

Paper BI-010

Making Sense of SAS® Enterprise Business Intelligence (EBI) Log Configuration Files to Gain Valuable Insight on User Behavior

Piyush Patel, Acxiom Corporation, Conway, AR

Sandeep Kharidhi, Acxiom Corporation, Conway, AR

ABSTRACT

This paper focuses on the benefits of monitoring user log-in activity. Without reliable logs it can be very difficult to keep track of usage. From a security standpoint, logs are one of the most important assets contained on the server. After all, without logs, how will an administrator know who is accessing the system and what information is being accessed from the server? By analyzing the log-in information, one can determine the amount of time spent by users accessing the portal, creating reports or performing other analyses.

SAS® EBI includes some very powerful features to track portal usage, yet not always are these tools enabled. This paper describes how to modify the log-in configuration files for Portal Web Applications and how to parse through the log files to monitor and track users' activity. This paper will also provide a step-by-step guide through the use of Information Delivery Portal or Web Report Studio to analyze the portal log usage.

KEYWORDS

EBI, Business Intelligence, OLAP, Portal

INTRODUCTION

SAS® EBI applications generate various types of log files that can be used for tracking portal usage and gain insight regarding user behavior. This paper discusses the characteristics of the Portal Usage Log and the OLAP Server Log and provides step-by-step guides to use these logs. These logs are valuable in managing portal access and usage so that the server administrators can make intelligent business decisions.

KEY AREAS OF FOCUS

- Monitor user logon activity to gain insight into usage trends
- Compute portal and cube usage
- Analyze server usage

PORTAL USAGE LOG

SETTING UP THE PORTAL LOG FILE

Portal logs are also called "front-end logs" because they store information when a user logs into a system and when they logout. To start collecting information about the users' log-in and logout attempts, a configuration file needs to be modified on the middle tier server (also known as web server).

The name of the configuration file is **logging_config_idp.xml**. The default location of this file is **/web/deployments/portal**. However, the default location can be changed to fit individual preferences.

To capture successes and failures of logging onto the portal, the following code must be added to the above mentioned XML file.

```
<LoggingContext name="ApplicationMonitor.UserService"
    priority="DEBUG"
    chained="false">
    <OutputRef outputID="IDP_FILE_3"/>
</LoggingContext>
<LoggingContext name="com.SAS®.portal.delegates.authentication.LogoffDelegate"
    priority="DEBUG"
    chained="false">
    <OutputRef outputID="IDP_FILE_3"/>
</LoggingContext>
```

```
<Output id="IDP_FILE_3"
  Type = "File"
  layoutPattern = "%d{ISO8601} [%-5p] %-20.20u %-40.40c - %m%n">
  <param name = "File"
    Value = "C:/SAS®/cfg/Levl/web/Deployments/Portal/log/portal_usage.log" />
</Output>
```

In addition to the above modification, a few additional changes can be made to the configuration files to include information related to:

- The types of messages stored
- Log type, file name and location
- Log message format
- Portal timeout interval

The information for making these changes can be found in the SAS® Web Infrastructure Kit: Administrator's Guide. Once the XML file has been modified, the middle tier server (also referred to as "servlet container") needs to be restarted before this change can take effect.

INFORMATION DERIVED FROM THE PORTAL LOG FILE

The sample portal usage log shown below demonstrates that User1 logged on to the server at 8:03 AM on June 16, 2008 and logged out at 8:14 AM. Thus, this person used this system for about 11 minutes in the first instance. The same user then logged back onto the server only for about four minutes at 8:32 AM on the same day.

```
2008-06-16 08:03:05,438 [DEBUG] ApplicationMonitor.UserService - type="login" status="success" uid="user1" domain="web" message=""
2008-06-16 08:14:10,397 [INFO ] .delegates.authentication.LogoffDelegate - Logging off(User Name): invalidateSession: true
2008-06-16 08:32:24,380 [DEBUG] ApplicationMonitor.UserService - type="login" status="success" uid="user1" domain="web" message=""
2008-06-16 08:36:26,613 [INFO ] .delegates.authentication.LogoffDelegate - Logging off(User Name): invalidateSession: true
```

Figure 1. Sample Portal Usage Log

The data on this log file can be further mined to gather more information regarding the logon attempts by users. However, the log file in its raw form is difficult to analyze. So the file needs to be converted into a SAS® dataset for easier manipulation and analysis.

