Build your own IDM Audit Dashboard

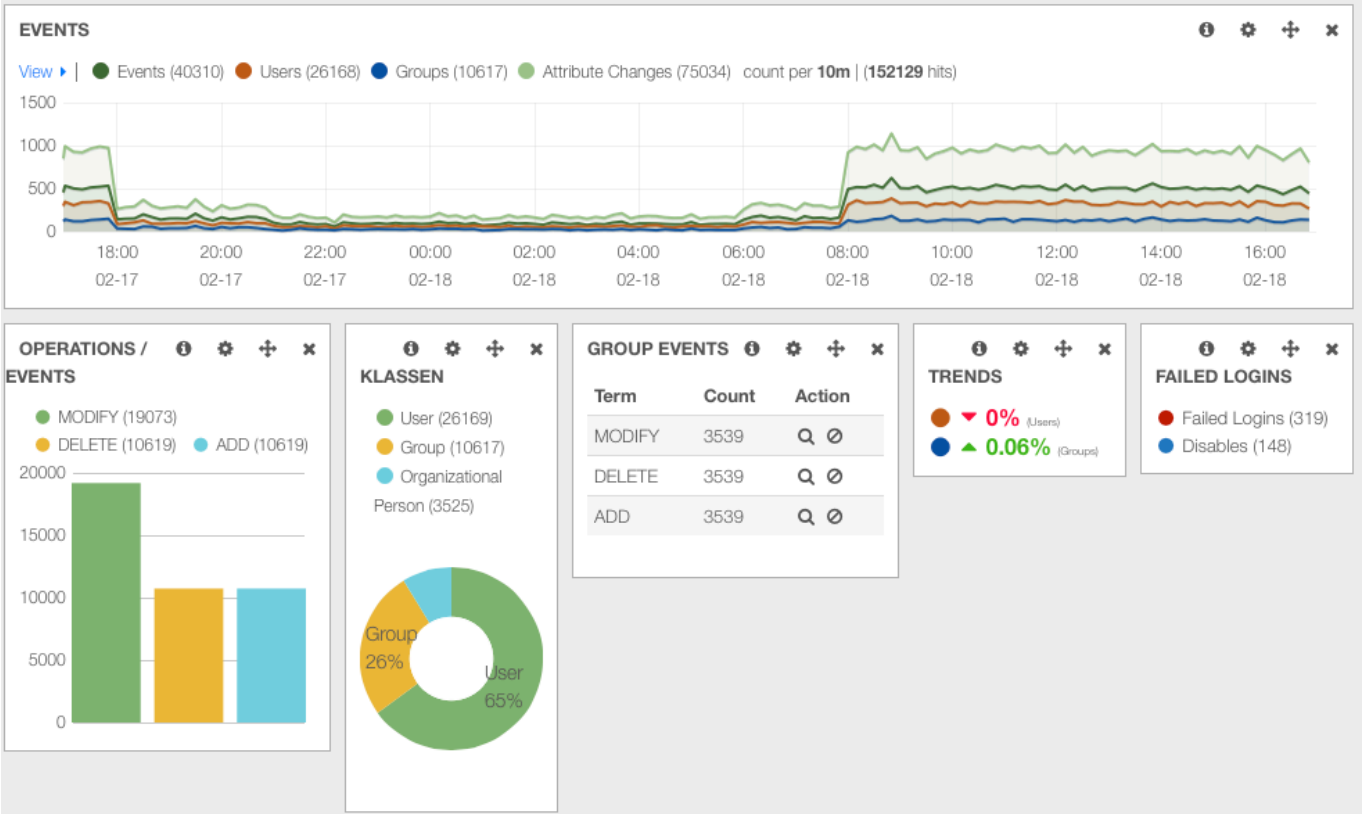
Open Horizons Magazine for OH Summit Budapest 2014
Special Edition Q2, 2014

by Andreas Fuhrmann, SKyPRO AG, Switzerland

The NetIQ Identity Manager is a very powerful Identity Management tool. It offers a lot of functionality for user provisioning, role based access control, segregation of duties, approval and recertification processes. But as it comes to audit what ever happens in your IDM system, the event and audit system (EAS), that is included in the IDM advanced edition, is not able to show me a accurate real time overview of all the events that have been processed. In addition the EAS system is not as easy to install and to configure as you might expect.

These are the reasons why we decided to develop our own IDM audit dashboard. The goal was to develop a powerful, flexible, simple to install and easy to use audit tool for building informative and meaningful dashboards and reports for audit and compliance purposes.

