2019

IIS Logs Analyzer v1.0

by Fabian Caignard (alias *B4tchM4n*)

IIS LOGS ANALYZER IS A SCRIPT WRITTEN BY FABIAN CAIGNARD IN POWERSHELL.

THIS DOCUMENT EXPLAINS HOW TO USE THIS TOOL.

Table of Contents

I. Introduction

A. What IIS Logs Analyzer does

IIS Logs Analyzer is a graphical tool to analyze, then export results in text files.
It was designed for System Administrators, IIS Administrator and Web or FTP sites Administrators to help them to have an overview of the IIS sites usage or user activity.
This script can discover IIS log files in default locations, but it is also possible to specify other log directories.
By default, it will discover IIS log files on local computer, but it can connect on remote computers.
Once the settings are defined and targets are selected, the script will read all log files in its scope of analysis then export the list of users and/or client IP addresses connections on Web and/or FTP sites per date.
By using this tool, you can easily know which users connected each day on each Web or FTP site on selected IIS servers.

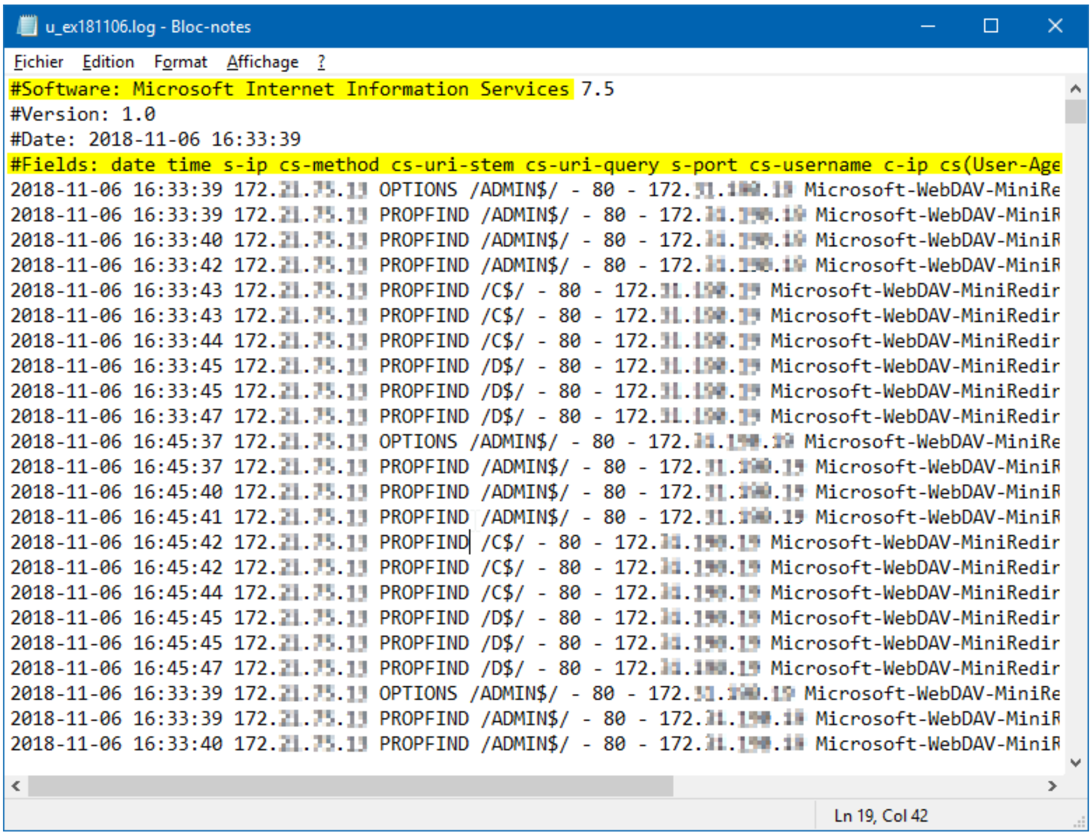
B. Requirements

The script requires Microsoft Windows PowerShell 5 to run properly.
In addition, to ensure a correct display of the graphical interface, it is recommended to run this script in an environment with:

- A minimum screen resolution of:	1024x768 or 1280x720
- Windows Text size and DPI setting set to	100%

C. Limitations

Only Microsoft IIS log files in W3C format can be analyzed by this tool. The log files must contain the software header `#Software: Microsoft Internet Information Services` to be considered as an IIS log but also the fields header (as in following screenshot) to be considered in W3C format.



