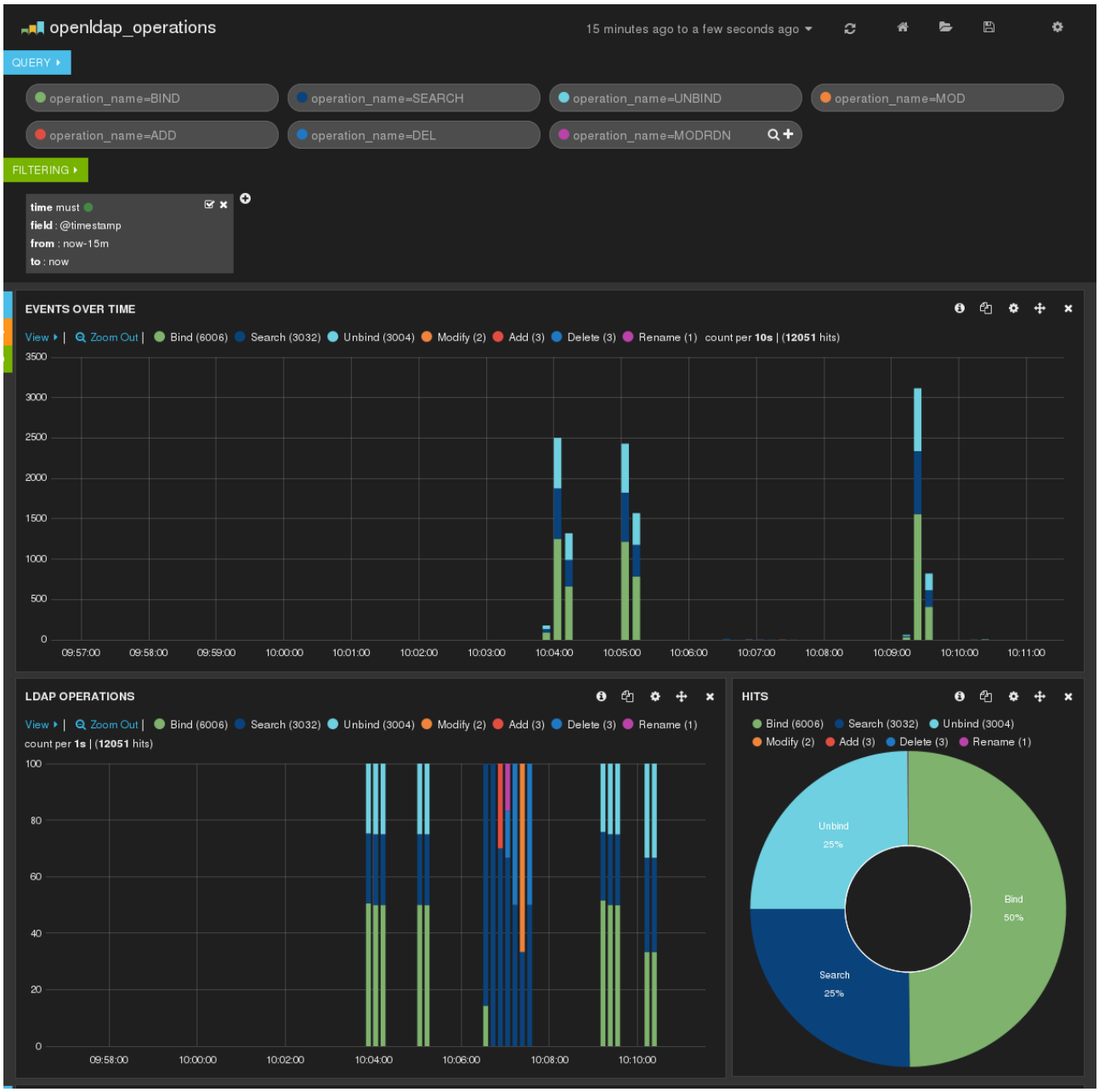
Parse OpenLDAP logs with ELK

ELK (Elasticsearch Logstash Kibana) is a software suite that allows to collect, analyze and visualize data.

I uses these tools to parse OpenLDAP logs and obtain charts and metrics on directory utilization, for example the repartition of LDAP operations, error codes, DN used to authentication, base search, etc. This analysis can be done dynamically by selecting a time frame, an operation kind, …



The result of my work is freely available here: https://github.com/coudot/openldap-elk

The presentation will first introduce the ELK stack, then the log format of OpenLDAP to finish by a demonstration of dynamic log analysis.

Speaker

Clément OUDOT works since 2003 on LDAP and Identity Management free softwares.

He is the leader of LemonLDAP::NG project (http://www.lemonldap-ng.org) and LDAP Tool Box project (http://ltb-project.org). He is also implied in LDAP Synchronization Connector (http://lsc-project.org).

Clément presented FederID at LDAPCon 2007, LemonLDAP::NG at LDAPCon 2011, LSC and OpenLDAP Password Policy at LDAPCon 2013.