# Report template

# Windows administration

|  |  |
| --- | --- |
| Location of measurement: | I.B413, place #: |
| Date / time of measurement: |  |
| Students: |  |
| Name of this file: | WindowsLab\_<Neptun code>.doc |
| Lecturer: | ... |

Hardware and software components to use:

|  |
| --- |
| Name of the equipment |
| PC |
| VMware Workstation |
| Windows 10 virtual machine |
|  |  |  |

|  |
| --- |
| **How to treat this document:**   * Fill in the yellow fields only! Do not forget to fill in the above header too! * Replace the <<screenshot>> texts with the corresponding screenshot required and provide a short explanation! * Send your completed report to the lecturer via email to hullam.gabor AT mit.bme.hu! * If you have any feedback regarding the Lab exercises feel free to send an e-mail to the lecturer! |

# 1. Analyzing running processes

|  |
| --- |
| Analyzing running processes using Process Explorer.   * **Before** doing the actual tasks it is worth to have a look at the user interface of Process Explorer (what kind of options can be set in the menus, how is it possible to display the lower panel and so on). * To accomplish the tasks it is required to run Process Explorer as **Administrator**! |

|  |
| --- |
| 1.1 Current processes |
| What are the currently running processes under the user name **Hallgato** after logging in? What functions do they provide? |
| <<screenshot>>  Answer: |
| How many **svchost.exe** are running currently on the machine? |
| <<number of svchost.exe processes>>  <<screenshot>> |
| What is the PID of the instance hosting the DNS Client service? |
| <<PID>>  <<screenshot>> |
| What other services are running within this instance of svchost? |
| Answer: |

|  |
| --- |
| 1.2 Windows Store applications |
| Let’s start one of the store applications from the Start screen (like Maps, News, Weather…)! |
| <<screenshot>> |
| How are these new applications displayed in Process Explorer (Use the Process Tree view and check under which process do they appear)? |
|  |
| How can we see if an application switches to Suspended mode after we use it? (e.g. we switch to Process Explorer) |
|  |

|  |
| --- |
| 1.3 Sessions and threads |
| How many **sessions** do the currently running processes belong to? Which users are associated to these sessions? |
| <<number of sessions, their identifiers, associated user>> |
| How many threads does the **csrss.exe** belonging to session one have? |
| <<number of threads>>  <<screenshot>> |

|  |
| --- |
| Summary  After solving this task it is expected to know and understand:   * how can we display the currently running processes and their properties * what system processes does a Windows based machine have * how are the services running * what is the life-cycle of Windows Store applications |

# 2. Investigating handles

|  |
| --- |
| 2.1 Display handles |
| Start an instance of **Notepad**!  What **registry keys** are accessed by this instance of Notepad (Ctrl + H)? |
| <<screenshot>> |
| Display the list of **DLLs** opened by Notepad(Ctrl + D)! |
| <<screenshot>> |
| What happens if we open a text file in Notepad? |
| <<screenshot>>  Answer: |

|  |
| --- |
| 2.2 Handles currently in use |
| In Windows it is not always possible to delete or replace a file if there are open handles to it. In this case Process Explorer can help us to identify the processes having open handles to the file in question ( Find / Find Handle or DLL…).  Search for processes (if any) having an open handle to the log file of OneDrive! |
|  |

|  |
| --- |
| Summary  After this task it is expected to know and understand:   * how can we display the handles (to files or DLLs) belonging to a process * how is it possible to search for open handles |

# 3. Managing services

|  |
| --- |
| 3.1 Information on services |
| Let’s have a look at the service named Security Accounts Manager on the Services user interface[[1]](#footnote-1) (press Win+W, then start to type services, then *View local services*)! |
| What is the role of this service? |
| Answer: |
| What is its short name? And what is its display name? |
|  |
| Which application belongs to this service? |
|  |
| Under which user account is this service running? |
|  |

|  |
| --- |
| 3.2 Service dependencies |
| What dependencies does this service have? |
| <<screenshot>> |

|  |
| --- |
| 3.3 Recovery possibilities |
| What recovery settings can be made for this service? |
| <<screenshot>>  Answer: |
| Investigate the recovery options for another service too! |
| Recovery possibilities:       <<screenshot>> |

|  |
| --- |
| 3.4 Svchost groups |
| Which running instance of svchost.exe consumes the most physical memory! |
| <<screenshot>> |
| What is the group name of this svchost instance (look at the Services tab of Task Manager)? |
|  |

|  |
| --- |
| Summary  After this task it is expected to know and understand:   * the settings a service may have * what is the purpose of svchost.exe * how is it possible to find the process under which a given service is running |

# 4. System management tools

|  |
| --- |
| 4.1 MMC modules |
| Start a **Microsoft Management Console** (mmc.exe)! |
| Investigate what kind of **snap-ins** could be added to this console! Assemble a console on which one can see management tools for **disks** and for **shares**! |
| <<screenshot>> |

|  |
| --- |
| 4.2 Event viewer |
| Start the **Event viewer**! Is there any **error** or warning type entry in the past seven days (in any of the logs)? If yes what is (are) the **source(s)** of it? (Use the summary displayed on the start screen of Event Viewer!) |
| Source(s):       <<screenshot>> |

|  |
| --- |
| 4.3 Searching the Event Viewer |
| Let’s see how can we search effectively among the vast amount of data by the help of **filtering** and **grouping**:  List the **Event ID**s logged by *Service Control Manager* (as the source) into the **System** log? (Use the *filtering* and *grouping* capabilities rather than manually investigate all of the log entries!) |
| * <<Event ID>>: <<textual description>> * …   <<screenshot>> |

|  |
| --- |
| Summary  It is expected that after finishing this task you know and understand the following:   * how to add a MMC snap-in to the MMC console * how can we display the event logs and how can we search and filter them |

