearch depending on your system.

(Please make sure that you have permission to install packages. Due the fact that Elasticsearch can not be running from "root" user you need to create some user, how to do this please look in Attachment 3)

To install elasticsearch on linux and configure start/stop scripts you need to run "./install-autostart.sh" from the elasticsearch-6.2.4 folder (with root priveleges)



a) On first step script will try to detect your Java home path, if it will be not found or you want to use own, you need to defined path end press Enter. If you agree with provided path, you can switch to step two.

b) on second step script will detect the location of your Elasticsearch installation, if you agree – just press Enter, if not, define your path and press Enter.

c) on third step script will ask you from which user you want Elasticsearch will be running, by default we use user "idm", if you created another please fill your username.

d) after configuration script installed all needed files and you can easy manage your Elasticsearch with start/stop commands.

Run following commands from root user

service elasticsearch start or /etc/init.d/elasticsearch start – for start

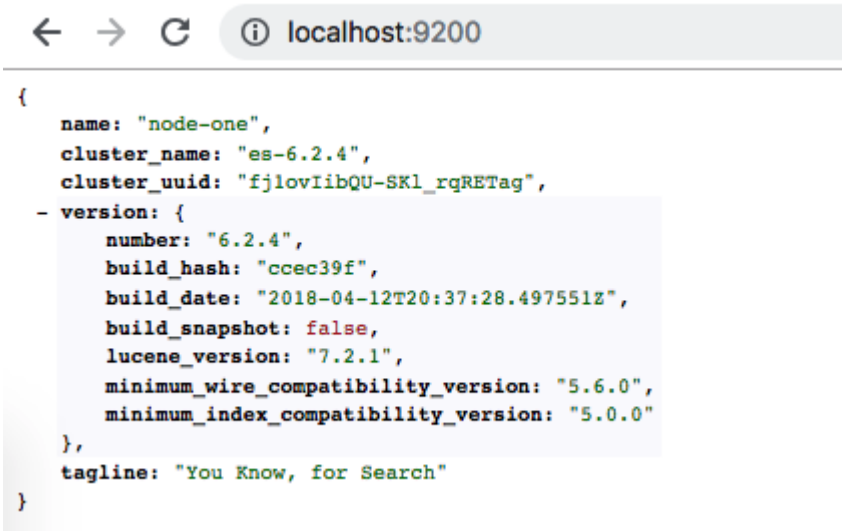
service elasticsearch stop or /etc/init.d/elasticsearch stop – for stop

service elasticsearch status or /etc/init.d/elasticsearch status – for check status

To make Elasticsearch runnable as a service on Windows, please follow the official instructions: https://www.elastic.co/guide/en/elasticsearch/reference/2.3/setup-service-win.html

3.3.1 Check if your Elasticsearch 6.2.4 is running

After your Elasticsearch server is started, please make sure that it is working correctly.
To check if Elasticsearch is running:
Open the following URL in a browser: http://127.0.0.1:9200
(by default Elasticsearch 6.2.4 already configured to listen localhost on port 9200)



If everything is successful, you will see JSON data with the current status of the Elasticsearch server.

Use CURL command (you should have installed CURL):
curl -XGET 'http://127.0.0.1:9200'

If everything is successful, you will see JSON data with the current status of the Elasticsearch server.

Now you can go to the next step.
For more details, please follow the official instructions for installation of Elasticsearch: https://www.elastic.co/guide/en/elasticsearch/reference/6.2/index.html

3.4 Install Kibana 6.2.4

If you plan to use Kibana 6.2.4 please make sure that Elasticsearch 6.2.4 installed and running.
The first step is to install Kibana:

1. Extract the archive

   Extract content of the "kibana-6.2.4-linux-x86_64.zip" file for linux,

   or kibana-6.2.4-windows-x86_64.zip file for windows

   - For Linux use the following command:

   unzip kibana-6.2.4-linux-x86_64.zip

   (After extraction "kibana-6.2.4-linux-x86_64" folder will be created automatically.)

   - For Windows please use Windows Explorer option "Extract All"

   (After extraction "kibana-6.2.4-windows-x86_64" folder will be created automatically.)

   - For Windows please use Windows Explorer option "Extract All"

   (After extraction "kibana-6.2.4-windows-x86_64" folder will be created automatically.)

2. Install Kibana depending on your system.

(Please make sure that you have permission to install packages. Due the fact that Kibana can not be running from "root" user you need to create some user, how to do this please look in Attachment 3)

To install Kibana on linux and configure start/stop scripts you need to run "./install-autostart.sh" from the kibana-6.2.4-linux-x86_64 folder (with root priveleges)

```
[root@idm46 kibana-6.2.4-linux-x86_64]# ./install-autostart.sh
Current application path is /mnt/disk2/skypro/acd_2_5_rls/kibana-6.2.4-linux-x86_64; Press ENTER
to continue or enter new application path

Current application will run from "idm" user; Press ENTER to continue or enter another user name.
 (User should be already created in system)

kibana-service  0:off   1:off   2:on    3:on    4:on    5:on    6:off
Done
[root@idm46 kibana-6.2.4-linux-x86_64]#
```

a) on first step script will detect the location of your Kibana installation, if you agree – just press Enter, if not, define your path and press Enter.

b) on second step script will ask you from which user you want Kibana will be running, by default we use user "idm", if you created another please fill your username.

d) after configuration script installed all needed files and you can easy manage your Kibana with start/stop commands.

Run following commands from root user

service kibana-service start or /etc/init.d/kibana-service start – for start

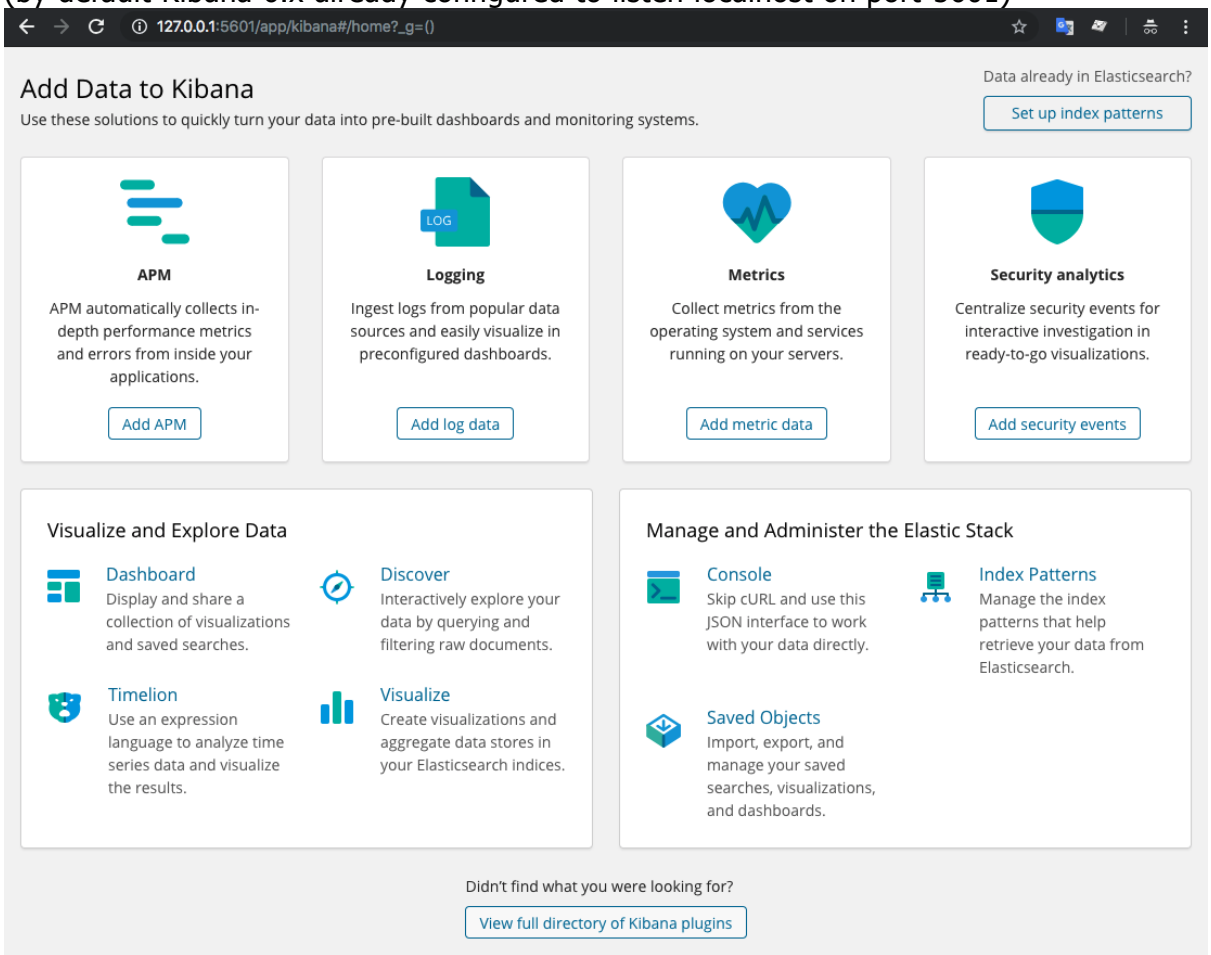
service kibana-service stop or /etc/init.d/kibana-service stop – for stop

service kibana-service status or /etc/init.d/kibana-service status – for check status

To make Kibana runnable as a service on Windows, please follow the official instructions: https://www.elastic.co/guide/en/kibana/6.2/windows.html

3.4.1 Check if your Kibana 6.2.4 is running

After your Kibana is started, please make sure that it is working correctly.
To check if Kibana is running:
Open the following URL in a browser: http://127.0.0.1:5601
(by default Kibana 6.x already configured to listen localhost on port 5601)



If everything is successful, you will see the Kibana default page.

Now you can go to the next step.

For more details, please follow the official instructions for installation of Kibana: https://www.elastic.co/guide/en/kibana/6.2/install.html

3.5 Install the Audit Proxy

1. Extract the archive.

Extract content of the "AuditProxy.zip"

- For Linux, use command:

unzip AuditProxy.zip

- For Windows, please use Windows Explorer option "Extract All"

(After extraction "AuditProxy" folder will be created automatically.)

2. Move the extracted folder.

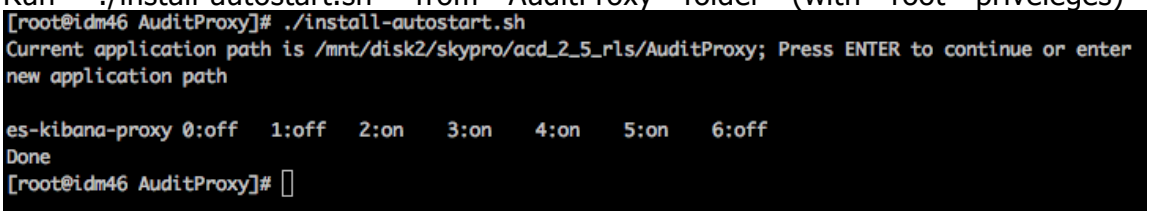
Move the extracted folder to the location you want.

- Linux: e.g., /opt/AuditProxy
- Windows e.g., \Programs\AuditProxy (you can delete the zip file afterwards)

3. For a production environment, we recommend making Audit Proxy runnable as a service with each system start. To make this, please follow these steps:

3.5.1 Install the Audit Proxy for Linux

a) Run "./install-autostart.sh" from AuditProxy folder (with root priveleges)



b) On first step script will detect the location of your AuditProxy installation, if you agree – just press Enter, if not, define your path and press Enter.

c) after configuration script installed all needed files and you can easy manage your AuditProxy with start/stop commands.

Run following commands from root user

service es-kiban-proxy start or /etc/init.d/es-kiban-proxy start – for start

service es-kiban-proxy stop or /etc/init.d/es-kiban-proxy stop – for stop

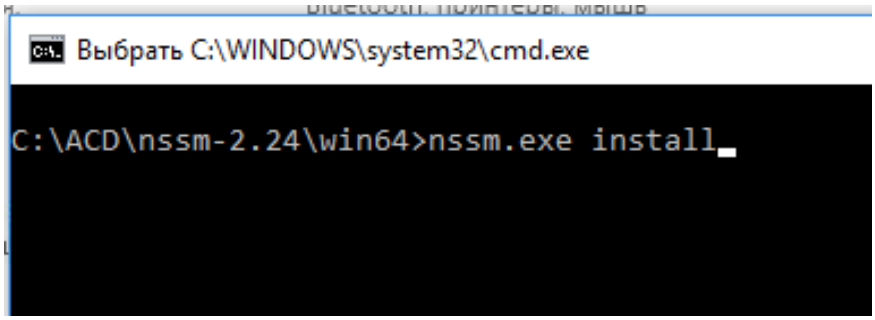
service es-kiban-proxy status or /etc/init.d/es-kiban-proxy status – for check status

d) for windows or mac-os please use corresponding executable file "kibana-http-proxy-win.exe" or "kibana-http-proxy-macos"

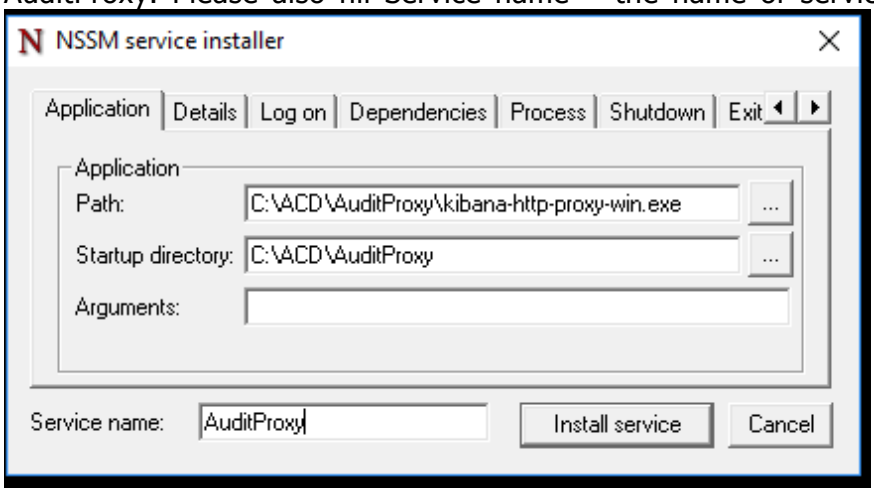
3.5.2 Install the Audit Proxy for Windows

a) To install you will need to use NSSM. Extract archive nssm-2.24.zip and run from nssm-2.24/win64 folder, command "nssm.exe install" (Use CMD shell).

b) After that application window will appear



c) Please fill the Path and Startup directory fields with location of your AuditProxy. Please also fill Service name – the name of service in Windows.



d) Press Install service button to finish.

e) Go to the Start -> Services and find AuditProxy service in list.

f) Start it.

3.5.3 Configure the Audit Proxy

By default Audit Proxy configured with default settings and it is possible to re-configure it via Audit Server admin panel. In some cases if you really need to do your settings manually, you need to edit config.json file, which placed in AuditProxy folder.

Each of this section have standard settings for web-service:

"port" – the number of network port

"username" – username which used for basic auth mechanism

"password" – password which used for basic auth mechanism

"useSSL" – flag which allow to enable or disable HTTPS protocol

"keyFile" – private key file used for HTTPS server (PEM – format)

"certFile" – certificate file used for encrypting HTTPS traffic (PEM format)

General section of AuditProxy config file is:

- "helpers" – web-service used for connection from AuditServer (admin interface)
- "elasticsearch" – web-service used for proxy Klasticsearch requests/responses
- "kibana" – web-service used for proxy Kibana requests/responses

- "ldap" contain settings for LDAP connection and user-rights groups

- "auditUrl" – url for back-auth with AuditServer

- "auditUrlCert" – certificate used for connection to AuditServer (if AuditServer had enabled SSL and use self-signed certificate)

3.6 Install and configure the Audit Server

3.6.1 Unpacking and manual start

The next step is the installation of the Audit Server components.
Make sure that you have Java installed. If no Java is installed, please follow the instructions on how to install Java on your system in chapter "3.1 Check and install Oracle Java."
The Audit Server is a self-extracting jar file. To install and start it please:

4. Extract the archive.

   Extract content of the "AuditServer.zip"

   - For Linux, use command:
   unzip AuditServer.zip
   - For Windows, please use Windows Explorer option "Extract All"

   (After extraction "AuditServer" folder will be created automatically.)

5. Move the extracted folder.

   Move the extracted folder to the location you want.

   - Linux: e.g., /opt/AuditServer
   - Windows e.g., \Programs\AuditServer (you can delete the zip file afterwards)

6. Check that your hostname is resolvable.

   Audit Server uses H2 database which mechanism is based on hostname of the server where it is running. Please make sure that hostname of your server is resolvable.

   - Linux hostname check

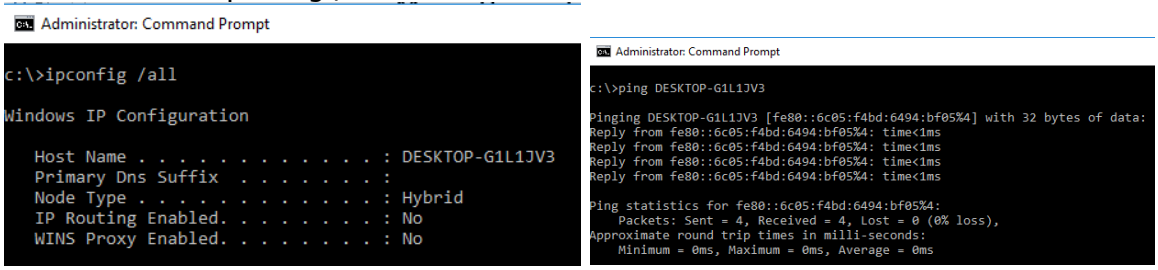
   Run command: **hostname**

```
ko@kostik-lin:~$ hostname
kostik-lin
ko@kostik-lin:~$ ping kostik-lin
PING kostik-lin (127.0.1.1) 56(84) bytes of data.
64 bytes from kostik-lin (127.0.1.1): icmp_seq=1 ttl=64 time=0.042 ms
^C
```

on Linux server terminal and you will get the hostname of your server
Try to ping your hostname, e.g. **ping your_host_name**
If all is ok you can continue; if the hostname is not resolvable please contact your system administrator or add a record to your /etc/hosts file.

- Windows hostname check

Run command: ipconfig /all



in windows Cmd console and you will get the hostname of your server
Try to ping your hostname, e.g. **ping your_host_name**
If all is ok you can continue; if the hostname is not resolvable please contact your system administrator or add a record to your Windows\System32\drivers\etc\hosts file.

3.6.2 Make runnable as a service for Linux

For a production environment, we recommend making Audit Server runnable as a service with each system start. To make this, please follow these steps:

a) Run "./install-autostart.sh" from AuditServer folder (as root user)

```
[root@idm46 AuditServer]# ./install-autostart.sh
JAVA_HOME path is: /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.121-1.b13.el6.x86_64/jre; Press ENTER to conti
nue or enter another path

Current application path is /mnt/disk2/skypro/acd_2_5_rls/AuditServer; Press ENTER to continue or enter
 new application path

audit-server    0:off   1:off   2:on    3:on    4:on    5:on    6:off
Done
[root@idm46 AuditServer]#
```

b) On first step script will try to detect your Java home path, if it will be not found or you want to use own you need to defined path end press Enter. If you agree with provided path, you can switch to step two.

c) On second step script will detect the location of your AuditServer installation, if you agree – just press Enter, if not, define your path and press Enter.

d) after configuration script installed all needed files and you can easy manage your AuditServer with start/stop commands.

Run following commands from root user

service audit-server start or /etc/init.d/audit-server start – for start

service audit-server stop or /etc/init.d/audit-server stop – for stop

service audit-server status or /etc/init.d/audit-server status – for check status

3.6.3 Make runnable as a process for Windows

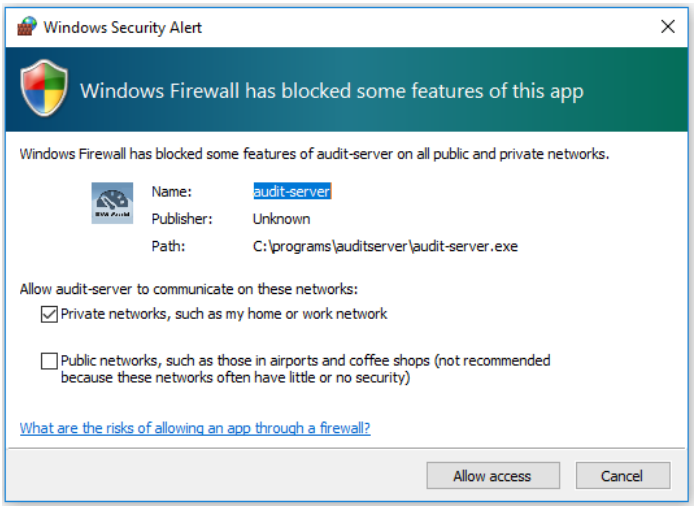
For a production environment, we recommend making Audit Server runnable as a Windows process with the system start. To make this, please follow these steps:

1. Open in editor "audit-server-64.ini" or "audit-server.ini", depending on your system architecture and Java.
2. Change "working.directory" variable with the path where the Audit Server is located, e.g., working.directory="c:\Programs \AuditServer".
3. Uncomment and change "vm.location" variable with location of the "JVM.dll" file (if your JAVA_PATH is not defined globally).

   e.g., vm.location="C:\program files\Java\jre1.8.0_91\bin\client\JVM.dll"

4. Run "audit-server-64.exe" or "audit-server.exe", depending on your system and Java installed.

   Please allow Firewall prompt. If everything is correct, you will see the Audit-Server process in the Windows Task Manager. You can end it by clicking the "End Process" button.