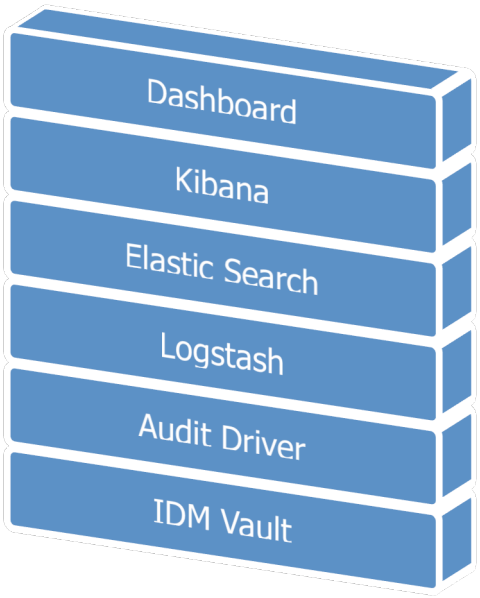
Our IDM Audit, Security and compliance dashboards deliver detailed information about all attribute values of any object in your directory at any time (present and history). We audit each event (adds, modifies, renames, moves and remove) that has taken place (see Grafic 1: audit dashboard sample) with previous and current value. And we save current object states regulary for compliance.



Grafic 1: audit dashboard sample

The components

The IDM audit dashboard consists of different components. Some are proprietary and some are open source tools. Following a list of the main components of the solution:



1. eDirectory as the IDM Data Vault
2. Audit Driver to synchronize the data
3. Logstash as data store
4. Elasticsearch as search and analytics engine
5. Kibana as the visualization dashboard
6. IDM Audit, security and report dashboards

Grafic 2: IDM audit dashboard components

All components are available for windows and linux. You can install all components on the same server or on different server. So you can install the Audit driver on one of your IDM Engine servers, elasticsearch on a second server and kibana on the third server. In case you want to make the Audit dashboard reachable from the internet you can keep the data in your internal and secure LAN and only place the kibana part on a web server in the DMZ.

eDirectory

Of course the base of everything builds eDirectory as the Identity Vault and the IDM engine. Thanks to the real time event system of eDirectory and the IDM engine we can trigger every event that takes place within eDirectory, whether it is a creation, modification, move, rename or removal of a object or attribute.

Audit Driver

We developed a very flexible driver listening to all the events on objects and attributes we want to audit in our audit database. Whenever you want to add more object classes or attributes to audit, just add them to the driver filter. No further attribute mapping is required. You do not even have to make changes to the elasticsearch database.

Logstash

Logstash helps you take logs and other time based event data from any system and store it in a single place for additional transformation and processing. Logstash parse all data sources into an easy to read JSON format. The most popular open source logging solution in the market today.

Elasticsearch

Elasticsearch (http://www.elasticsearch.org) is used as our flexible and powerful, distributed real time search and analytics engine. Architected from the ground up for use in distributed environments where reliability and scalability are must haves. Elasticsearch gives you the ability to move easily beyond simple full-text search. Through its robust set of APIs and query DSLs, plus

clients for the most popular programming languages, Elasticsearch delivers on the near limitless promises of search technology.

Elasticsearch delivers realtime data regardless of your incoming data stream. It scales horizontally out of the box. As you need more capacity, just add more nodes, and let the cluster reorganize itself to take advantage of the extra hardware. Elasticsearch clusters are resilient – they will detect and remove failed nodes, and reorganize themselves to ensure that your data is safe and accessible.

Kibana

Kibana works seamlessly with elasticsearch to visualize your data (http://www.elasticsearch.org) and offers a lot of different graphical building blocks. For the visualization no coding is required. Kibana delivers real time analyses of streaming data into the elasticsearch. Create ticker-like comparisons of queries across a time range. Compare across days or a rolling view of average change. To better understand large volumes of data, easily create bar, line and scatter plots, or pie charts and maps.

IDM Audit & Security Dashboard

We preconfigured two dashboards with the Kibana visualization components. The IDM Audit Dashboard visualizes in histograms, pie and bar charts all events of the different object classes that have been taken place within a specific period of time. It shows trends and important security information like amount of failed logins or disabled users.

The security dashboard visualizes important security information as amount of intruder locks, login intruder attempts, amount of users that have been disabled or enabled within a specific time period.

