



Utilities

Framework NET Genium



Content

1 Backup directory	4
1.1 BackupServerService.exe.....	4
1.2 BackupServer.exe	4
1.3 FileBackup.exe	4
1.4 SqlBackup.exe	4
1.4.1 /bandwidth.....	5
1.4.2 /br	10
1.4.3 /datagridsettings.....	10
1.4.4 /deletedata	11
1.4.5 /deletelogs	11
1.4.6 /dirstats.....	12
1.4.7 /exportchanges	12
1.4.8 /exporttable.....	13
1.4.9 /find.....	14
1.4.10 /findattachment.....	14
1.4.11 /findselects.....	15
1.4.12 /findunsafetags.....	15
1.4.13 /importtable.....	15
1.4.14 /movegroups.....	17
1.4.15 /moveyear.....	17
1.4.16 /readdbfiles	17
1.4.17 /reademlfiles.....	17
1.4.18 /rebuildindexes	18
1.4.19 /remove.....	18
1.4.20 /removeunsafetags.....	18
1.4.21 /reorganizeindexes	18
1.4.22 /replace	18
1.4.23 /resetdatepickers	18
1.4.24 /rightsgroups	19
1.4.25 /run.....	19
1.4.26 /sysfind	19
1.4.27 /sysreplace	19

1.4.28	/unusedfiles	20
1.4.29	/unusedqueries	21
1.4.30	/unusedscripts.....	21
2	"Bin" directory	22
2.1	ApplicationManager.exe	22
2.2	FileUpload.exe	22
2.3	LogService.exe.....	23
2.4	OnlineUsers.exe.....	23
2.5	PrintPdf.exe	23
2.6	ResendEmlFiles.exe	24
2.7	Restart.exe	25
2.8	RunningQueries.exe	25
2.9	RunScript.exe	25
2.10	Setup.exe	26
2.11	Update.exe and FinishUpdate.exe.....	26
3	"Config\Tools" directory	29
3.1	Deactivate.exe	29
3.2	Activate.exe	29
3.3	GrantLogin.sql.....	29
3.4	GrantLogin.bat.txt	29
3.5	MemoryDumps.txt	29
3.6	SSL.reg	30
3.7	SSL-ie6.reg.....	32
3.8	TracingRequests.txt.....	34
3.9	TuningQueries.sql.....	34
3.10	TuningQueries.txt.....	34
3.11	WALTU.exe	35

1 Backup directory

More detailed information about the applications listed below is described in the separate “Backup” manual.

1.1 BackupServerService.exe

Service installed on the client station, intended for regular download of backups performed on the server by the “BackupServer.exe” program.

1.2 BackupServer.exe

Program run on the server manually or by a scheduled task, intended for backup:

- IIS server settings,
- setting up scheduled tasks,
- Firebird and MSSQL databases and
- directories.

1.3 FileBackup.exe

Program run on the server manually or by a scheduled task, intended for backup:

- IIS server settings,
- NET Genium and
- file attachments.

With the “/restore” switch, it also restores the backed up files and creates a “log” file in the current working directory with a list of files that have been restored and those that have not.

1.4 SqlBackup.exe

Program for backing up and restoring Firebird and MSSQL databases, and for performing a number of service operations using switches. Service operations are always performed in the current database defined in the “ConnectionString.txt” file. Each use of the command with parameters below generates text files with the extension “.log” in the location from which “SqlBackup.exe” is run, which contain a report on the operation of the application with the given parameter. These files are not overwritten with each use of the command, but are expanded. If the program is running and the parameters it requires are not specified for the relevant switch, the user will be asked for these parameters. All specifications of the switches and their parameters are case-sensitive, which means that uppercase and lowercase letters are taken into account.

- ❗ *Switches can also be specified when running the “SqlBackup.exe” program without a parameter. When the following screen appears, you need to enter the text of the switch, and confirm by pressing the “enter” key.*

```
NET Genium SQL Server Backup/Restore Utility
Copyright (C) NetGenium s.r.o. 2003-2013. All rights reserved.
Backup or restore (B/R/BALL/RALL/BTHIS/E/I/ET/IT)? _
```

i Information about processed logs is stored in "log" files.

p Example of information in the "log" file:

```
TABLE susers RECORD ID 1
* loginname: Administrator
```

Indicates that a record has been processed in the "susers" table that has ID 1 in this table. The processed value is "Administrator" in the "loginname" column.

1.4.1 /bandwidth

The "SqlBackup.exe" program, run with the "/bandwidth" parameter, reads all "log" files created by IIS logging and measures how NET Genium loads the internal computer network in which the NET Genium server is located. The result of the command is the calculation of the amount of data that flows through a given NET Genium after a certain time. To run the "SqlBackup.exe /bandwidth" command, you must have the "SqlBackup.exe" file copied to the directory where the log files created by IIS are located. In addition to the "Bandwidth.txt" file, which is created when the command is run, a summary of the results is displayed on the command line, from where it is possible to find out the total number of bytes, number of days and hours, number of bytes in 24 hours. Next, for each date, the time when the most bytes were transferred, the number of bytes transferred in peak time, and the bandwidth of the bandwidth are indicated.

l Use: "SqlBackup.exe /bandwidth"
Creates a "Bandwidth.txt" file located in the current working directory

```
Total bytes: 62,92 MB
Sent: 61,69 MB
Received: 1,23 MB

Total dates: 2 (2014-11-14 11:48:18 - 2014-11-18 09:56:52)
Total bytes per day: 31,46 MB

Total hours: 94
Total bytes per 24 hours: 16,04 MB

2014-11-14

Peak bytes per second: 10,35 MB
Peak time: 14:40
Peak bandwidth: 1,38 MBit/s

2014-11-18

Peak bytes per second: 356,31 kB
Peak time: 08:30
Peak bandwidth: 47,51 kBit/s
```



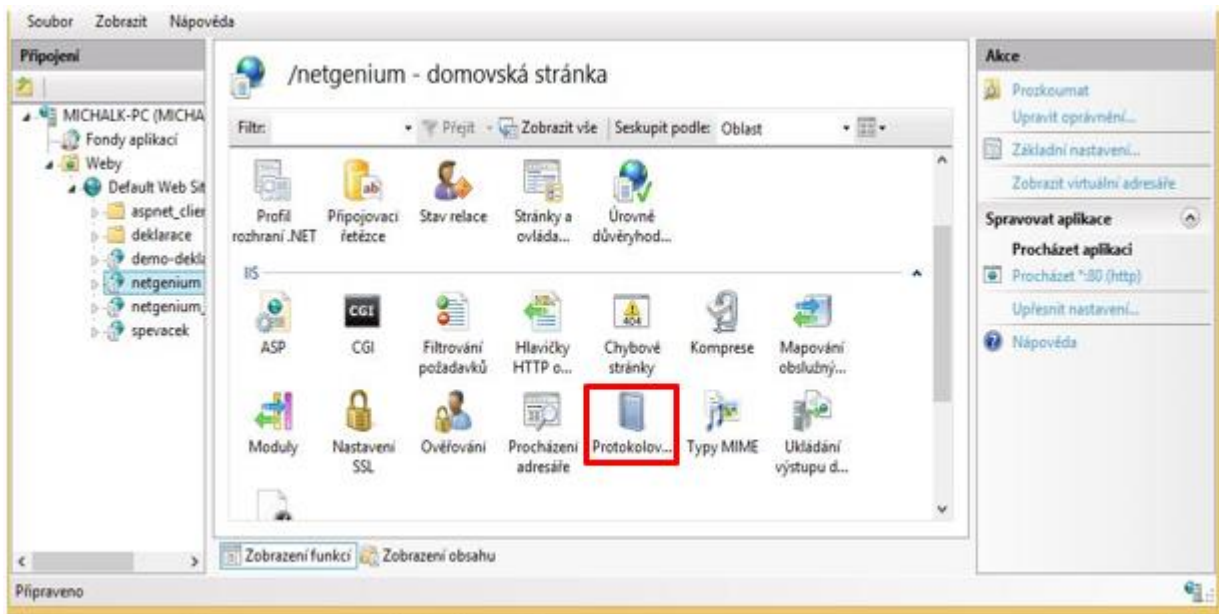
Bandwidth.txt

To create “log” files in IIS, you must enable and set “Logging”.

