1. Установка и настройка elasticsearch-curator

* cd /etc/yum.repos.d/
* sudo vim curator.repo

*[curator-5]*

*name=CentOS/RHEL 7 repository for Elasticsearch Curator 5.x packages*

*baseurl=https://packages.elastic.co/curator/5/centos/7*

*gpgcheck=1*

*gpgkey=https://packages.elastic.co/GPG-KEY-elasticsearch*

*enabled=1*

* sudo yum install elasticsearch-curator
* sudo mkdir /var/es-storage
* sudo chown –R elasticsearch:elasticsearch /var/es-storage
* update /etc/elasticsearch/elasticsearch.yml

elasticsearch.yml.template

* systemctl restart elasticsearch
* curl –user elastic:123321 –XPUT 'localhost:9200/\_snapshot/important\_storage' –H 'Content-Type: application/json' –d ' {"important\_storage":{"type":"fs","settings":{"compress":"true","location":"/var/es-storage/important\_storage"}}}'
* sudo mkdir /etc/es-curator
* create /etc/es-curator/config.yml

config.yml.template

* create /etc/es-curator/action\_file.yml

action\_file.yml.template

* sudo chown –R elasticsearch:elasticsearch /etc/es-curator
* sudo mkdir /var/log/es-curator
* sudo chown –R elasticsearch:elasticsearch /var/log/es-curator
* create /etc/cron.d/curator

curator.template

Пояснение: При данной настройке elasticsearch-curator каждый месяц будет выполнять следующие действия

* Создавать резервную копию индексов возрастом более 1 месяца, начинающихся с префикса u-i-, и сохранять ее в репозитории important\_storage. Место хранения резпозитория можно изменить, по умолчанию это /var/es-storage;
* удалять индексы возрастом более 3 месяцев, начинающиеся с префикса u-;
* удалять резервные копии возрастом более 1 года, начинающиеся с префикса important-.

Данное поведение можно изменить в любой момент с помощью модификации конфигурационных файлов action\_file.yml и curator. Для лучшего понимая конфигурационных файлов рекомендуется обратиться к документации:

* <https://www.elastic.co/guide/en/elasticsearch/client/curator/5.4/index.html>
* <https://www.elastic.co/guide/en/elasticsearch/reference/current/modules-snapshots.html>
* <https://help.ubuntu.com/community/CronHowto>

1. Создание резервных копий вручную

* Для создания резервной копий в формате csv, необходим установленный и настроенный x-pack (см. secure.docx). Для созданий резервной копии необходимо в интерфейсе kibana перейти в раздел Discover выбрать вкладку Reporting и нажать на кнопку Generate CSV (Рисунок 1).