Third the report dashboard shows historic information about all object values for compliance purposes. You can schedule how often the current state of objects has to be saved to our audit system and the period we have to keep the data.

Installation

To install the IDM Audit Dashboard go to our web site http://www.skypro.ch and download the complete installation file *audit.rar*. This file contains all the needed packages. After download unpack it. You should have the following files:

- audit-driver.xml — the IDM driver to the lucene DB
- auditdriver.jar — appshim component for the IDM driver
- IDM Audit Dasboard.json — IDM Audit Dashboard example
- IDM Security Dashboard.json — IDM Security Dashboard example
- IDM Compliance Dashboard.json — IDM Compliance Dashboard example
- common-io-1.4.jar — appshim components for the IDM driver
- elasticsearch-1.0.0.tar.gz — lucene with elasticsearch
- json-simple-1.1.1.jar — appshim components for the IDM driver
- kibana-3.0.0ms5.tar.gz — kibana visualization components
- template.json — json template for the driver appshim

Install elasticsearch and logstash

The first step is to install elasticsearch and logstash. Unpack the *elasticsearch-1.0.0.tar.gz* file. Tha package contains both components. The content of the file will be unpacked in the directory *elasticsearch-1.0.0*. Copy the whole unpacked directory to your standard program directory. On SUSE linux we propose to copy it to */opt/elasticsearch-1.0.0*. To start the elasticsearch engine type

- on linux: bin/elasticsearch
- on windows: bin/elasticsearch.bat

If no java is installed download and install the latest java. If there is no java path configured in your Linux environment define the JAVA_HOME path like "*export JAVA_HOME=/jre"*. If elasticsearch won't start make sure you have installed the latest jre version 7.

Install Kibana

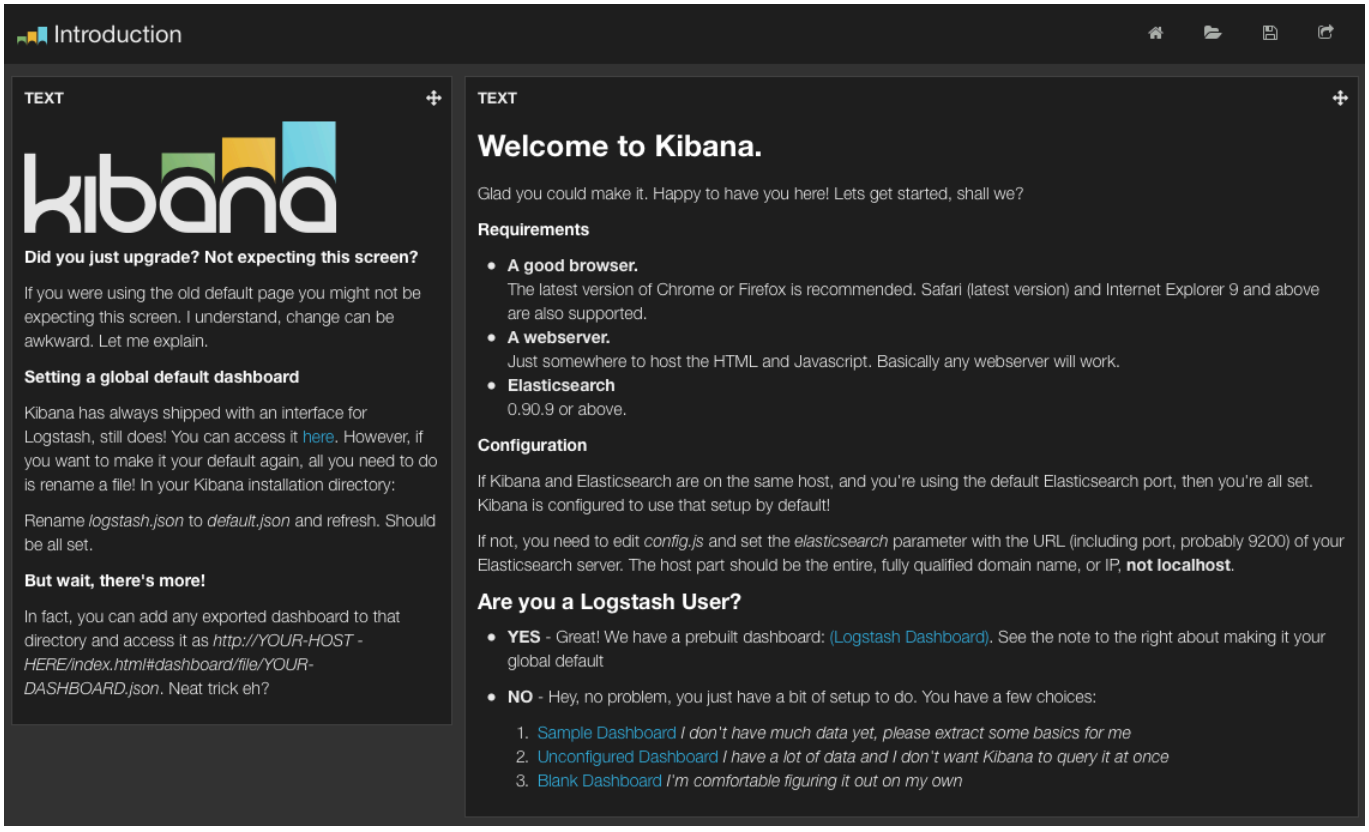
The second step is the installation of the kibana component. Unpack the kibana-latest.zip. Copy the unpacked directory to your web server folder. On SUSE linux we propose */srv/www/htdocs/kibana*. Open the *config.js* file in the kibana directory and set the elasticsearch parameter to the fully qualified hostname of your elasticsearch server like