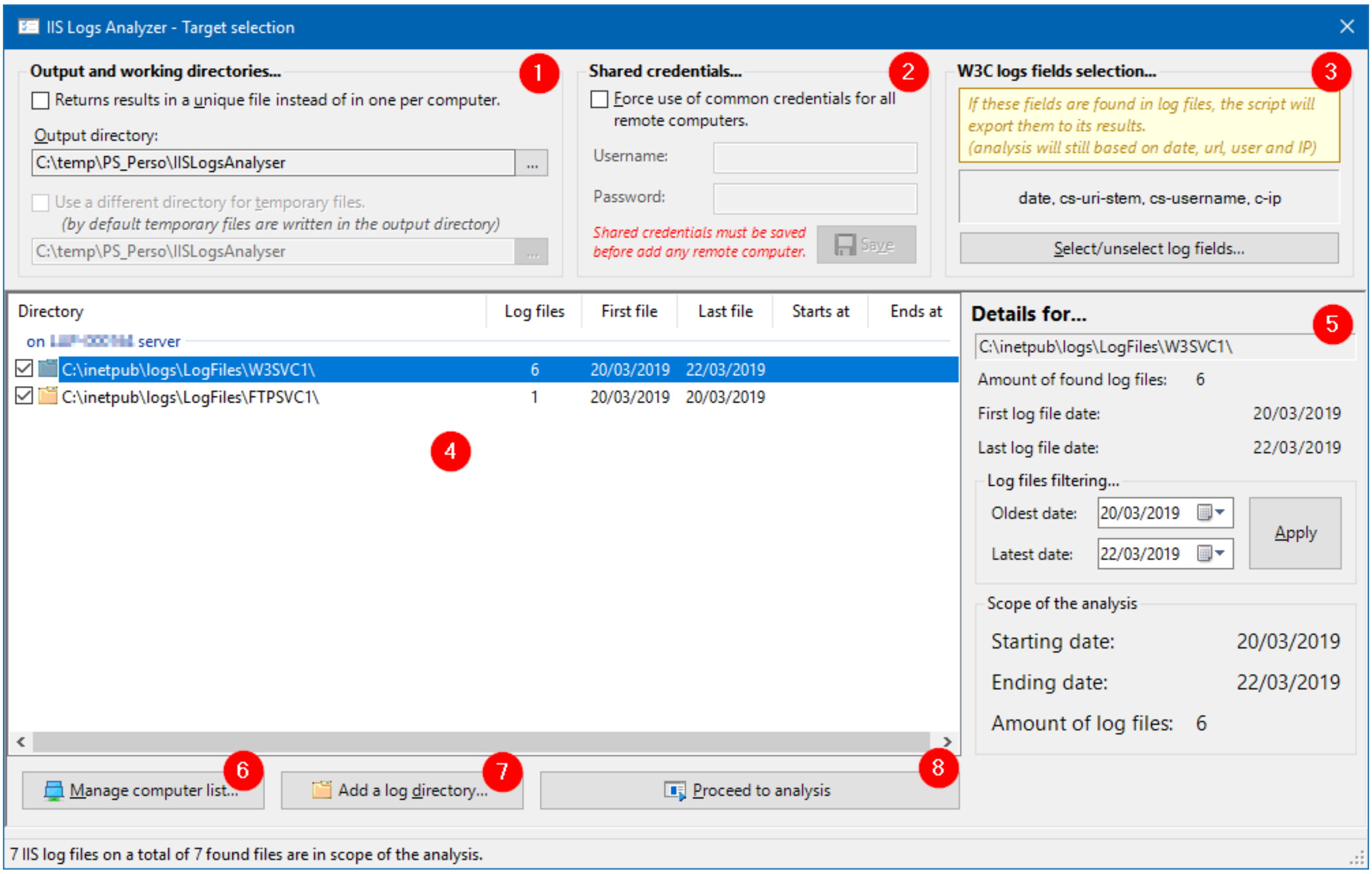
```
#Software: Microsoft Internet Information Services 7.5
#Version: 1.0
#Date: 2018-11-06 16:33:39
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Age
2018-11-06 16:33:39 172.[redacted] OPTIONS /ADMIN$/ - 80 - 172.[redacted] Microsoft-WebDAV-MiniRe
2018-11-06 16:33:39 172.[redacted] PROPFIND /ADMIN$/ - 80 - 172.[redacted] Microsoft-WebDAV-MiniR
2018-11-06 16:33:40 172.[redacted] PROPFIND /ADMIN$/ - 80 - 172.[redacted] Microsoft-WebDAV-MiniR
2018-11-06 16:33:42 172.[redacted] PROPFIND /ADMIN$/ - 80 - 172.[redacted] Microsoft-WebDAV-MiniR
2018-11-06 16:33:43 172.[redacted] PROPFIND /C$/ - 80 - 172.[redacted] Microsoft-WebDAV-MiniRedir
2018-11-06 16:33:43 172.[redacted] PROPFIND /C$/ - 80 - 172.[redacted] Microsoft-WebDAV-MiniRedir
2018-11-06 16:33:44 172.[redacted] PROPFIND /C$/ - 80 - 172.[redacted] Microsoft-WebDAV-MiniRedir
2018-11-06 16:33:45 172.[redacted] PROPFIND /D$/ - 80 - 172.[redacted] Microsoft-WebDAV-MiniRedir
2018-11-06 16:33:45 172.[redacted] PROPFIND /D$/ - 80 - 172.[redacted] Microsoft-WebDAV-MiniRedir
2018-11-06 16:33:47 172.[redacted] PROPFIND /D$/ - 80 - 172.[redacted] Microsoft-WebDAV-MiniRedir
2018-11-06 16:45:37 172.[redacted] OPTIONS /ADMIN$/ - 80 - 172.[redacted] Microsoft-WebDAV-MiniRe
2018-11-06 16:45:37 172.[redacted] PROPFIND /ADMIN$/ - 80 - 172.[redacted] Microsoft-WebDAV-MiniR
2018-11-06 16:45:40 172.[redacted] PROPFIND /ADMIN$/ - 80 - 172.[redacted] Microsoft-WebDAV-MiniR
2018-11-06 16:45:41 172.[redacted] PROPFIND /ADMIN$/ - 80 - 172.[redacted] Microsoft-WebDAV-MiniR
2018-11-06 16:45:42 172.[redacted] PROPFIND /C$/ - 80 - 172.[redacted] Microsoft-WebDAV-MiniRedir
2018-11-06 16:45:42 172.[redacted] PROPFIND /C$/ - 80 - 172.[redacted] Microsoft-WebDAV-MiniRedir
2018-11-06 16:45:44 172.[redacted] PROPFIND /C$/ - 80 - 172.[redacted] Microsoft-WebDAV-MiniRedir
2018-11-06 16:45:45 172.[redacted] PROPFIND /D$/ - 80 - 172.[redacted] Microsoft-WebDAV-MiniRedir
2018-11-06 16:45:45 172.[redacted] PROPFIND /D$/ - 80 - 172.[redacted] Microsoft-WebDAV-MiniRedir
2018-11-06 16:45:47 172.[redacted] PROPFIND /D$/ - 80 - 172.[redacted] Microsoft-WebDAV-MiniRedir
2018-11-06 16:33:39 172.[redacted] OPTIONS /ADMIN$/ - 80 - 172.[redacted] Microsoft-WebDAV-MiniRe
2018-11-06 16:33:39 172.[redacted] PROPFIND /ADMIN$/ - 80 - 172.[redacted] Microsoft-WebDAV-MiniR
2018-11-06 16:33:40 172.[redacted] PROPFIND /ADMIN$/ - 80 - 172.[redacted] Microsoft-WebDAV-MiniR
```

