|  |  |
| --- | --- |
| Title Of The Document | SAP MII Servers Backup and Recovery |
| Reference | **GIS-I-LSG-3761/EN** |
| Purpose | Required MII configuration of the Backup of File system and Databases, covering basic restore information |
| Scope | * Shopfloor systems MII Worldwide * To be used by Local IT during project phase and for replacement of old equipment |
| Related Documents | [**FAU-I-LSG-5250**](http://group.intranet.faurecia/sites/fes/fcp/Lists/FCP/DispForm.aspx?ID=3557) Faurecia Corporate Data Backup Policy  [**GIS-F-LSG-3507**](http://group.intranet.faurecia/sites/gis/Templates%20Instructions/GIS-F-LSG-3507-EN_Faurecia_Location%20Data%20Backup%20Concept%20Form.doc) Faurecia Location Data Backup Concept Template   * + - * **[CCBO Shareplace entrypoint for Simpana](http://group.shareplace.faurecia/sites/itio_cc/galaxy/Shared%20Documents/Forms/AllItems.aspx" \t "_blank)**   [**[Best Practice](http://group.shareplace.faurecia/sites/itio_cc/galaxy/Shared%20Documents/Forms/AllItems.aspx" \t "_blank)**](http://group.shareplace.faurecia/sites/Local_IT_Infrastructure_Standards/best%20practice/Simpana/Simpana%20Best%20Practice%20-%20SQL%20iDA.doc) [for setup Simpana SQL agent](http://group.shareplace.faurecia/sites/itio_cc/galaxy/Shared%20Documents/Forms/AllItems.aspx" \t "_blank) |
| Issue N° | 04 |
| Description Of Changes | Update Database backup schedule |
| Cancels And Replaces | Issue 03 – 11.03.15 - Simpana reference included, requirements updated  Issue 02 – 17.04.2013 - SSMS Restore Tutorials  Issue 01 - 22.10.2012 - Creation |
| Owner | Jakub NAJBERK (MII team coordinator) |
| Approved By | Bernard LAURENT (Back office Director) |

**Table of Contents**

[1 Scope and Applicability 3](#_Toc416276749)

[2 Prerequisites 3](#_Toc416276750)

[3 Introduction 3](#_Toc416276751)

[4 Simpana – standard backup system 4](#_Toc416276752)

[4.1 General Simpana reference in summary: 4](#_Toc416276753)

[4.2 Legacy backup systems 5](#_Toc416276754)

[4.3 Location Data Backup Concept 5](#_Toc416276755)

[5 Backup configuration 5](#_Toc416276756)

[5.1 MII system backup set 5](#_Toc416276757)

[5.2 MII SQL database backup set 6](#_Toc416276758)

[5.3 MII Backup Schedule Policy 7](#_Toc416276759)

[5.4 Storage Policy – Retention Times 8](#_Toc416276760)

[6 Virtual Machine file copy backup 9](#_Toc416276761)

[7 Restore & Disaster Recovery 9](#_Toc416276762)

[7.1 RPO requirements 9](#_Toc416276763)

[7.2 RTO requirements 10](#_Toc416276764)

[8 Appendix 1 11](#_Toc416276765)

[Appendix 2 19](#_Toc416276766)

# Scope and Applicability

This specification explains the basics for MII server system and its backend MSSQL database backups and restores.

# Prerequisites

The backup tools installation and configuration will be done by local IT just after the MII will be installed by 9TechSF admin team - but prior to go-live to have time to approve its proper functionalities. It will be supported by the CC Backoffice Simpana team during the first Simpana preparation on site.

Acquisition of Simpana licenses is also one of prerequisites for the MII servers purchase by local IT.

**All database restores must be supervised or executed by 9TechSF team!**

# Introduction

The MII server is an application system comprising of SAP Netweaver stack application framework, XMII application and components of Faurecia developed functionalities.

Location of data on MII servers are:

**C: Basic MSSQL databases.**

**G: Applications – MII system, utilizing services, backend software. including.**

**H: MII database files.**

**L: Transaction log files.**

Like every other system the MII requires administration and regular monitoring and maintenance, including backup.

This document provides general guidance and recommendations how to set up MII system and database backup configuration and which rules have to be followed at the responsibility of local IT staff.

Local MII SQL database must be backed up with Faurecia Standard CommVault Simpana with the SQL online agent.

**To implement only Simpana file system backup agent is NOT sufficient.**

Refer to [Documentation for Simpana](http://group.shareplace.faurecia/sites/itio_cc/galaxy/Shared%20Documents/Forms/AllItems.aspx) of CC backoffice in intranet.