To turn on logging in IIS

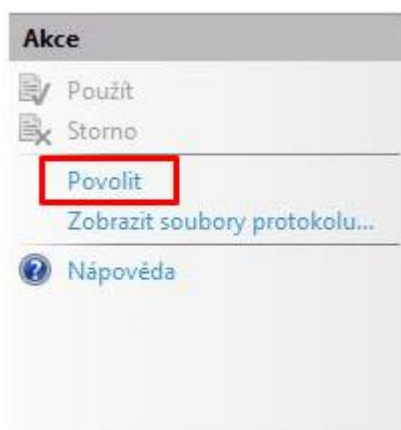
➔ Open the “Logging” function

- “Logging” can be set for both IIS and individual applications running in IIS. In both cases, the “Logging” function opens in the middle part of the “Internet Information Services Manager” window in the “IIS” section under the “Logging” button.

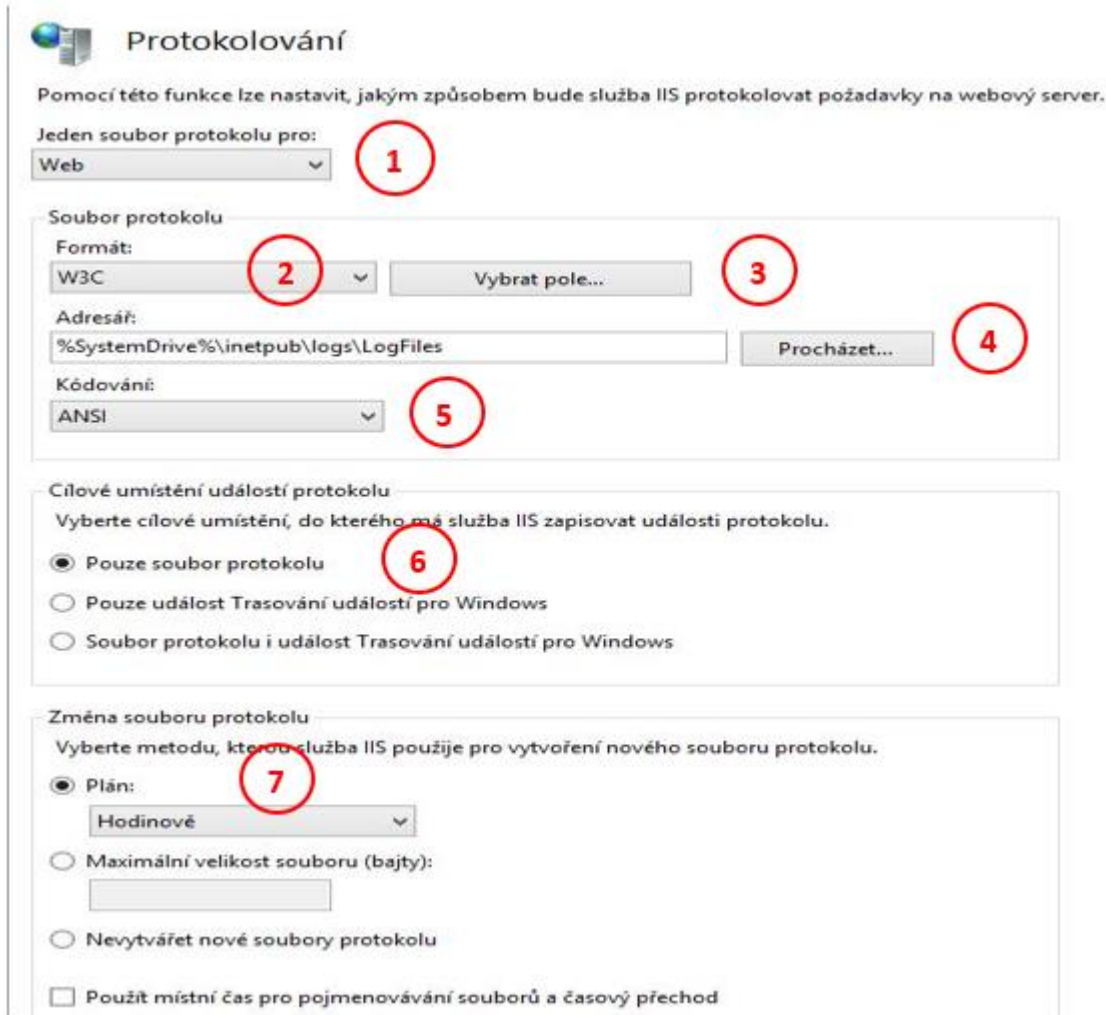


➔ Click the “Allow” button

- Pressing the “Enable” button ensures that the log file is written according to the settings.



Logging settings



Protokolování

Pomocí této funkce lze nastavit, jakým způsobem bude služba IIS protokolovat požadavky na webový server.

Jeden soubor protokolu pro: **1**
Web

Soubor protokolu

Formát: **2**
W3C **3** Vybrat pole...

Adresář:
%SystemDrive%\inetpub\logs\LogFiles **4** Procházet...

Kódování:
ANSI **5**

Cílové umístění událostí protokolu

Vyberte cílové umístění, do kterého má služba IIS zapisovat události protokolu.

6 Pouze soubor protokolu
 Pouze událost Trasování událostí pro Windows
 Soubor protokolu i událost Trasování událostí pro Windows

