Proactive management of your federation

Authors and Presenter: Yasvanth Babu
Affiliation: HEAnet CLG, Dublin, Ireland.
Keywords: Log Analysis; Data; ELK; Edugate; Shibboleth;

Yasvanth Babu is a middleware system administrator in HEAnet CLG. His responsibilities in the team is to deploy/manage/support IDP and SP for Ireland's higher education institutions.

Presentation Description:

Log analysis is used to process computer-generated data that helps an organization to pin point different kinds of problems and to mitigate them. For some organizations, log analysis is a part of regulation for managing their infrastructure such as security and audit compliance, incident response, forensics and so on. The data for log analysis is an extracted from many different sources such as operating system, application and networking devices which is available in raw format.

HEAnet has enabled routine log analysis for its federation service 'Edugate'. Edugate is our Single-Sign-On service for Irish Higher Education, which eliminates the use of multiple usernames and passwords for web services. These web service ranges from online Library services to virtual earning environments. Edugate is adopted by 45 HEAnet client institutions and provides access to 170+ services, including 310 private services. Edugate also partners with eduGAIN supported by 2140 Research & Education institutions.

Now the question can arise "How does log analysis on federated events help us to be more productive?" The answer wouldn't be just simply yes, because the expected result is to generate yearly graphs on number of logins via Edugate which helps the Edugate member clients/institutions to track the usage of Edugate, but also addresses other uses for librarians and IT managers which was not expected.

Let us categorise the problems addressed for Librarians and IT Managers or IAM system admins.

1. Institutions pay for access to journals and other services. Are they being used?

In other words, is Edugate is used? Librarians can track the usage the of Edugate to see whether the use of a service is increasing or decreasing. Addressing this problem will benefit the Institution to check whether the subscription provides value for money.(Here the subscription service also refers to HEAnet Hosted or managed Identity Provider.)

Secondly, Tracking the user accessing which service can also benefit the Institution allowing it to cancel poor value subscriptions, if the service is not popular among the student because the institution pays flat fee rate to the service(login based on number students or staff registered not by number of logins to the service). Below we could see a cost per login is calculated by the librarians.

Total No. Of user = 1000
Cost for service A in 2016 = € 5000/yr(€ 5/user)
Cost for service B in 2016 = € 2500/yr(€2.50/user)

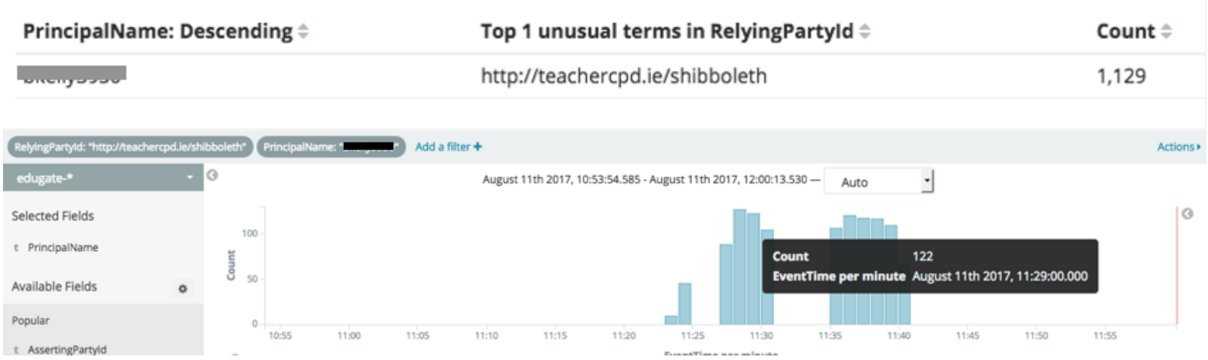
In 2016, 600 unique users accessed to service A and 200 unique users accessed to service B. In following year there is €1000 increment in subscription fee to the service B which rounds of €3500 and there is 10% increase in unique user accessed for both the service. We could see that there is the price of the service A is 125% higher than the service B, whereas unique users access is 300% higher to Service A when compared with service B. From the above example we could see the service A is popular among the student and benefits the institution for the fee paid to the service provider. In upcoming year the institution can use the price to other services instead of continuing subscription to service B.

1.b Tracking and Disabling service from federation.

In above scenario, the low number activity of service is captured to benefit the Institution Librarians, Whereas for IT admins can perform the same analysis to disable the services in the federation which are not utilized by the institution users. By disabling/removing the service can reduce and total size of the metadata to speed up the startup time of IDP and SP software.

2. Institutions have users whose accounts may be compromised

There are technical benefits for IT managers or Identity and Access Management (IAM) system administrators too. IT teams in an organization can encounter cases where a user account is compromised due to weak password or sharing of user credentials. This can be identified by tracking the number of user login(X) in a given time(Y) period or there a change in geo-location. For example If user A access 10 service in 15 sec can be considered suspicious activity, which can then trigger further investigation on the user activity. This can be either compromised accounts or browser looping which is rapid cycle of redirection from SP to IDP. From the below figure we can see that user has logged in to a service for 1129 times in 5 min which not a normal activity. Such activities are tracked and suitable web filtering can be placed to mitigate in future.



PrincipalName: Descending	Top 1 unusual terms in RelyingPartyId	Count
[redacted]	http://teachercpd.ie/shibboleth	1,129

RelyingPartyId: "http://teachercpd.ie/shibboleth" PrincipalName: "[redacted]" Add a filter +

August 11th 2017, 10:53:54.585 - August 11th 2017, 12:00:13.530 — Auto

Count 122
EventTime per minute August 11th 2017, 11:29:00.000

3. Are an institution’s users trying to access resources that aren’t subscribed to?

The concept of federated access or SSO is by authenticating the user in campus or organization IdP (Identity Provider) and authorized by SP (Service Provider) with the user attributes released/exchanged from an IdP to the SP, if the required attributes are not released or recognized by service then access for an user is not granted. A comparison of attributes required with attributes released will help identify accesses that were unauthorized when it possibly should have been authorized. This is particularly useful for SP’s that may have a low volume of logins, but may provide a benefit of high value to the organization.

You may think the effort to do this should be so challenging and require a significant amount of data for performing this task. That is not the case, the log analysis process for Shibboleth based IdP’s is performed on a single file (idp-audit.log) which records the transactions between Shibboleth IdP and SP. Log analysis when coupled with alerting, can lead to proactive management of a federation in real-time, identifying problems that often go unreported for months.

Not only the above given problems where addressed using IDP audit events, furthermore such as student analytics are yet to be discussed in TNC18. I hope that sharing my idea with other fellow NRENs to solve the problems for their clients, not just technical problems.