Example of a Microsoft IIS log file in W3C format

D. User Interface overview

The tool user interface is composed of 2 main panels:

- The upper panel contains groups of controls to set toll's global settings.
- The downer panel contains targets of script analysis and controls to add, remove, and adjust items selection in its scope.



IIS Logs Analyzer - Target selection

Output and working directories...

☐ Returns results in a unique file instead of in one per computer.

Output directory: C:\temp\PS_Perso\IISLogsAnalyser [...]

☐ Use a different directory for temporary files.
(by default temporary files are written in the output directory)

C:\temp\PS_Perso\IISLogsAnalyser [...]

Shared credentials...

☐ Force use of common credentials for all remote computers.

Username:

Password:

Shared credentials must be saved before add any remote computer.

W3C logs fields selection...

*If these fields are found in log files, the script will export them to its results.
(analysis will still based on date, url, user and IP)*

date, cs-uri-stem, cs-username, c-ip

Directory	Log files	First file	Last file	Starts at	Ends at
on [redacted] server					
☑ C:\inetpub\logs\LogFiles\W3SVC1\	6	20/03/2019	22/03/2019		
☑ C:\inetpub\logs\LogFiles\FTPSVC1\	1	20/03/2019	20/03/2019		

Details for...

C:\inetpub\logs\LogFiles\W3SVC1\

Amount of found log files: 6

First log file date: 20/03/2019

Last log file date: 22/03/2019

Log files filtering...

Oldest date: 20/03/2019

Latest date: 22/03/2019

Scope of the analysis

Starting date: 20/03/2019

Ending date: 22/03/2019

Amount of log files: 6

7 IIS log files on a total of 7 found files are in scope of the analysis.

Main window of IIS Logs Analyzer

1 You can define here script's output settings. Controls in this area allow you to:

- force script to concatenate all its results in 1 unique output file
- change the directory where script will save output files

Please note that it is not possible yet to select another directory to store temporary files.