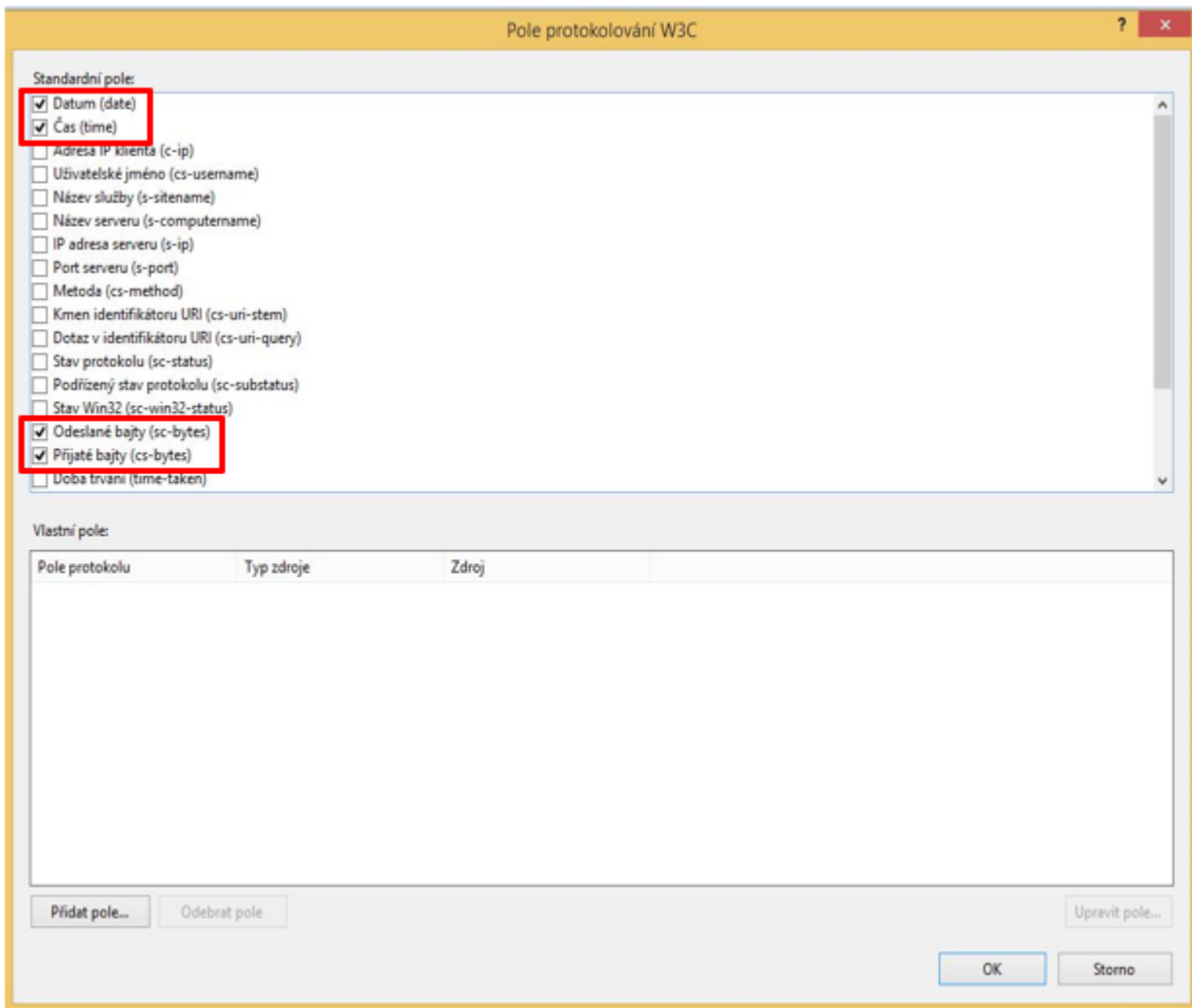
Změna souboru protokolu

Vyberte metodu, kterou služba IIS použije pro vytvoření nového souboru protokolu.

7 Plán:
Hodinové
 Maximální velikost souboru (bajty):

 Nevytvářet nové soubory protokolu
 Použít místní čas pro pojmenovávání souborů a časový přechod

- ↪ **1** – set the logging validity for “Web” as for the selected application from IIS
- ↪ **2** – set the log file format. You must select “W3C” for the “SqlBackup.exe /bandwidth” command. Other options:
 - “IIS”
 - “NCSA”
 - “Own”
- ↪ **3** – press the “Select field” button. Only selecting the “W3C” option will allow you to select a field in the log file. For the functionality of the command “SqlBackup.exe /bandwidth” it is necessary to select the fields “Date”, “Time”, “Sent bytes (sc-bytes)”, “Received bytes (cs-bytes)”.



- ↳ 4 – set the log file storage path. The default path is “% SystemDrive%\inetpub\logs\LogFiles”
- ↳ 5 – set the log file encoding. Options:
 - UTF – 8
 - ANSI
- ↳ 6 – set the destination for logging events
 - In addition to the defined log file, it is also possible to write “Logging” to the “Event tracing for Windows” event. However, for the analysis run by the “SqlBackup.exe /bandwidth” command, it is necessary to select the “Log file only” option.

↪ **7** – set the method of IIS writing to the log file. Select the “Schedule” option, which can be selected from the following options:

- “Hourly”
- “Daily”
- “Weekly”
- “Monthly”

1.4.2 /br

The “SqlBackup.exe” program run with the “/br” parameter backs up and restores the database defined in the “ConnectionString.txt” file. The reason for this operation is to reorganize the database file, free up shrinking space, and recreate all indexes on Firebird databases. For MSSQL databases, this operation is also possible, but it has no practical significance.

1.4.3 /datagridsettings

The “SqlBackup.exe” program run with the “/datagridsettings” parameter overrides the datagrid settings of all portal users according to the datagrid settings of the selected user. After starting the application with the command “/datagridsettings”, the user must fill in the login name of the user, according to whose datagrid settings the datagrid settings will be overwritten by other users.

```
NET Genium DataGrid Settings Utility
Copyright (C) NetGenium s.r.o. 2003-2016. All rights reserved.
Usage: SqlBackup.exe /datagridsettings [loginname] [dgid]
Type the login name: _
```

In addition, the user can choose from two types of profiles that specify the datagrids for which the settings will be overwritten:

- “All datagrids” – the settings of all datagrids in the portal will be overwritten
- “Type datagrid ID” – the settings of only the selected datagrid will be overwritten

```
NET Genium DataGrid Settings Utility
Copyright (C) NetGenium s.r.o. 2003-2016. All rights reserved.
Usage: SqlBackup.exe /datagridsettings [loginname] [dgid]
Type the login name: doubrava.jan
  1) All datagrids
  2) Type datagrid ID
Select profile: _
```

After that, the user is already shown a message whether the datagrid settings were overwritten. When overwriting the settings of individual datagrids for individual users, the default settings of the given datagrid are always overwritten.

```
NET Genium DataGrid Settings Utility
Copyright (C) NetGenium s.r.o. 2003-2016. All rights reserved.
Usage: SqlBackup.exe /datagridsettings [loginname] [dgid]
Type the login name: doubrava.jan
  1) All datagrids
  2) Type datagrid ID
Select profile: 2
Type the datagrid ID: 69
Please wait...
DataGrid settings finished successfully.
```

↩ Use: "SqlBackup.exe /datagridsettings [loginname] [dgid]"

1.4.4 /deletedata

The "SqlBackup.exe" program run with the "/deletedata" parameter deletes the contents of all tables in the database except the "susers", "susergroups", "slayout" and "sholiday" tables.

↩ Use: "SqlBackup.exe /deletedata"

1.4.5 /deletelogs

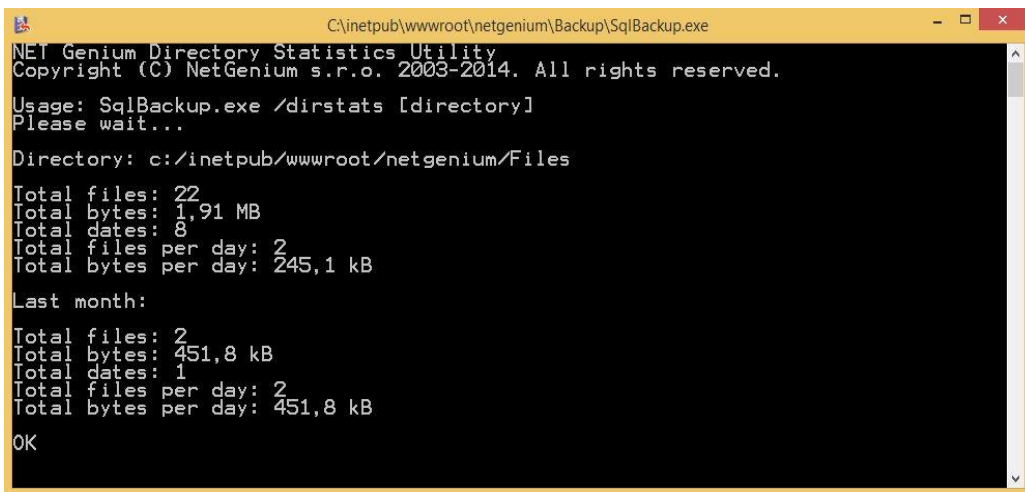
The "SqlBackup.exe" program, run with the "/deletelogs" parameter, deletes the contents of the "stables_stats", "sviewpages_stats", "squerybuilder_stats", "snggef_stats" and "sngscript_stats" log tables, and deletes the log files located on the "Logs\yyyy-mm-dd" subdirectorie.

