Process mining of events log from Windows

Radim Dolak, Milena Janakova, Josef Botlik

Silesian University in Opava, School of Business Administration in Karvina,
Department of Informatics and Mathematics, Karvina, Czech Republic
{dolak,mija,botlik}@opf.slu.cz

Abstract. We can use process mining also for analyzing events log from windows operating systems. The event is characterized by Microsoft as a record of a computer's alerts and notifications. Every recorded event has any significant occurrence in the system or in a program that requires being notified. Process mining should be used for troubleshooting of some windows system errors that are stored in the mentioned events log. The case study deals with using Disco software tool for process mining of events log from windows 10 operating system. There will be mentioned some steps of this case study such as acquisition, preparing, importing and process mining of data from Windows 10 events log.

Keywords: process mining, events log, operating system, windows

Introduction

There are many processes performed by windows operation system that store the information about events in the log files. Basic process mining techniques are used for extracting event logs from data sources such as information systems databases, transaction logs, web pages, excel files, results of information process audits etc. We will discuss the issue of analyzing event logs from Windows system.

1 Process mining

Process mining is defined as a relatively young research discipline that sits between computational intelligence and data mining on the one hand, and process modeling and analysis on the other hand [2]. The process mining spectrum is quite broad and extends far beyond process discovery and conformance checking. Process mining objectives are overlapping with those of other approaches, methodologies, principles, methods, tools, and paradigms [1]. Process Mining Manifesto [11] deals with very important aspects such as process discovery, conformance checking, social network or organizational mining, construction of simulation models with the possibility of model extension and repair.

Process mining has an important role in information technology (IT) and operating systems too. The reason is using this process for monitoring and analyzing realized activities of system processes and applications that are running on operating systems.

2 Operating Systems

The operating system effectively manages available hardware sources and it makes their easier use. [3] The operating system creates a big interface between IT users and hardware for this goal. The verify access uses distribution operation system into defined layers as memory and process management. Other layers create drivers, file system, network communication, user interface, and applications. [12] Benefit of such layers is that every layer has assigned the own responsibility and lower layer performs the requirements from higher layers.

There are many operating systems and IT users or enterprises select by preferences and defined requirements. Main requirements are quick response time, intuitive navigation in an available interface, automatic system of alerts with advice for the solution of existing problems, or high system availability, fast recovery after failure and high security too. [13] In this situation, operating systems must be in very good condition because they must realize all requirements placed on them.

3 Windows 10 operating system and its event logs

Windows 10 is the latest version of operating system from Microsoft. IT users select from 32 or 64-bit version and distribution on USB, DVD or with a personal computer. [14] From a view of IT developers and programmers, there is needed view in detail on an operating system. Interest is focused on an operating system with its system events and also on applications that are running in the environment of an operating system. The reason is a need for monitoring, security, and tuning for better operating system use. Default request is to have operating system faster and more flexible; therefore, operating systems must bring a large number of changes, an extension of the menu, customizing for available panels and natural support with a web browser.

From system view, important records are about events that are focused on low-memory conditions, a higher number of accesses to a disk. Responsible monitoring uses default available event logs to determine conditions and context of errors. Prevention is the great benefit of such monitoring of event logs because system user is available to identify potential problems. [9] Windows operating system events are divided into five types as an error, warning, information, success audit, and failure audit:

- Error event indicates a basic problem with a level loss of data or functionality.
- Warning event indicates a possible problem in future.
- Information event describes the successful activity of applications, drivers etc.
- Success audit is event recording an audited security access with a successful result.
- Failure audit is event recording an audited security access with fails.

Event logs create records about realized activities (events) in implemented operation system and its applications that are running on the system. This information is useful in diagnostics of available hardware or software problems. Many authors of studies have interest in this topic that is dedicated:

- Performance analysis for games based on event tracking for Windows. [17]
- Analyze Microsoft Windows event logs for artifacts that may be pertinent to an investigation. [10]
- The windows event log for digital forensic cases. [4]

Windows 10 uses Event Log Viewer for display various events from applications, security issues, setup, system and other events that are created on a personal computer. This interface is easy to analyze and solve difficulties and errors of system and applications. There are used basic elements for event logging such as event log key, event sources, event categories, event identifiers, message files, event log records and event data. We can read from events log for example information about successful completion of a task (installing, updating) or we can see warnings events that are notified potential problems (low memory or low disk space). Important are also security events and warnings about unsuccessful activities. Each event in a log entry contains the following information [15]:

- Date: The date the event occurred.
- Time: The time the event occurred.
- User: The username of the user who was logged on when the event occurred.
- Computer: The name of the computer.
- Event ID: A Windows identification number that specifies the event type.
- Source: The program or component that caused the event.
- Type: The type of event (information, warning, error, security success audit etc.)