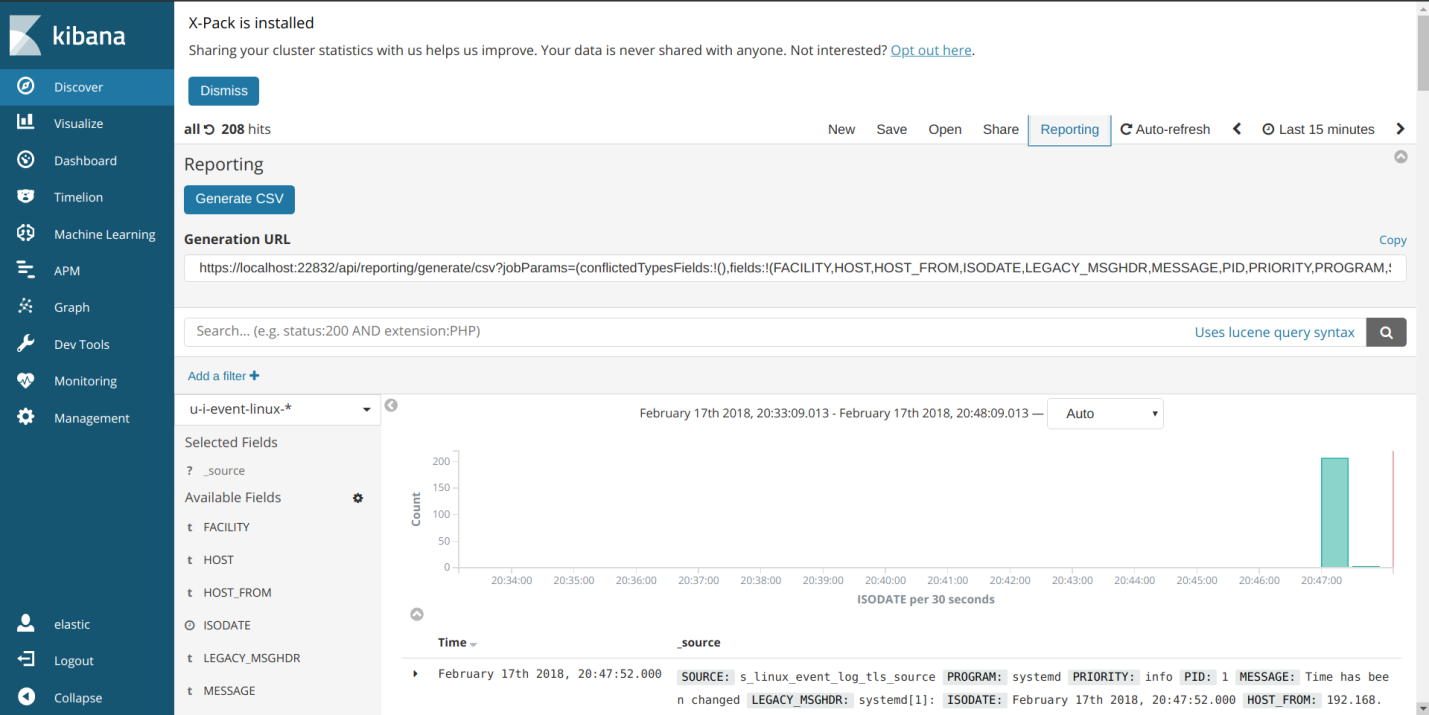


Рисунок 1 – CSV

* Создание резервной копии в формате json. Для создания резервной копии необходимо в интерфейсе kibana перейти в раздел Management выбрать вкладку SavedObjects, указать необходимые элементы и нажать на кнопку Export (Рисунок 2).

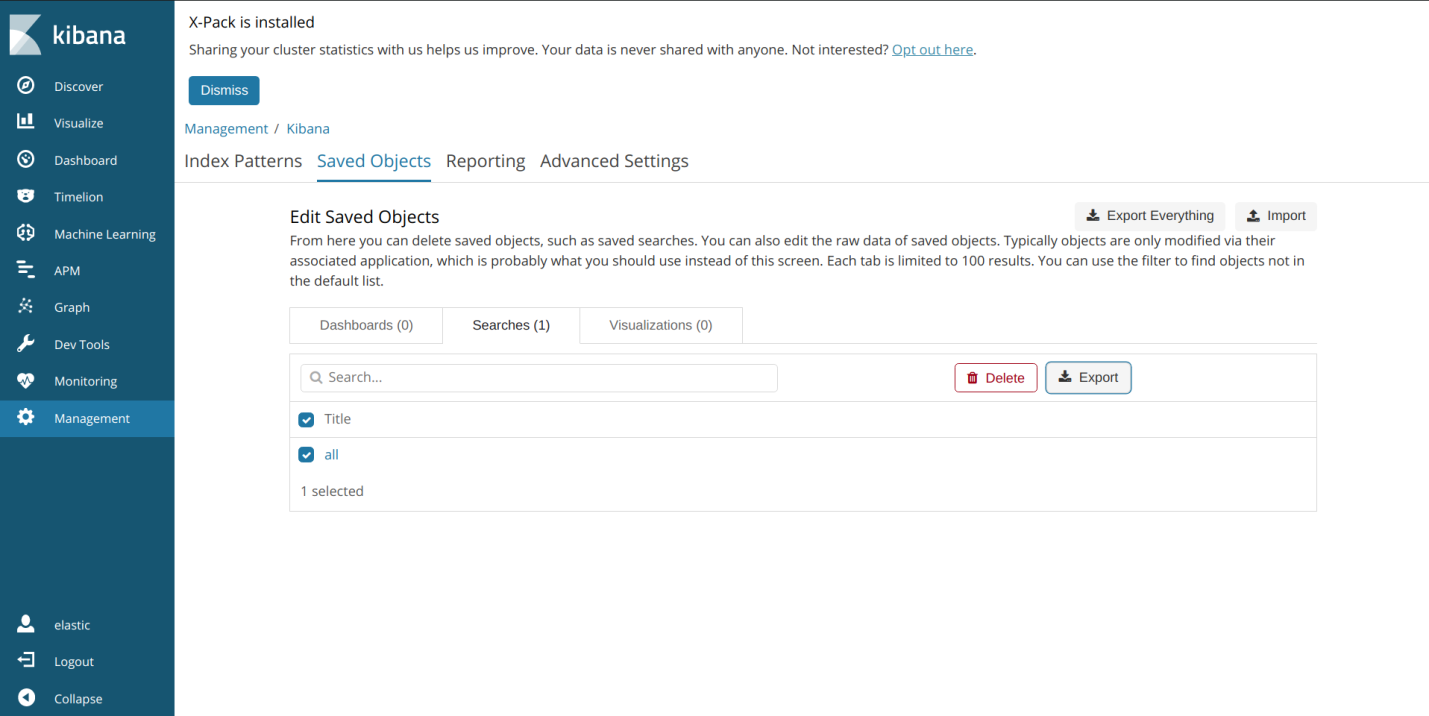


Рисунок 2 – JSON

* Создание shapshot копии вручную. Удобнее всего для этой задачи использовать curator\_cli:
* <https://www.elastic.co/guide/en/elasticsearch/client/curator/5.4/singleton-cli.html>

или использовать curl для обращения к REST API предоставляемым elasticsearch:

* <https://www.elastic.co/guide/en/elasticsearch/client/curator/5.4/singleton-cli.html>