↩ Use: "SqlBackup.exe /deletelogs [createdbeforeindays]"

1.4.6 /dirstats

The "SqlBackup.exe" program, run with the "/dirstats" parameter, determines the total size and number of files that have been created to date in that directory. If the command is run without a parameter, the size and number of files are calculated for the current directory. If a parameter is entered (path to the required directory), the size and number of files are calculated for the specified directory. The report itself displays the calculated data first for the entire directory and then for the files created in the last month.

Use: "SqlBackup.exe /dirstats [directory]"



```
C:\inetpub\wwwroot\netgenium\Backup\SqlBackup.exe
NET Genium Directory Statistics Utility
Copyright (C) NetGenium s.r.o. 2003-2014. All rights reserved.
Usage: SqlBackup.exe /dirstats [directory]
Please wait...
Directory: c:\inetpub\wwwroot\netgenium\Files
Total files: 22
Total bytes: 1,91 MB
Total dates: 8
Total files per day: 2
Total bytes per day: 245,1 kB
Last month:
Total files: 2
Total bytes: 451,8 kB
Total dates: 1
Total files per day: 2
Total bytes per day: 451,8 kB
OK
```

1.4.7 /exportchanges

The "SqlBackup.exe" program run with the "/exportchanges" parameter exports a list of all data differences between the current database defined by the "ConnectionString.txt" file in the "Config" directory and the other database whose "connection string" is entered after starting the program "SqlBackup.exe" with the "/exportchanges" parameter.

1.4.8 /exporttable

The "SqlBackup.exe" program run with the "/exporttable" parameter exports the database structure of the selected table and all data stored in the selected table. The exported table can be defined in the following ways:

By selecting from the list of user tables that the program "SqlBackup.exe" finds in the NET Genium database

```
NET Genium Table Export Utility
Copyright (C) NetGenium s.r.o. 2003-2016. All rights reserved.

Usage: SqlBackup.exe /exporttable [name]

  1) Select table from list
  2) Type table name
  3) Type query

Select profile: 1

  1) mon$attachments
  2) mon$call_stack
  3) mon$context_variables
  4) mon$database
  5) mon$io_stats
  6) mon$memory_usage
  7) mon$record_stats
  8) mon$statements
  9) mon$transactions
 10) ng_akce
 11) ng_akce_history
 12) ng_aktivitanewslett
 13) ng_aktivitanewslett_history
 14) ng_aktivitasync
 15) ng_aktivitasync_history
 16) ng_aktivitawebu
 17) ng_aktivitawebu_history
 18) ng_bankovniucet
 19) ng_bankovniucet_history
 20) ng_bankovnivypis
 21) ng_bankovnivypis_history
 22) ng_bankuhrada
```

By inserting the database identifier of the table

```
NET Genium Table Export Utility
Copyright (C) NetGenium s.r.o. 2003-2016. All rights reserved.

Usage: SqlBackup.exe /exporttable [name]

  1) Select table from list
  2) Type table name
  3) Type query

Select profile: 2
Type the table name: ng_akce_
```

By inserting an SQL query

```
NET Genium Table Export Utility
Copyright (C) NetGenium s.r.o. 2003-2016. All rights reserved.
Usage: SqlBackup.exe /exporttable [name]
  1) Select table from list
  2) Type table name
  3) Type query
Select profile: 3
Type the query: SELECT id FROM ng_akce_
```

For the last two options, you must specify the correct table identifiers, otherwise an error will be returned when exporting the table. For the first two options, all columns and data are exported. In the third option, it is possible to limit the number of exported columns from the database structure of the table as well as the number of exported data (SQL query condition).

↩ *Use: "SqlBackup.exe /exporttable"*
Creates an XML file located in the same directory as the "SqlBackup.exe" program, in the name of which the table export date and the table name are specified (eg "2016-10-31-ng_action")

1.4.9 /find

The "SqlBackup.exe" program run with the "/find" parameter searches the string specified by the parameter in all text columns of all user tables. The exact match of the value in the given column with the specified parameter is searched for, not a substring.

↩ *Use: "SqlBackup.exe /find value"*
Creates a "Find.log" file located in the same directory as the "SqlBackup.exe" program

1.4.10/findattachment

The "SqlBackup.exe" program run with the "/findattachment" parameter searches for the use of the file attachment specified by the parameter – its ID. The command returns all occurrences (tables) in which the searched file attachment is located. The search is performed in the following places:

- "image" column in the "sappgroups" table
- "def" column in the "sviewfields" table for "RichText" controls
- "val" column in the "scolumns" table for "RichText" controls
- "value" column in the "schat" table
- In all user tables in columns of type "File" or "Image", or in columns of type "RichTextBox" if the user confirms that he should search in these columns

↩ *Use: "SqlBackup.exe /findattachment value"*
Creates a "FindAttachment.log" file located in the same directory as the "SqlBackup.exe" program



FindAttachment.log

1.4.11/findselects

The "SqlBackup.exe" program run with the "/findselects" parameter searches for SQL queries starting with the "SELECT" clause in all files (typically logs) in the directory specified by the "directory" parameter.

↩ Use: "SqlBackup.exe /findselects directory"
Creates a "FindSelects.log" file located in the same directory as the "SqlBackup.exe" program

1.4.12/findunsafetags

The "SqlBackup.exe" program, run with the "/findunsafetags" parameter, searches the database for any dangerous tags that may have been created by the database, such as SQL Injection. NET Genium itself is secure against SQL Injection, but the weak point may be web applications connected to the NET Genium database.

↩ Use: "SqlBackup.exe /findunsafetags"
Creates the "FindUnsafeTags.log" and "FindUnsafeTags_Trash.log" files located in the same directory as the "SqlBackup.exe" program, where all dangerous tags are listed

1.4.13/importtable

The "SqlBackup.exe" program run with the "/importtable" parameter imports the contents of the database table into NET Genium. The imported table is selected from the list of XML files that the "SqlBackup.exe" program finds in the "Backup" directory.

```
NET Genium Table Import Utility
Copyright (C) NetGenium s.r.o. 2003-2016. All rights reserved.
Usage: SqlBackup.exe /importtable
  1) 2016-10-31-ng_akce.xml
Select table to restore:
```

The "SqlBackup.exe" application also displays a menu to the user, from which the user chooses whether to import the selected table directly or to perform an import test of the selected table first. The result of the test is a file with the extension ".sql" and with the same name as the name of the imported file, which contains a list of all SQL queries necessary for importing the contents of the database table.

```
NET Genium Table Import Utility
Copyright (C) NetGenium s.r.o. 2003-2016. All rights reserved.
Usage: SqlBackup.exe /importtable
  1) 2016-10-31-ng_akce.xml
Select table to restore: 1
  1) Import table
  2) Import table (test)
Select profile:
```

After selecting the import profile, the "SqlBackup.exe" program will ask the user:

- if all records found in the database in the table corresponding to the identifier of the imported table are to be deleted first, and if not, then
 - if the import will include at least 1 "INSERT" query,
 - if the import will include at least 1 "UPDATE" query,
 - and if the import includes at least 1 "INSERT" query, whether records with the same ID as the records contained in the import XML file ("DELETE") should be deleted,
- and whether to disable all indexes located in the imported table before starting the import.

```
NET Genium Table Import Utility
Copyright (C) NetGenium s.r.o. 2003-2016. All rights reserved.
Usage: SqlBackup.exe /importtable
  1) 2016-10-31-ng_akce.xml
Select table to restore: 1
  1) Import table
  2) Import table (test)
Select profile: 2
DELETE all records from the table (Y/N)? y
DISABLE all indexes on the table (Y/N)? y_
```

```
NET Genium Table Import Utility
Copyright (C) NetGenium s.r.o. 2003-2016. All rights reserved.
Usage: SqlBackup.exe /importtable
  1) 2016-10-31-ng_akce.xml
Select table to restore: 1
  1) Import table
  2) Import table (test)
Select profile: 2
DELETE all records from the table (Y/N)? n
INSERT any records (Y/N)? n
UPDATE any records (Y/N)? y
DISABLE all indexes on the table (Y/N)? y
```


- ↩ *Use: "SqlBackup.exe /importtable"*
Creates a "ImportTable.log" file located in the same directory as the "SqlBackup.exe" program



ImportTable.log

1.4.14/movegroups

The "SqlBackup.exe" program run with the "/movegroups" parameter rennumbers all user groups except the "Administrators" (ID 1) and "Users" (ID 2) user groups. The command adds the number specified in the parameter to the user group ID. It is also possible to insert negative values into the parameter – renumbering downwards. If the user group has a newly calculated ID of less than 2, the command returns an interrupt and the renumbering is not performed. The command also scans all rights tables, javascripts ("jsUserInGroup" function) and scripts ("USERSINGROUP", "TEFUIG" and "TESUIG" functions) and sets new user group IDs in them.

- ↩ *Use: "SqlBackup.exe /movegroups number"*
Creates a "MoveGroups.log" file located in the same directory as the "SqlBackup.exe" program



MoveGroups.log

1.4.15/moveyear

The "SqlBackup.exe" program run with the "/moveyear" parameter moves the year in all date columns of all user tables and in all text columns of all user tables where the date occurrence is found. The change will not be made for the "sholiday", "sinvalidlogins", "sstatistics" and "ssynchro" tables. The command adds the number of years specified as a parameter to each date. It is also possible to insert negative values into the parameter – renumbering downwards.

- ↩ *Use: "SqlBackup.exe /moveyear numberofyears"*
Creates a "MoveYear.log" file located in the same directory as the "SqlBackup.exe" program



MoveYear.log

1.4.16/readdbffiles

The "SqlBackup.exe" program run with the "/readdbffiles" parameter analyzes all "dbf" files in the directory in which the program is run and creates a detailed report for each "dbf" file with the contents of the "dbf" file.

- ↩ *Use: "SqlBackup.exe /readdbffiles [directory]"*

1.4.17/reademlfiles

The "SqlBackup.exe" program run with the "/reademlfiles" parameter analyzes all "eml" files in the directory in which the program is run and creates a detailed report for each "eml" file with the contents of the "eml" file.

- ↩ *Use: "SqlBackup.exe /reademlfiles [directory]"*

1.4.18/rebuildindexes

The "SqlBackup.exe" program run with the "/rebuildindexes" parameter defragments all indexes whose percentage fragmentation is greater than or equal to the value of the "fragmentationthreshold" parameter. Index rebuilding is recommended in cases where index fragmentation is greater than 30%.

↩ *Use: "SqlBackup.exe /rebuildindexes fragmentationthreshold"*
Creates a "RebuildIndexes.log" file located in the same directory as the "SqlBackup.exe" program

1.4.19/remove

The "SqlBackup.exe" program run with the "/remove" parameter looks for the string specified by the parameter in all text columns of all user tables, and replaces it with an empty string. To find a string, it is not necessary to exactly match the value in the given column with the specified parameter, it can also be a substring.

↩ *Use: "SqlBackup.exe /remove value"*
Creates a "Remove.log" file located in the same directory as the "SqlBackup.exe" program

1.4.20/removeunsafetags

The "SqlBackup.exe" program run with the "/removeunsafetags" parameter removes from the database all dangerous tags that could have been created by infecting the database, for example using SQL Injection. NET Genium itself is secure against SQL Injection, but the weak point may be web applications connected to the NET Genium database.

↩ *Use: "SqlBackup.exe /removeunsafetags"*
Creates a "RemoveUnsafeTags.log" file located in the same directory as the "SqlBackup.exe" program

1.4.21/reorganizeindexes

The "SqlBackup.exe" program run with the "/reorganizeindexes" parameter defragments all indexes whose percentage fragmentation is greater than or equal to the value of the "fragmentationthreshold" parameter. Index reorganization is recommended in cases where index fragmentation is less than 30%.

↩ *Use: "SqlBackup.exe /reorganizeindexes fragmentationthreshold"*
Creates a "ReorganizeIndexes.log" file located in the same directory as the "SqlBackup.exe" program

1.4.22/replace

The "SqlBackup.exe" program run with the "/replace" parameter searches for the string specified by the first parameter in all text columns of all user tables, and replaces it with the string specified by the second parameter. The exact match of the value in the given column with the specified parameter is searched for.

↩ *Use: "SqlBackup.exe /replace oldvalue newvalue"*
Creates a "Replace.log" file located in the same directory as the "SqlBackup.exe" program

1.4.23/resetdatepickers

The "SqlBackup.exe" program run with the "/resetdatepickers" parameter resets the "From" filter to the default settings in all datagrids or charts with a date range filter.

↩ *Use: "SqlBackup.exe /resetdatepickers"*

1.4.24/rightsgroups

The "SqlBackup.exe" program running with the "/rightsgroups" parameter attempts to assign an existing authorization group entry to each user on the system based on its defined user groups. If the application cannot find a matching permission group record, the application creates a new permission group record. This newly created permission group will have the same name and user groups as the user.

↩ *Use: "SqlBackup.exe /rightsgroups"*

1.4.25/run

The "SqlBackup.exe" program run with the "/run" parameter executes all the commands listed in the file that is specified as the "file" parameter. It is typically used in conjunction with "/unusedfiles" and "/unusedqueries" – the file name is given as a parameter.

↩ *Use: "SqlBackup.exe /run file"*

Creates a "Run.log" file located in the same directory as the "SqlBackup.exe" program

The "file" parameter can also be a log file that contains "SELECT" statements. All these commands will be run again, and the output file "Run.log" will record both the line from the original file and the result of the local execution of the query – the time of evaluation of the SQL query and the number of records returned.

❗ *The "file" parameter can be specified as:*

- File name itself (located in the same directory as the "SqlBackup.exe" program)
- Relative path to a file on disk (watch out for scheduled tasks that run in the "Windows")
- Absolute path to the file on disk

1.4.26/sysfind

The "SqlBackup.exe" program run with the "/sysfind" parameter looks for the string specified by the parameter in all text columns of all system and user tables. To find a string, it is not necessary to exactly match the value in the given column with the specified parameter, it can also be a substring.

↩ *Use: "SqlBackup.exe /sysfind value"*

Creates a "SysFind.log" file located in the same directory as the "SqlBackup.exe" program

1.4.27/sysreplace

The "SqlBackup.exe" program, run with the "/sysreplace" parameter, finds the string specified by the first parameter in all text columns of all system and user tables, and replaces it with the string specified by the second parameter. To find a string, it is not necessary to exactly match the value in the given column with the specified parameter, it can also be a substring.

↩ *Use: "SqlBackup.exe /sysreplace oldvalue newvalue"*


Creates a "SysReplace.log" file located in the same directory as the "SqlBackup.exe" program

1.4.28/unusedfiles

The “SqlBackup.exe” program, run with the “/unusedfiles” parameter, looks for:

- Orphaned files in the “Files” folder that are not referenced in the “sfiles” database table – STANDALONE UNUSED FILES section.
- Database records in the “sfiles” table and the corresponding files in the “Files” folder, which are not used anywhere in the system – UNUSED FILES section.
- Invalid references in user tables that reference non-existent database records in the “sfiles” table – MISSING ENTRIES IN 'SFILES' TABLE section.
- Database records in the “sfiles” table whose files do not physically exist on the disk – section MISSING FILES IN 'NETGENIUM/FILES' DIRECTORY.