One issue to be aware of with the portal log is that the logout activity is not always captured. This happens when users do not logout but close their browser or move to another web page. In such cases, the log out time has to be inferred by setting a default time (as for example 30 or 60 minutes). For each log entry, information can be retained regarding log-in or logout date/time, type, status, uid, message attributes, etc. After successfully converting the file in SAS®, the administrator can calculate the time spent by a user by subtracting the logon time from the logout time. Also, one record per log-in/logout event can be retained as well as deriving other variables, such as number of attempts, for reporting purposes. These entries can also be organized by user types and user groups.

OLAP SERVER LOG

SETTING UP THE OLAP LOG FILE

On the OLAP server, a new log file is automatically created every day to collect information related to the usage of the OLAP server. While the Portal Usage log tracks when a user logged in or out of the server, the OLAP server log tracks the actual time spent by the user on reading the raw data or running reports from the cubes on the OLAP server.

The log file is located on <configdir>\Levl\SAS®Main\OLAPServer\logs. The default format of the name of the log file is **OLAPServer_YYYY.MM.DD.log** (for example, OLAPServer_2008.06.16.log).

INFORMATION DERIVED FROM THE OLAP LOG FILE

The sample OLAP log shown below demonstrates that User1 started using the cube at 8:07 AM on June 16, 2008 and logged out at 8:10 AM. Thus, this person used this cube accessing information for about 3 minutes in the first instance.

```

20080616:08.07.12.45: 00102450: New client connection (499) accepted from server port 5451 for user user1.
Encryption level is Credentials using encryption algorithm SASProprietary. Peer IP address and port are 166.166.166.1234.
20080616:08.10.29.16: 00102605: Client connection (499) closed.
20080616:08.34.31.58: 00102606: New client connection (501) accepted from server port 5451 for user user1.
Encryption level is Credentials using encryption algorithm SASProprietary. Peer IP address and port are 166.166.166.6789.
20080616:08.34.48.14: 00102712: Client connection (501) closed.

```

Figure 2. Sample OLAP Server Log

Compared to the portal usage log, data contained within the OLAP server log file is quite simple and does not need much manipulation to derive actual time spent by the user. Every entry in this file includes a unique ID which can be tied back to when a particular user started using the cube. From this file, the administrator can calculate the actual time spent running reports for each user.

DASHBOARD REPORTS

Using both the log files, one can create dashboard reports that can be used for administrative purposes. These reports can highlight major trends in user activities. A sample dashboard report is provided below:

