EVS DATABASE LOGS PROCEDURE

Prerequisites:

- Use our Web portal to enter a new issue, and fill out all fields required. Always indicate the client workstation (name, IP address, serial number) and user role.
- **Do NOT** use 7z or other zipper. Use classic Windows zipper to zip the logs directory.
- Follow the procedure according to the product below to collect their respective logs files.
- If the problem can be easily reproduced, it will be better to backup all logs, then flush the entire C:\EVSLogs directory (EVS Services must be stopped). The biggest advantage will be to have smaller logs and easier to analyze.
- If you suspect a memory leak, please use “Procdump.exe” and collect Windows event logs entries. The usage is described in this document.
- Always indicate a timestamp when the error occurred and a print screen of the error. If the problem happened systematically please include with the logs a short Video showing the problem and steps to reproduce it.

How to collect logs:

- Provide a timestamp of the issue (matching the Windows clock from the Database Servers)
- Grab the following logs on standalone database servers but also on both members of the mirroring relationship.
  Grab the folder C:\Evslogs, this folder contains logs from:
    - EvsDBip service (in charge of the virtual IP address – Use Web Monitoring to know the Virtual IP Address).
    - EVS Database Monitoring
    - XSecure (used for the IP Engine license, IP floating license or a Xedio Control Center)
    - IP API (if installed)
    - XSquare (if installed)
- Grab an export of the Windows event logs (system & application) in evt or evtx format (according to your OS).
- Grab the SQL logs located on the partition S:\ in the folder:
    - S:\MSSQL.1\MSSQL\LOG for SQL20005
    - S:\MSSQL10_XX.MSSQLSERVER\MSSQL\LOG for SQL2008

  Take the latest ERRORLOG, ERRORLOG.1, etc ... covering the timestamp of the issue
  Take the latest SQLAGENT.OUT, SQLAGENT.1,... covering the timestamp of the issue **if the issue is linked to a maintenance jobs failure.**
  When files are collected zip the entire directory in order to save space.
- Open the "Web Monitoring" page (shortcut available from EVS SQL Taskbar) and grab a screenshot of the whole desktop.
- Open folders and grab screenshots from following folders content:
    - S:\MSSQL.1\MSSQL\DATA for SQL20005
    - S:\MSSQL10_XX.MSSQLSERVER\MSSQL\DATA for SQL2008

Extra logs files.

- If a corruption/loss of the data is suspected, grab a backup of the database hosted on the servers.
- If a maintenance job is marked as failed but the files were written to E:\DB_Backups: open the management studio/SQL Server Agent/Jobs/Right click "View History"/Export. Grab a print screen and include it in the issue report.
- If the issue is linked to blocking connection, latency or "fulltext" catalog problems: open the "SQL Infos & Logs" from the EVS Sql tool bar and 'Dump all the information to a log file'
- If the issue seems to be linked to a RAID Controller / SAS Disk problem, open the MegaRaid Storage Manager and export the logs (Main Menu\Logs\Save as text). A print screen of the error message is also essential.
  This log export may be also useful in case of unexpected database failover.
- If any unexpected reboot of the server is encountered (pop up found on the desktop after the Windows restart), always check if there is no minidump file (.dmp) in the c:\Windows\Minidump folder.
  Please zip the whole folder and provide it to us.

How to use Procdump.exe

Procdump.exe is a software from Microsoft to be used to collect a dump file upon application crash

How to collect a dump file upon application crash.
If a software is generating .dmp files and if the R&D is complaining that the dmp file is not complete enough, you may use the procdump.exe to generate a full dmp file.
Procdump.exe software can be downloaded from: http://technet.microsoft.com/en-us/sysinternals/dd996900

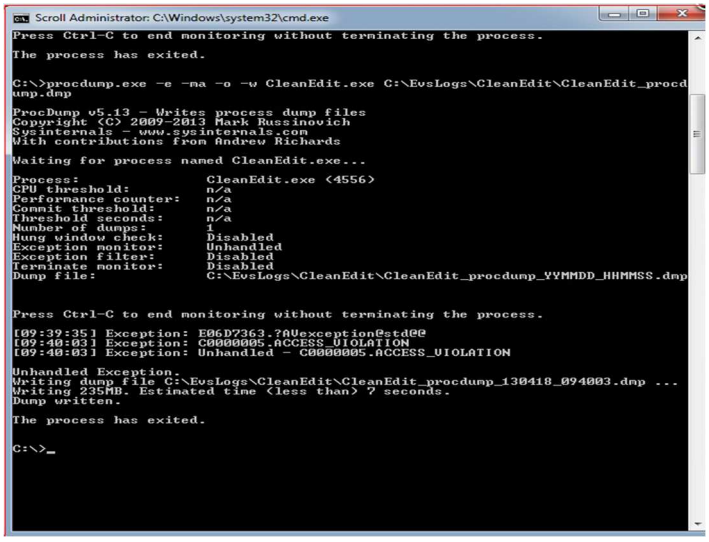
_ Copy procdump.exe anywhere on the machine (eg: C:\Temp\procdump.exe).
_ Launch procdump.exe with the right arguments: `procdump.exe -e -ma -o -w application_name.exe dump_file.dmp`

`Arguments details:`

-e	Write a dmp when the process encounters an unhandled exception
-ma	Write a dmp file with all process memory
-o	Overwrite the dmp if it exists
-w	Wait for the process if it does not already exists
-accepteula	Automatically accept the Sysinternals license agreement

`i.e. with Clean edit application:`
`procdump.exe -e -ma -o -w CleanEdit.exe C:\EVSLogs\CleanEdit\CleanEdit_procdump.dmp`

_ Launch the application and try to make it crash.
_ once the crash happened, collect the generated dmp file



If the R&D is asking a dmp file of a running application, you may use the procdump.exe to generate a full dmp file.
The procedure will be the same as described before:
_ Copy procdump.exe anywhere on the machine (eg: C:\Temp\procdump.exe).
_ Launch procdump.exe with the right arguments.
I.e. XedioIngest.exe

```
procdump.exe -ma -o -w XedioIngest.exe
C:\EVSLogs\XedioIngest\XedioIngest_procdump.dmp
```