2 You can force script to use the same credentials to connect on all remote computers.
These settings must be defined before adding any remote computer: once a remote computer is added, it is not anymore possible to set shared credentials.
These credentials are never used to work on local computer.
Please note that it is recommended to run the script as a user account which have sufficient permissions to browse and read IIS log files (at least on local computer).

3 This section lets you see and select W3C log fields to export in script's results.

4 This left zone lists found log directories and displays:

- Amount of IIS log files in them
- Dates of older and most recent files
- (when defined) Starting and ending dates of limit range to analyze

All log directories are grouped by computer.

5 This right zone is only displayed when a directory is highlighted in the left zone.

It shows details about selected directory and allows you to define dates limit range for it.

6 This button opens a window to manage (add, remove, set specific credentials, etc.) remote computers.

7 This button opens a dialog which allows you to add undiscovered log files directories.
Please note that this button only allows to add directories, 1 by 1, and does not allow to remove any.

8 This button launches the script analysis. After clicking on it, be patient: this operation could take long time depending on amount and size of log files in the scope.
Please not that this button is only available when at least 1 directory containing log files is selected.

For more details on using this tool, please see next chapter.

II. How to use it

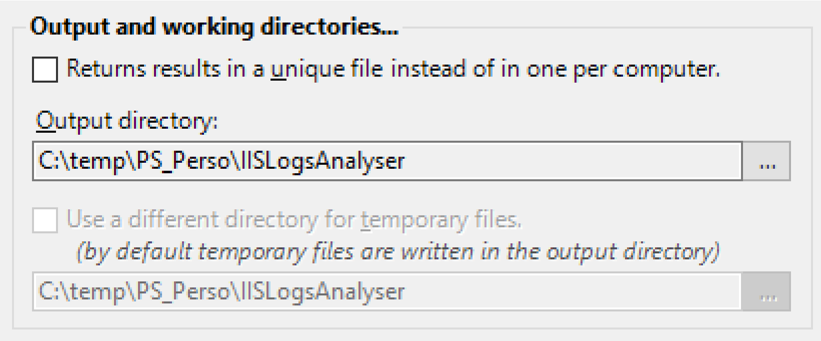
A. Common settings

1. How to define tool's directories

By checking the "Returns results in a unique file instead of in one per computer." option, the script will concatenate all its results in a unique output text file.
If this option is not checked, the script will create 1 output file per computer and per "instance" (the log directory represents here the instance).

By default, the script will save its output files in its own directory. If you are running the tool's script from an USB key or a read-only directory, it is then recommended to modify the output directory.

To modify the output directory, simply click the "…" button, and select or create a directory in the appearing folder selection dialog box.



Output and working directories...

□ Returns results in a unique file instead of in one per computer.

Output directory:
C:\temp\PS_Perso\IISLogsAnalyser ...

□ Use a different directory for temporary files.
(by default temporary files are written in the output directory)
C:\temp\PS_Perso\IISLogsAnalyser ...

Output and working directory settings

2. About credentials

By default, the script will use the credentials of user account which is running it to work on local computer and connect then work on remote computers.
If the current user account does not have sufficient permissions on remote computer, the script allows you to use either custom credentials (specified computer per computer), either common and shared credentials.

It is not possible to specify any credential to work with local computer, the only way in this case is to run the script as a user account with sufficient permissions.

To use custom credentials for each remote computer, you should define it in Computer management windows of the tool (please see chapter II.B.2).

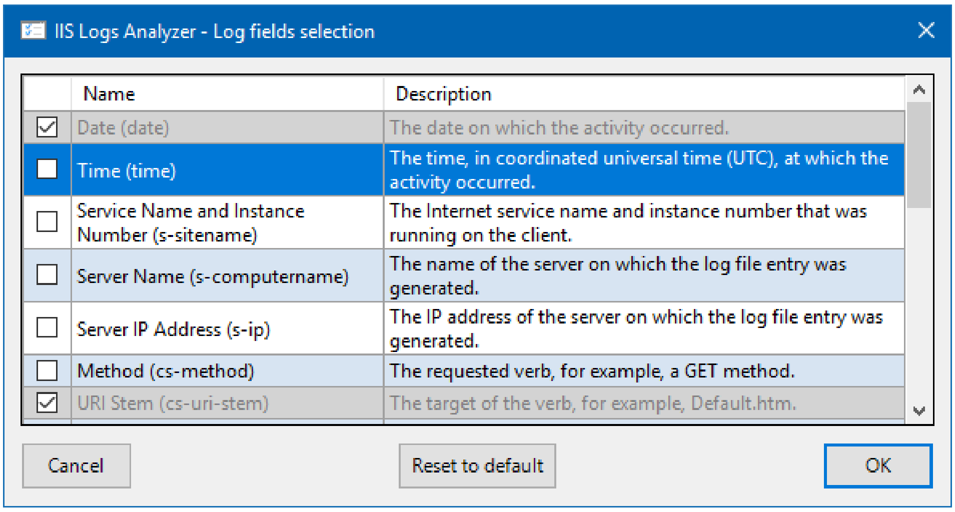
To use common and shared credentials to connect and work on all remote computers, Shared credentials must be defined and saved before adding any remote computer.
Once a remote computer is added to the tool, the “Shared credentials…” features are locked and unchangeable.