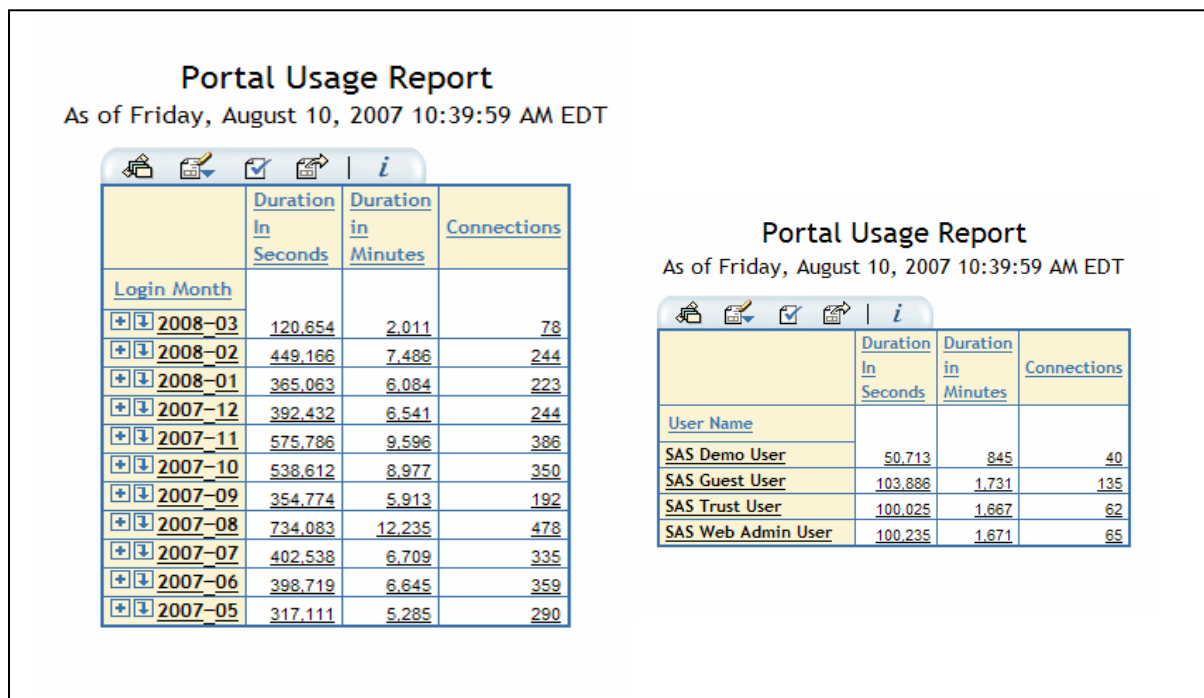


Figure 3. Sample Dashboard Reports (Actual user data not shown for security reasons)

The vital information contained in these log files can be used in various ways. Dashboard reports have successfully been used for the following purposes:

- Information security audits – audit when unauthorized users attempt to access the system.
- Enhanced cube design – improve the cube design by analyzing what users have accessed consistently.
- Introduction of aggregation to improve performance – determine the patterns that users normally aggregate reports to modify the cube to run reports faster.
- User activity monitoring – monitor the frequency of user cube access and whether certain users should have continued access based on usage.
- Justification of user change requests – monitor user requests to allocate resources to resolve the most commonly faced user issues.

ADDITIONAL REPORT SAMPLES

The data can be used to generate additional charts as needed. Two samples are shown in Figure 4. The chart on the left shows average time users spent in minutes each time they logon on to the portal. The graph on the right shows hours of peak and off peak activity on a given days.

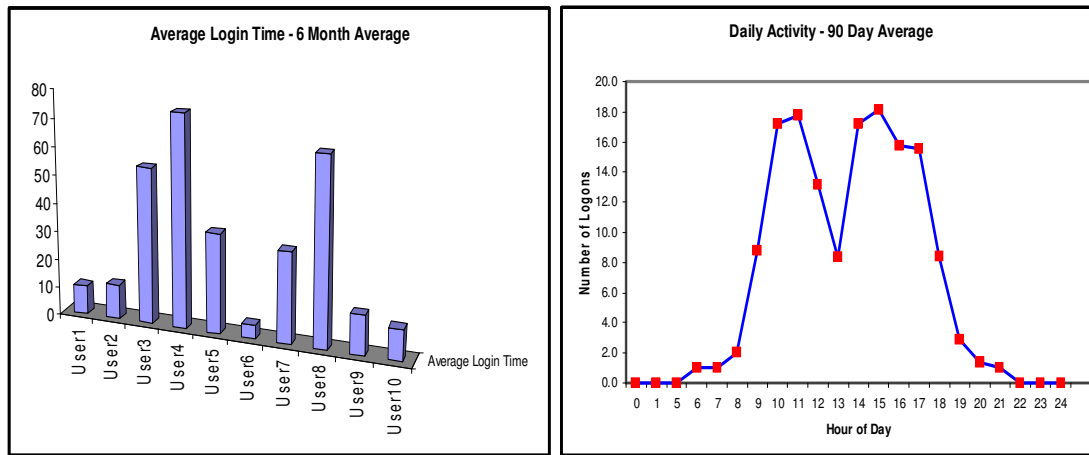


Figure 4. Sample Trend Reports

CONCLUSIONS

Log files can provide critical user information for any application. By making simple changes to the configuration file within the SAS® EBI application, organizations can collect important data for tracking purposes. Once the data is gathered, valuable insight can be gained on user activity in support of critical business decisions. The SAS® EBI log files are easy to setup and multiple log files can be aggregated to create dashboard reports. Considering the benefit and knowledge that can be collected from these log files, creating the datasets, dashboards and reports is a small investment when compared to the expected return.

REFERENCES

SAS® Web Infrastructure Kit: Administrator's Guide

CONTACT INFORMATION

Your comments and questions are valued and encouraged. Contact the author:

Name: Piyush Patel
Enterprise: Acxiom Corporation
Address: 301 E. Dave Ward Drive
City, State ZIP: Conway, AR 72032
Work Phone: 770-619-1933
E-mail: Piyush.Patel@Acxiom.com
Web: www.acxiom.com

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration. Other brand and product names are trademarks of their respective companies.