elasticsearch: "http://elasticsearch.mycompany.com:9200

To check whether your kibana is running open your web browser and enter the URL

http://elasticsearch.mycompany.com/kibana

The default kibana welcome page should open.



Grafic 3: Kibana default welcome page

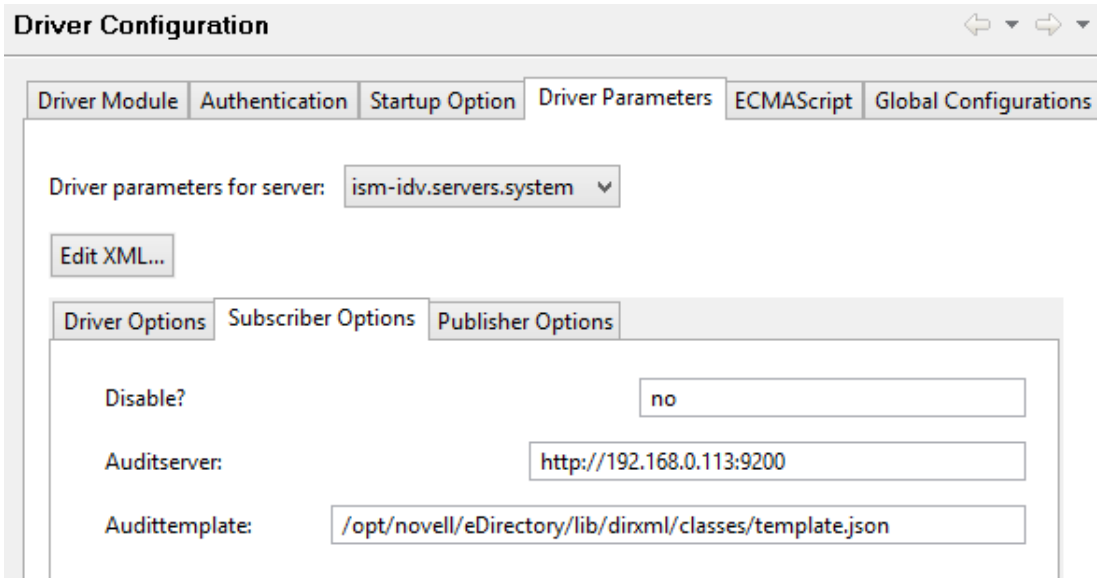
Build the Audit Driver

Before we start to create the audit driver with designer we have to copy the needed files for the driver appshim. Copy following files

- auditdriver.jar
- common-io-1.4.jar
- json-simple-1.1.1.jar
- template.json

to the dirxml class directory. On SUSE linux the default path is /opt/novell/eDirectory/lib/dirxml/classes. Look for your dirxml class directory *eDirectory/lib/dirxml/classes* on your server.

To build the driver open designer. Create a new driver by import the driver file *audit-driver.xml*. Right click the driver and open the driver properties. Go to the *Driver Configuration* and open the *Driver Parameters* Tab. Klick the *Subscriber Options* tab. Provide the correct parameters of your elasticsearch server and the folder and filename where you have placed the json template.



