Analysis and information security assessment of the Windows operating system

K Yu Zhigalov 1, V V Nadrshin2 and R I Aliev3

1 Institute of Control Sciences of Russian Academy of Sciences
2 Irkutsk National Research Technical University, 83, Lermontov str., Irkutsk, 664074, Russia
3 Chechen State University, 17a, Dudaev Boulevard, Grozny, 364015, Russia

E-mail: nadrshin@ex.istu.edu

Abstract. Any application consists of many components (bases, frameworks, loaders), and errors in the component settings are liable to lead to various consequences. Even the smallest component can compromise the overall security of the application. It is acceptable to work quite effectively with event logs if one comprehends their formation principle. That is what the paper is devoted to. The material in the paper will be valuable for both information security specialists and ordinary users.

1. Introduction
The command shell of WindowsPowerShell being installed with the Windows operating system provides more flexible methods for viewing and filtering events. The Get-EventLog cmdlet is at the heart of WindowsPowerShell, for which one can apply the following parameters: “After”, “AsBaseObject”, “AsString”, “Before”, “ComputerName”, “EntryType”, “Index”, “InstanceID”, “List”, “LogName”, “Message”, “Newest”, “Source”, and “UserName.” The parameters are designed to control the level of event details and their format, to include or exclude particular types of events in the result, etc. It is also probable to save a customized script for more efficient work (format*.ps1) [1-3].

2. Results and Discussion
It is required to enter the Get-EventLog command in the PowerShell to view the events, and then specify the log name and any parameters for filtering and detailing events. For instance, the command “Get-EventLog - Logname “Application” displays information about all events that have been recorded in the “Application” log, as shown in Figure 1.

There are the following event properties: “Number”, “Time”, “Record Type”, “Source”, “Event ID”, and “Message”, which can be viewed using the “Event Viewer” snap-in.

Generally, the following event properties are displayed: “Event Code”, “Computer”, “Event Sequence Number”, “Task Category”, “Category Code”, “Level”, “Event Message”, “Source”, “Word Wrap”, “Instance ID”, “Event Generation Date”, “Event Recording Date”, “User”, “Site”, and “Subunit.” An example of displaying events with a specific set of properties is demonstrated in Fig. 2.
The result is displayed both as a table (Format-Table) and as a list (Format-List).

The command shell of “PowerShell” reads events in the order which they have been logged, starting with the last record. One of the shell advantages is flexible filtering and sorting of events, for example, displaying events for a certain period of time or displaying recent events. The given filtration can be configured using the following procedures [4-6].

1. Events registered up to a certain moment – “Before” parameter.
2. Events fixed after a certain moment – “After” parameter.
3. Output of the latest events – “Newest” parameter indicating the number of such events.

Combinations of the above parameters are also feasible.

One is able to sort the events applying the Sort-Object command. Grouping happens due to Group-Object.

Frequently, error and warning events have to be analyzed. The filter allows us to display the events that have an “error” value in the EntryType property. The Where-Object command, where the selected events are directed and saved in a variable, is used for the above actions. Figure 3 shows the search for such events.

The Where-Object command makes it possible to find events by any property.
The command shell of “PowerShell” allows us both to view and filter events, and to customize logs. The Wevtutil command line utility (WindowsEventCommandLineUtility) is used to customize the logs. Various actions with logs can be performed introducing the given command, namely, change their configuration, archive, clear, export, etc [7, 8].

There are 12 commands and a variety of advanced options for centralized control and configuration of event logs in the Wevtutil system utility. All commands and parameters have both full and short forms.

**Creation of a log archive.** It is acceptable to export the event log to an offline file by dint of the Archive-log command.

Specifying the Locale (-l) parameter, an archive copy of the event log is created with subdirectories of the selected locales. If this parameter is not specified, then the archive with the default locale will be created.

**Complete clearing of the event log.** The Clear-Log (-cl) command is applied for the complete clearing of a specific event log.

A log backup is created by means of the Backup (-bu) option before clearing the event log. If the parameter is not specified, the backup log will not be created.

**List of event log titles.** The Enum-Logs (-el) command is brought into use to list the names of all logs available on the computer (Fig. 4). The Find parameter is to be applied for efficient search due to the large number of logs on a computer.

“Text” is the sought part of the log title.

**List of event sources registered in the system.** The Enum-Publishers command is displayed a list of event sources. There can be a lot of event sources in the system, therefore the Find parameter, specifying the search, is introduced together with the given command.

“Text” is the sought part of event sources.

**Export of the event log in the “.evtx” format.** Export-Log command (-epl) is intended to export the event log in “.evtx” format.

The following parameters are used with the command:

- Logfile (-lf) — specifying the path to the exported event log. The parameter is available with True/False values.
- Structuredquery (-sq) — the file will have the request in a structured way. The parameter is available with True/False values.
- Query (-q) — the ability to use a saved XPath search with a filter. The parameter is available only if the value is True.
- Overwrite(-ow) — overwriting the log if a file with the same name already exists in the folder. The parameter is available with True/False values.