5. Open in editor "AuditServerTask.xml", (which is located in "service-script" folder of your Audit Server installation).

   f. Replace path between <command></command> tags.

   (The path should correspond to your "audit-server.exe" or "audit-server-64.exe" location.)

```
<Actions Context="Author">
  <Exec>
    <Command>C:\Programs\AuditServer\audit-server.exe</Command>
  </Exec>
</Actions>
```

6. Save file.
7. Run cmd.exe, CMD window will be opened.
8. Go to the folder where your Audit Server is located.

9. e.g., c:\Programs\AuditServer

10. Run the command for import AuditServerTask.xml to Task Scheduler:

schtasks /create /tn "AuditServer" /xml "service-script/AuditServerTask.xml" /RU "Administraror" /RP "YourPassword"

(Replace "Administrator" and "YourPassword" with the user name and the password of the user you would like to start Audit Server with).

*Make sure that the user which you use to run an Audit Server has Administrator permissions, because only with this permissions Audit Server will be started without logging in.

11. After the task has been successfully created, you need to restart your server.

3.6.4 First start of Audit Server

Start the Audit Server with the script or batch file, depending on your system:

- Linux first-run.sh
- Windows first-run.bat

(If JAVA_HOME variable is not defined on your system, you may have to adjust the path to Java Runtime Environment in script/batch file. The path to Java depends on your Java installation).

The first start wizard will running:

```
bash-3.2$ ./first-run.sh
This is application first launch! Configurating wizard will be started!
Connected
Your Server ID is: e17f7c80-ae91-4390-9e03-acb89523f9d7
License key (you can skip and install it later):
[Enter = ]

Audit Server IP address:
[1 = 10.242.2.3, 2 = 192.168.1.127, 3 = 127.0.0.1, 4 = custom define, Enter = 127.0.0.1]
1
Audit Server Portnumber:
[Enter = 3190]

Administrator Username:
[Enter = admin]

Administrator Password:
demodemo
Enable HTTPS for AuditServer:
[1 = yes, 2 = no, Enter = no]

Elasticsearch version:
[1 = 1.4, 2 = 6.x, Enter = 6.x]

Use Proxy service for Elasticsearch and Kibana:
[1 = yes, 2 = no, Enter = yes]

Proxy service IP adress:
[1 = 10.242.2.3, 2 = 192.168.1.127, 3 = 127.0.0.1, 4 = custom define, Enter = 127.0.0.1]
1
Proxy service portnumber:
[Enter = 9090]

Proxy Service username:
[Enter = admin]

Proxy Service password:
[Enter = changeit]

Checking proxy service connection...
```

- On first step Wizrd will print you your serverID, if you already have License key, you can type or past it from clipboard. You can skip this step and install License key later, in this case AuditServer will run in Trial mode.

- Next step ask you about IP address which will be used to server Audit server, choose one from list (detected) or define your own.

- Defined port number which will be used, you can hit enter to use default port 3190

- Administrator username – the name which will be used for local authentication to AuditServer (it can be used even if you have no connection to LDAP server)

- Administrator password – the password for Admin user

- Enable HTTPs encryption – is AuditServer will server with HTTPS or not. If you answer yes, additional questions will be asked, Keystore Type, Keystore and Privat key passwords and name of keystore. (make sure that keystore placed in the same folder where AuditServer located).

- Elasticsearch version – choose version of elasticsearch which you want to use. ES 1.4 will work with Kibana 3.x, Elasticsearch 6.x will work with Kibana 6.x

- Proxy service IP address – the IP address of server where AuditProxy running.

- Proxy service portnumber – then portnumber for admin interface of AuditProxy. By default AuditProxy use portnumber 9090, if config.json of AuditProxy was changed by you manually, please defined correct portnumber.

- Proxy service username – the name for basic auth to AuditProxy admin interface, By default AuditProxy use username "admin", if config.json of AuditProxy was changed by you manually, please defined correct username.

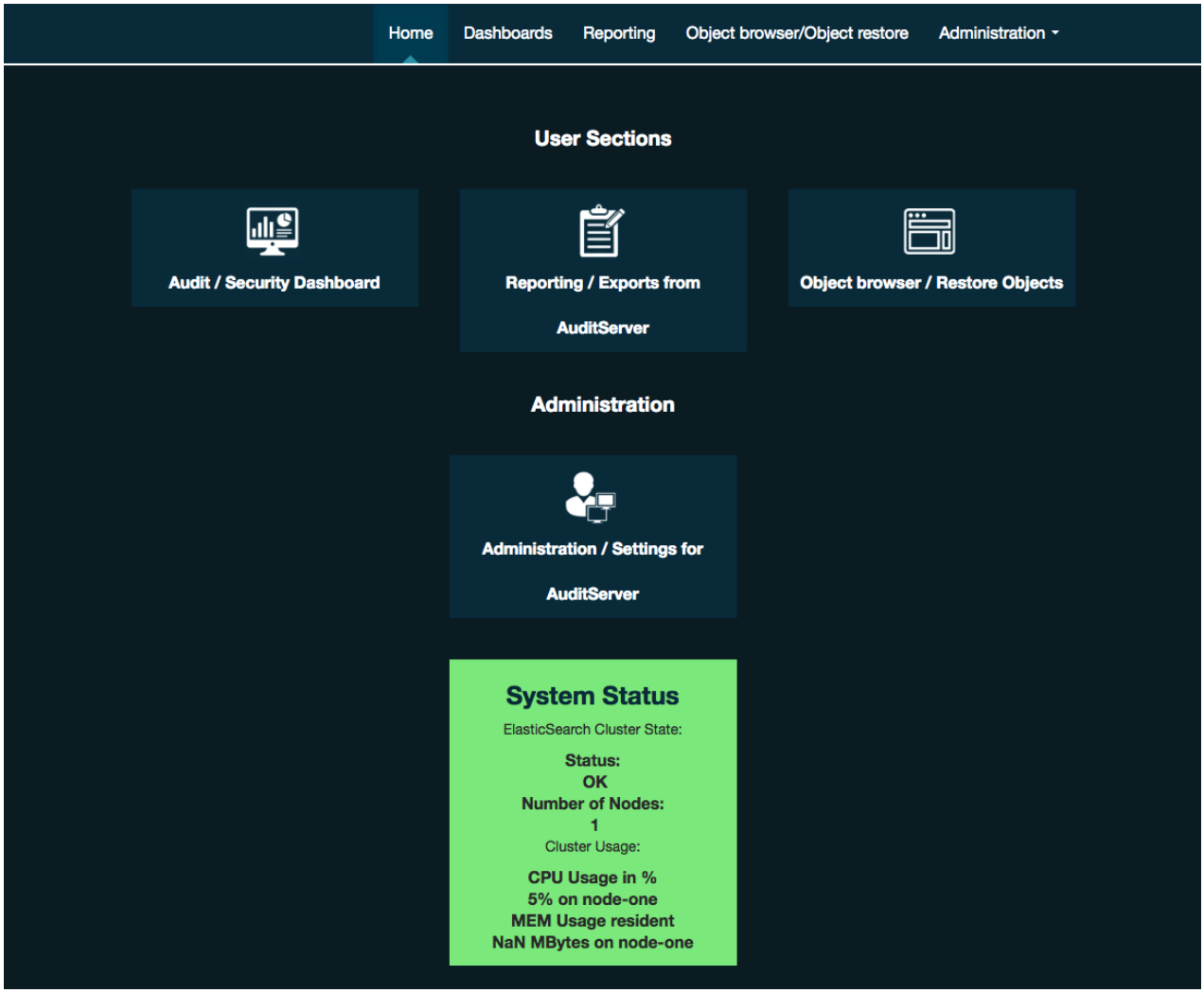
- Proxy service password – the password for basic auth to AuditProxy admin interface, By default AuditProxy use password "changeit", if config.json of AuditProxy was changed by you manually, please defined correct password.

- After all steps complete, you will see "Checking proxy service connection...", and then if everything fine AuditServer wizard will install all needed data to Elasticsearch. If something not correct, you will see " Proxy Service Not running or seetings not correct! Do you want to define settings again ? [y/n]:", this means that AuditServer can't connect to AuditProxy, please check is IP addresses, portnumbers, username/password is defined correct. You can re-configure your settings with answer "Y". If you sure that all settings is correct, please check your Firewall settings. If this not helps, please contact to our Support to resolve this issue.

- After AuditServer successfully configured it will be started.

3.6.5 Check if your Audit Server is running

To check your Audit Server, please open the following URL in browser: http://HOST:3190 (Where HOST is the name or IP address of the server on which the Audit Server is installed. e.g., http://127.0.0.1:3190)
The Audit Server Home will be opened. Don't worry if no System Status information appears on the bottom. You have to configure the connection to the Elasticsearch server first, if it is not running or not running on your local Audit Server engine.



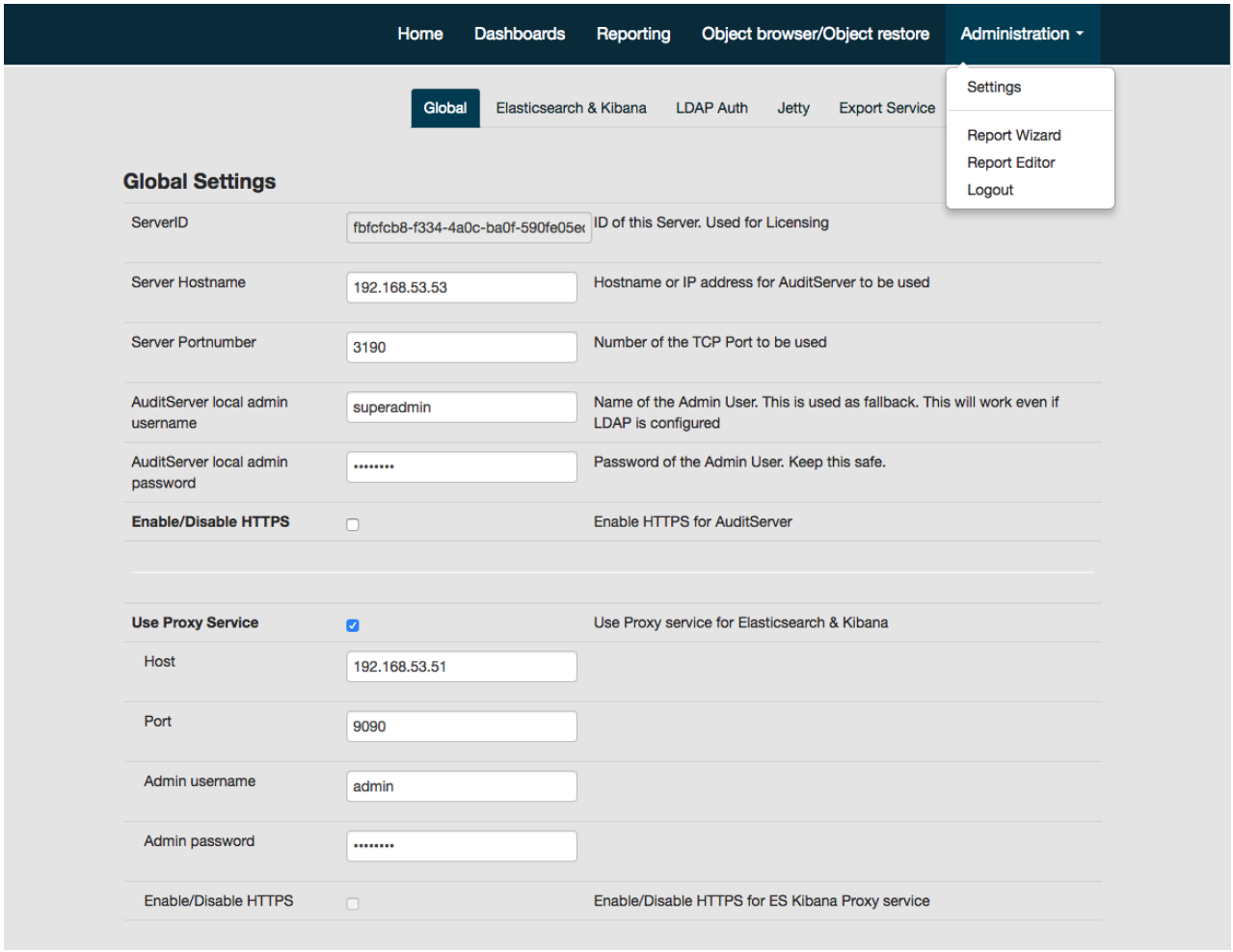
After you confirm that AuditServer running and started successfully, you can stop it by pressing "CTRL+C" in your console. And then use general way to start/stop it which is described in part 3.4.2 & 3.4.3

3.6.6 Configure the Audit Server

Before you can use the Audit Server, you have to configure the connection to the Elasticsearch server (if you not used configuration wizard described in part).

1. Click "Settings" from "Administration" menu. When User Name and Password are prompted, leave them empty and press Log In.

The basic configuration page will look like this:

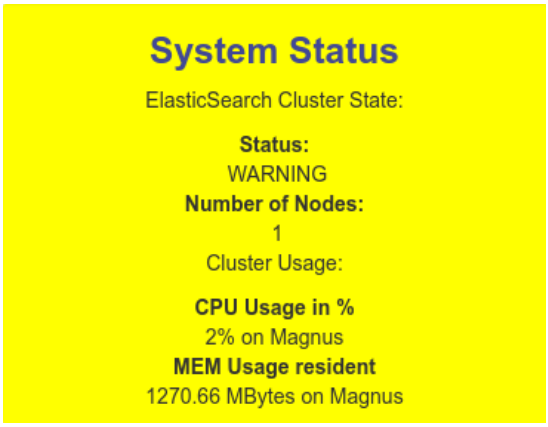


2. Paste your license code if you have it. If no license is available, the Audit Server will work in trial mode.
3. Enter the port number of your Audit Server. By default it is 3190.
4. Specify the user ID and the password for the admin account. Please write it down. You won't be able to open the administration page afterwards without these credentials.
5. Please enter the URL and the port of your Elasticsearch server. By default it is:

   http://HOST:9200/
6. If you use Elasticsearch 6.x please fill checkbox for "Use Proxy Service" entry, define hostname, port and username/password for access AuditProxy. HTTPS need to be checked if you enabled HTTPS for AuditProxy, AuditServer and installed certificates. If you use Elasticsearch 1.4 you don't need to use AuditProxy, leave "Use Proxy Service" unchecked and fill Elasticsearch settings in next tab "Elasticsearch & Kibana"
7. Save changes.
8. Restart the Audit Server.

9. Check the Elasticsearch server connection.

If your configuration is OK, you'll see a green (or yellow) status of your Elasticsearch server at the bottom of the home screen. The yellow warning means that you do not have an Elasticsearch cluster in place so your system is not fault-tolerant.



3.7 The Audit Driver

3.7.1 Create the driver

1. **Extract the archive**

   Extract the content of the "AuditDriver.zip" file (where 1.x is version of your AuditDriver).

   After extraction, an "AuditDriver" folder will be created automatically. All files and folders, mentioned in this paragraph, are inside of this folder.

2. **Copy needed Java classes and template files**

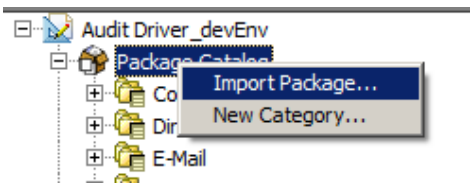
   Copy the driver appshims files to the dirxml class directory of your IDM server:

   - auditdriver.jar
   - commons-codec-1.10.jar
   - common-io-1.4.jar
   - httpclient-4.5.3.jar
   - httpcore-4.4.6.jar
   - json-simple-1.1.1.jar
   - template.json

   e.g., On SUSE Linux the default path is the following:
   "/opt/novell/eDirectory/lib/dirxml/classes"
   Check your dirxml class directory eDirectory/lib/dirxml/classes on your server.
   On Windows the path can be the following:
   "c:\NetIQ\IdentityManager\NDS\lib"

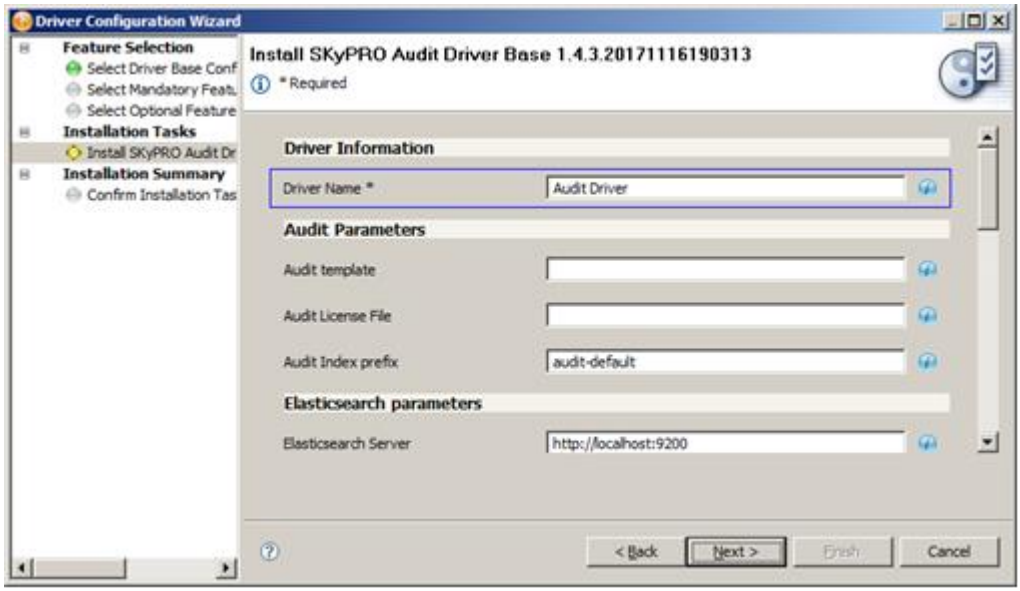
3. Create the Driver

   Right click on "Package Catalog" -> "Import Package...".



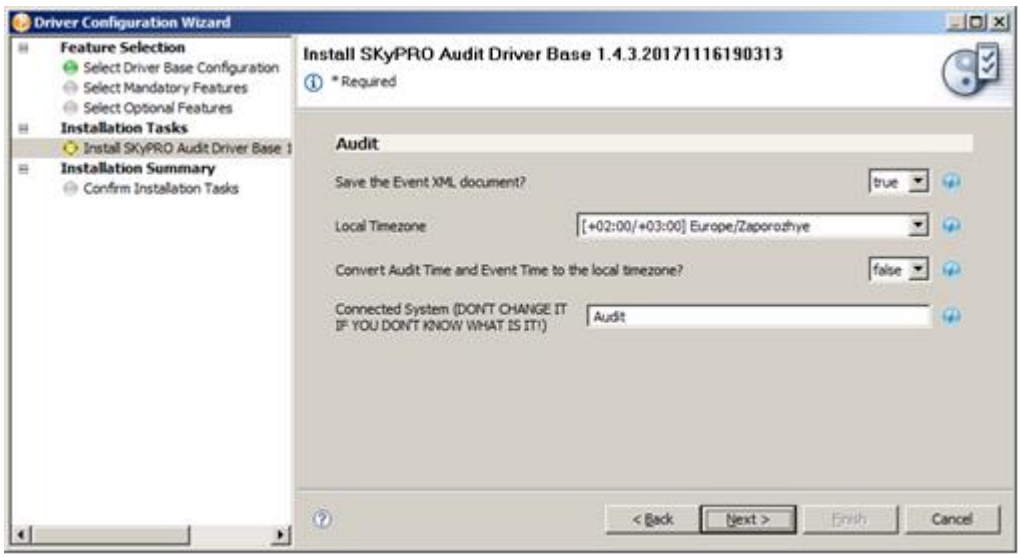
   Click the button "Browse..." and find the file "sp_ad_base_x.x.x.jar" (where x.x.x – version of package). Then click "Open" and "Ok". New package "SKyPRO\Audit Dashboard\SKyPRO Audit Driver Base" will appear in your Package Catalog.

   Right click on the Driverset, "New" -> "Driver...", select the package "SKyPRO Audit Driver Base" and click "Next". Enter the driver name.