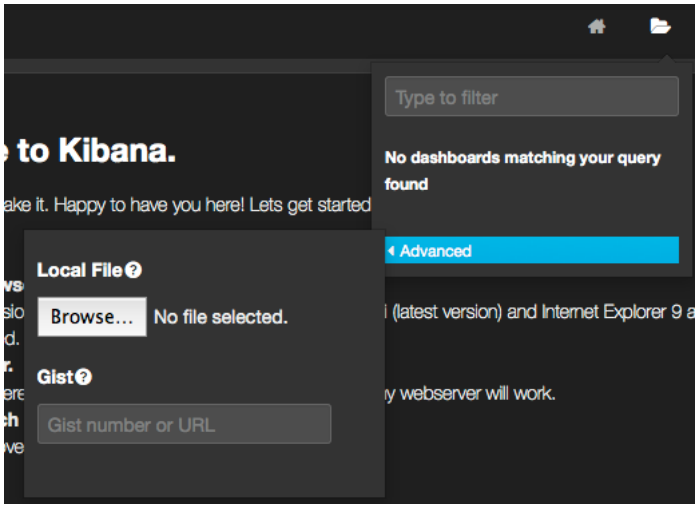
Grafic 4: audit driver parameters

Deploy the driver to your IDM server. If you want to monitor more or less objects or attributes just open the driver filter and change the filter accordingly.

To test the driver start the driver and change the description attribute of a user. The modify event should be successfully synchronized to the elasticsearch database.

Install the sample dashboards

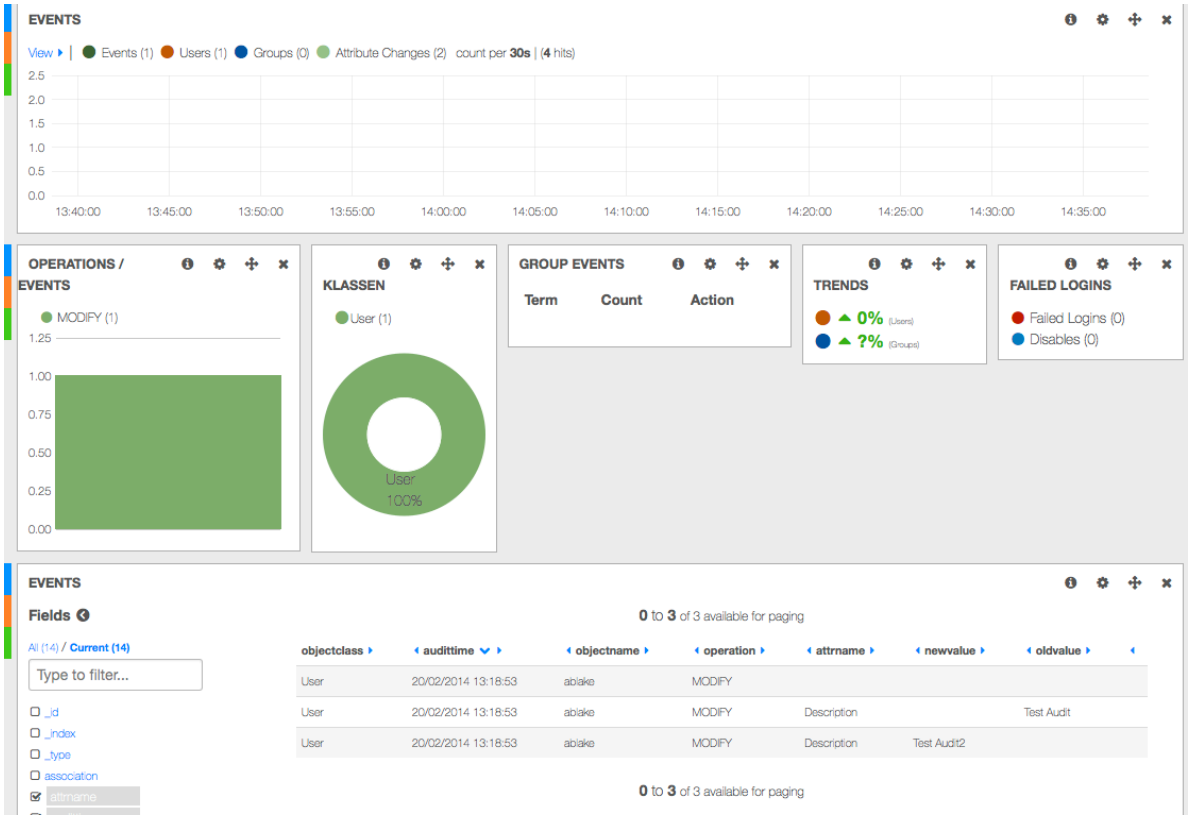
Now you're almost ready to go. For your convenience we provided two dashboards files. The IDM Audit Dashboard example file *IDM Audit Dashboard.json* and the Security Dashboard example file *IDM Security Dashboard.json*. Open the kibana home page, click the folder icon in the upper right corner, go to *advanced* and click the *Browse* button under local files and select the provided dashboard example files to load our IDM Audit and Security Dashboard examples (see Grafic 5: load the IDM Audit Dashboard example). Click the *save* button, also located in the upper right corner, to save the dashboard in your kibana environment. Now you can select this dashboard anytime with the folder button.