3. How to select exported IIS log fields

By default, the selected W3C logs fields are:

- date (Date of log event)
- cs-uri-stem (browsed or requested Url)
- cs-username (username who requested Url)
- c-ip (IP address of client computer)

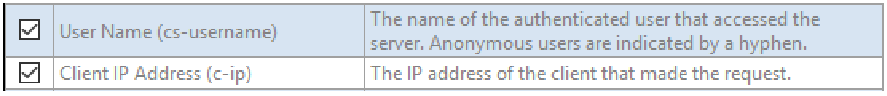
By click on “Select/unselect log fields…” button, you can modify selected fields (see screenshot below).



	Name	Description
☑	Date (date)	The date on which the activity occurred.
□	Time (time)	The time, in coordinated universal time (UTC), at which the activity occurred.
□	Service Name and Instance Number (s-sitename)	The Internet service name and instance number that was running on the client.
□	Server Name (s-computername)	The name of the server on which the log file entry was generated.
□	Server IP Address (s-ip)	The IP address of the server on which the log file entry was generated.
□	Method (cs-method)	The requested verb, for example, a GET method.
☑	URI Stem (cs-uri-stem)	The target of the verb, for example, Default.htm.

W3C log fields selection dialog box

In the selection dialog box, some fields are grayed and not modifiable: these fields are considered as mandatory to let the analysis working properly.
If one of the mandatory fields is missing in a log file, the log file will be ignored by the script.



☑	User Name (cs-username)	The name of the authenticated user that accessed the server. Anonymous users are indicated by a hyphen.
☑	Client IP Address (c-ip)	The IP address of the client that made the request.

At least one of the fields between User Name and Client IP Address fields is mandatory: it is then impossible to unselect both.

To restore script default selected fields, simply click on “Reset to default” button.

Be advise that selecting additional fields does not modify the analysis profile.
So, in example, if “Time” field is selected here, the results of script will not be more relevant.

Log files discovery

4. How the log files discovery works

By default, on script loading, it looks for default W3SVC***x*** or FTPSVC***x*** or MSFTPSVC***x*** (where ***x*** is an instance ID) IIS log files locations in:

- C:\Windows\System32\LogFiles
- C:\Inetput\logs\LogFiles

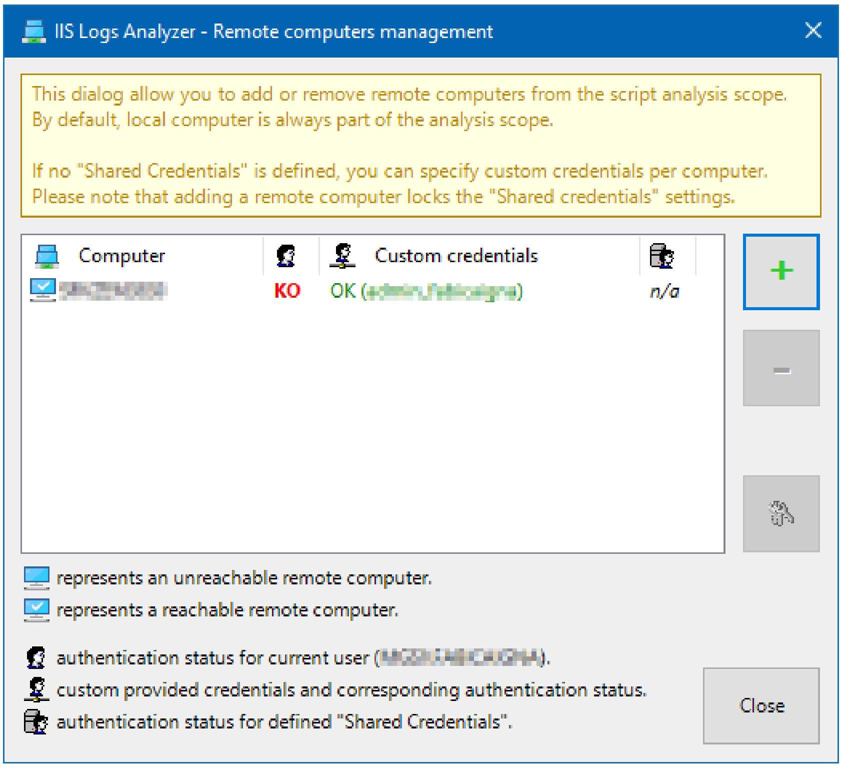
In each found directory, script looks then for .log files and checks files first line.