Driver Name	Just driver name nothing more :)
Audit template	Enter the full path to your template.json.
Audit License File	Full path to the file containing Audit Driver Licence key on your IDM Server. Leave blank if you use the Audit Driver along with the Audit Server
Audit Index prefix	Prefix for the Index in the Elasticsearch. Format of Index name: "<index-prefix>-<index-date>". Exaple: audit-default-2017.07.05 Please don't change it if you don't know why you are doing it.
Elasticsearch (ES) and Logstash (LS) parameters (they are the same but for different datastore systems)	
ES/LS Server	Address of your ES/LS Server (for instance, http://localhost:9200). Fill this parameter to use Elasticsearch and/or Logstash.
ES/LS document type name	Elasticsearch (or Logstash) document type name. Please don't change it if you don't know why you are doing it.
User	If defined then driver will use Basic Authentication to access ES/LS server. Leave empty to work with ES/LS without any authentication.
Password	
SSL KeyStore Type	These parameters should be filled in case of using HTTPS

SSL Certificate filepath	connection
SSL passphrase	



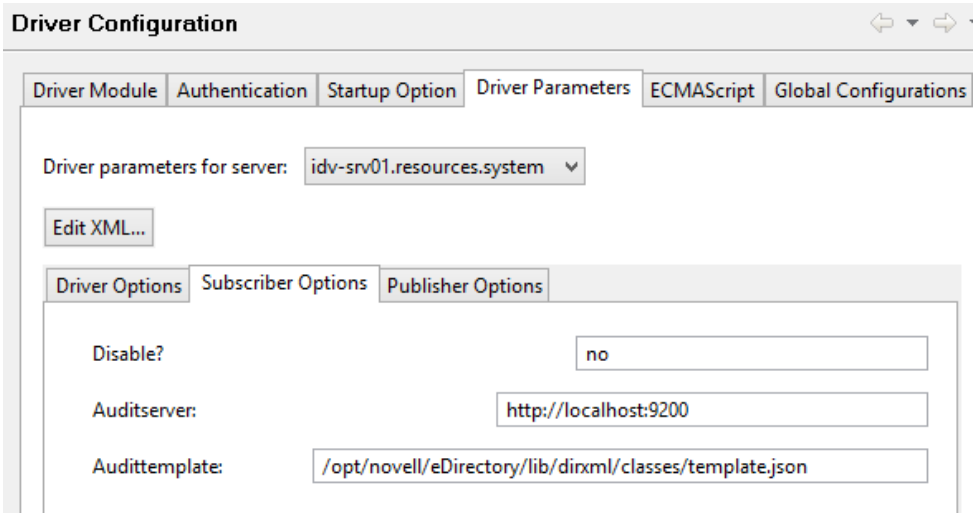
Save the Event XML document?	Save whole event xml document to view/use it in Audit Dashboard.
Local Timezone	Local timezone for converting Audit Time and Event Time. Format: "[UTC offset/UTC DST offset] Timezone name"
Convert Audit Time and Event Time to the local timezone?	Audit Time and Event Time are in UTC timezone. You can check this option and choose your local timezone for these times. Server Time will be in local timezone regardless of this option
Connected System	Value for the parameter "Connected System". If you change this parameter, the dashboard called "Audit Dashboard" will not work and should be reconfigured. So please DON'T CHANGE IT IF YOU DON'T KNOW WHAT IS IT!

Finish the installation.

4. Configure the Driver

If you didn't configure the driver parameters while creating the driver, you can configure them later. Right click the Driver and open the Driver properties. Go to the *Driver Configuration* and open the *Driver Parameters* Tab.

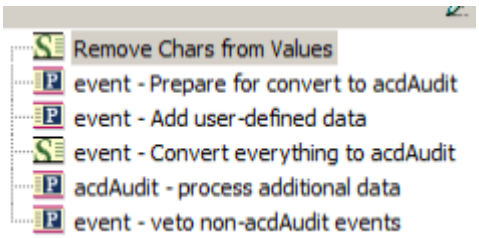
Click the "*Subscriber Options"* tab. Description for all parameters you can find above in the paragraph "3. Create the Driver".



5. Check the correct sequence of policies

Sometimes there is a trouble in IDM Designer: if several policies are situated in one policy set, after creating the driver from the package they can appear in wrong sequence.

Please check the sequence of policies in Subscriber Event policy set. Correct sequence you can see on the picture.



6. Adjust Driver filter

If you want to monitor certain objects or attributes, just open the Driver filter and change the filter accordingly. You do not have to change anything else!

7. Deploy the Driver

Right click on the Driver and choose live/deploy. Define "Security Equivalences", select an object which will be a Security Equivalent for the driver. Please note that you should select an object with enough permission to audit all necessary objects and attributes. Usually it should be the Administrator.

Click "Exclude 'Administrative Roles'" and select the objects you want to exclude from the audit. Only exclude the "admin" object, if you do not explicitly want to audit the "admin" user.

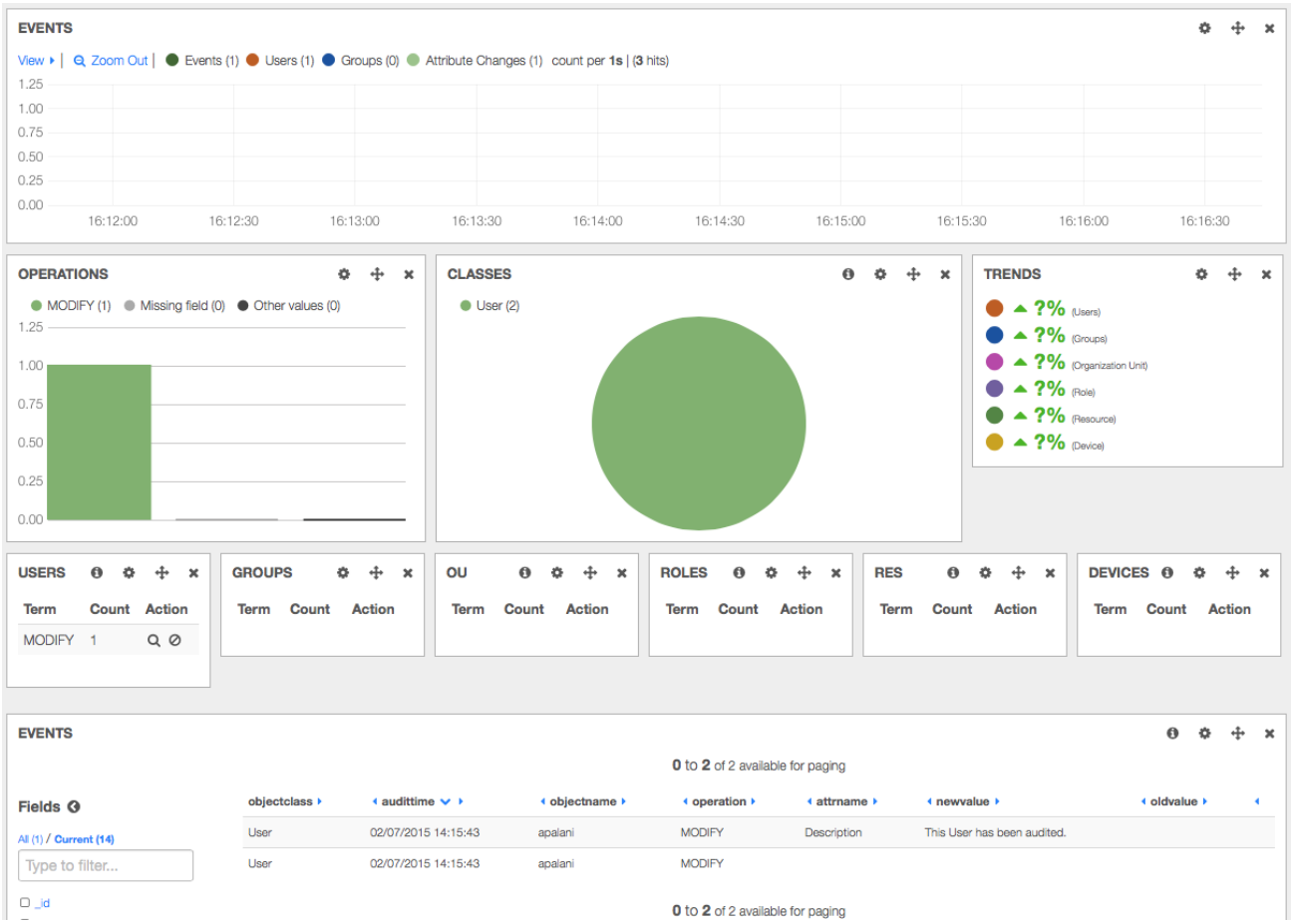
8. Driver licensing

The Audit Driver reads a license from Elasticsearch server at each start of the Driver. Also the Audit Driver can read a license key from the file specified in Driver Parameters.
To update Driver license you need to restart the Driver.
If license is not found or Driver has no connection to the ES server, the trial mode will be enabled.

3.7.2 Test the driver

To test the Driver, start the Driver and change description attribute of the user to, e.g., "This user has been audited". The modify event should be successfully synchronized with the Audit Server.

Open your browser and navigate to your Audit Dashboard URL by default on port 3190. From the home screen, click "Dashboards" (enter username and password, if you have defined one) and select "IDM Audit Dashboard". Click the refresh button in the upper right corner and open the event table at the bottom by pressing the expand triangle icon. You should see the Modify event for attribute "Description".

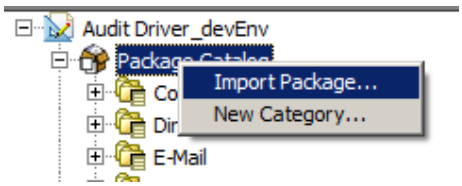


3.7.3 Update the driver

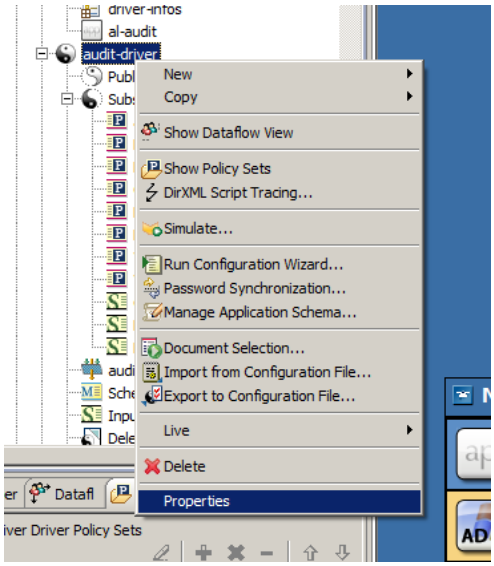
To update the Audit Driver you should:

- Stop Audit Driver;
- Update (replace) the driver appshim files in the dirxml class directory of your IDM server as described in paragraph 3.7.1.2 "Copy needed Java classes and template files";

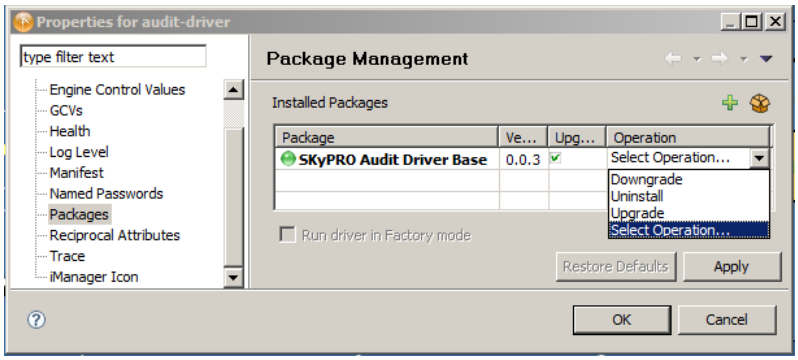
import new version of package "SKyPRO Audit Driver Base" to your IDM Designer project's Package Catalog. Click on "Package Catalog" -> "Import Package…", click "Browse…" and find the file sp_ad_base_x.x.x.jar;



- update the version of package "SKyPRO Audit Driver Base" in your Audit Driver. Open Audit Driver's properties;



- open the tab "Packages", find the line "SKyPRO Audit Driver Base" and select the operation "Upgrade", set new version;



- Deploy the driver changes to IDM Vault. Right click on Audit Driver -> Live -> Deploy…
- Update Elasticsearch mapping for today audit index. Start the console command
  curl -XPUT http://ES_SERVER:9200/INDEX_NAME/audit/_mapping?ignore_conflicts=true -d @mapping.json
  Where "ES_SERVER" – hostname or IP address of your ElasticSearch server,

"INDEX_NAME" is a today audit index name (for example "audit-default-2018.03.16"),
"mapping.json" – is json file located in your AuditDriver folder.
(CURL utility should be installed in your system).

- Restart IDM
- Start the Audit Driver

4.Install the Report Service

Make sure you have installed Java. If Java is not installed, please follow the instructions on how to install Java for your system in chapter 3.1 "Check and install the Oracle Java."

4.1 Extract and manual start

1. To install the Report Service, please follow these steps:

Extract archive.

Extract content of the "AuditReport.zip" file (where 1.x is version of your AuditReport)

For Linux, use command: **unzip AuditReport.zip**
For Windows, please use Windows Explorer option "Extract All"

(After extraction, an "AuditReport" folder will be created automatically.)

2. Move extracted folder.

Move the extracted folder to the location you want.

Linux: e.g., /opt/AuditReport
Windows: e.g., \Programs\AuditReport

(You can delete .zip file afterwards)

3. Configure Report Service.

Open the Report Service configuration file "reportservice.yml" using a text editor.
Provide the correct parameters to connect to your directory using LDAP.

ldapserver: URL and port of your eDirectory LDAP server
userdn: DN of the user that connects to your LDAP

This user must have read rights to all object and attribute data you would like to store:

esserver: URL and port of your Elasticsearch server
userpw: Password of the LDAP user
templatename: Filename of the JSON template
mandant: Name of the tenant in case you enabled the multitenant feature of the Audit Server

```
config:
   ldapserver: 'ldap://localhost:389'
   userdn: 'cn=admin,ou=users,o=system'
   userpw: 'netiq000'
   esserver: 'http://localhost:9200/'
   templatename: 'template.json'
   mandant: 'default'
```

4. Manually start and stop.

Start the Audit Report with the script or batch file depending on your system:

- Linux: start.sh
- Windows: start.bat

(If JAVA_HOME variable is not defined in your system, you may have to adjust the path to Java Runtime Environment in script or batch file. The path to Java depends on your Java installation.)

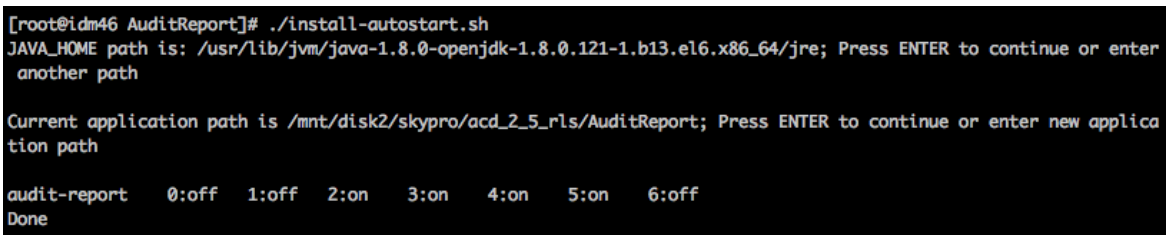
To stop the Audit Server, please use the following way depending on your system:

- Linux: stop.sh
- Windows: close the CMD window

4.2 Make runnable as service for Linux

For a production environment, we recommend making Audit Report runnable as a service. To make this, please follow these steps:

a) Run "./install-autostart.sh" from AuditServer folder (as root user)



b) On first step script will try to detect your Java home path, if it will be not found or you want to use own you need to defined path end press Enter. If you agree with provided path, you can switch to step two.

c) On second step script will detect the location of your AuditReport installation, if you agree – just press Enter, if not, define your path and press Enter.

d) after configuration script installed all needed files and you can easy manage your AuditReport with start/stop commands.

Run following commands from root user

service audit-server start or /etc/init.d/audit-report start – for start

service audit-server stop or /etc/init.d/audit-report stop – for stop

service audit-server status or /etc/init.d/audit-report status – for check status

1. Schedule runs.

Add crontab entry with the command from the user you are currently logged in, e.g., from the user *root*:

crontab -e

entry: 05 1 * * * service audit-report start

4.3 Make runnable as a service for Windows

For production environment, we recommend making Audit Report runnable as a Windows process scheduled to create a daily snapshot. To make this, please follow these steps:

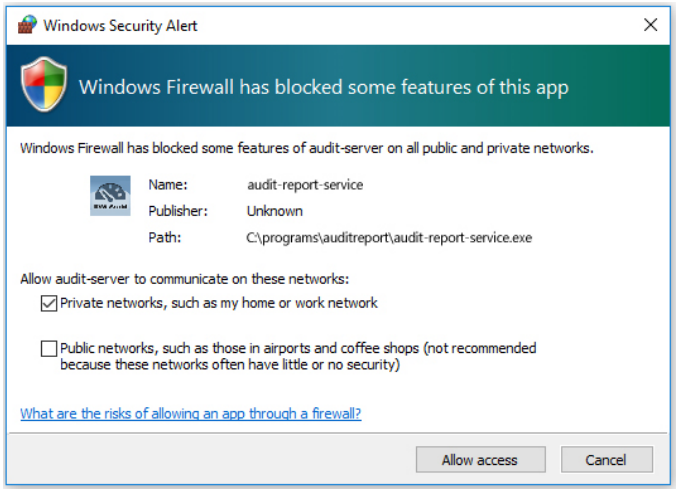
1. Open in editor "audit-report-64.ini" or "audit-report.ini", depending on your system architecture and Java.
2. Change "working.directory" variable with path where Audit Report is located, e.g., working.directory="c:\Programs\AuditReport".
3. Uncomment and change "vm.location" variable with location of "JVM.dll" file (if your JAVA_PATH not defined globally).

e.g., vm.location="C:\program files\Java\jre1.8.0_91\bin\client\JVM.dll"

4. Run "audit-report-64.exe" or "audit-report.exe", depending on your system and Java.

Please allow Firewall prompt.

If everything is correct you will see audit-report process in Windows Task Manager. (You can end it by clicking the "End Process" button.)



5. Scheduled start.

Open in editor "AuditReportTask.xml" (which is located in the "service-script" folder of your Audit Report installation).

6. Replace Date and Time between <StartBoundary></StartBoundary>.

e.g., 2017.03.16T00:05:00 means that task will be started from 2017.03.16 at 00:05:00 and will continuously start at that time.

```
<Triggers>
  <CalendarTrigger>
    <StartBoundary>2017-03-16T00:05:00</StartBoundary>
    <Enabled>true</Enabled>
    <ScheduleByDay>
      <DaysInterval>1</DaysInterval>
    </ScheduleByDay>
  </CalendarTrigger>
</Triggers>
```

7. Replace path between <command></command> tags.

(The path should correspond to your "audit-report.exe" or "audit-report-64.exe" location.)

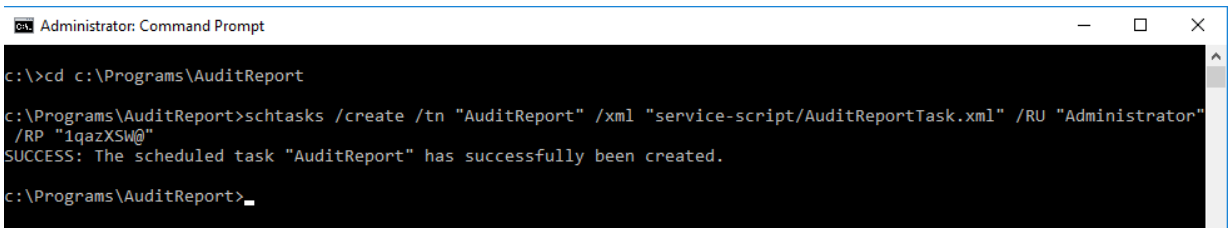
```
<Actions Context="Author">
  <Exec>
    <Command>C:\Programs\AuditReport\audit-report-service.exe</Command>
  </Exec>
</Actions>
```

8. Save file.
9. Run cmd.exe; it will open CMD window.
10. Go to the folder where your Audit Server is located.

e.g., c:\Programs\AuditReport

11. Run the command to import AuditReportTask.xml to Task Scheduler:

schtasks /create /tn "AuditReport" /xml "service- script/AuditReportTask.xml" /RU "Administraror" /RP "YourPassword"

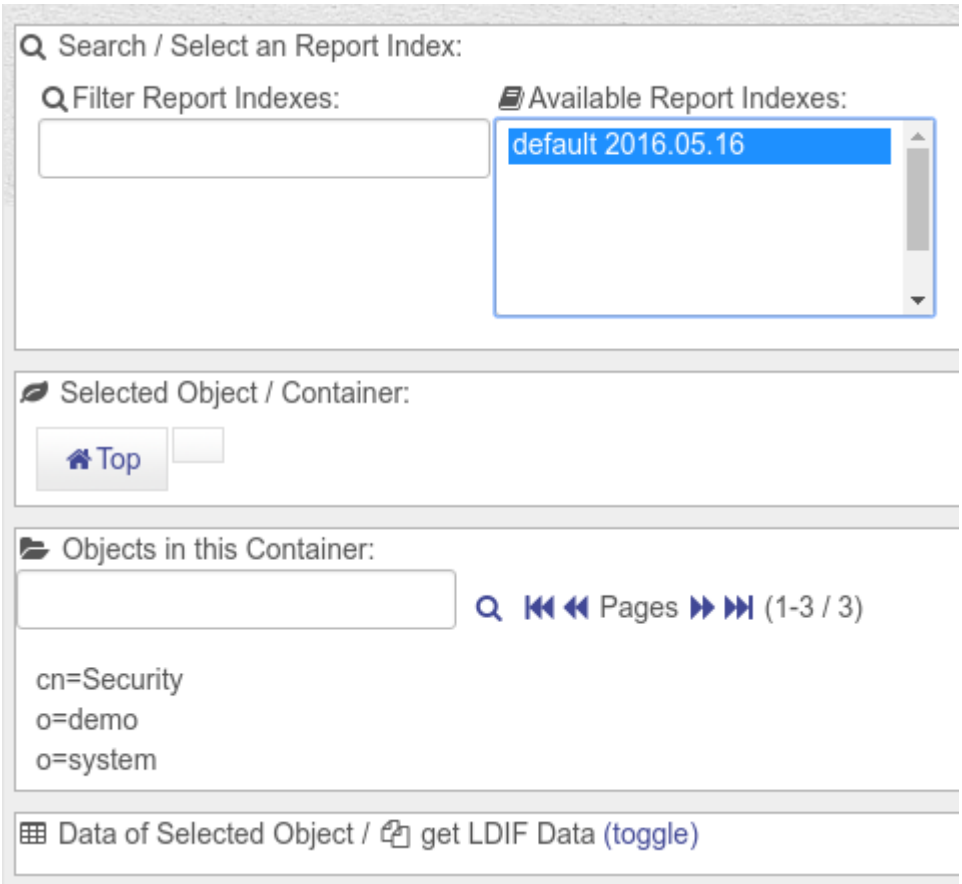


Replace "Administrator" and "YourPassword" with the user name and the password of the user you would like to run Audit Server with.