Grafic 5: load the IDM Audit Dashboard example

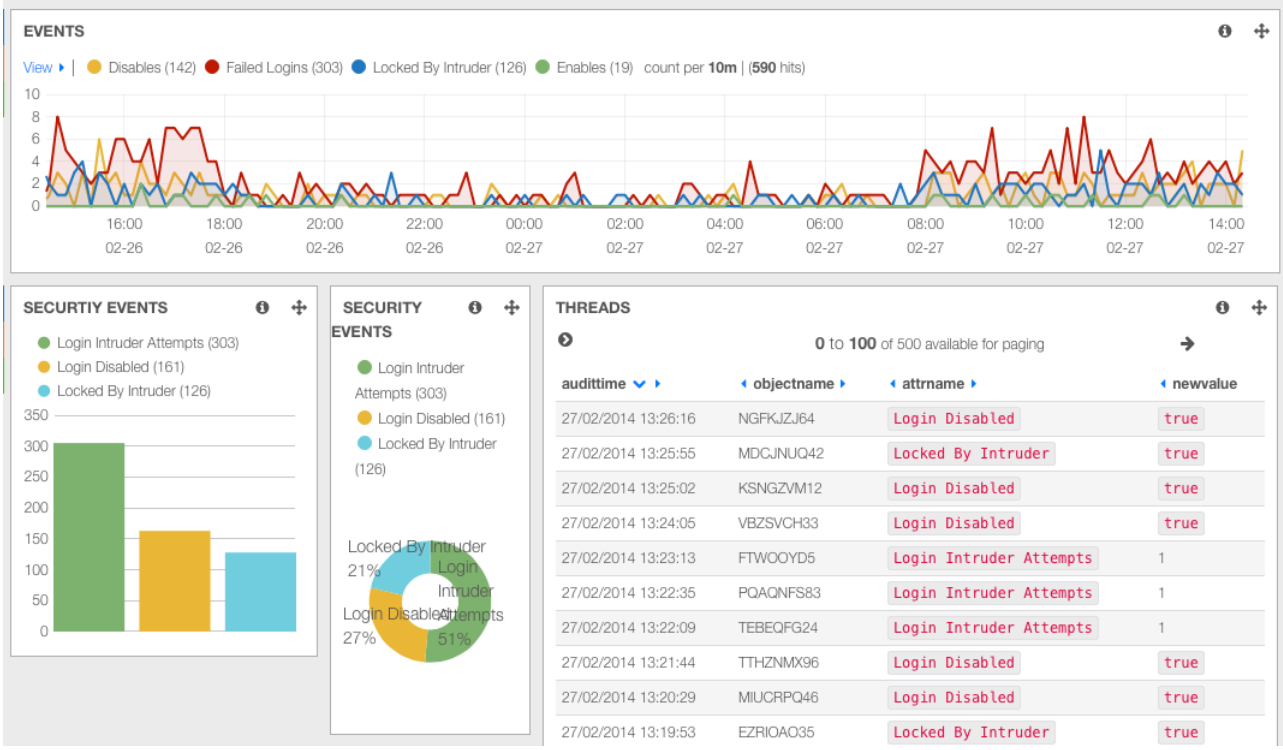
The IDM Audit Dashboard shows a visualized history of events on objetcs with histograms and charts. You see how many events have been processed by your IDM engine and how many different object classes have been involved. You see trends and amount of failed logins and users that have been disabled.