# 5. Investigating load and performance

|  |
| --- |
| 5.1 Task Manager |
| Let’s have a look at the GUI of the redesigned **Task Manager**! Switch to the **Processes** view and watch how the usages of the various resources are displayed like a thermal map (to do that make some load in the background – like playing a HD video on Youtube)! |
| <<screenshot>> |

|  |
| --- |
| 5.2 Resource Monitor |
| Start the **Resource Monitor** (probably the easiest way to do that is through the **Performance** view of the **Task Manager**)!  Based upon the counter values displayed on the start page which process **read the most from the disk**? |
| <<process name>>  <<screenshot>> |
| Which process uses the most **physical memory**? |
| <<process name>>  <<screenshot>> |

|  |
| --- |
| 5.3 Performance Monitor |
| If we are interested in even deeper performance data then **Performance Monitor** (perfmon.exe) is the most suitable tool. |
| After starting it, add a counter measuring the packets per second sent by the network interface! |
| <<the way of adding the counter>>  <<screenshot>> |
| Generate some network traffic! Then make a graph showing that traffic! |
| <<screenshot>> |

|  |
| --- |
| Summary  By the end of this task you expected to know and understand:   * how is it possible to investigate the most important performance data * be familiar with the capabilities of Task Manager and Resource Monitor * be able to observe and capture the values of the performance counters |

# 6. Manage users

|  |
| --- |
| 6.1 Creating users and groups |
| Open the **Local Users and Groups** MMC snap-in (do not use the simplified interface presented in the User Accounts entry in Control Panel)! |
| Create a new user (User Name: **testuser**; Full Name: **Test User**, Password: **pass**)  Do not allow the user to change his/her password! |
| <<screenshot>> |
| Create a group named **Teachers** and add the user created before to it! |
| <<screenshot>> |

|  |
| --- |
| 6.2 SID |
| The system identifies users and groups not by their name but rather by their SID (*Security Identifier*). |
| Query the **SID** of the **computer**, the **Administrator** and the **newly created user** using Sysinternals *psgetsid* (c:\program files\sysinternals\psgetsid.exe)! Run psgetsid.exe from a windows command line (cmd)! |
| <<SID of the computer>>  <<SID of the Administrator>>  <<SID of the user>>  <<screenshot>> |
| What is the structure of an **SID** belonging to a **user**? |
| Answer: |

|  |
| --- |
| Summary  Now it is expected to know and understand:   * how can be users and groups created * what properties they have * what is the purpose and structure of SIDs |

# 7. Managing file permissions

|  |
| --- |
| 7.1 The Runas command |
| In this section we investigate the permissions of various users. To avoid frequent logouts and logins we use an instance of Total Commander under the name of a different user by the help of the runas command.  Start a **Total Commander** under the name of **testuser** (runas)! |
| <<command>> |
| Create a folder named *acltest* on drive C:! What are the permissions just after creation, why? |
| <<screenshot>>  Answer: |

|  |
| --- |
| 7.2 Changing permissions |
| Remove the permissions in a way that only the Teachers group shall have full control over the folder! (Do not use Deny rules! Disable inherited permissions) |
| <<description of the solution>>  <<screenshot>> |
| Check whether the user **Hallgato** is really unable to open that folder while the user **testuser** is able to do that and can also create files in that folder! |
| <<screenshot>> |

|  |
| --- |
| 7.3 Change ownership |
| Even in this case Administrators are able to access folders like this by first acquiring its ownership! |
| In the spe**cial set**tings on the **Ownership** tab set the Administrators group as the new owner of this folder! |
| <<screenshot>> |

|  |
| --- |
| 7.4 Effective rights |
| Change the permissions on the folder **acltest** in a way that the groups Administrators and Teachers shall have full control over it while testuser shall have only read rights (do not use Deny rights)! |
| <<screenshot>> |
| Test whether testuser is able to write/create a file in that folder? What can be observed? What is the cause? |
|  |
| Let’s create a group named **Students** and add testuser to it! Set the access permissions of Students to **allow read** rights and **deny write** rights. (To make the changes on group memberships effective you need to restart Total Commander.) |
| Test again whether testuser is able to change the content of that folder? What can be observed now? How can you explain it? |
| <<screenshot of the modified access rights>>  <<result>>  <<explanation>> |

|  |
| --- |
| Summary  After you finished this task it is expected to know and understand:   * the operation of Windows’ file permissions * be able to change file permissions * figure out the effective permissions * understand how are file permissions operate on shared files and folders |

# 8. OPTIONAL TASK: Local Security Policy

|  |
| --- |
| 8.1 |
| We can access the local security policy in **Control Panel** by selecting **Administrative Tools**.  Make proper settings in the **logging policy** to log also the **successful and unsuccessful login attempts** the **change on security policy** and the **use of system rights**! |
| <<screenshot>> |

|  |
| --- |
| 8.2 |
| Make proper settings to require passwords having at least 8 character length and to lock an user after 3 unsuccessful login attempts! |
| <<screenshot>> |
| Check if the system really locks out the test user after 3 unsuccessful login attempts (we do not need to log off just use *runas* three times)! |
| <<screenshot>> |
| In cases like this what kind of events can be observed in the security session of the event log? |
|  |

1. Can be reached also here: Control Panel / System and Security / Administrative tools / Services [↑](#footnote-ref-1)