In addition to the log file, the “SqlBackup.exe” program (run with the “/unusedfiles” parameter) can also create a “UnusedFiles” directory in the current location of the “SqlBackup.exe” program, where copies of found files from the UNUSED FILES section will be stored. The optional “copyfiles” parameter must be specified to run this function (“SqlBackup.exe /unusedfiles /copyfiles”).

 *Use: “SqlBackup.exe /unusedfiles” followed by “SqlBackup.exe /run UnusedFiles.log”
Creates a “UnusedFiles.log” file located in the same directory as the “SqlBackup.exe” program*

 *Example content:*

```
// STANDALONE UNUSED FILES

DELETE FILE 0.zip

// UNUSED FILES

// mail-ico-facebook.gif
DELETE FROM sfiles WHERE id = 19596
DELETE FILE 19596.gif

// MISSING ENTRIES IN 'SFILES' TABLE


// SELECT ng_comment FROM ng_task WHERE id = 2831

// MISSING FILES IN 'NETGENIUM/FILES' DIRECTORY

// SELECT ng_attachment1 FROM ng_crmdocument_history WHERE id = 499// 22-7 Offer
```

1.4.29/unusedqueries

The "SqlBackup.exe" program run with the "/unusedqueries" parameter searches for all unused SQL queries stored in the "squerybuilder" table. To delete unused SQL queries, it is necessary to call the command "SqlBackup.exe /run file", where the created log file "UnusedQueries.log" will be inserted as a parameter.

 Use: "SqlBackup.exe /unusedqueries" followed by "SqlBackup.exe /run UnusedQueries.log"
Creates the "UnusedQueries.log" file located in the same directory as the "SqlBackup.exe" program



UnusedQueries.log

1.4.30/unusedscripts

The "SqlBackup.exe" program, run with the "/unusedscripts" parameter, finds and deletes all unused records stored in the "sngscript" table.

 Use: "SqlBackup.exe /unusedscripts"

2 “bin” directory

2.1 ApplicationManager.exe

A program designed for importing and exporting applications to and from NET Genium. By default, applications are exported to an “xml” file, which can be large (even several GB) depending on the size of the application and the amount of user data. “ApplicationManager.exe” is used to export or import these large applications – if the export or import was performed from the NET Genium web interface, it could happen that the IIS web server cannot accept (upload) such a file, or subsequently process or application. import. For this reason, it is much more efficient to use the “ApplicationManager.exe” application.

2.2 FileUpload.exe

A program designed for regular uploading of individual files or entire directories to a remote server on which NET Genium with the “FileUpload” application is installed. This application consists of a file transfer interface (this interface is a standard part of every NET Genium), as well as the “FileUpload Document” edit form and the “FileUpload Documents” view page. Neither the edit form nor the view page is a standard part of NET Genium, so they need to be imported first. For this purpose, the file “FileUpload.nga” is prepared in the “Install” directory, which can be imported into any application group as a normal application.

Each individual file or the entire directory uploaded to the server must have a separate profile created in NET Genium – an entry in the “FileUpload Document” table. This profile includes the name of the transferred file and the password for its transfer. We transfer entire directories to the server by first packing them in a “zip” archive, and then transfer it to the server – of course if it has the appropriate profile created, and it is chosen for this profile that the file should be unzipped after transfer to the server.

If we run the program “FileUpload.exe” in any directory on the disk, the contents of the current directory will be compared with all profiles defined in the table “Document FileUpload”, and then we will be prompted to confirm the transfer of those files that have a profile created by their name in NET Genium.

“FileUpload.exe” requires a remote NET Genium URL and a file transfer password each time you run it.

These two parameters can be passed to the program in three ways:

- by calling the program “FileUpload.exe” with two parameters “URL” and “Password”, which are separated by a space (even the password itself can contain spaces), eg “FileUpload.exe https://www.netgenium.com/netgenium password transfer”,
- by creating the text file “FileUpload.ini” in the root directory on the disk from which we run the program “FileUpload.exe”, which on the first line contains the URL of the remote NET Genium, and on the second line the password for the transfer,
- by manually entering the URL and password for the transfer directly in the running program “FileUpload.exe” (which is very impractical when running the program frequently).


The “FileUpload.exe” program can package the entire directory into a “zip” archive using the “-Z” parameter, followed by the archive name without a space after “-Z” and also without the “.zip” extension at the end.

“FileUpload.exe” packages one of the following directories based on its location on disk:

- the entire parent directory if we are in the “bin” or
- only the directory in which we are located, unless it is a “bin” directory.

The “FileUpload.exe” program can also automatically delete all files that have been successfully uploaded to the server.

To enable this function, the “/D” parameter must be selected.

 *Examples:*


```
FileUpload.exe https://www.netgenium.com/netgenium password for transmission
FileUpload.exe/Zarchivename https://www.netgenium.com/netgenium password for transmission
FileUpload.exe/Zarchivename
```

2.3 LogService.exe

Program designed for logging successfully executed programs/services to the database table “ng_windowsservice”. The program is mainly used for scheduled batch file execution using scheduled Windows tasks. The service name is defined by the “ServiceName” parameter – under this name the service is logged into the database. The default interval after which the service should start again is set by the “IntervalInMinutes” parameter. It is possible to pass the text string “%errorlevel%” to the optional parameter “ErrorLevel”, which is a variable available in any “bat” file and which returns the current error code. If “LogService.exe” detects that this code is anything other than 0, it does not log the service.

 *Use:*

```
LogService.exe ServiceName IntervalInMinutes [ErrorLevel]
```

 *Example “bat” file:*

```
xcopy/D/H/E "D:\inetpub\wwwroot\netgenium" \\NAS-NETGenium\Files
LogService.exe BackupFiles 1440 %errorlevel%
```

2.4 OnlineUsers.exe

A program designed to evaluate a list of users who are online – with the last page visited in the last hour.

 *Creates the “OnlineUsers.log” file in the “Logs” directory and opens this file at the same time*

2.5 PrintPdf.exe

A program designed to print a record to a PDF print template. The program accepts the parameters “Button ID” (ID of the button located in the edit form) and “Record ID” (ID of the record in the database).

2.6 ResendEmlFiles.exe

A program designed to search for all “eml” files in the “Logs” directory, and then send them using an SMTP server. E-mails are saved in this directory automatically if there is any problem with sending them from the NET Genium environment, eg due to high SMTP server load or poor connectivity.

- After a successful e-mail, the corresponding “eml” file is deleted from the “Logs” directory.
- If the e-mail(s) cannot be sent again by “ResendEmlFiles.exe”, they will remain unchanged in the “Logs” directory, and an e-mail will be sent to the portal administrator with a list of failed files.

It is common to run “ResendEmlFiles.exe” as a scheduled Windows task. The scheduled task can be created either manually or automatically using the “Setup.exe” program, or by running the “ResendEmlFiles.exe” program with the “-task” parameter.