**Information about event log configuration.** Current information about the event log configuration can be displayed by clicking the Get-Log (-gl) command.
“Log name” means the event log name for which one is able to view the configuration. Format is a parameter responsible for the format of the received file. Text format is used as standard, but XML format can be specified.

**Information about the state of the event log.** The Get-Log-Info (- Gli) command is meant to display the data for a specific event log.

The command has a Format parameter to represent information in one form or another.

**Information about the event sources.** The Get-Publisher (- Gp) command displays the data output about registered event sources in the system. The command is convenient to apply for external applications.

The Source means the full name of the event source registered in the system. The Getevent (- ge) parameter allows one to get the entire list of event sources in the form of metadata. The parameter is available with True/False values. The Getmessage (- gm) parameter serves for displaying a specific event message instead of its identifier. The Format parameter is described above.

**Installation of sources and event logs using a manifest.** The Import-Manifest (- Im) command sets up event sources and logs by a manifest.

The specified parameters mean the replacement of the element supplier, and its values indicate the file path.

**Request information about events from the log.** It is possible to view current and archived event logs by dint of the Query-Events command (- Qe).

Logfile, Structuredquery, Query, Format, Locale are similar to the command parameters indicated above. The Bookmark (- bm) parameter specifies the complete path of the file through bookmarks. The Savebookmark (-sbm) parameter is the same as the Bookmark, but the file format must be XML. The Reversesedirection (- rd) parameter displays events in reverse order. The latest events will be first displayed if the parameter is True. The Count (- c) parameter adjusts the number of displayed events.

**Changing the log configuration.** The Set-Log (- Sl) command allows changing the log configuration (Fig. 5). The following parameters are applied with the command:

- **Enabled (- e)** — activation or deactivation of the event log;
- **Quiet (- q)** — command display. The command implementation will not be notified to the user if the value is True;
- **Maxsize (- ms)** — maximum size of the log file;
- **AutoBackup (- ab)** — automatic archiving of the event log. The parameter is available with True/False values;
- **LogFileName(- lfn)** — specifying the event log name;
- **Level (- l)** — value of the event log filtering level;
- **Keywords (- k)** — keyword filtering;
- **Retention (- rt)** — prohibition of overwriting events in the log. The parameter is accessible with True/False values.

![Figure 5. Set-Log command](image)

**Deleting sources and event logs using the manifest.** Uninstall-Manifest (- Um) - deletion of the event log source by means of the manifest. Example:
3. **Conclusion**

Thus, the following tools for analyzing log files have been considered: the “PowerShell” command shell and the Wevtutil command line utility (WindowsEventsCommandLineUtility). As a result, programs for automatic analysis of log files have been written.

**References**

[1] Kondratiev V V, Karlina A I, Guseva E A, Konstantinova M V and Gorovoy V O 2018 Structure of Enriched Ultradisperse Wastes of Silicon Production and Concretes Modified by them *IOP Conference Series: Materials Science and Engineering* **463**(4) 042064

[2] Martyushev N V, Egorov Yu P and Utiev M 2002 Computer analysis of the material structure *Proceedings of the 8th International Scientific and Practical Conference of Students, Post-Graduates and Young Scientists: Modern Technique and Technologies* 1213783 pp 159–161

[3] Sysoev I A, Kondrat’ev V V, Zimina T I and Karlina A I 2018 Simulation of the Energy States of Electrolyzers with Roasted Anodes at Elevated Currents *Metallurgist* **61**(11–12) 943–949

[4] Suslov K V, Solonina N N and Smirnov A S 2011 Smart Grid: A new way of receiving primary information on electric power system state *IEEE PES Innovative Smart Grid Technologies Conference Europe* 6162654

[5] Solodusha S, Suslov K and Gerasimov D 2016 Applicability of Volterra integral polynomials in the control systems of electric power facilities *Proceedings of International Conference "Stability and Oscillations of Nonlinear Control Systems" (Pyatnitskiy's Conference)* 7541227

[6] Gura D A, Gura A Y, Volkova T A and Lipilin D A 2020 Recreational space as a factor of sustainable development of coastal geosystems of the Krasnodar region *IOP Conference Series: Earth and Environmental Science* **579**(1) 012007 doi:10.1088/1755-1315/579/1/012007

[7] Sivtsov A V, Yolkin K S, Kashlev I Mô Karlina A I 2020 Processes in the Charge and Hearth Zones of Furnace Working Spaces and Problems in Controlling the Batch Dosing Mode during the Smelting of Industrial Silicon and High-Silicon Ferroalloys. *Metallurgist* **64**(5-6) 396–403

[8] Ershov V A, Karlina A I, Karlina Y I 2021 Process Control System for Producing a Silica-Based Modifying Additive. *Metallurgist* **65**(3-4) 446–453