If the first line begins by `#Software: Microsoft Internet Information Services` it adds the log file in its list of log files.

Finally, the scripts display the list of discovered directories and log files details (amount of IIS log files and first and last files dates).

5. How to add a remote computer

To add a remote computer in the scope of the script, click first on "Manage computer list…" button.



IIS Logs Analyzer - Remote computers management

This dialog allow you to add or remove remote computers from the script analysis scope.
By default, local computer is always part of the analysis scope.

If no "Shared Credentials" is defined, you can specify custom credentials per computer.
Please note that adding a remote computer locks the "Shared credentials" settings.

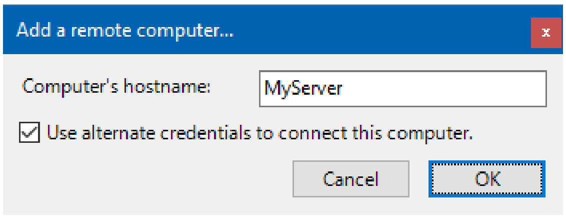
Computer		Custom credentials	
[redacted]	KO	OK ([redacted])	n/a

represents an unreachable remote computer.
represents a reachable remote computer.

authentication status for current user ([redacted]).
custom provided credentials and corresponding authentication status.
authentication status for defined "Shared Credentials".

Remote computers management window

In the appearing "Remote computers management" window, click on "**+**" button, then provide computer name in the next dialog box (see screenshot below).



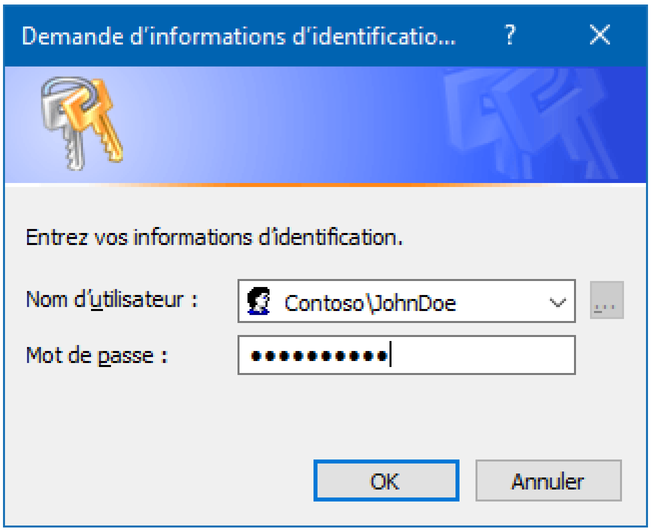
Add a remote computer…

Computer's hostname: MyServer

☑ Use alternate credentials to connect this computer.

Computer addition dialog

To define custom credentials, check the “Use alternate credentials to connect this computer.” option (only available if shared credentials were not previously activated), then provide your custom credentials in the authentication dialog (see screenshot below).



Demande d’informations d’identificatio...

Entrez vos informations d’identification.

Nom d’utilisateur : Contoso\JohnDoe

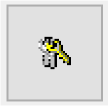
Mot de passe : ●●●●●●●●●●●

Authentication dialog (sorry, it’s in French!)

To remove a remote computer from script scope (and all its log directories and log files list), simply click on “-“ button.

To define custom credentials on one or more remote computers, highlight computers in the list, then click on credentials button (representing keys, see picture below).
This button is only available:

- When “Shared credentials” features were not previously activated
- For newly added remote computers (it is not possible to define credential for already discovered computers.



Credentials button

If one or more of the selected computers already have custom credentials defined, it will first clear the stored credentials, then you will have to click again on the button to define new credentials

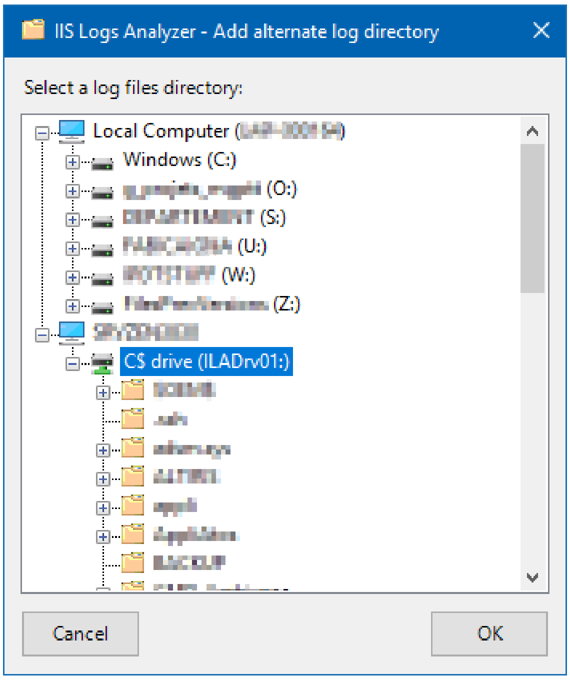
Provide your custom credentials in the authentication dialog.