The program “ResendEmlFiles.exe” also allows you to search for and send all “eml” files from all NET Genies located on the server. As part of resending email messages, it is possible to send “eml” files from all NET Genies at once or only from selected NET Genies. Definitions from which NET Geniums will be resent “eml” files are given in the configuration file “ResendEmlFiles.exe.config”, which is located in the same directory as “ResendEmlFiles.exe”.

```
<configuration>
  <appSettings>

    <add key="ngdirs" value="D:\inetpub\wwwroot"/>
    <add key="ngdir" value="E:\inetpub\wwwroot\netgenium1"/>
    <add key="ngdir" value="E:\inetpub\wwwroot\netgenium2"/>

  </appSettings>
</configuration>
```

The “ngdirs” parameter specifies the directory on the disk where multiple NET Genies are stored. “ResendEmlFiles.exe” will find all NET Geniums in this directory, and will try to resend all “eml” files from the “Log” directory. Except for those who have the file “SkipResendEmlFiles.txt” located in the “Config” directory (it does not matter its content).

The “ngdir” parameter specifies the directory on the disk in which one specific NET Genium is stored, from the “Logs” directory of which the “ResendEmlFiles.exe” program will try to resend all e-mail messages.

The “ResendEmlFiles.exe” program must be placed together with other required files in a separate directory on the disk, eg in the “D:\ResendEmlFiles” directory. The following files are a necessary part of the “ResendEmlFiles” directory for the correct functionality of resending “eml” files from multiple NET Genies:

- “ResendEmlFiles.exe”,
- “ResendEmlFiles.exe.config” and
- “NETGeniumConnection.dll”.

When resending e-mails, the "ResendEmlFiles.log" log file is supplemented with a list of all NET Geniums that were listed in the "ResendEmlFiles.exe.config" configuration file.

- If e-mail messages from a given NET Genium are successfully resent, the log file "ResendEmlFiles.log" shows "OK" next to the path to the given NET Genium.
- If the NET Genium was found due to the "ngdirs" parameter and also contains the "SkipResendEmlFiles.txt" file in the "Config" directory, the "ResendEmlFiles.log" log file shows "SKIP" next to the path to the NET Genium.

2.7 Restart.exe

Program designed to restart NET Genium. This is accomplished by creating or deleting a "Restart.txt" file in the "bin" directory – it takes advantage of the IIS feature that any change to the contents of the "bin" directory will result in a restart of the web application.

2.8 RunningQueries.exe

A program designed to evaluate a list of currently processed database queries.

↩ *Creates the "RunningQueries.htm" file in the "Logs" directory, and opens this file at the same time*

2.9 RunScript.exe

A program designed to run a script specified using a control ID – a button located solely on the view page. The optional parameter "UserID" represents the ID of the user under whose login name the script will run. If the optional parameter is not specified, the script will run under an anonymous user.

↩ *Use: "RunScript.exe<ID> [<UserID>]"*

The "RunScript.exe" program is mainly used in scheduled tasks. The scheduled task can be created either manually or using the "Setup.exe" program, which automatically creates a scheduled task with the following parameters based on the specified control ID:

- in the "NET Genium" folder,
- in a subfolder named after the portal,
- with the name of the scheduled task, which is derived from the name of the button,
- at the specified time – the default time is set to "06:00",
- optionally with set repetition twice per hour – at 30 minute intervals for 18 hours.

↩ *When creating a scheduled task manually, the "Program or script" field must contain the full path to the "RunScript.exe" program on the computer disk, the "Add arguments (optional)" field must contain the control ID and optionally a space and user ID. The "Run in (optional)" field does not need to be filled out.*

2.10 Setup.exe

A program designed to install NET Genium, which allows:

- Create a virtual directory
- Authorize the NetworkService user account to write to the NET Genium directory
- Create a database
 - Firebird
 - MSSQL
- Authorize the NetworkService user account to access the MSSQL database
- Create a scheduled task for BackupServer.exe (server backup)
- Create a scheduled task for SqlBackup.exe (database backup)
- Create a scheduled task for FileBackup.exe (attachment backup)
- Create a scheduled task for Update.exe (update)
- Create a scheduled task for ResendEmlFiles.exe
- Create a scheduled task for RunScript.exe
- Create a scheduled task for RunScript.exe
 - "Setup.exe" is the recommended method for creating scheduled tasks associated with the execution of button scripts located on viewing pages or in editing forms.
 - In the dialog of the "Setup.exe" program there are input fields for
 - Button ID,
 - time of the scheduled task run,
 - and the "2x/h" checkbox, which defines that the scheduled task will be run periodically 2x per hour for 18 hours.

Scheduled tasks created by the "Setup.exe" program can also be manually set directly in the "Task Scheduler":

- All scheduled tasks are created in all "NET Genium" that already exists or "Setup.exe" already creates
- Scheduled jobs are set to run in the context of the user account "SYSTEM" with the highest privileges

2.11 Update.exe and FinishUpdate.exe

The "Update.exe" program is intended for updating NET Genium to its latest version. Automatically updates to:

- latest full version or
- the latest test version, if the "Tester.txt" file is present in the "Config" directory (it does not matter its contents).

The file with the latest version of NET Genium is always first searched in the "Update" directory – "netgenium4.zip" for the full version and "netgenium4t.zip" for the test version. If this file does not exist in the "Update" directory, it will be automatically downloaded from the NetGenium website.

It is also possible to run the "Update.exe" program as a scheduled Windows task, thus ensuring a regular daily update of NET Genium, typically performed at night. However, "Update.exe" must be run by the task scheduler with the "-j" parameter – this is a fully automated update that does not require user confirmation. The scheduled task can be created either manually or automatically using the "Setup.exe" program, or by running the "Update.exe" program with the "-task" parameter.

```
rem Running an automated update that does not require user confirmation
Update.exe -j

rem Automatic creation of a scheduled task
Update.exe -task
```

When the update is complete, the “FinishUpdate.exe” program starts automatically, which:

- updates the “Web.config” file in the NET Genium root directory according to the various settings located in the configuration files,
- copies the “FileUpload.exe” program to the Windows system directory – this ensures that the program can be run from the command line without having to specify a path to it,
- deletes the old “Update.exe” and the “NETGeniumConnection.dll” library, and replaces them with the new versions located under the provisional names “Update.new” and “NETGeniumConnection.new”.

The second area where you can use the “Update.exe” program is a bulk update of NET Genium, which is located on the server. As part of a bulk update, it is possible to update all NET Geniums at once or only selected NET Geniums. The definition that will be updated by NET Genium is listed in the configuration file “Update.exe.config”, which is located in the same directory as “Update.exe”.

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <appSettings>

    <add key="dir" value="D:\inetpub\wwwroot\www.netgenium.com\Download"/>

    <add key="ngdirs" value="D:\inetpub\wwwroot"/>
    <add key="ngdir" value="E:\inetpub\wwwroot\netgenium1"/>
    <add key="ngdir" value="E:\inetpub\wwwroot\netgenium2"/>