If you have executed the change of a user description attribute you should see this modify event already in your dashboard (see Grafic 6: IDM-Audit Dashboard example). In the *Operation / Events* graphic you see one modify event. In the *Classes* graphic you see one user object so far was audited. In *Events* table at the bottom you see the basic data. You see three entries of object class user with objectname "ablake". The first entry is the modification event. The second entry shows the old value "Test Audit" of the modified attribute *description* and the third entry shows the new value "TestAudit2".



Grafic 6: IDM-Audit Dashboard example

Now load the IDM Security Dashboard. This dashboard shows important security information. You see all failed logins, user that have been locked by intruder detection, intruder attempts, users that have been disabled or enabled.



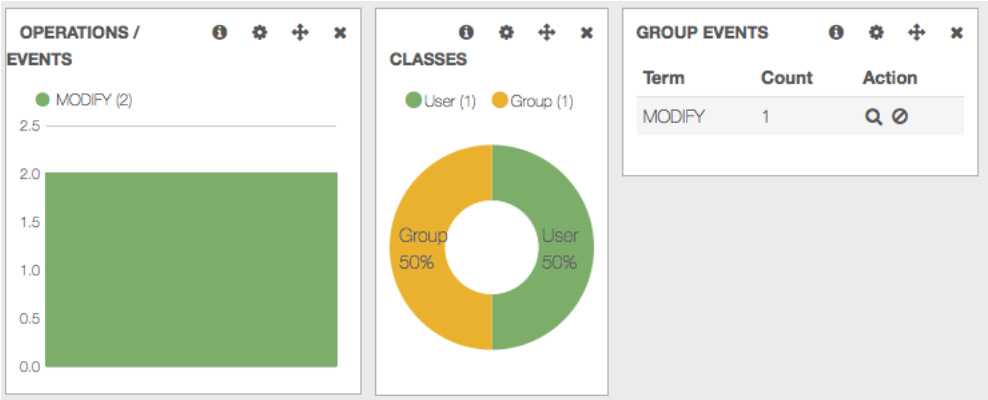
Grafic 7: IDM Security Dashboard

The compliance dashboard shows the data history of objects. Objects states are saved to the Audit tool on a regularly base. 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. The compliance team will be pleased.

Grafic 8: IDM Compliance Dashboard

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 see now one modification.



Grafic 9: 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.

Grafic 10: IDM Audit Dashboard Event Histogram

Understand the IDM Audit Dashboard

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

1. query
2. filter
3. row
4. 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 and users that have been disabled.

Filter

With filters you filter the data you have selected with your query. E.g. you only want to have user objects or objects with a specific objectname. Most you will use the filter to narrow the time frame of events you want to see like only changes that have taken place the last 24 hours.

Our standard filter selects only events of type "audit". For reporting purposes we have additional type like "report" that gathers 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 ar any time to the position you want to have them.

Panel

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

Work with Panels

Change an existing Panel

We have a panel called *GROUP EVENTS*. Wouldn't it be nice to show both user and group events? Click the configure icon in the *GROUP EVENTS* panel. In the *General* tab change the title to "*Events / Class"*. In the *Panel* tab change the *Field* Parameter from *operation* to *objectclass*. Now not the operations like *Modify, Add* etc. are counted but different object classes are counted. In the *view Options* change the style from *table* to *bar*. Activate the *Queries* tab and deactivate *Users* and active *Events.* Save the panel settings. The graphic has changef to a pie chart showing the events that occurred per class in the given time frame.