Like Windows Event Viewer, Event Log Explorer accesses Windows event logs and event log files from both local and remote servers. However, unlike Event Viewer, you can view several event logs (and log files) at one time — in different windows or even in one consolidated window (merged event log view). [5]

Windows operating system identifies significant events on a computer such for example when system encounters an error, windows installs updates or some user logs on. We can see the detailed information that is recorded in events logs by using the Event Viewer which is a tool of operation system Windows. Windows keeps the following useful logs according to McGrath and Michael Price [7]:

- Application Log - the Application log records events logged by programs. For example, a database program might record a file error.
- Security Log - the Security log records security events, such as valid and invalid logon attempts, and events related to resource use, such as creating, opening, or deleting files or other objects.
- System Log - this log records event logged by Windows system components. For example, the failure of a driver or other system component to load during startup.

4 Case study: Possibilities of using Process mining of events logs from Windows 10

We have obtained events logs (application, security, and system) from windows 10 system from one computer situated in the university computer room. It was necessary to transformed default events log into a form suitable for import into the Disco tool. We can see the minimum requirements for importing events log to Disco tool for example in Disco User´s Guide [6]. There are necessary at least three elements in events log for providing process mining analysis in Disco: Timestamp, Case ID, and Activity. We can also use other elements such as for example resources, costs, state, priority etc. We can see columns of transformed events log for importing process into Disco tool on the left side of bullet item list and the right side is representing columns in Disco.

- Event=Case ID in Disco
- Source=Resource in Disco
- Description=Activity in Disco
- Date&Time = Timestamp in Disco

Process mining analysis in Disco consists of tools for representing process model map, activity event classes, events over time, an overview of using resource and tasks queues.

Process model map

Process model map is favorite and useful tool because it is interactive and users will have the opportunity to make basic or deeper insight how many processes occurred. Users can choose if they want to see only the most frequent paths in the flow but it is also possible to change the level of details using the interactive setting in the software (setting detail of paths in percent). It is possible to manage how many different numbers of activities you want to see in process model map.

Information about activity event classes

Very important is information about the most conducted activity event classes. We can see for example top 10 activity event classes for all analyzed types of events log such as Application events log, Security events log, System events log.

Events over time

We can see an overview of events during recorded time in events log in the form of log timeline figures. There are some periods with an increased occurrence of events according to using of the computer room and specific ways of working on a PC.

Overview of using resources

There was provided a detailed analysis of using resources. We can analyze for example top 10 resource classes for all analyzed types of events log.

5 Conclusion

The main goal of this paper was to use process mining techniques to analyzed processes in Windows 10 operating system. We can suppose that every recorded event in Windows 10 has any significant occurrence in the system or in a program that requires being notified. We have analyzed in Disco process mining tools real events log from Windows 10 operating system workstation. We have used process mining techniques especially for analyzing information such as errors, alerts etc.

Acknowledgment

The work was supported by SGS/8/2018 project called "Advanced Methods and Procedures of Business Processes Improvement".

References

1. van der Aalst, W. M. P.: Process Mining: Data Science in Action. Springer, Berlin (2011)
2. van der Aalst, W. M. P.: Process Mining: Discovery, Conformance and Enhancement of Business Processes. Springer, Berlin (2016)
3. Anderson, T., Dahlin, M.: Operating Systems: Principles and Practice. Recursive Books, ISBN-10 0985673524 (2014)
4. Codona, B.: Analysis and Evaluation of the Windows Event Log for Forensic Purposes. Undergraduate project dissertation, Napier University (2007)
5. Event Log Explorer, https://eventlogxp.com/features.html
6. Fluxicon Disco User's Guide, https://fluxicon.com/disco/files/Disco-User-Guide.pdf McGrath, M., Price, M.: Windows 10 in easy steps - Special Edition: To venture further. In Easy Steps Limited, Warwickshire (2015)
7. Leonhard, W.: Windows 10 All-in-One For Dummies. For Dummies, ISBN 978-1-119-03872-6 (2015)
8. Microsoft, About Event Logging, https://msdn.microsoft.com/en-us/library/windows/desktop/aa363632(v=vs.85).aspx (2017)
9. Mullinix, M. D.: An Analysis of Microsoft Event Logs. Capstone Project Submitted to the Faculty of Utica College (2013)
10. Process Mining Manifesto, http://www.win.tue.nl/ieeetfpm/lib/exe/fetch.php?media=shared:process_mining_manifesto-small.pdf
11. Silberschatz, A., Galvin, P. B., Gagne, G.: Operating System Concepts. Wiley, ISBN-10: 1118063333 (2012)
12. Stallings, W.: Operating Systems: Internals and Design Principles. Pearson, ISBN-10: 0133805913 (2014)
13. Techsupportall, 3 Methods to Create a Bootable Windows 10 USB / DVD Installer, https://www.techsupportall.com/how-to-create-a-bootable-windows-10-usb-disk-dvd-installer/ (2016)
14. TechTarget, http://searchwindowsserver.techtarget.com/definition/Windows-event-log (2016)
15. Tidrow, R., Boyce, J., Shapiro, J. R.: Windows 10 Bible. John Wiley & Sons, Indianapolis (2015)