    <add key="nointernet" value="false"/>

  </appSettings>
</configuration>
```

- The “dir” parameter indicates the path to the directory with the latest versions of NET Genium – to the directory with the “netgenium4.zip” and “netgenium4t.zip” files. The “dir” parameter can only be used on the NetGenium production server, where the archives with the new versions are distributed.
- The “ngdirs” parameter specifies the directory on the disk where multiple NET Geniums are stored. The “Update.exe” program finds all NET Geniums in this directory and updates it. Except for those who have the file “SkipUpdate.txt” located in the “Config” directory (it does not matter its contents).
- The “ngdir” parameter specifies the directory on the disk in which one specific NET Genium is stored, which the “Update.exe” program will update.
- The “nointernet” parameter indicates that the Internet is not available on the server and that updates will always be performed from the “netgenium4.zip” and “netgenium4t.zip” files stored in the current directory together with the “Update.exe” program.

The "Update.exe" program must be placed together with other required files in a separate directory on the disk, eg in the "D:\Update" directory. The following files are a necessary part of the "Update" directory for the correct operation of the bulk update:

- "FinishUpdate.exe",
- "NETGeniumConnection.dll",
- "Update.exe.config" and
- "Update.exe".

When starting the bulk update, the log file "Update.log" is supplemented with a list of all NET Genies that were listed in the configuration file "Update.exe.config".

- If the NET Genium is successfully updated, the log file "Update.log" shows "OK" next to the path to the NET Genium.
- If the given NET Genium is already current at the time of the update, the log file "Update.log" next to the path to the given NET Genium is "Up-to-date".

If the given NET Genium was searched for thanks to the parameter "ngdirs" and at the same time contains the file "SkipUpdate.txt" in the "Config" directory, the log file "Update.log" next to the path to the given NET Genium states "SKIP".

3 “Config\Tools” directory

3.1 Deactivate.exe

The “Deactivate.exe” program deactivates NET Genium – IIS and the NET Genium web application remain running, but any work in NET Genium is prevented. Users are redirected to the “UnderConstruction.aspx” website every time they request to work in NET Genium. Deactivation consists in creating the file “UnderConstruction.txt” in the directory “Config”. The content of the file defines the HTML code that is displayed to the user on the “UnderConstruction.aspx” web page.

3.2 Activate.exe

The program “Activate.exe” activates NET Genium resp. deletes the “UnderConstruction.txt” file from the “Config” directory.

3.3 GrantLogin.sql

The “GrantLogin.sql” file contains a sample list of commands that are used to grant “sysadmin” database access to the “IIS APPPOOL\DefaultAppPool” user account.

```
sp_grantlogin 'IIS APPPOOL\DefaultAppPool'  
go  
sp_addsrvrolemember 'IIS APPPOOL\DefaultAppPool', 'sysadmin'  
go
```

3.4 GrantLogin.bat.txt

The “GrantLogin.bat.txt” file is a sample batch file that contains a list of commands to run the “GrantLogin.sql” file.

```
@echo off  
echo Please wait...  
osql -S(local)\SQLEXPRESS -E < GrantLogin.sql  
pause
```

3.5 MemoryDumps.txt

The “MemoryDumps.txt” file contains a procedure for analyzing “memory dumps” to troubleshoot application performance or functionality issues.

- 1) Download and install Debug Diagnostic Tool v2 Update 2 (<https://www.netgenium.com/download/DebugDiagx64.msi>)
- 2) Locate memory dumps (C:\Users\abc\AppData\CrashDumps)
- 3) Run DebugDiag
- 4) Default Analysis/ CrashHangAnalysis
- 5) Add Data Files

6) Start Analysis

3.6 SSL.reg

The "SSL.reg" program is used to set the recommended security configuration of HTTPS protocols on the server side. The program is started by double-clicking on the "SSL.reg" file, and the configuration settings are made by writing to the registers. The recommended configuration only allows the use of the "TLS 1.2" protocol, and prohibits the older "TLS 1.1" and "TLS 1.0" protocols, including outdated "SSL" protocols and weak ciphers.

```
Windows Registry Editor Version 5.00
```

```
; https://www.ssllabs.com/ssltest
```

```
; Disable TLS 1.0
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0]
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client]
```

```
"DisabledByDefault"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server]
```

```
"Enabled"=dword:00000000
```

```
; Disable TLS 1.1
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1]
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client]
```

```
"DisabledByDefault"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server]
```

```
"Enabled"=dword:00000000
```

```
; Enable TLS 1.2
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2]
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
```

```
"DisabledByDefault"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server]
```

```
"Enabled"=dword:00000001
```

```
; Disable SSL 2
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL
2.0]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL
2.0\Client]
"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL
2.0\Server]
"Enabled"=dword:00000000

; Disable SSL 3

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL
3.0]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL
3.0\Client]
"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL
3.0\Server]
"Enabled"=dword:00000000

; Disable Diffie-Hellman Key Exchange

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlg
orithms\Diffie-Hellman]
"ServerMinKeyBitLength"=dword:00000800

; Disable RC4

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4
128/128]
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4
40/128]
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4
56/128]
"Enabled"=dword:00000000

; Disable 3DES

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple
DES 168]
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple
DES 168/168]
"Enabled"=dword:00000000
```

3.7 SSL-ie6.reg

The “SSL-ie6.reg” program is used to set the security configuration of HTTPS protocols on the server side, necessary for the functionality of obsolete devices such as Internet Explorer version 6, old tablets, mobile phones, etc. The program is started by double-clicking on the “SSL-ie6.reg” file, and the configuration settings are made by writing to the registry. This configuration allows the use of “TLS 1.2”, “TLS 1.1” and “TLS 1.0”, and disables outdated “SSL” protocols and weak ciphers.

```
Windows Registry Editor Version 5.00

; https://www.ssllabs.com/sslltest

; Disable TLS 1.0

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.0]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.0\Client]
"DisabledByDefault"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.0\Server]
"Enabled"=dword:00000001

; Disable TLS 1.1

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.1]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.1\Client]
"DisabledByDefault"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.1\Server]
"Enabled"=dword:00000001

; Enable TLS 1.2

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.2]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.2\Client]
"DisabledByDefault"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.2\Server]
"Enabled"=dword:00000001

; Disable SSL 2

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL
2.0]
```



```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL
2.0\Client]
"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL
2.0\Server]
"Enabled"=dword:00000000

; Disable SSL 3

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL
3.0]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL
3.0\Client]
"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL
3.0\Server]
"Enabled"=dword:00000000

; Disable Diffie-Hellman Key Exchange

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlg
orithms\Diffie-Hellman]
"ServerMinKeyBitLength"=dword:00000800

; Disable RC4

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4
128/128]
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4
40/128]
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4
56/128]
"Enabled"=dword:00000000

; Disable 3DES

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple
DES 168]
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple
DES 168/168]
"Enabled"=dword:00000000
```

3.8 TracingRequests.txt

The "TracingRequests.txt" file contains the procedure for tracing web requests.

- 1a) Server Manager/ Add roles and features
- 2a) Web Server (IIS)/ Web Server/ Health and Diagnostics/ Tracing
- 3) Run IIS
- 4) Select top node and click 'Failed request tracing rules'
- 5) Click Add...
- 6) All content (*)
- 7) Status code(s): 401-999
- 8) Select website and click 'Failed request tracing rules'
- 9) Edit Site Tracking...
- 10) Enable

3.9 TuningQueries.sql

The "TuningQueries.sql" file contains a sample list of commands that are used to debug database queries in the "SQL Server Database Engine Tuning Advisor".

```
use netgenium
go
SELECT ...
SELECT ...
```

3.10 TuningQueries.txt

The "TuningQueries.txt" file contains the procedure for debugging database queries in the "SQL Server Database Engine Tuning Advisor".

- 1) Run SQL Server Management Studio
- 2) Right click on the instance name and select 'Reports/ Standard Reports/ Performance - Top Queries by Total CPU Time'
- 3) Identify top queries with constants in a condition that can be improved with indexes
- 4) Right click on the background of the report and select 'Print/ Excel'
- 5) Open printed Excel file
- 6) Create 'netgenium.sql' file and insert top queries using the following syntax:

```
use netgenium
go
SELECT ...
SELECT ...
```

- 7) Run SQL Server Database Engine Tuning Advisor
- 8) Click 'Start New Session'
- 9) Select 'File' as a 'Workload' and browse for 'netgenium.sql'
- 10) Mark 'netgenium' database
- 11) Click 'Start Analysis'

- 12) Analyze 'Recommendations' tab
 - 13) Create new indexes as recommended
-

3.11 WALTU.exe

The “WALTU.exe” program is used to browse all links from the specified web application URL. It is used, for example, for stress tests, where it is specified in how many threads “WALTU.exe” should run, or to determine the availability of links (dead links, or incorrectly set destination rights).