* Make sure that user which you use for run Audit Report have Administrator permissions, because only with this permissions Audit Report will be started without logging in.

4.4 Check the history

The Report Service will create a snapshot with the name "default yyyy.mm.dd". To access the snapshot please open your browser and navigate to your Audit Dashboard. Select "Object Browser/Object Restore". Choose the snapshot you have just taken of the available Report Indexes and browse through the directory tree.



5 Install the Audit Export service

Make sure you have installed Java. If Java is not installed, please follow the instructions for how to install Java for your system in chapter 3.1 Check and Install Oracle Java.

5.1. Extract and manual start

1. Extract archive.

   Extract content of the "AuditExport.zip" file (where 1.x is version of your AuditExport)

For Linux, use command:

unzip AuditExport.zip

- For Windows, please use Windows Explorer option "Extract All".

(After extraction, "AuditExport" folder will be created automatically.)

2. Move extracted folder.

Move the extracted folder to the location you want.

- Linux: e.g., /opt/AuditExport
- Windows: e.g., \Programs\AuditExport

(You can delete the .zip file afterwards.)

3. Manually start and stop.

Start the Audit Export service with the script or batch file, depending on your system:

- Linux: start.sh
- Windows: start.bat

(If JAVA_HOME variable is not defined in your system, you may have to adjust the path to Java Runtime Environment in script or batch file. The path to Java depends on your Java installation.)

To stop the Audit Export service, please use the following way, depending on your system:

- Linux: stop.sh
- Windows: close the CMD window

5.2 Make runnable as service for Linux

For a production environment, we recommend making Audit Export runnable as a service on each system start. To make this, please follow these steps:

1. Move script file which is located in the "service-script" folder to your "/etc/init.d" folder.

sudo mv ./service-script/audit-export /etc/init.d/audit-export

2. Open in editor "audit-export" file and change the APP_PATH variable with the path where your Audit Export service is located.

sudo vi /etc/init.d/audit-export

(e.g., APP_PATH="/opt/idm/AuditExport")

3. Give this script executable permission (e.g., 775, but you can set it lower).

sudo chmod 775 /etc/init.d/audit-export

4. Include in startup list with default startup priority.

sudo update-rc.d audit-export defaults

5. Reboot server or start the Audit Export as service.

sudo service audit-export start

5.3 Make runnable as service for Windows

For a production environment, we recommend making Audit Export runnable as a Windows process by each system start.

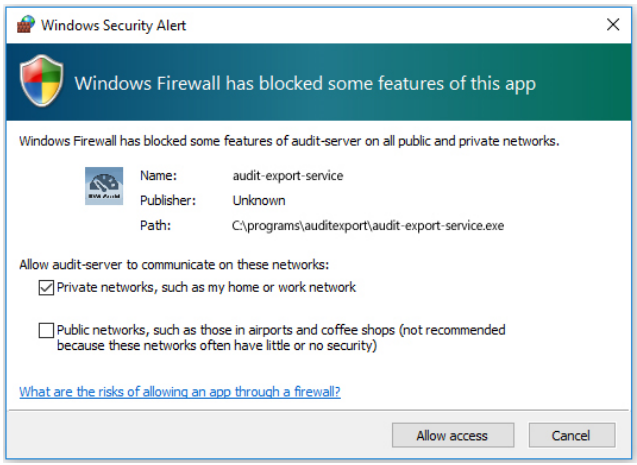
1. Open in editor "audit-export-64.ini" or "audit-export.ini", depending on your system architecture and Java.
2. Change "working.directory", depending on the path where Audit Export is located, e.g., working.directory="c:\Programs\AuditExport".
3. Uncomment and change "vm.location", depending on the location of the "JVM.dll" file (if your JAVA_PATH not defined globally).

   e.g., vm.location="C:\program files\Java\jre1.8.0_91\bin\client\JVM.dll"

4. Run "audit-export-64.exe" or "audit-export.exe", depending on your system and Java.

   Please allow Firewall prompt.

   If everything is correct you will see the audit-export process in Windows Task Manager. (You can end it by clicking the "End Process" button.)



5. Open "AuditExportTask.xml" in editor (which is located in the "service-script" folder of your Audit Export installation).

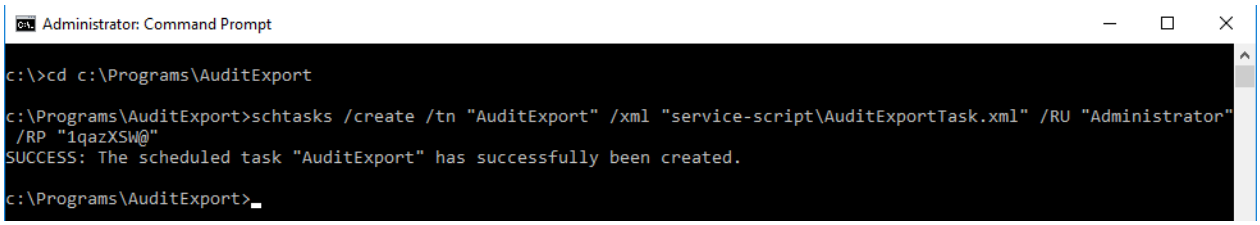
   Replace the path between <command></command> tags.
   (The path should correspond to your "audit-export.exe" or "audit-export-64.exe" location.)

```
<Actions Context="Author">
  <Exec>
    <Command>C:\Programs\AuditExport\audit-export-service.exe</Command>
  </Exec>
</Actions>
```

6. Save File.
7. Run cmd.exe; it will open a CMD window.
8. Go to the folder where your Audit Server is located.

   e.g., c:\Programs\AuditExport
9. Run command to import AuditExportTask.xml to Task Scheduler:

   schtasks /create /tn "AuditExport" /xml "service- script/AuditExportTask.xml" /RU "Administraror" /RP "YourPassword"



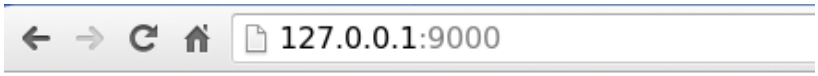
   Replace "Administrator" and "YourPassword" with the user name and password of the user you would like to start Audit Server with.

   * Make sure that user which you use for run Audit Export have Administrator permissions, because only with this permissions Audit Export will be started without logging in.

10. After the task is successfully created, you need to restart your server.

5.4 Check if your Audit Export service is running.

Open in browser following the URL http://HOST:9000.
(Where HOST is name or IP address of server where Audit Export is installed, e.g., http://127.0.0.1:9000)



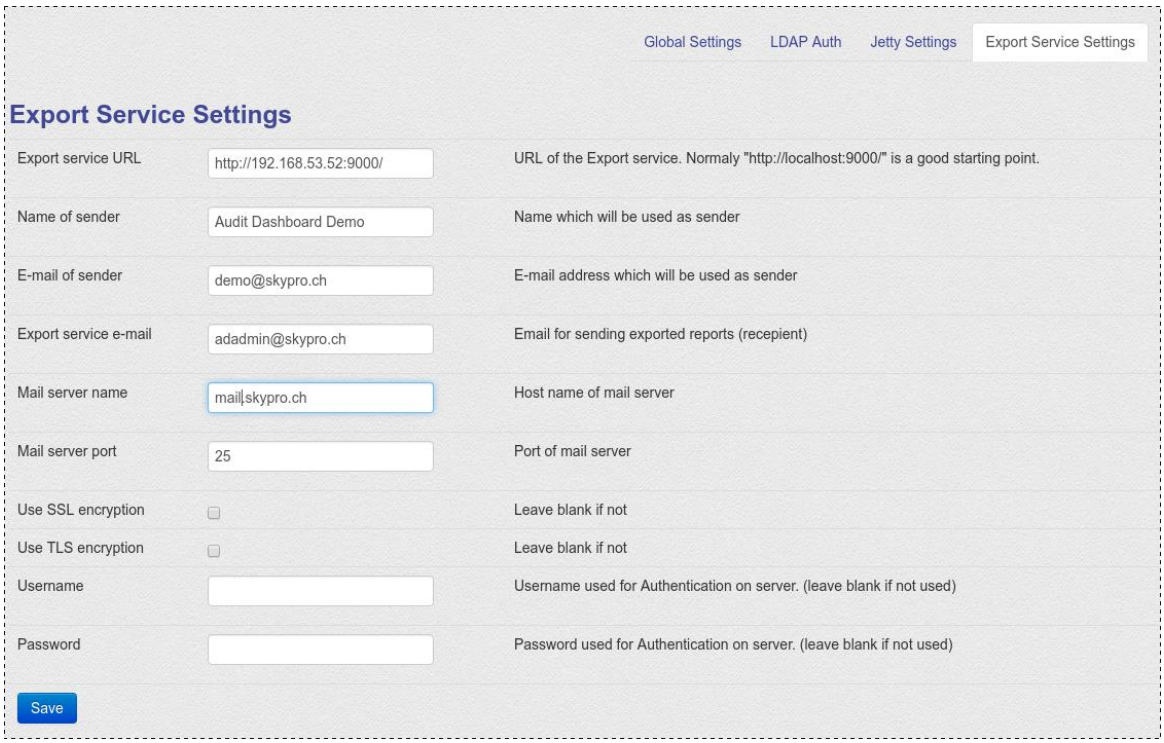
Your new application is ready.

If everything is successful, you will see this page.

5.5 Configure the Audit Export

Before you can use the Export service, you have to configure the connection to it and to the mail server settings.

1. Click "Settings" from the "Administration" menu.



2. Export service URL.

   Please enter the URL and port of your Export server.

   By default this is: http://HOST:9000/
3. Enter the port number of your Audit Server. By default, it is 3190.
4. Specify your mail server setting.
5. Save.
6. Restart the Audit Server.

6 Dashboards

Now you're almost ready to go. For your convenience, we have provided several sample dashboards. Also here you can find a manual how to create your own dashboard and modify existing.

6.1 Sample dashboards

- **IDM Audit Dashboard** - this dashboard provides real-time information about all events on specific objects that are taking place on your IDM server engine. Data for this dashboard are produced by Audit Driver.

- **IDM Security Dashboard** - this dashboard illustrates security threats that might have occurred like intruder attempts, intruder locks, and login disables/enables. Data for this dashboard are produced by Audit Driver.

- **IDM Compliance Dashboard** - the compliance dashboard shows the data history of objects. We provide historical views of users, groups, roles, resources, and assignments. This helps to verify attributes and assignment states in different time periods. Objects states are saved to the Audit tool on a regular basis. Because the Audit tool knows the historical values and all the changes that might have taken place in a specific period of time, it can prove and validate data values of any object at any time. Your compliance team will be pleased. Data for this dashboard are produced by Report Service.

- **IDM Driver Dashboard** - this dashboard provides real-time information about all events that occurred in your own IDM Driver, what objects it handles and what operations it does with objects. How to configure your driver to audit it with Driver Dashboard please see Attachment 1.

- **IDM Workflow Dashboard** - this dashboard shows the information about workflows and events occurred in them. How to configure your workflows to audit them with Workflow Dashboard please see Attachment 2.

- **Mandant A/B Audit Dashboards** - this is an example of the multitenant feature of the Audit dashboard to allow different dashboard views for individual groups.

- **Blank** - with the blank template you can start to build your own dashboard from scratch.

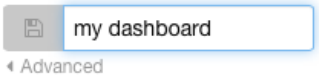
6.2 Dashboards on Kibana 3 (Elasticsearch 1.4.4)

6.2.1 Modify a Dashboard

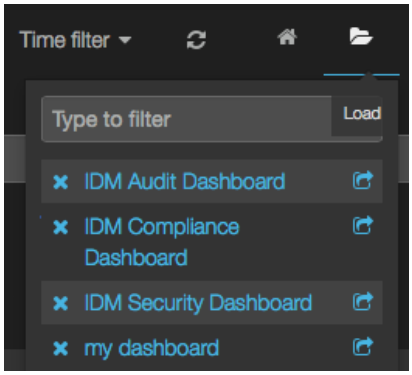
Open the Audit Server home page and click the "Dashboard" button on top. Select the IDM Audit dashboard example to start with.

Click the save button located in the upper right corner.

Then choose "my dashboard" as the name for the new dashboard and save it. Now you have a copy of the original Audit dashboard to play around with.



To select this dashboard you have to go back to the dashboard overview and select the blank dashboard. Click on the folder icon to load your copy "my dashboard".

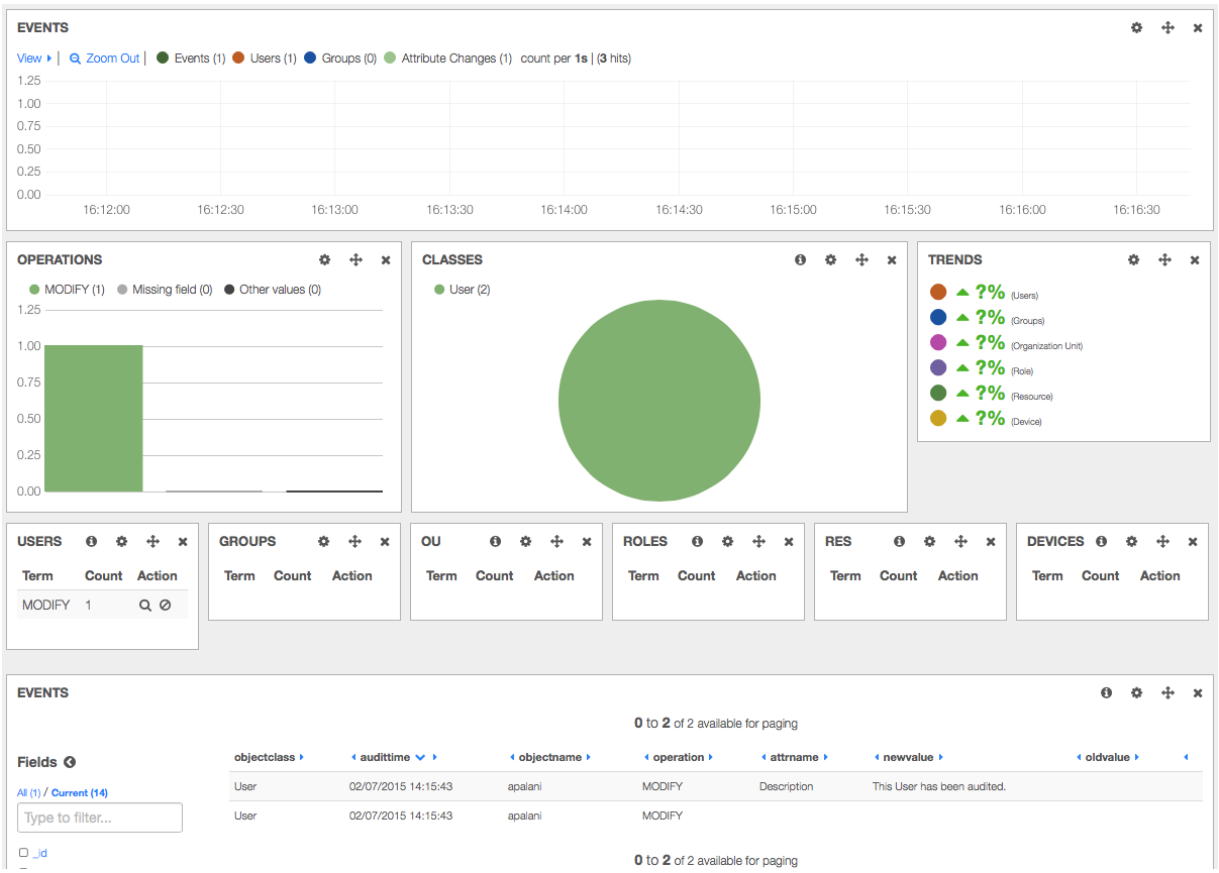


Graphic 3: Load your IDM Audit Dashboard "my dashboard" example

The IDM Audit Dashboard shows a visualized history of events on objects with histograms and charts. You can see how many events have been processed by your IDM engine and how many different object classes have been involved. You see trends and the amount of different operations on different objects that have occurred.

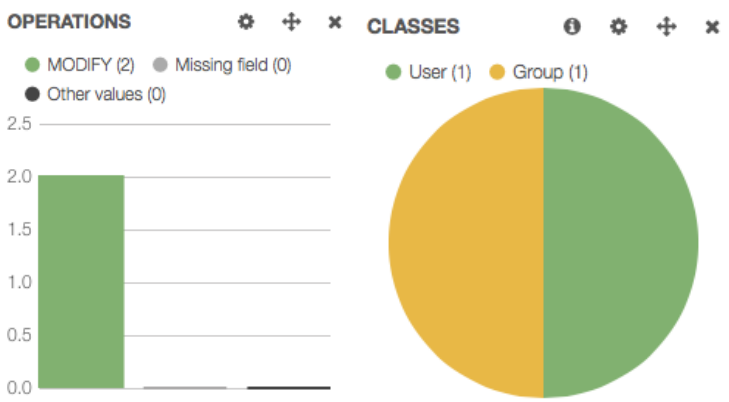
If you have executed the change of a user description attribute – as mentioned in chapter 3.7.2 – you should see this modified event already in your dashboard.

In the Operation/Events graphic you see one modify event. In the Classes graphic you see that one user object so far was audited. In the Events table at the bottom you see the basic data. You see two (maybe three if the description had an old value) entries of object class user with its object name. The first entry is the modification event. The second entry shows the new value "This user has been audited". If the attribute was already valued we even have three entries. We see the old value and the new value.



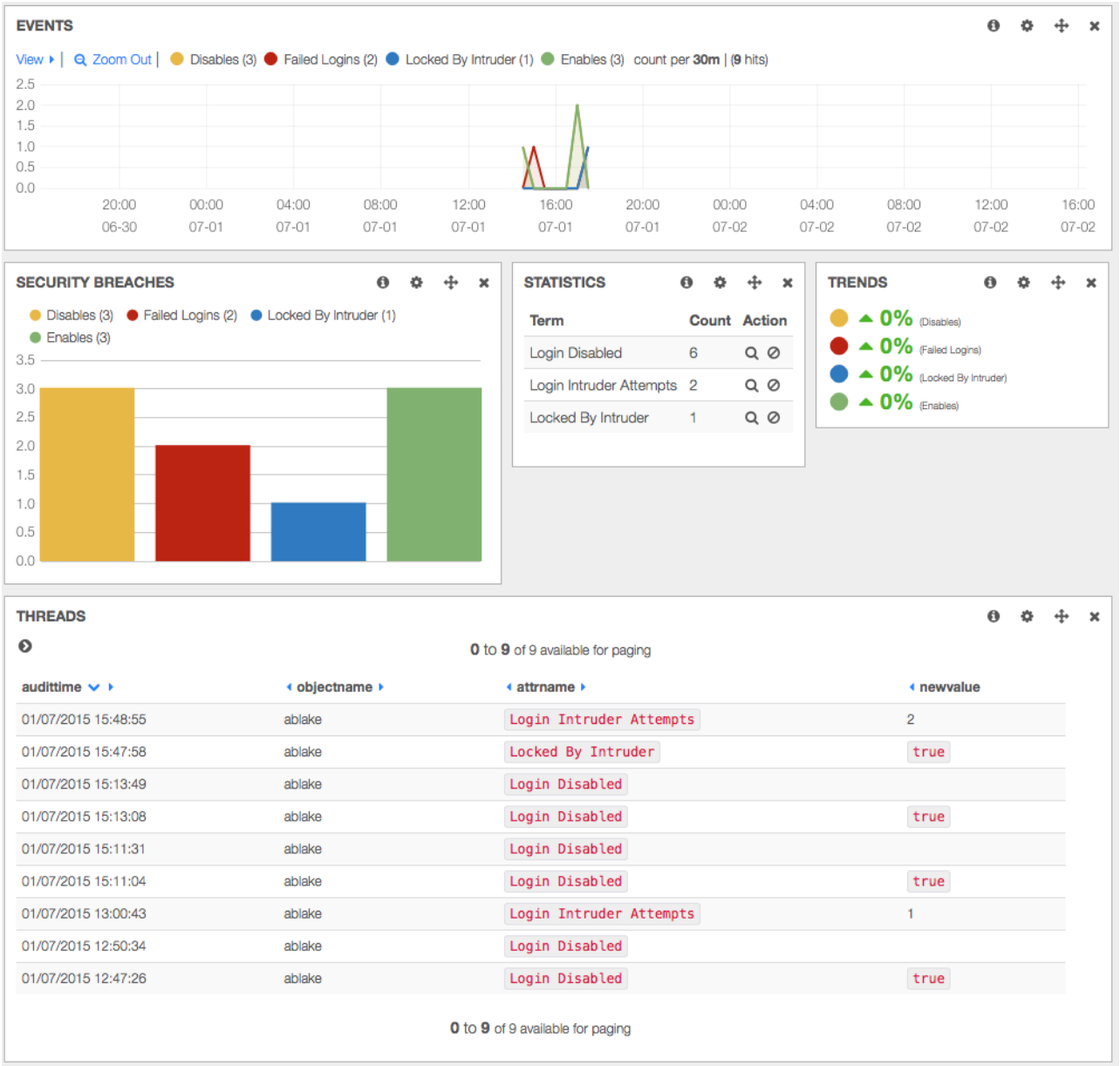
6.2.2 Experience the IDM Audit Dashboard

Now change the description of a group object and look at the dashboard again. You will see two modification events under OPERATIONS and two classes Users and Group. Also in the GROUP EVENTS you now see one modification.