The newly added computers will pass in the log directories discovering process on closing the “Remote computers management” window.

Be advice that this process can take a long time with some remote computers, particularly when there are lots of files and/or slow network performances.

6. How to add a specific log directory

If an IIS log directory was not discovered by the script's discovery process, you can add custom directory. To add a directory, click on "Add a log directory…" button, then browse the directory tree to select a directory (see screenshot, on next page).



IIS Logs Analyzer - Add alternate log directory

Select a log files directory:

- Local Computer ([redacted])
  - Windows (C:)
  - [redacted] (O:)
  - [redacted] (S:)
  - [redacted] (U:)
  - [redacted] (W:)
  - [redacted] (Z:)
- [redacted]
  - C$ drive (ILADrv01:)
    - [redacted]

Log directory selection dialog

This Log directory selection dialog shows all drives of the local computer and only C drive (mounted in a PSDrive) of the remote computers.

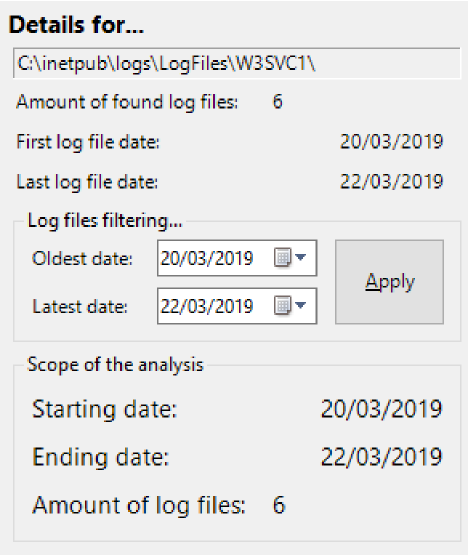
By selecting a directory, the script will try to discover first if the selected directory contains any "LogFiles" named folder and any W3SVC***x*** or FTPSVC***x*** or MSFTPSVC***x*** (where ***x*** is an instance ID) named log directory. If some are found, it will add all of them to its scope list, if not, the selected directory only will be added. Then, the script displays log files details (amount of IIS log files and first and last files dates) for newly discovered directories.

Targets and Analysis Scope

7. How to adjust date range of files to analyze

To adjust (reduce in most of cases) the date range of the analysis, the adjustment must be done directory by directory:

Highlight a directory in the left side list of the main window, then, in the right zone, adjust dates in Calendar pickers in “Log files filtering…” (see screenshot below).



Details for...

C:\inetpub\logs\LogFiles\W3SVC1\

Amount of found log files: 6

First log file date: 20/03/2019

Last log file date: 22/03/2019

Log files filtering...

Oldest date: 20/03/2019

Latest date: 22/03/2019

Scope of the analysis

Starting date: 20/03/2019

Ending date: 22/03/2019

Amount of log files: 6

Details on a selected directory

Once dates are defined, do not forget to click on “Apply” button.