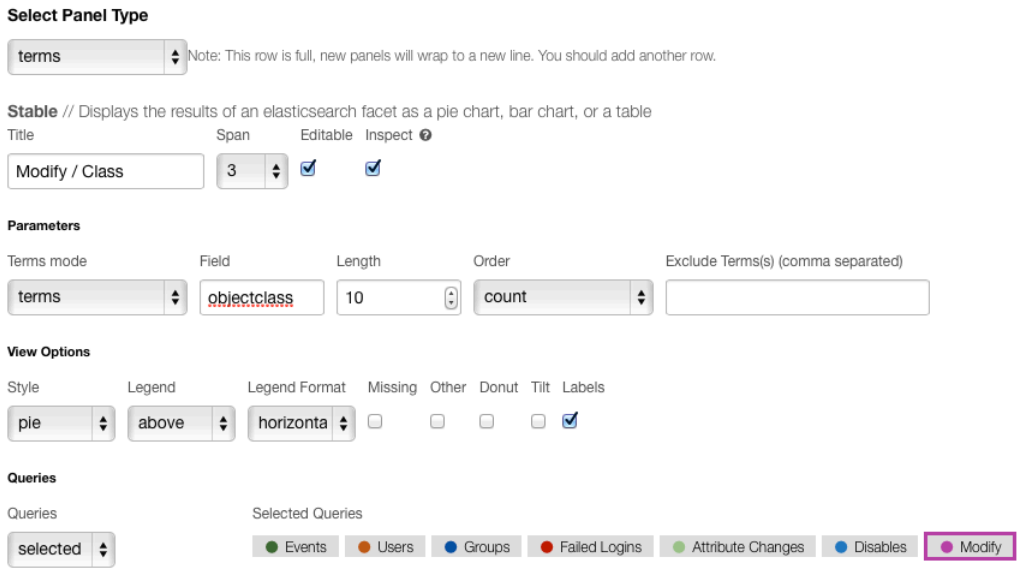
Grafic 11: Graphic for events per class

Add a new Panel

Imagine we want to have a pie chart showing us all modify events per class. First we add a new query for all modify events. In the *QUERY* row click the "+" sign at the right. Enter the following query string `*operation:"MODIFY" AND event:"true"*`. This selects all events that are not the actual attribute changes but only the modify event. Click the colored dot on the left, as *Legend value* enter *"Modify"* and pin the query.

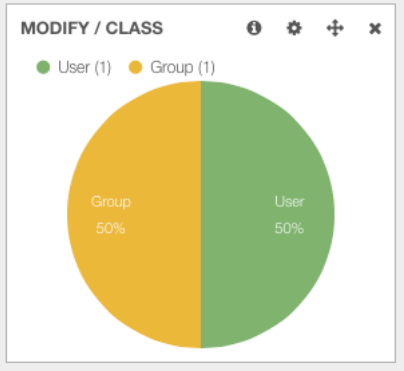
Grafic 12: define new query

You should see a new pinned query. Now go to the row with the *OPERATIONS / EVENTS* panel on the left and click the green „+" symbol to add a panel. As panel type select *terms*. As *title* type *Modify / Class*. In the *Parameters* type *objectclass* in the *Field* value. Uncheck *Missing* and *Other* in the *View Options* and select *pie* as the graphic view. In the *Queries* dropdown chose *selected* and activate the pinned *Modify* query. Save the panel.



Grafic 13: define a new panel

Bravo you successfully added a new panel showing a bar with the amounts of modifies per class that looks like this.



Grafic 14: new MODIFY / CLASS dashboard panel

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

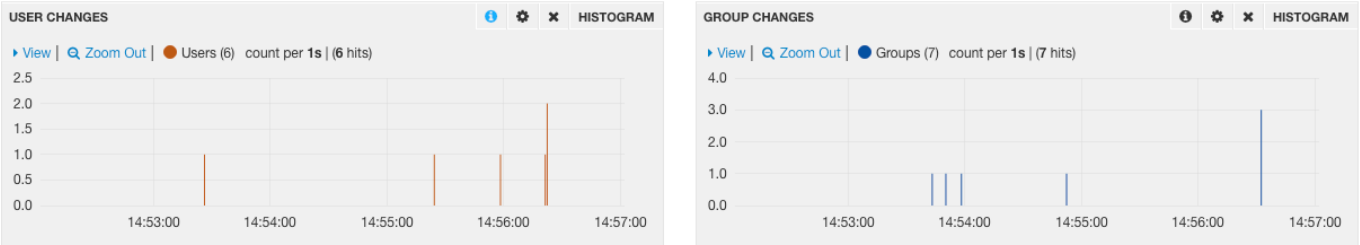
Create new row

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. First go to the bottom of the dashboard on click *ADD A ROW*. In the title field enter *"User & Group Statistics"* and press *Create Row*. Move the new row above the *Events* row in the dashboard settings.

Now you have an empty row where we can add new panels. Press *"Add panel to empty row"*. Select *"histogram"* as panel type. Enter *"User Changes"* in the field *Title* and change the *Time Field* from *"@timestamp"* to *"_timestamp"*. Change the span value to *"6"*. 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.

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



Grafic 15: new row with two Histograms

Conclusion

With our IDM Audit driver and the open source components elasticsearch and kibana we're able to create powerful IDM Audit 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. Kibana is a very powerful and easy to use visualization component offering a lot of graphical building blocks. In the upcoming version of our IDM Audit Dashboard we will even log current states of object on a scheduled base. So we know the values of all attributes at any time in the history for compliance purposes.