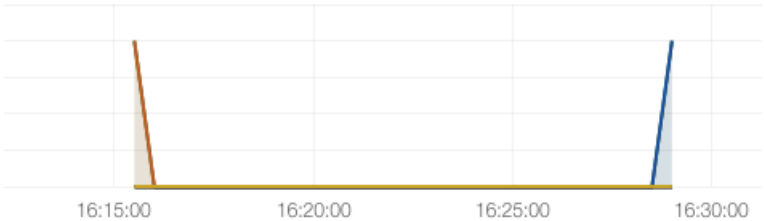


Graphic 5: IDM Dashboard Operations and Classes

Also in the event Histogram you see these two modifications in the timeline. You see the user event in orange, the group event in blue, and the attribute changes in light green. Also have a look at the table at the bottom. You see three new entries for the group modification.



Graphic 1: IDM Security Dashboard



Graphic 6: IDM Audit Dashboard Event Histogram

6.2.3 Understand the IDM Audit Dashboard

There are some base elements you have to know about to understand the dashboards.

1. Query

4. Filter
5. Row
6. Panel

Query

With queries, you select all the elements you want to display in your dashboard. You can pin queries so you can use them in panels directly to select specific data. In all panels you can decide to use data from all pinned or unpinned queries or select data from specific pinned queries.
We have predefined some pinned queries to select events, users, groups, failed logins, attribute changes, etc.

Filter

With filters, you obviously filter the data you have selected with your query. For example, you only want to have user objects or objects with a specific object name. Often you will use the filter to narrow the time frame of events you want to see, such as only changes that have taken place the within the last 24 hours.
Our standard filter selects only events of type "audit". For reporting purposes, we have additional types like "report" that contain all data of an object at a specific time.

Row

A row can hold one or multiple panels. You can add new rows at the bottom. You can move rows at any time to the position you want to have them.

Panel

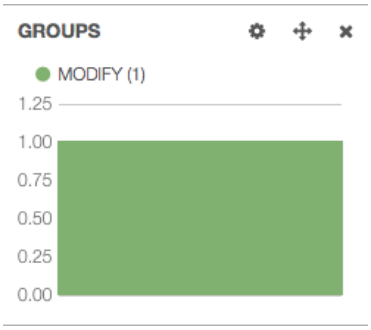
Panels are the actual graphical building blocks of the dashboard. Panels can show maps, tables, histogram, hits, pie charts, statistics, trends, or just explaining text.

6.2.4 Work with Panels

6.2.4.1 Change an existing Panel

We have a panel called GROUPS that shows a summary of all different group events. Wouldn't it be nice to show this instead of a table as a bar graphic?

1. Click the configure icon in the *GROUP* panel. 
2. In the *Panel* tab change the *Style* from *table* to *bar*.
3. Now the events will be displayed as bars.



Graphic 1: Graphic for events per class

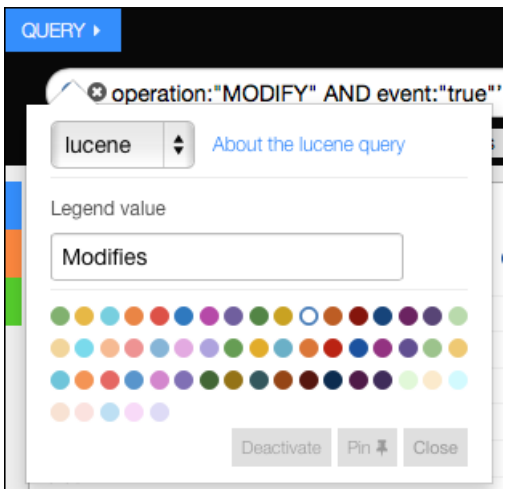
6.2.4.2 Add a new Panel

Now we want to create a pie chart showing us all modified events per class. First we add a new query for all modified events. To add a query, we have to enable the query bar.

1. Click the configure dashboard on the right top.
2. Select "*Controls"* from the available tabs.
3. Enable *"Query"* in the section *"Pulldowns".*
4. Click "*Save".*

The query panel appears as the first panel. Open the panel with a click on the "Query" panel. Now we add a new Query.

5. In the *QUERY* row click the "+" sign at the right.
6. Enter Query string
   Enter the following query string `*operation:"MODIFY" AND event:"true"*". This selects all events that are not the actual attribute changes but only the modified event.
7. Pin the Query
   Click the colored dot on the left, as *Legend value* enter *"Modifies"* and pin the query.



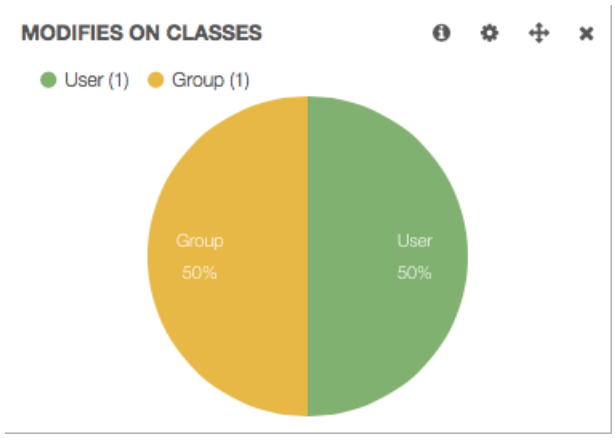
Graphic 2: Define new query

You should see a new pinned query. Now we add a new pane.

8. Add panel
   Go to the row with the *OPERATIONS* panel on the left and click the green "+" symbol to add a panel.
9. Panel type
   As panel type select *terms*.
10. Title
    As *title* type enter *Modifies on Classes* and adjust the span value to 3.
11. Field value
    In the *Parameters* type *objectclass* in the *Field* value.
12. Options
    Uncheck *Missing* and *Other* in the *View Options* and select *pie* as the graphic view.
13. Query
    In the *Queries* dropdown choose *selected* and activate the pinned *Modifies* query.
14. Save the panel.

Graphic 9: Define a new panel

Bravo! You successfully added a new panel showing a pie with the amounts of modifies per class that looks like this.



Graphic 30: New MODIFY on classes panel

Now you can play around with new rows, add new panels, and experiment with all the various graphical building blocks.

6.2.4.3 Create new row

New we're going to create a new row with new panels. The goal is to create a separate histogram and pie chart for user and group events.

15. First go to the bottom of the dashboard on click ADD A ROW.

7. Select tab "Rows".

8. In the title field on the right enter "User & Group Statistics".

9. Click "Create Row".

10. Move the new row above the Events row in the dashboard settings.

11. Press "Save".

Add panels

Now you have an empty row where we can add new panels.

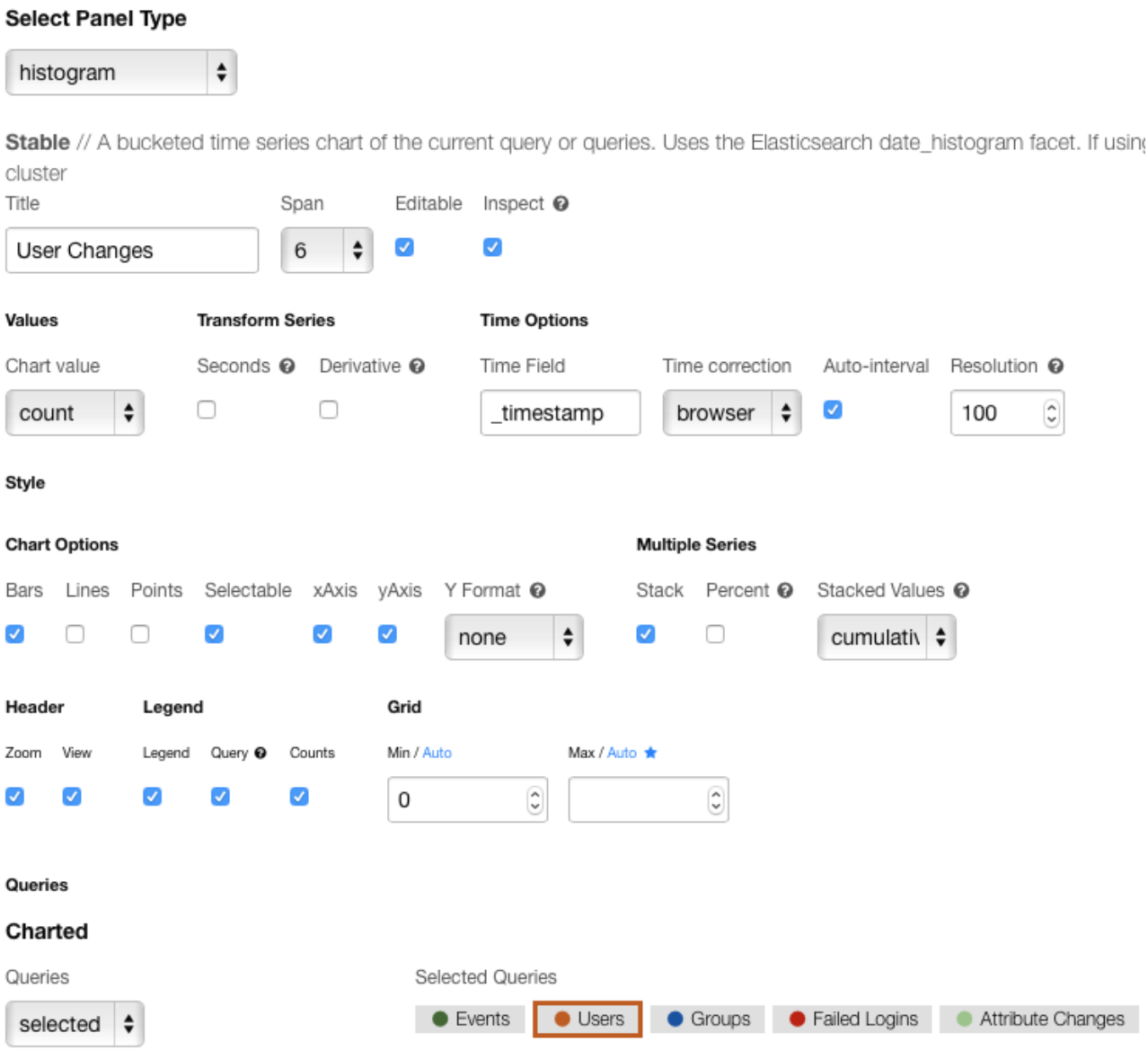
16. Press "Add panel to empty row".

17. Select "histogram" as panel type.

18. Enter "User Changes" in the field Title and change the span value to "6".

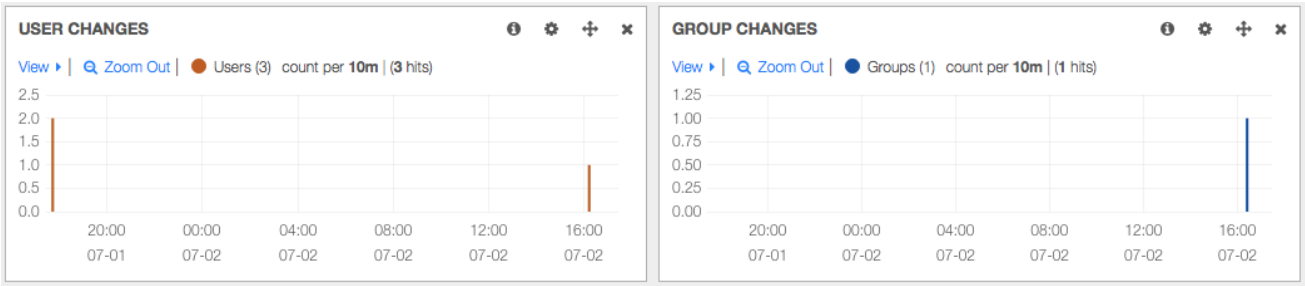
19. Change the Time Field from "@timestamp" to "_timestamp".

20. Change the Queries to "selected" and enable Users.



Add a second histogram panel for groups and name it "Group Changes", change the Time Field, correct the span value, and change the Queries to enable Groups only.

Congratulations! You successfully added a new row to histogram panels. Now create, modify, and delete some users and groups in your directory and you will show the events in these histograms.



Graphic 11: New row with two histograms

6.3 Dashboards on Kibana 6 (Elasticsearch 6.x)

Dashboard in Kibana 6 is a container for the Visualizations and Saved Searches. So to add some data to the dashboard you should create required Visualization or Saved Search and then add it to the Dashboard. All Visualizations are situated in the menu "Visualize", all Saved Searches are situated in the menu "Discover"

Please note: to make any corrections in the Kibana you should have Administrator rights in the Audit Server.

6.3.1 Create new visualization.

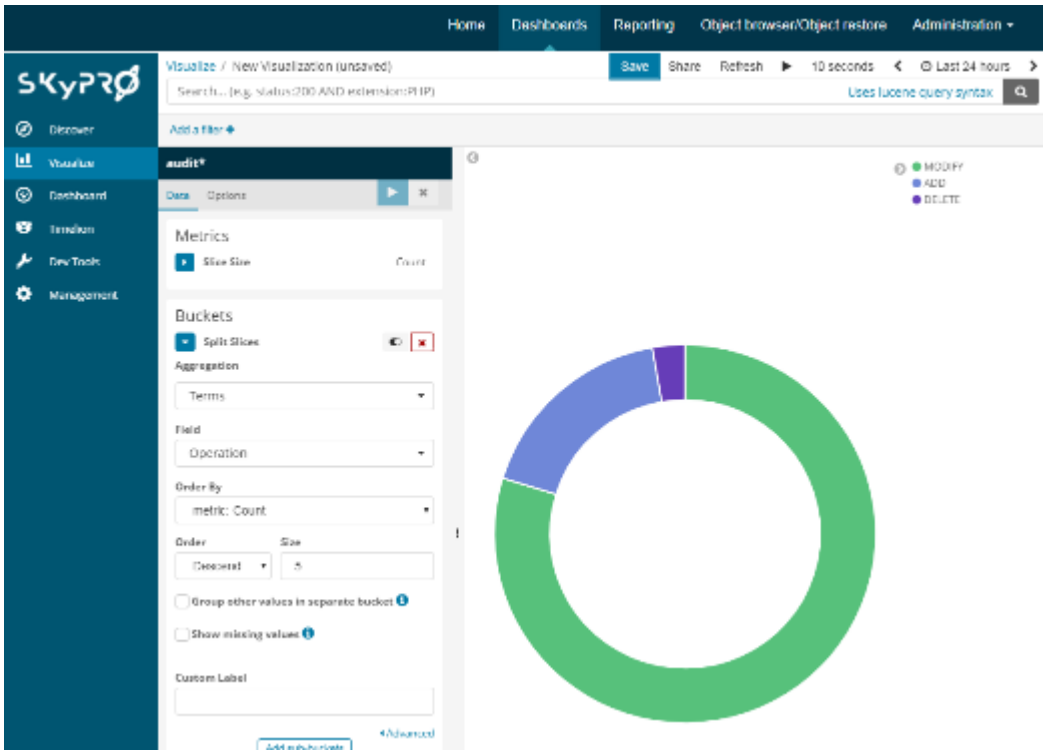
Open the Audit Server home page and click the "Dashboards" button on top. Click on any dashboard. On the left panel select "Visualize".

Click "+" button above the visualization list.

For example, we want to create pie chart that will show operations for Audit Dashboard.

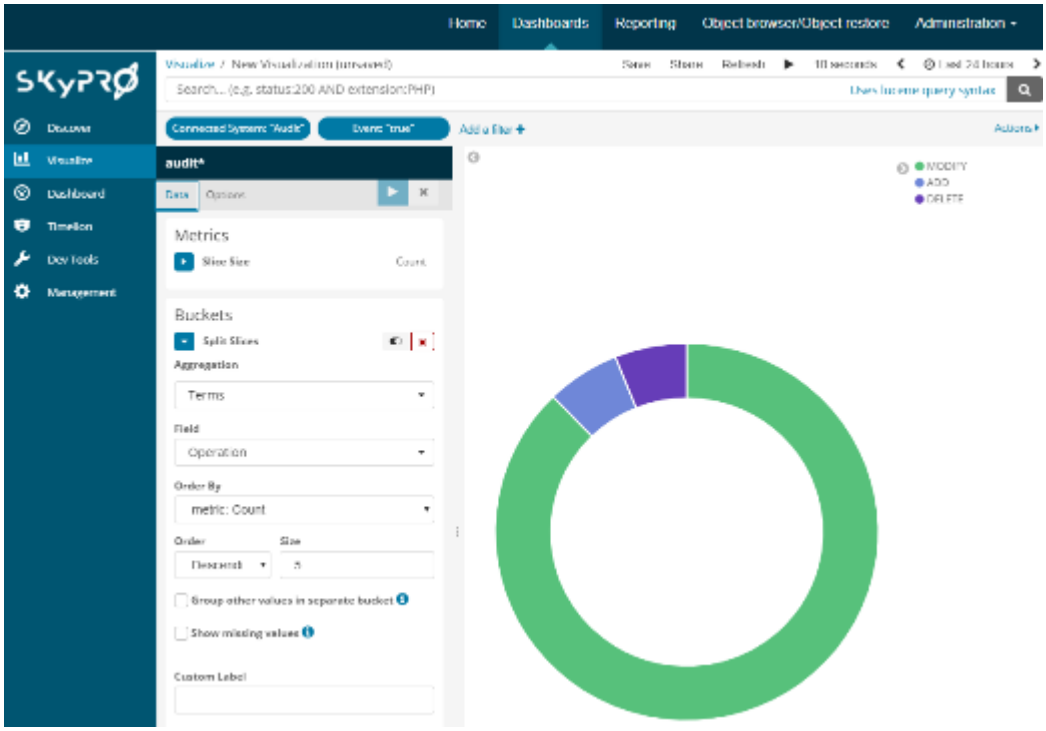
We select Pie Diagram, select index "audit*".

On the next screen we select "Split Slices" in the "Buckets", set "Aggregations" = "Terms", "Field" = "Operation", "Order By" = "Count". And then click on the blue "Triangle" button.

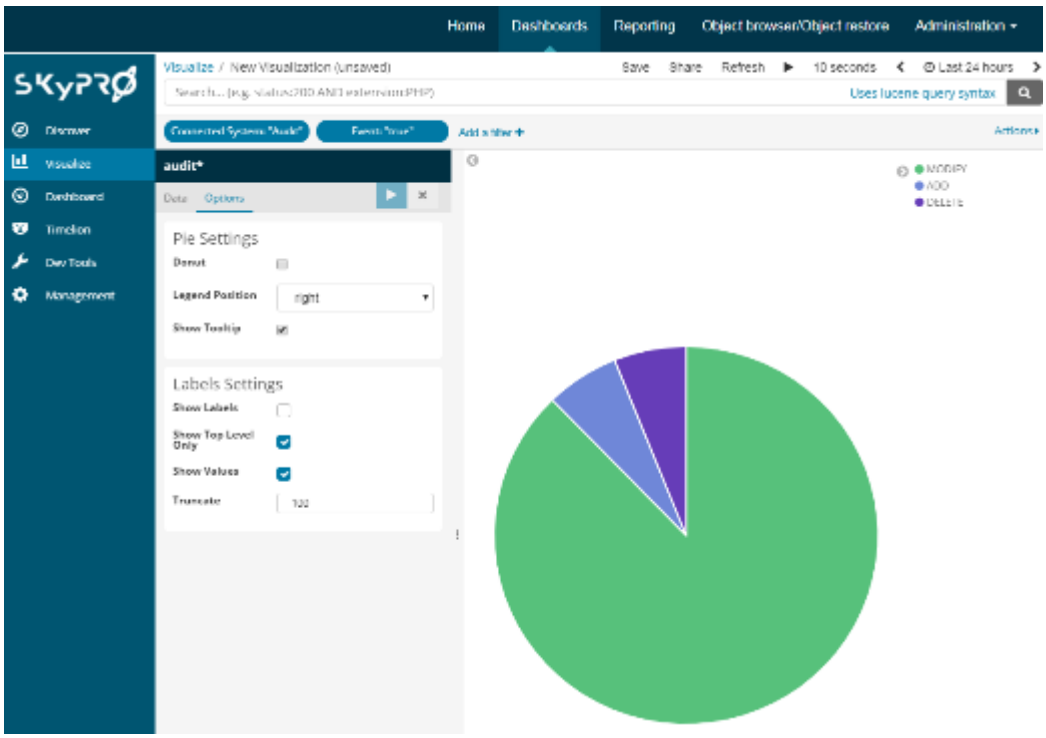


Let's add a filters to catch only events that should be shown in the Audit Dashboard.