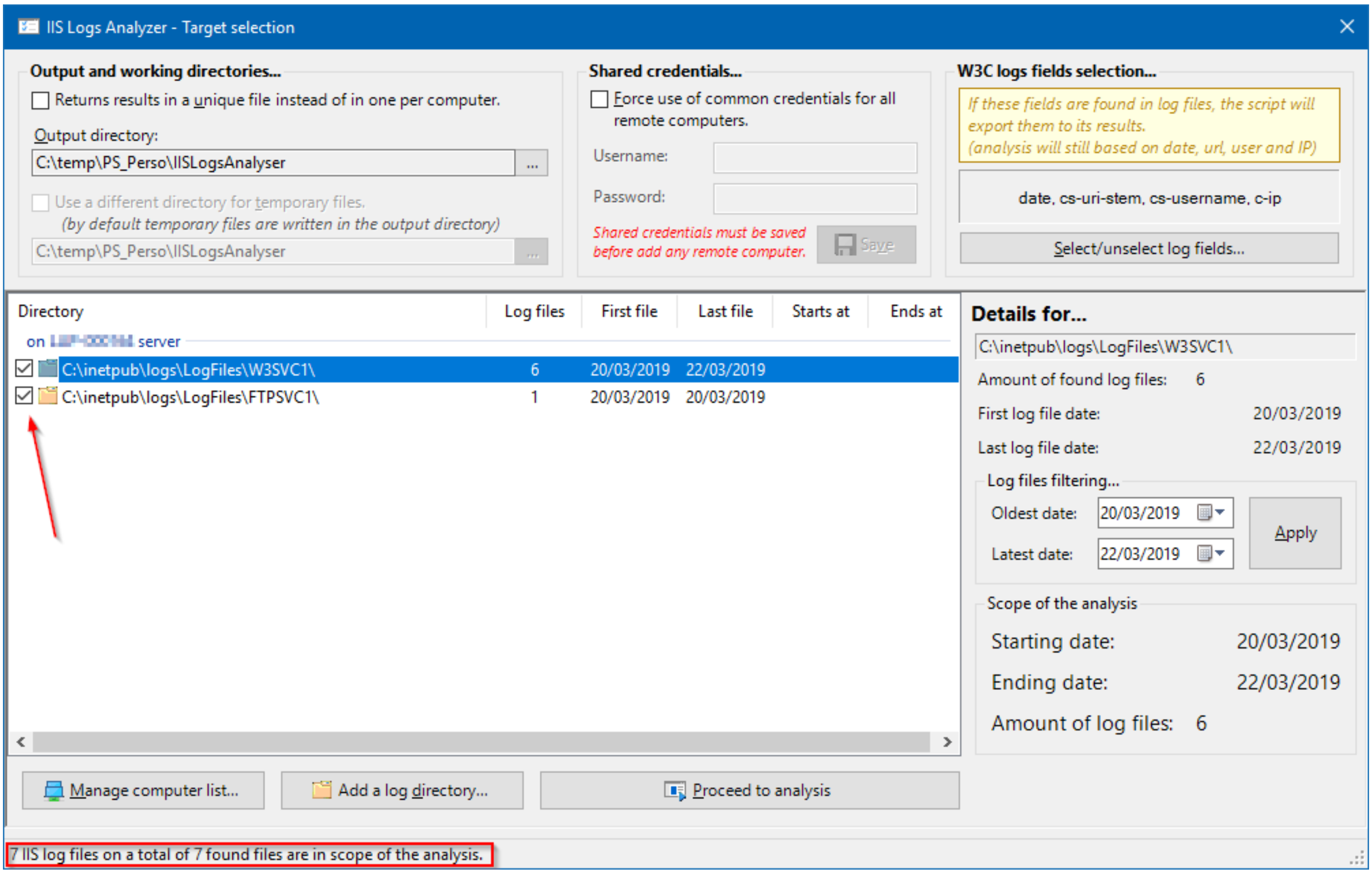
A “Clear” button took now the place of the “Apply” button.

The “Scope of the analysis” section shows you then the amount of log files which will be analyzed by the script.

To reset the date range limitation and selected back the whole of the IIS log files in the selected directory, click on the “Clear” button (only available when a date range is already applied on the selected directory).

8. How to change log directories selection

If you want to ignore a log directory and remove it from the scope of analysis of the script, simply uncheck checkbox beside the log directory name in the left side list (as shown by the red arrow in screenshot below).



IIS Logs Analyzer - Target selection

Output and working directories...

☐ Returns results in a unique file instead of in one per computer.

Output directory: C:\temp\PS_Perso\IISLogsAnalyser

☐ Use a different directory for temporary files.
(by default temporary files are written in the output directory)

C:\temp\PS_Perso\IISLogsAnalyser

Shared credentials...

☐ Force use of common credentials for all remote computers.

Username:

Password:

Shared credentials must be saved before add any remote computer.

W3C logs fields selection...

If these fields are found in log files, the script will export them to its results.
(analysis will still based on date, url, user and IP)

date, cs-uri-stem, cs-username, c-ip

Directory	Log files	First file	Last file	Starts at	Ends at
on [redacted] server					
☑ C:\inetpub\logs\LogFiles\W3SVC1\	6	20/03/2019	22/03/2019		
☑ C:\inetpub\logs\LogFiles\FTPSVC1\	1	20/03/2019	20/03/2019		

Details for...

C:\inetpub\logs\LogFiles\W3SVC1\

Amount of found log files: 6

First log file date: 20/03/2019

Last log file date: 22/03/2019

Log files filtering...

Oldest date: 20/03/2019

Latest date: 22/03/2019

Scope of the analysis

Starting date: 20/03/2019

Ending date: 22/03/2019

Amount of log files: 6

7 IIS log files on a total of 7 found files are in scope of the analysis.

IIS Logs Analyzer scope of analysis change

By adjusting date ranges and directories selection, the script shows you the amount of log files in the scope of its analysis on the total amount of found IIS log files.

Be advice than the analysis can take long time, so please be patient.