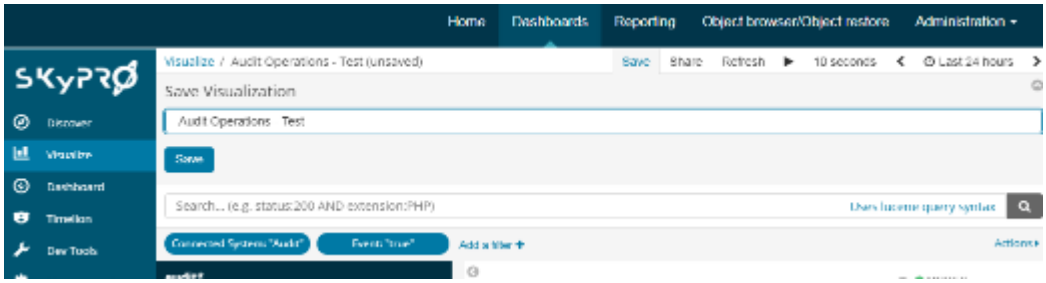
Click "Add a Filter" on the top, Select "Connected System", "is" and "Audit". And then "Save" button. And one more filter: "Event", "is", "true".



Now you see that we actually done this chart! Some little visual things.
We go on the "Options" tab and remove "Donut" tick.



Now looks much better. We can save it. Click on "Save" in the top, enter name for this visualization and click "Save" button. We will call it "Audit Operations – Test".

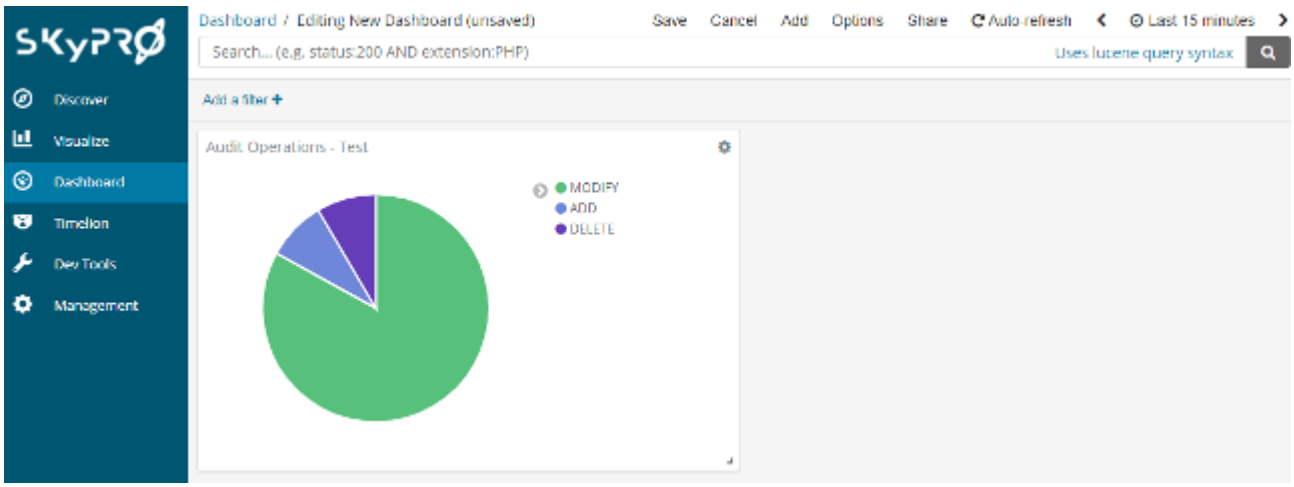


6.3.2 Create new dashboard.

Now we will create new dashboard and add our visualization into it.

On the left panel select "Dashboard". Click "+" button above the dashboards list.

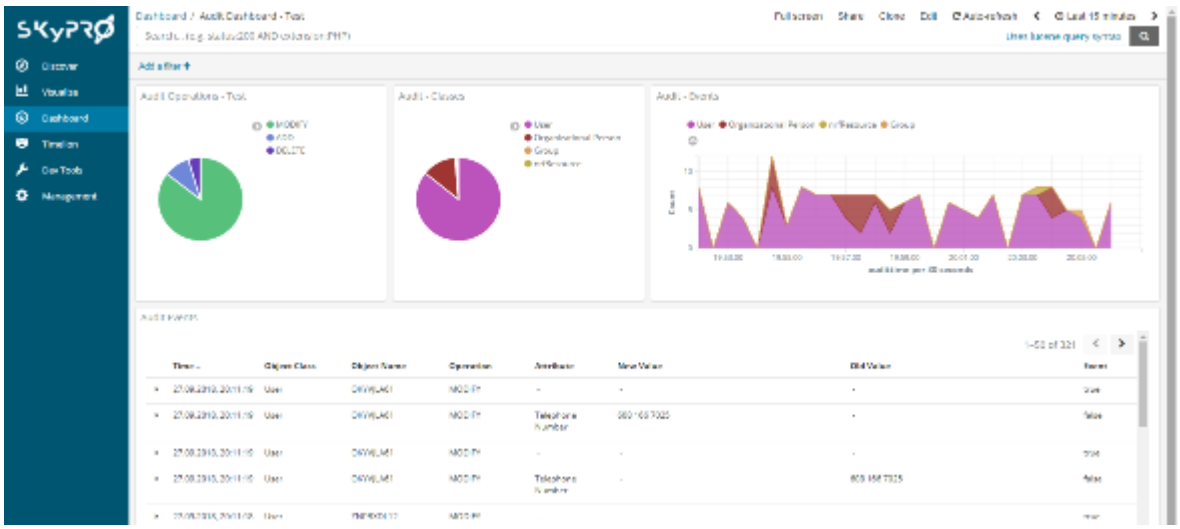
Then click on "Add" in the top. Now we see full list of Visualizations and Saved Searches. Find our visualization "Audit Operations – Test" and add it. Then again click on "Add" in the top to close this list.



Now we can save this dashboard as "Audit Dashboard – Test".

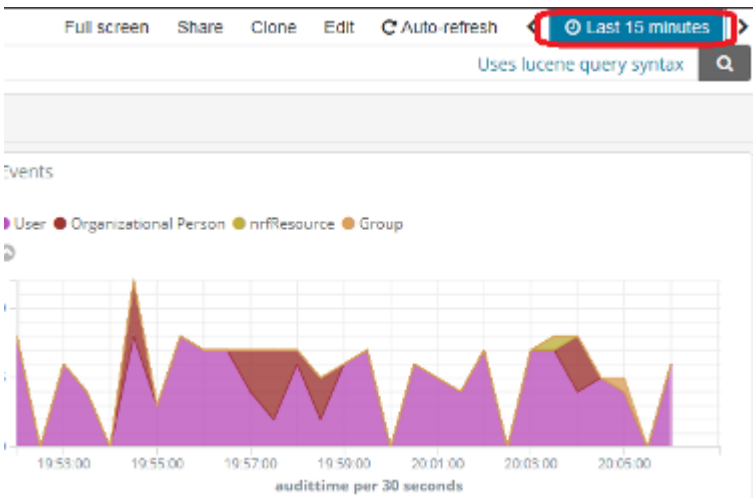
Now let's add more visualizations into the dashboard.

Click on "Edit" in the top, then click on "Add" and select several visualizations and Saved Search. You can change a size of visualization and it's position with a mouse.

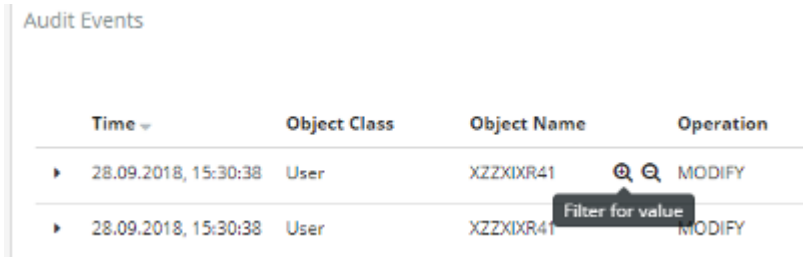


6.3.3. Using the dashboards

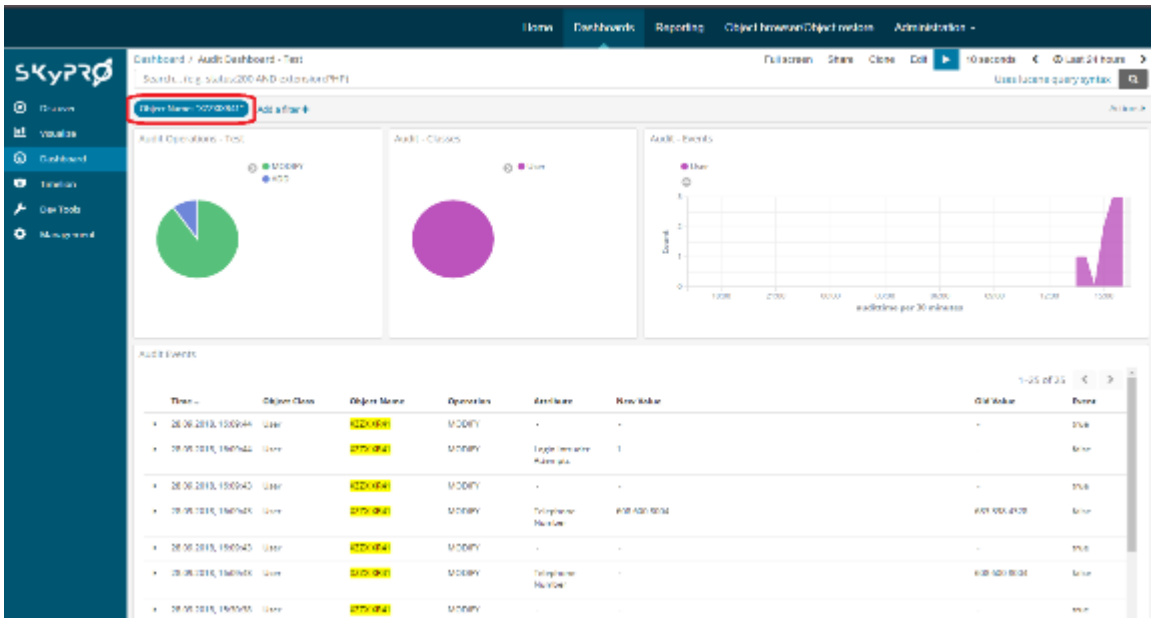
In the dashboard you can choose the period for which you need the information. Please click on "Time Range" in the top right corner.



In the Filters row you can create one or more filters to select only the data you need.
For example, let's select all events for some particular user.
We point on the Object Name in the Audit Events table. And then click on "+" magnifier.



Now we see events only for this user. And in the Filters row we see a new filter.

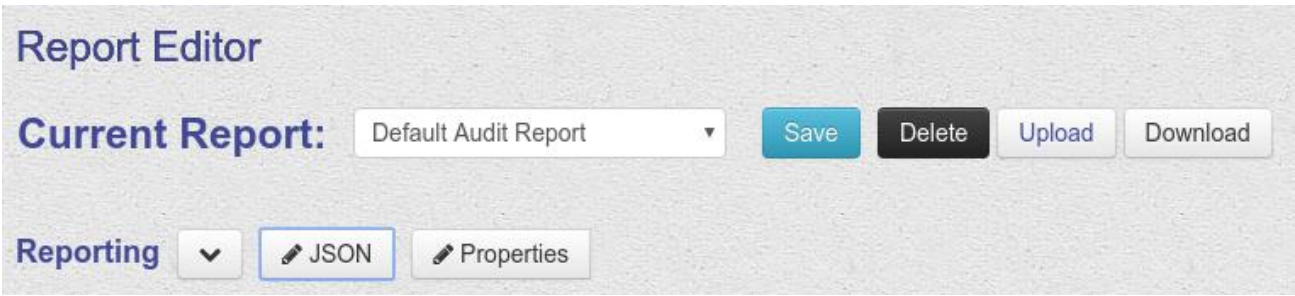


We can turn on/off this filter, can delete or edit it. Also we can pin it, then it will always be pinned on this dashboard.

7 Report Editor

Besides predetermined reports you can also create your reports and edit existing ones.
To start editing the reports you need to go to report editor Administration → Report Editor

7.1 Actions in Report Editor



In order to choose a report you would like to edit, please select it from the drop-down list "Current report".

The following buttons are also available:

Save – save current changes;

Delete – delete the current report;

Upload – upload a new report from the JSON file;

Download – download the current report as a JSON file.

When editing complex objects or units of the report the following buttons will be available:

- collapse or expand block.

JSON – view and edit the current report in JSON format;

Properties – choose options to show and options to hide. This drop-down menu is available for the whole report and for the complex objects with additional options.

+ Field - add object or field.

Field - remove object or field.

- change order of elements.

7.2 Report editing

Find below the description of the fields in Report Editor. The parameter type is shown in brackets:

- (string) – 1-line string;
- (integer) - 1-line string, but value must be an integer value;
- (text) – a multi-line input field;
- (check) – field with 2 positions: "checked" and "unchecked";
- (select) (option 1, option 2, ...) – field with a list, you could select a single value from;
- (block of parameters) - block of parameters.

The Report ID (string)
Name (ID) of the report that will be used when you import it into ElasticSearch.

Display Name (string)
Name of the Report which user will see while creating the report.

Regex Filter for Index selection (string)
Regular expression for finding the right indexes in ElasticSearch. The system searches the data array (indexes) in ElasticSearch, matched with the specified regular expression, and displays these indexes to the user when creating a report. The names of found indexes are previously converted using **Index Rename JavaScript.**
E.g., if:

- parameter "Regex Filter for Index selection" = "*^report*";
- parameter "Index Rename Javascript" = "*return input.substring(7).replace("-"," ").capitalizeFirstLetter();*".

then the found index "*report-default-2016.04.03*" will be converted for the user into "*Default 2016.04.03*".

Index Rename Javascript (text)
The system searches the data array (indexes) in ElasticSearch, defined by regular expression, specified in the parameter **"Regex Filter for Index selection"**, and shows these indexes to the user when creating a report. The names of found indexes are previously converted by javascript, specified in this parameter.
E.g., if:

- parameter "Regex Filter for Index selection" = "*^report*";
- parameter "Index Rename Javascript" = "*return input.substring(7).replace("-"," ").capitalizeFirstLetter();*".

then the found index "*report-default-2016.04.03*" will be converted for the user into "D*efault 2016.04.03*".

Show Indexselection (check)
allows the user to select the necessary ElasticSearch Index when creating a report. Typically, different indexes refer to different dates. If this field is unchecked, then the selection window for the Index will not be shown and the report will always be created based on the data contained in the Index specified in the parameter **"Indexname, if no Indexselection is used"**.

Indexname, if no Indexselection is used (string)

Name of Index to create a report. This parameter is valid, if the parameter **"Show Indexselection"** is unchecked.
If this parameter is empty and the parameter **"Show Indexselection"** is unchecked, then all indexes fitted the template **"Regex Filter for Index selection"** will be used.

Title for the fix given index (string)
Title for the Index, entered in the parameter "Indexname, if no Indexselection is used".

Sort Fieldname (string)
Fieldname for sorting query results in Report.

Sort Direction (select) (asc, desc)
Sorting direction for query results in Report.

Fields to retrieve data from (block of parameters)
The list of fields to be received from the data array and displayed (or used otherwise) in the report. You can add, delete, and change the sequence of the fields in the report. The field names of the data are to be entered in the parameters **Field 1 - Field n (string).**

Number of Records to Fetch and Display (string)
Number of records that will be shown in Report.

The Report Directive / Logic (text)

Filtertemplate definitions (block of parameters)

Predefined Queries (block of parameters)

Aliases and view options for fields (block of parameters)

If you would like to change names for the standard attributes, displayed in your report, you can create an Alias for this field.
Field "Name of field" (string) should contain a name of the attribute, which you are creating an Alias for. Field "Alias" (string) contains a name, which will be displayed instead of the standard attribute name.
"Hide from view" (check) - allows to hide the attribute and the value in a result report. But you still can use this value for your own purposes.
* All the options configured in this section effect the reports which are exported and the web-presentation of the report (in case of using "Automatic table view" see the item "The Report Template / Content").

List definitions (block of parameters):

Sometimes the additional data are needed which can be used later when creating the report. This option allows uploading data into the name lists.
List definition has the following fields:
Filtername – a name of the list, where the additional data will be uploaded (type: String).
Filterquery – a query whereby the data will be uploaded (type: JSON).
Fields to retrieve – defines the fields which you would like to upload into the list (type: Strings).
Keyfieldname – a name of the field, that will be used as a key (type: String).

Maximum Size of Records to retrieve – Maximum size for the uploaded data (type: Int).
How to use the data uploaded with "List definition" see the item "The ES Result Post Processing (server-side)".

Filter definitions (block of parameters):

Each element of this unit is a description of the filter:

- **Filtertype (select) (hidden, search, select, selectsearch, selectperiod).**
  Template for filter displaying.
  Here you can choose the template displaying this filter when creating the report:
  - hidden - this filter is applied to the data, but it's not displayed;
  - search - the filter is displayed as search input field;
  - select - the value list with a selection option is displayed;
  - selectsearch = select + search
  - selectperiod - select a period (for a field of "date-time" type)
- **Internal Filtername (string)**
  This Name can be used to refer to this filter within the report.
- **Filter Title (string)**
  Filter name, which the user will see when creating the report
- **Attribute to Filter on (string)**
  Name of the attribute in the data array, to which the filter is applied.
- **Type of this Filter (select) (or, and)**
  Logical ratio of values, which you selected in the interface of the filter. This field has a sense if there are several values selected in the interface of the filter.
- **Querystring (string)**
  Querystring of records from the data store, which will be displayed in the interface of the filter. For example, to desplay all users you can use the following string:
  *objectClass: inetOrgPerson AND cn: **
- **Template to use for this Filter. If not defined, Template equals type of filter (string).**
  Name of the filter displaying template. The name should match the "Filtertype" parameter.
- **Sort direction (select) (asc, desc)**
  Records sort direction, that is used when displaying the filter interface.
- **Maxiumum Size of Records to retrieve (integer)**
  The maximum number of records that can be displayed in the filter.
- **List of Filter we depend on**
  List of parent filters, which effect present filter. That is, before the filter applying records are filtered with specified filters. So called filter chain is created. When the user changes selected records in the parent filter, the records list get updated in this filter.
  - Used filter 1 (string) - internal name of the parent filter.
  - Used filter 2 (string)
  ...
  - Used filter n (string)
- **Query Reformat Script. 'return input;' (text)**
  Script for postprocessing the records, displayed in the interface of this filter. With Javascript you can do simple data conversion, got from the data store.
- **Query Keyattribute (string)**
  Key attribute for a query.

Field, which will be substituted into the query to the data store when you select a record in the filter interface.

- **Query Valueattribute (string)**
  Value attribute for a query.
  Field, which will be displayed in the record list. That means, the record in the filter interface will be identified by this field.
- **Regexp for filtering (text)**
  Javascript code which forms Regular expression based on user selected value. (type: Javascript)
  To create REGEXP filtering rule for Elasticsearch which based on user selected values you need define "Attribute to Filter on" and create javascript function which return REGEXP. Fields "Value to Filter the Atttribute", "Query Keyattribute" should be not defined.
  Function for REGEXP can operate with internal variable "selected" which contain value(s) which user selected in filter. This variable can contain string or array of strings, dependent what user selected.
  Example script which creates REGEXP from selected by user values.

```
var regexp;
if (selected.length > 1) {
var mapped = selected.map(function(el){return ',cn=' + el + ','});
regexp = '.*' + '(' + mapped.join('|') + ')' + '.*';
} else {
regexp = '.*' + '(' + ',cn=' + selected[0] + ',' +')' +'.*';
}
```

- **Predefined values (will be used instead of Elastic search data) (string)**
  JSON array that will be used as predefined filter values, the format of the array objects key → value, e.g. [{"key1" : "value1"}, {"key2": "value2"}, {"key3": "value3"}] (type: JSON aray)
  Sometimes you may need to create a filter that will contain custom values as opposed to the values obtained from Elasticsearch.
  In order to use this feature you need to fill in the field "Predefined values" with JSON Array, type: key → value, e. g. [{"key1" : "value1"}, {"key2": "value2"}, {"key3": "value3"}]

The Report Template / Content (text)

This field allows you to define how the web-presentation of your report will look. By default the basic presentation is created using Report Wizard but you can redefine it at any time using HTML, AngularJS, JavaScript.

Note! If you would like to use your definition for the web-presentation, please set up an id attribute equal to "manual-table" in the tag <table>. If you would like to use an automatic generation, set up an id attribute equal to "auto-table" in the tag <table>.

The ES Result Post Processing (server-side) (text)

Using JavaScript in this section you can operate any results received from ElasticSearch. JavaScript created by you will be implemented for any entry received from ElasticSearch. For incoming and outgoing values stays a variable "record", which is the String presentation of JSON object.

You can use the following variable and functions in your JavaScript:
- **"record"** (String presentation of record), to use it as JSON object you can convert it by method JSON.parse(record).
- **"lists"** (String presentation of pre-loaded data which can be defined in "List definition"), to use it as JSON object you can convert it by method JSON.parse(lists)
- result (Boolean variable, if it contains **"true"** value the current record will be used in the result array, if not - **"record"** will be missed.
- **"request"** (String presentation of JSON object which sends to ElasticSearch a request), to use it as JSON object you can convert it by method JSON.parse(request)
- print (value) – (function which prints variable content to AuditServer console or log file). Example of use: print ("Record: " + record) - will print record data to console or log file.

Example of usage:

```
var jsonRecord = JSON.parse(record);
// convert string presentation of record to JSON object
var jsonLists = JSON.parse(lists); convert string presentation of
pre-loaded lists to JSON object
var result = true;
// set result to true, so all records will be used in result

function getValueByListAndKeyAndAttrname(sListName, sKeyName,
sAttrname){
// search value in list with name "sListName", with key "sKeyName",
by attribute "sAttrname"
var result = '';
for (i in jsonLists){
var keyname = jsonLists[i].keyname;
if (i == sListName) {
if ((typeof jsonLists[i].hits !== "undefined") && (typeof
jsonLists[i].hits.hits !== "undefined")) {
var hits = jsonLists[i].hits.hits;
for (j in hits) {
if (typeof hits[j].fields !== "undefined") {
for (k in hits[j].fields){
if ((k == keyname) && (hits[j].fields[k][0] == sKeyName)) {
var field = hits[j].fields[k];
result = hits[j].fields[sAttrname];
}}}}}
return result;
}

function parsenrfRoleCategoryKey(jsonRecord){
// custom parse function which replace "nrfRoleCategoryKey" with
"description" value from pre-loaded "cimlistaux" list
if (typeof jsonRecord.fields.nrfRoleCategoryKey !== "undefined") {
//check is nrfRoleCategoryKey field exist
for (i in jsonRecord.fields.nrfRoleCategoryKey){ // loop all values
in array
var nrfRoleCategoryKey = jsonRecord.fields.nrfRoleCategoryKey[i];
// get current element from array
```

```
var nrfRoleCategoryKeyValue =
getValueByListAndKeyAndAttrname("cimlistaux", nrfRoleCategoryKey,
"description");
// get “description” for current nrfRoleCategoryKey from list
“cimlistaux”
if (nrfRoleCategoryKeyValue != ""){jsonRecord.fields['description'] =
nrfRoleCategoryKeyValue;}
}}}

function filter (){
// your filtering functionlity
if (typeof jsonRecord.fields !== "undefined"){
// check is fields exist
parsenrfRoleCategoryKey(jsonRecord);
// run some parse function
}
record = JSON.stringify(jsonRecord);
// string presentation of record which will returned as result of
processing
//print ("record: " + record);
// print result record to AuditServer console (or log file)
}

filter();
// run filter function.
```

Template for Exporting (Table Template for PDF report (JSON schema description)) (text)

You can create your customized table type for PDF reports. For this table type is used JSON object with the following sections.

Array of the table objects:
e.g. `[{table1},{table2},{table3}]`

Any object Table can include the following fields and values:

“width” – width of the table on the page in percentage terms (value type is float, e.g. 100f) (required field)
“cell-count” - column count in the table (value type is integer, e.g. 2) (required field)
“cell-width” - width of the columns in percentage terms (value type is float array e.g. ["30f","70f"]) (optional field)
“cells” - array of the cells objects (required field)
e.g. `cells:[{cell1},{cell2},{cell3}]`

Any cell object can include the following fields and values:
“header” - the value of this field will be used for table header (Value type is a field name. If the field has an Alias, then it will be used.) (optional value)
“value” - the value in this field will be used for values. (Value type is a field name.) (optional value)

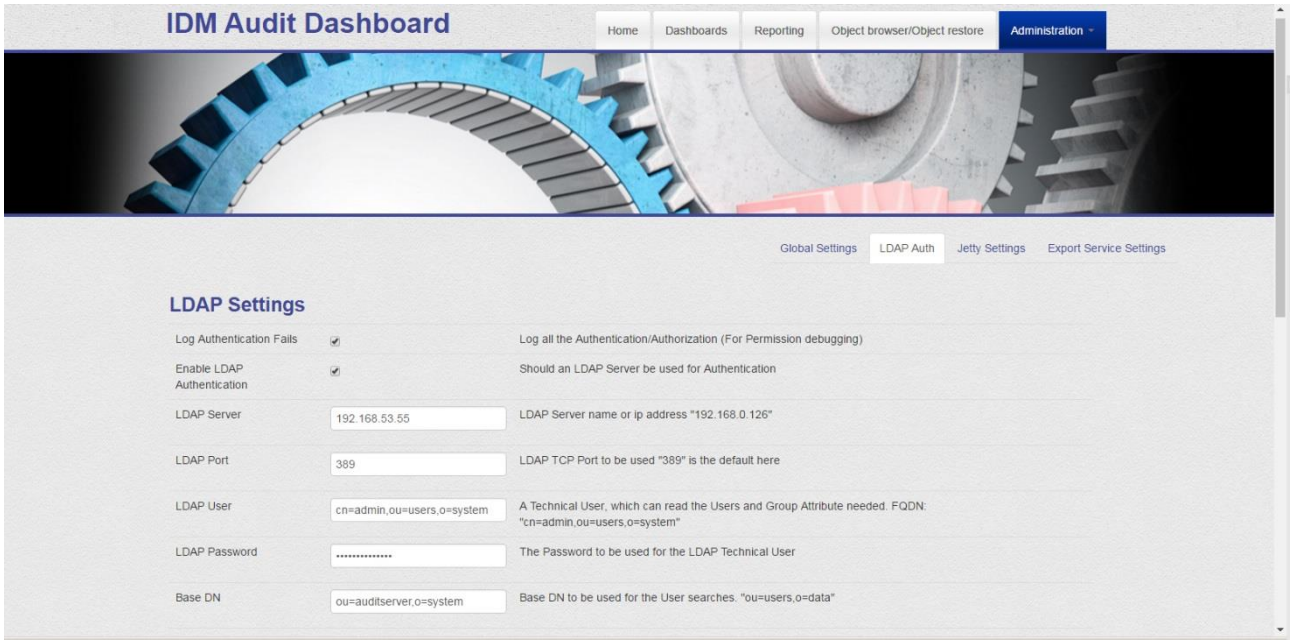
"colspan" - Specifies the number of columns a cell should span (optional value)
"rowspan" - Specifies the number of rows a cell should span (optional value)

Example for object JSON describing a table:

```
[{
      "width": "100f",
      "cells-count": 2,
      "cells-width": [
            "30f",
            "70f"
      ],
      "cells": [{
            "header": "company"
      }, {
            "header": "cn"
      }, {
            "value": "company"
      }, {
            "value": "cn"
      }]
}, {
      "width": "100f",
      "cells-count": 4,
      "cells": [{
            "header": "nrfContainerRoles"
      }, {
            "header": "nrfAssignedRoles"
      }, {
            "header": "nrfInheritedRoles"
      }, {
            "header": "nrfMemberOf"
      }, {
            "value": "nrfContainerRoles"
      }, {
            "value": "nrfAssignedRoles"
      }, {
            "value": "nrfInheritedRoles"
      }, {
            "value": "nrfMemberOf"
      }]
}]
```

8 Configuring LDAP authentication for Audit Server

To setup the LDAP authentication for your Audit Server you should open the menu "Administration" -> "Settings" and go to the tab "LDAP Auth".



Settings for LDAP authentication:

- Log Authentication Fails – put all authentication/authorization events to Audit Server log file;
- Enable LDAP Authentication – enable or disable the LDAP authentication;
- LDAP Server – LDAP Server name or IP address. E.g., "127.0.0.1" or "localhost";
- LDAP Port – LDAP TCP Port to be used ("389" by default);
- LDAP User – a technical user, which can read the required attributes of Users and Groups. E.g., "cn=admin,ou=users,o=system";
- LDAP Password – a password for the LDAP User;
- Base DN – Base DN to be used for User searches. E.g., "ou=users,o=data". All Users and Groups, which are related to the LDAP Authentication, should be placed here;
- Use Groups – you can use Groups for the Advanced Authorization. Using the Groups Authorization, you can turn on/off certain Dashboards and Reports for each user set. You can set permissions for a Group and then add Users to this Group;
- Membership Attribute – a User attribute with the DNs of the Groups/Objects for Authorization ("groupMembership" by default);
- Membership Right Mapping Attribute – a Group attribute where the permission information (Regular Expressions for the URL Rights) is stored. Multiple Regex can be used, use ";" to split ("description" by default);
- Group Filter (Regex) – Regex to be used to filter Groups which should be processed for Group Authentication. For all Groups, use ".*" ("ASR-" by default means "process all groups started with 'ASR-'");
- Authentication Timeout – in how many milliseconds an Authenticated User should be removed from the Cache and be reauthenticated against the LDAP Directory (10000 by default);

- Use LDAP Filter – you can turn on/off the LDAP Filter for Authentication/Authorization. Users filtered in that way will get the Rights defined below;
- Authentication/Authorization LDAP Filter – If a User matches this LDAP Filter, it gets the rights to the Dashboards / Reports defined below. Example: "(&(ou=Technics)(cn=A*))" Mean all Users with the Attribut ou=Technics and a cn staring with "A" will get the rights defined;
- Rights Users get via LDAP Filter – If a User matches the LDAP Filter, this are the Rights this User will get. Full Rigths ".*" / Only to Read Stuff "GET:.*;POST:.*" / Write needs "PUT:.*" where .* is regex and can be used to match URLs etc.

Please note: configuring a Group of LDAP authentication for Dashboards have little differences in Kibana 3 and Kibana 6. Please check the examples for more information.

Example 1: configuring a Group to be able to see only certain Dashboards (and nothing else)(for Kibana 3).

Let us suppose we have a DLAP Authentication enabled and properly configured. The "Use Groups" is also enabled and configured "by default".

1. Create a group "ASR-Dashboards-1" in the container defined in the Base DN" option.
2. Edit the group "ASR-Dashboards-1", put in Description: `\/dashboards\/.+(?<!json)$;IDM(%20|\s)Audit(%20|\s)Dashboard.json;IDM(%20|\s)ActiveDirectory(%20|\s)Dashboard.json`
   It means: enable all dashboard stuff except Dashboards itself; enable "IDM Audit Dashboard"; enable "IDM ActiveDirectory Dashboard".
   Please note that names of your dashboards will be processed "as is" and as URL-encoded strings. For example: if you would like to see a dashboard named "IDM Audit & Compliance Dashboard", you should add to the group description: "`IDM(%20|\s)Audit(%20|\s)(%26|&)(%20|\s)Compliance(%20|\s)Dashboard.json`".
3. Add users to this group.
4. The users of this group will see only 2 dashboards on the dashboard panel and will have no access to any other part of the Audit Server (of course if they are not members of any other LDAP Authentication Group).

Example 2: configuring a Group to be able to see only certain Dashboards (and nothing else) (for Kibana 6)

Let us suppose we have a DLAP Authentication enabled and properly configured. The "Use Groups" is also enabled and configured "by default".

1. Create a group "ASR-Dashboards-1" in the container defined in the Base DN" option.

2. Edit the group "ASR-Dashboards-1", put in Description: `\/dashboards\/.+(?<!json)$;IDM Audit Dashboard;IDM ActiveDirectory Dashboard`
It means: enable all dashboard stuff except Dashboards itself; enable "IDM Audit Dashboard"; enable "IDM ActiveDirectory Dashboard".

3. Add users to this group.

4. The users of this group will see only 2 dashboards on the dashboard panel and will have no access to any other part of the Audit Server (of course if they are not members of any other LDAP Authentication Group).

Example 3: configuring a Group to be able to see only certain Reports (and nothing else)

Let us suppose we have a DLAP Authentication enabled and properly configured. The "Use Groups" is also enabled and configured "by default".

1. Create a group "ASR-Reports" in container defined in "Base DN" option.
2. Edit the group "ASR-Reports", put in Description: `\/reports\/(?!(Indexer\/|wizard|editor)).*;default-users$;default-role$;test2$`
   It means: enable all report stuff except Reports itself, Report Wizard and Report Editor; enable report "default-users"; enable report "default-role"; enable report "test2".
3. Add required users to this group.
4. Users from this group will see only 3 reports and will have no access to any other part of Audit Server (of course if they are not members of any other LDAP Authentication Group).

Example 4: configuring a Group to be able to change the Audit Server Settings

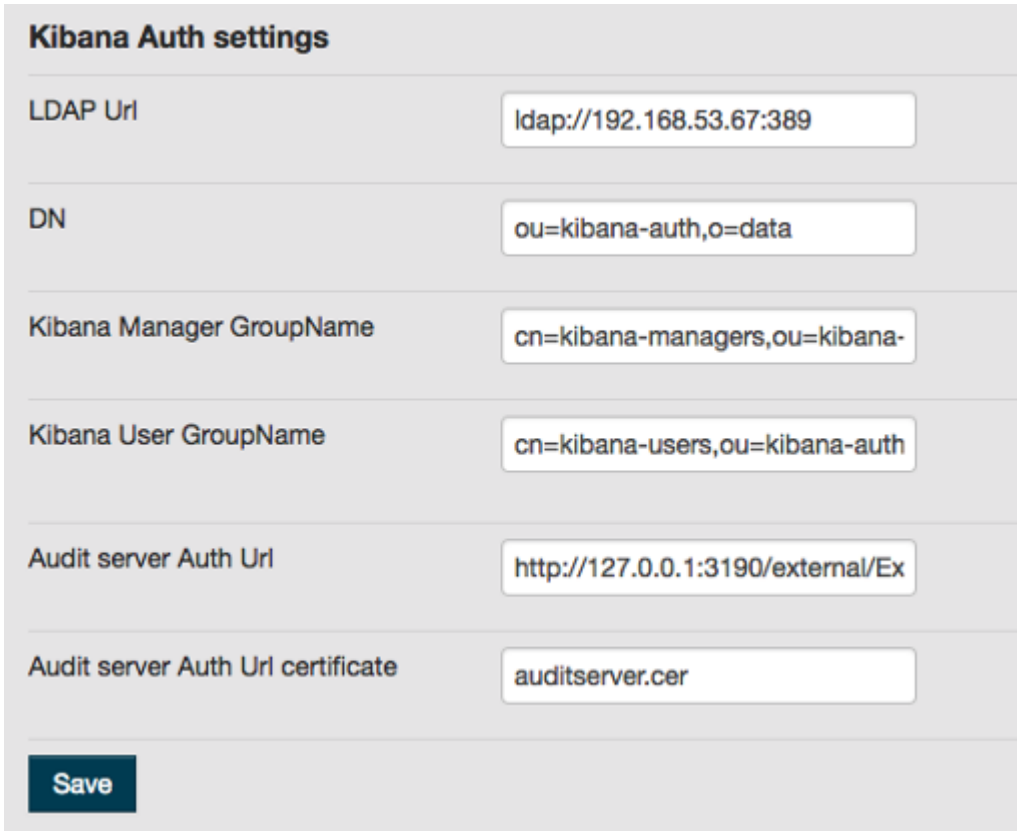
Let us suppose we have a DLAP Authentication enabled and properly configured. The "Use Groups" is also enabled and configured "by default".

5. Create a group "ASR-Settings" in container defined in "Base DN" option.
6. Edit the group "ASR-Settings", put in Description: `\/admin`
   It means: enable Settings.
7. Add required users to this group.
8. Users from this group will be able to configure the Audit Server Settings but will have no access to any other part of Audit Server (of course if they are not members of any other LDAP Authentication Group).

Configuring manager access to Dashboards for Kibana 6.

If you want to allow some LDAP users to make changes in the Dashboards you can make it using ES & Kibana Proxy Settings.

Please open the menu "Administration" -> "Settings", go to the tab "ES & Kibana Proxy" and scroll down to "Kibana Auth settings".



Settings for Kibana LDAP Authentication:

- LDAP Url – url to LDAP server in format "ldap://host:port". You can get LDAP host and port from the LDAP settings (see above);
- DN – base DN for searching Users and Groups. You can get base DN from the LDAP settings (see above);
- Kibana Manager GroupName – DN of group members of which will have Kibana Manager rights (will be able to edit and create the dashboards). By default Audit Server admin has Kibana Manager rights;
- Kibana User GroupName - DN of group members of which will have Kibana User rights (will be able just to view the dashboards). **By default all LDAP users have Kibana User rights**;
- Audit server Auth Url – please leave the default value;
- Audit server Auth Url certificate - please leave default value.

And now all you need to do is just add required LDAP users into Kibana Manager group (of course LDAP Authentication should be enabled as described above).

Conclusion

With the IDM Audit & Compliance Dashboard, you can create powerful dashboards in no time. All components fulfill every requirement you could expect from a professional SIEM (Secure Identity and Event Management) solution.

Elasticsearch is able to process thousands of events per second, can be clustered, and guarantees automatic failover and high availability.

The Audit Server is a very powerful and easy to use visualization component offering a lot of graphical building blocks.

The Report Service logs current states of object on a scheduled basis so we know the values of all attributes at any time in the history for compliance purposes. You can generate reports on historical data and export them to Excel. You can browse through historical data and even restore single objects via an LDIF export.

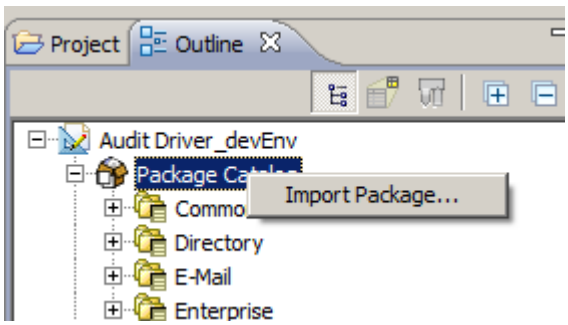
Attachment 1

Setting the audit of your own Driver using IDM Driver Dashboard.

In order to audit the events that occur in your drivers, you should do the following:

1. Install the package "SKyPRO Audit Driver Helper" into the IDM Designer (sp_ad_h_X.X.X.jar where X.X.X – version of package).

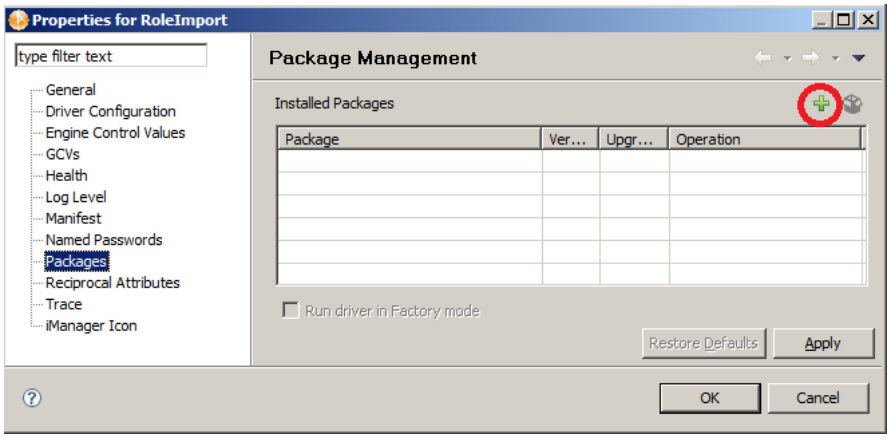
- - right click on the "Package Catalog" and select "Import Package...";



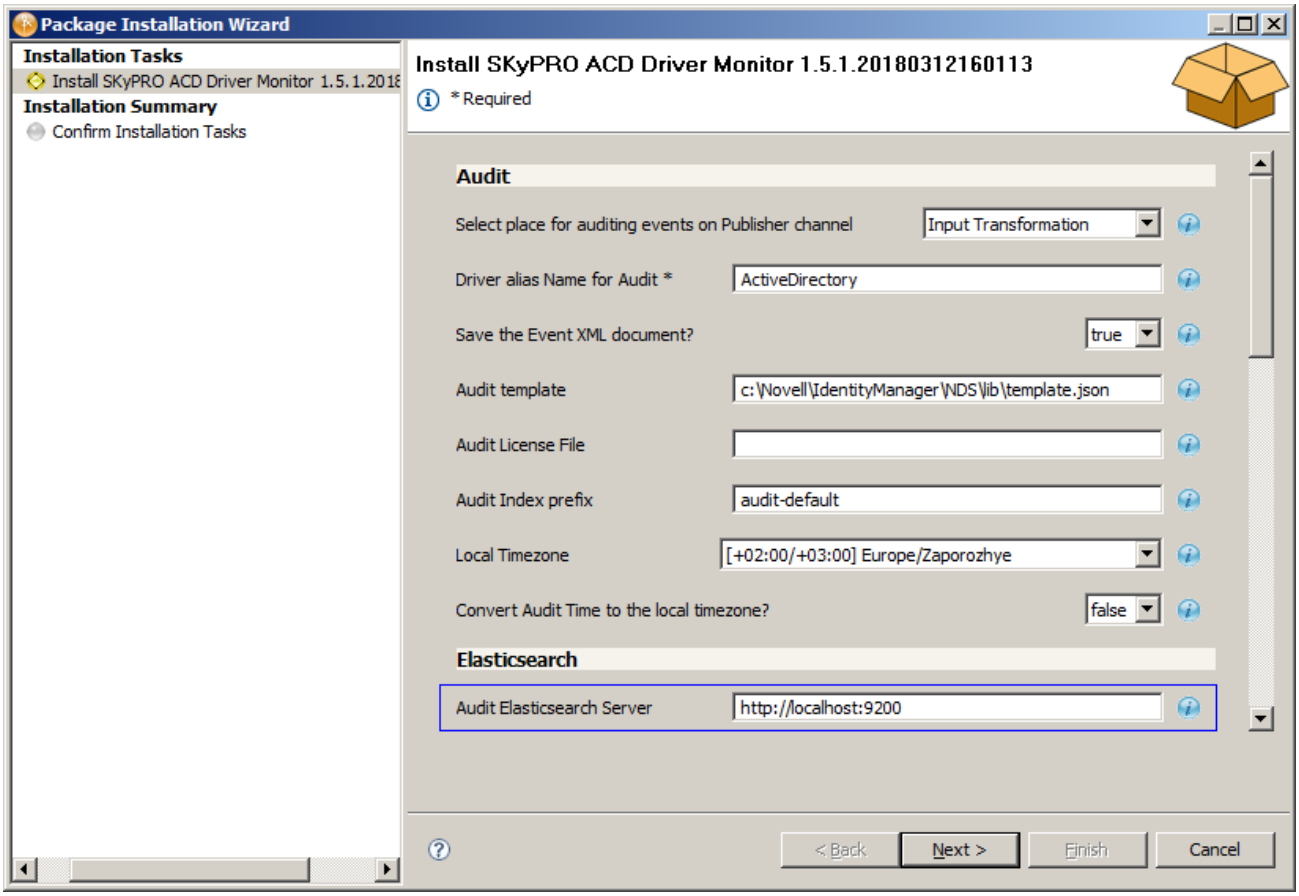
- - click the button "Browse..." and select the file "sp_ad_h_X.X.X.jar".

2. Install package into your Driver.

- - open Driver Properties by double clicking on the driver;
- - on the "Package" tab click on button "Add package";



- - select "SKyPRO Audit Driver Monitor" and click "OK";
- - specify required GCVs.



Description of the most parameters you can find in the paragraph 3.7.1.4 "Create the Driver". Please note that "Location for Audit Objects" should be the container of type "acdAuditPod".

- - finish installation.

Additional fields.

You can add some additional fields to see them in your Driver Dashboard. For doing this you should:
- according to the place you've chosen to audit driver events on Publisher Channel, open the policy "SPACDM-pub-itp-audit-event-opdata-userdef" (for Input Transformation), "SPACDM-pub-etp-audit-event-opdata-userdef" (for Event Transformation) or "SPACDM-pub-ctp-audit-event-opdata-userdef" (for Command Transformation). On Subscriber Channel it will be a Command Transformation policy "SPACDM-sub-audit-event-opdata-userdef";
- open the rule "Add user defined parameters";
- add an action "set operation property 'audit-additional-info'". Value should have a format: FieldName1=FieldValue1;…;FieldNameN=FieldValueN.

For instance, you can add the "Domain Name" and "Logon Name" fields to see it in Active Directory Dashboard. For this you can use the following part of DirXML script:

```
<do-set-op-property name="audit-additional-info">
      <arg-string>
            <token-text xml:space="preserve">Domain Name=</token-text>
            <token-global-variable name="drv.domain.dns.name"/>
            <token-text xml:space="preserve">;Logon Name=</token-text>
```

```
            <token-lower-case>
                  <token-attr name="msDS-PrincipalName"/>
            </token-lower-case>
      </arg-string>
</do-set-op-property>
```

Status:

You can check how some event was processed by the Driver Monitor, was it processed successfully or not.
When Audit Driver Monitor processes an event, it puts the processing status into operation properties:

- "audit-sendresult-text" - text information, contains error message in case of error;
- "audit-sendresult-bool" - "true" in case of success, "false" in case of error.

And then you can use these operation properties

Remark:

Please note that successful auditing of driver events depends on the correct position of policies from the package "SKyPRO Audit Driver Monitor" in your driver. So please check the correct position of these policies after installing and updating the package "SKyPRO Audit Driver Monitor".
Correct position of SKyPRO Audit Driver Monitor (SPACDM) policies in your driver:

Input Transformation	SPACDM-sub-audit-status2eDir SPACDM-sub-audit-status2ES **<your_driver_policies>** SPACDM-pub-itp-audit-event-opdata SPACDM-pub-itp-audit-event-opdata-userdef SPACDM-pub-itp-audit-event2eDir SPACDM-pub-itp-audit-event2ES
Publisher Event Transformation	SPACDM-pub-etp-audit-event-opdata SPACDM-pub-etp-audit-event-opdata-userdef SPACDM-pub-etp-audit-event2eDir SPACDM-pub-etp-audit-event2ES **<your_driver_policies>**
Publisher Command Transformation	**<your_driver_policies>** SPACDM-pub-ctp-audit-event-opdata SPACDM-pub-ctp-audit-event-opdata-userdef SPACDM-pub-ctp-audit-event2eDir SPACDM-pub-ctp-audit-event2ES SPACDM-pub-audit-event-execute SPACDM-pub-audit-status2eDir SPACDM-pub-audit-status2ES
Subscriber Command Transformation	**<your_driver_policies>** SPACDM-sub-audit-event-opdata SPACDM-sub-audit-event-opdata-userdef SPACDM-sub-audit-event2eDir SPACDM-sub-audit-event2ES

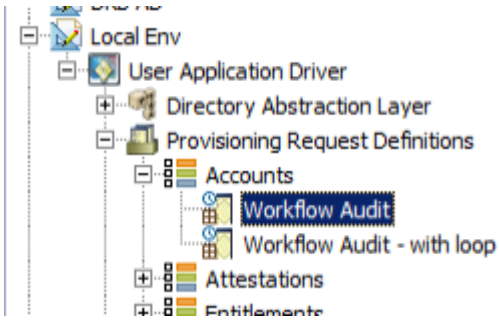
Attachment 2

To configure your workflows to audit them with Workflow Dashboard you should have the IDM Designer version 4.0.2 or higher.

To audit your workflows' events, please do the following:

1 Add PRDs "Workflow Audit" and "Workflow Audit – with loop" to your User Application driver: in the IDM Designer right click on User Application driver, "Import from Configuration File..." and select a file "WorkflowAudit.xml" and then "WorkflowAudit-withloop.xml".

2 Now you can find the PRD "Workflow Audit" and "Workflow Audit – with loop" in "Provisioning Request Definitions" -> "Accounts".



All required Mapping and Rest Activities you can find in this PRD. Just copy it to your workflow.

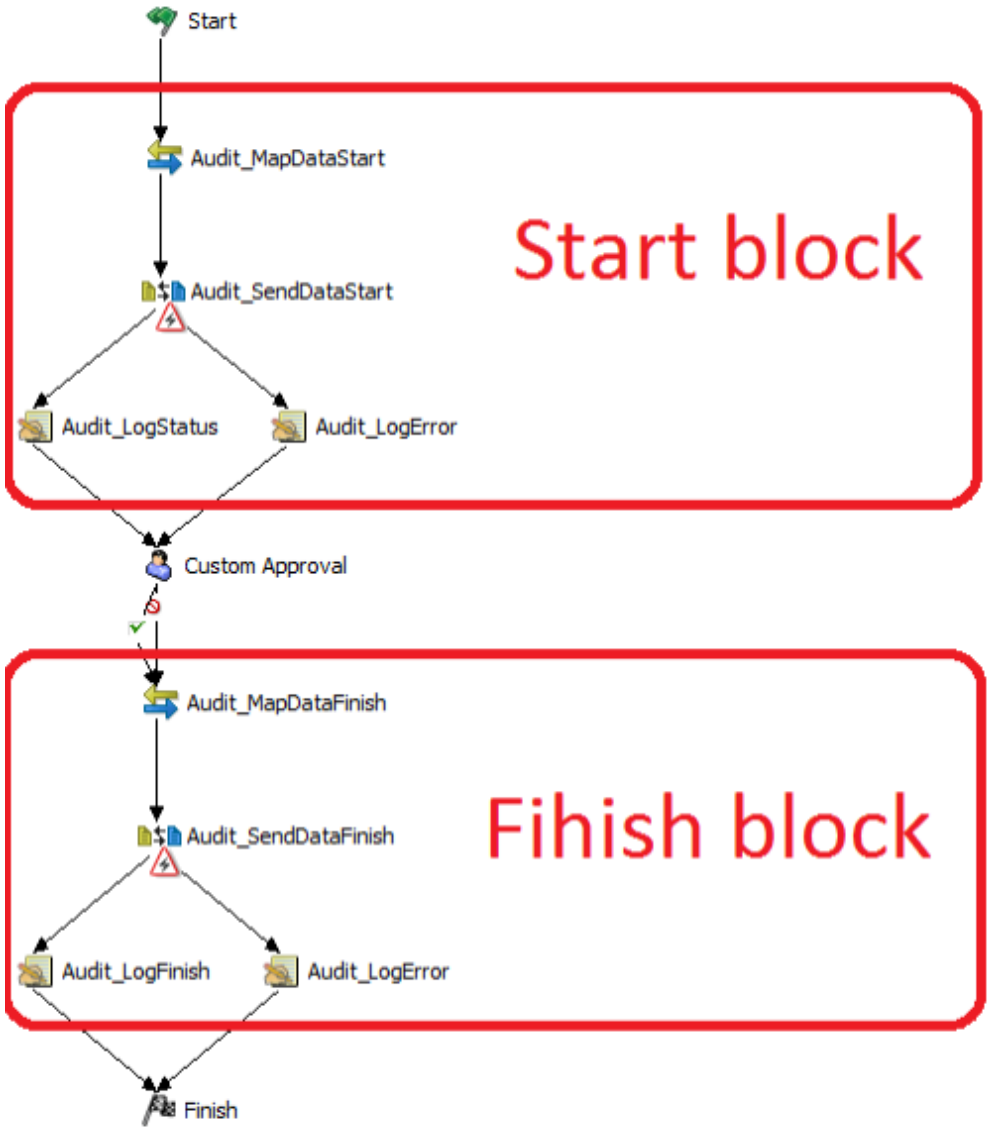
3 Install ElasticSearch mapping rules for workflow index with command:

```
curl -XPOST http://ES_SERVER:9200/_template/workflow_template -d
   @es_workflow-template.json
```

Where "ES_SERVER" – hostname or IP address of your ElasticSearch server, "es_workflow-template.json" – is json file located in your AuditDriver folder.

(CURL utility should be installed in your system).

PRD "Workflow Audit" contains several activities required for auditing the workflow.



Here you can see several activities which help you to set up auditing of your own workflows.

Start block – the activities block which should be put at the beginning of the audited workflow. This block contains:

- Audit_MapDataStart – mapping activity to initially fill data for Workflow Dashboard and Report. Also here you can configure Elasticsearch settings.
- Audit_SendDataStart – REST activity to send data to Elasticsearch. Has 2 outgoing flows, with type "forward" and "error".
- Flow "forward" goes to Audit_LogStart, just for logging status of sending to ES.
- Flow "error" goes to Audit_LogError, for logging error (for example, when ES server is not available).

Finish block – the activities block which should be put at the end of the audited workflow. This block contains:

- Audit_MapDataFinish – mapping activity to complete data for Workflow Dashboard and Report.
- Audit_SendDataFinish – REST activity to send data to Elasticsearch. Has 2 outgoing flows, with type "forward" and "error".
- Audit_LogFinish and Audit_LogError do the same things as in start block.

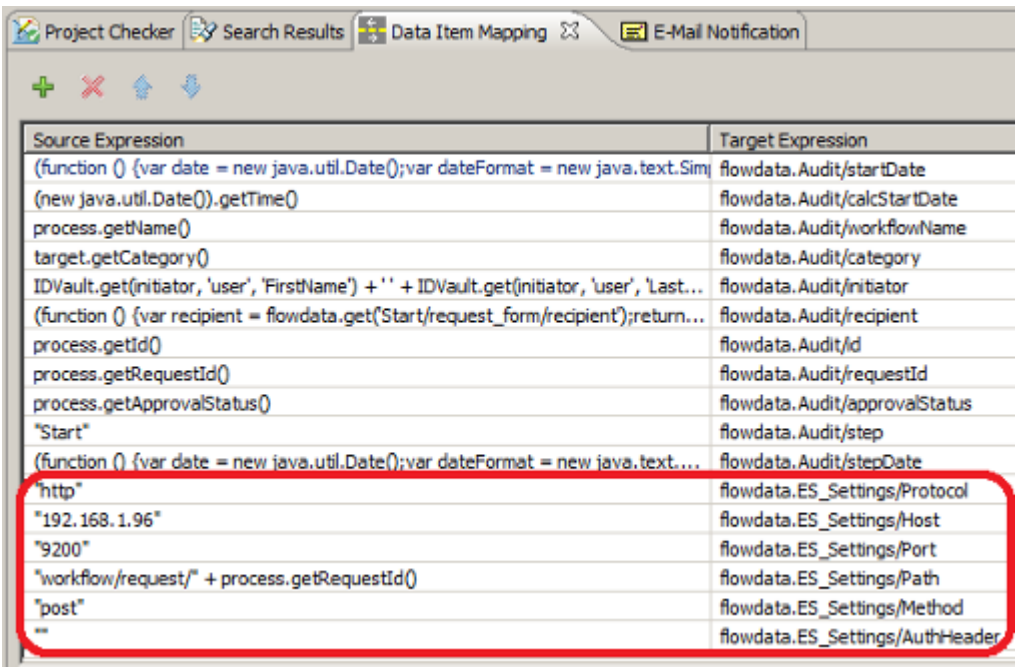
Tasks you should do for each workflow you would like to audit:

1 Copy to the workflow (at the very begin) all activities from the Start block.

2 Copy to the workflow (at the very end) all activities from the Finish block

3 Open «Data Item Mapping» for the Mapping Activity « Audit_MapDataStart» (right click on the activity -> «Show Data Item Mapping») and fill the Elasticsearch settings. Input your ElasticSearch Server protocol, host, port, path and method.

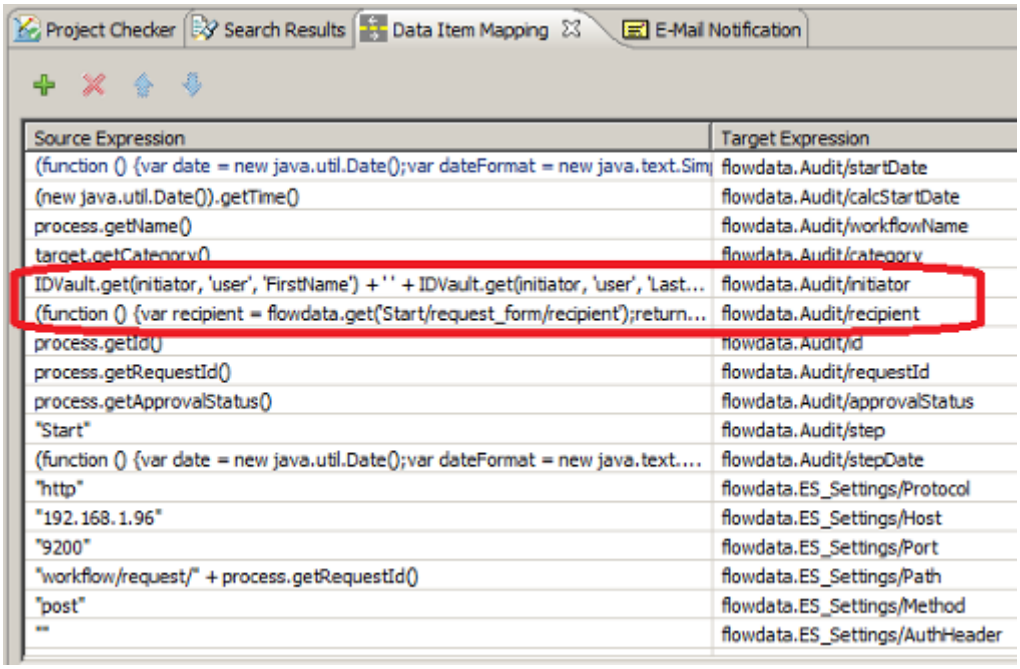
If you use ElasticSearch server included into ACD package, you just need to input your Audit Server host into the parameter "flowdata.ES_Settings/Host" and leave other parameters by default.



If you use the Basic Authentication on your ElasticSearch Server, you should fill the parameter "flowdata.ES_Settings/AuthHeader" with the following value (please change "es_login:es_password" with your data):

"Basic " + java.lang.String(Packages.org.apache.commons.codec.binary.Base64().encodeBase64(java.lang.String("es_login:es_password").getBytes("UTF-8")),"UTF-8")

4 Also as you can see in «Data Item Mapping» for the Mapping Activity «Audit_MapDataStart», to identify initiator and recipient for Workflow Dashboard we use First Name and Last Name attributes. But you can change it to any attribute(s) you like to identify users.

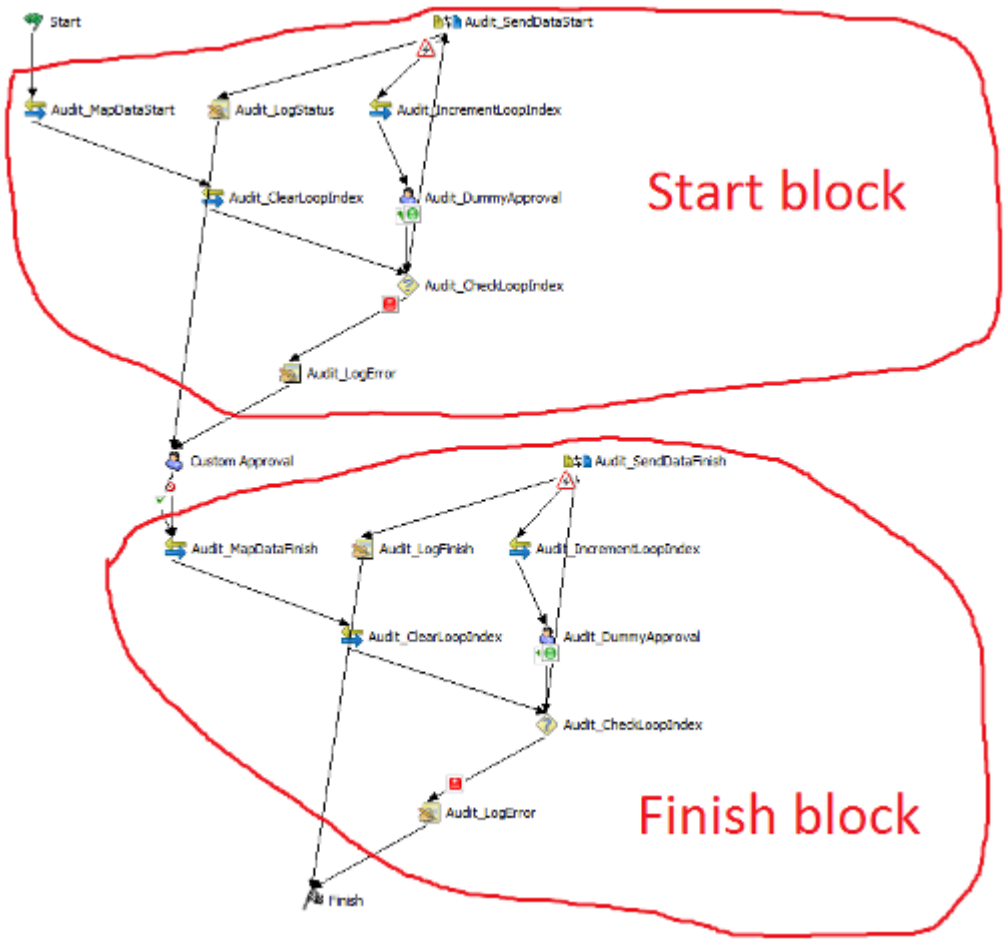


5 If you want to audit not only start and end of workflow, but also some other places you can copy activities from Finish block in every place you want to audit in your workflow. For instance, if you have several Approval Activities and want to know where exactly this workflow gets stuck, you can add activities from Finish block before the every Approval Activity, in Mapping Activity fill the parameter "flowdata.Audit/step" with a value "Approval 1", "Approval 2" and so on.

6 Result of posting data to ES with the Rest Activity is saved to the parameters "flowdata.ES_status" and "flowdata.ES_content". You can use this information for debug purposes (actually both these attributes will be added to workflow log by "Audit_LogStatus" activity).

Please note that the audit data in Elasticsearch, related to the certain workflow, is overwritten by each Rest Activity in the workflow. So in the Workflow Dashboard you will always see just newest information about your workflows states.

In case of not very good network connection between Elasticsearch/Audit Server and your IDM/UA Server you can have a situation when you miss audit events from your workflow. In this case we recommend to send audit messages to ES several times using loops.
In the PRD "WorkflowAudit-withloop.xml" you can find example how to make sending loops.



Here you can see Start block and Finish block, as before. And you can use these blocks as described above.
In the activity "Audit_MapDataStart" you can find several additional fields for configuring loops:

- flowdata.variables/MaxIterations – sending loop iterations count;
- flowdata.variables/LoopSleepInterval – pause between iterations (minutes).

Update Workflow

While updating the ACD to the new version you might need to update also Elasticsearch mapping rules for Workflow index. For this you should make two things:

1) update global template;

2) update Workflow index mapping.

How to update global template you can find in the paragraph "Install ElasticSearch mapping rules" of this Attachment.

To update the Workflow index mapping you should input a console command:
curl -XPOST http://ES_SERVER:9200/workflow/request/_mapping?ignore_conflicts=true -d @es_workflow-mapping.json

Where "ES_SERVER" – hostname or IP address of your ElasticSearch server, "es_workflow-mapping.json" – is json file located in your AuditDriver folder.
(CURL utility should be installed in your system).

And then you can import and use the new version of PRD "Workflow Audit" for auditing your workflows as described above.
Unfortunately there is no automatic way to update all required activities in your workflows which you already configured for auditing them. You will have to make all changes in your activities manually.

Attachment 3

To run Elasticsearch and Kibana 6.x on Linux system you need to have user different from root user.

It is simple to create user from command line:

Enter command from root user:

useradd <username>

Where <username> The name of user which you want to create.