**Realization of these requirements must be in accordance to global standards of Corporate Data Backup Policy** [FAU-I-LSG-5250/EN](http://group.intranet.faurecia/sites/fes/fcp/Lists/FCP/DispForm.aspx?ID=3557) .

# Simpana – standard backup system

An installed basis of Faurecia standard for data backup CommVault Simpana is recommended to

backup the primary MII server at the location concerned.

Minimum recommended Simpana standard components:

- **Simpana Media Agent server with Disk Library.**

- At least one **Tape Library with barcode reader and one LTO tape drive** according to Faurecia standard.

The detailed architecture for data backup will be defined by Faurecia Competence Center Back Office (CCBO) under consideration of the requirements and the situation at the location concerned.

Requested Simpana agents for MII server:

- iDataAgent for Windows file system

- iDataAgent for MS SQL database on Windows

CommVault licenses will have to be purchased by the requestor of the backup in close

cooperation with CCBO and applied to the Simpana central control server by CCBO.

Install Simpana with recommended agents, following standard instructions of CommVault online documentation of the currently installed release of Simpana at the central control server.

General information on Simpana for Local IT presented here:

[Simpana Local IT](http://group.shareplace.faurecia/sites/itio_cc/galaxy/Shared%20Documents/SimpanaDetailsLocalIT2013.ppt)

## General Simpana reference in summary:

1. Connect to Simpana Commcell Console:  
   Simpana admin request with template GIS-F-LSG-3510 – let approve – send to CC Backoffice  
   <http://group.intranet.faurecia/sites/gis/Templates%20Instructions/GIS-F-LSG-3510%20Administrative%20Rights%20Local%20Managed%20Services.doc>
2. Basic Subclient configuration:  
   <http://group.shareplace.faurecia/sites/itio_cc/galaxy/Shared%20Documents/Forms/AllItems.aspx>
3. Contents of backups, exclusions / filter 🡪 **Subclient**  *(see chap. 5.1, 5.2)*
4. Checking backups, check for failed items in backup history 🡪 **Subclient**
5. Performing restores 🡪 **Never overwrite user’s data**
6. Retention of backups 🡪 **Storage Policy Copy** *(see chap. 5.4)*<http://group.shareplace.faurecia/sites/itio_cc/galaxy/Shared%20Documents/Forms/AllItems.aspx>
7. Schedule Policy, **MII**, Insequence, Doubletake (offline database at secondary, deactivate backup activity for SQL iDA) *(see chap. 5.3)*
8. Tape cartridge handling, Export Locations, Number of Media in Scratch Pool
9. Solving issues:   
   DNS (nslookup), Binding Order, Network Interface Settings full/half duplex,   
   “unknown changer” as medium changer in device manager, VSS error, {Offline Files}, system resources.
10. Set up reporting / alerting
11. Using help and online documentation  
    <http://group.shareplace.faurecia/sites/itio_cc/galaxy/Shared%20Documents/1_Install%20Simpana%20pre-requirements.doc>

## Legacy backup systems

Due to formerly existing equipment and tools at some locations concerned, temporary use of legacy backup infrastructure which is still reliable is allowed. The configuration of legacy backup systems must follow as much as **the same Backup Set Configuration, Storage Policy and Schedule Policy** as for Simpana.

The Faurecia Data Backup Policy standard has to be followed in any case: [Corporate Data Backup Policy](http://group.intranet.faurecia/sites/fes/fcp/Lists/FCP/DispForm.aspx?ID=3557) - [FAU-I-LSG-5250/EN](http://group.intranet.faurecia/sites/fes/fcp/Lists/FCP/DispForm.aspx?ID=3557).

The deadline for the migration to the Simpana backup system from legacy systems must be defined by date of the go-live of MII servers.

## Location Data Backup Concept

Use the template form [GIS-F-LSG-3507](http://group.intranet.faurecia/sites/gis/Templates%20Instructions/GIS-F-LSG-3507-EN_Faurecia_Location%20Data%20Backup%20Concept%20Form.doc) to document and verify backup configuration for the MII server on location concerned in accordance to requirements as further, chap.5.

Owners of MI data will sign the concept with 9TechSF Admin team by the go-live of the MII system.

# Backup configuration

## MII system backup set

The system backup set will be controlled by the Simpana file system agent.

Based on SAP recommendations for a MII backup it must include:

|  |
| --- |
| **MII file system backup must include:** |
| * Windows System Files + System State |
| * Program files and necessary entries |
| * G:\usr\\*.\* and all subfolders |

Following files could either be open during backups and cannot be backed up, or do not need to be backed up.  
Exclude them:

|  |
| --- |
| **Backup set Exclusions (to find details, failed files log from backup job could help)** |
| * PRINTER\_LOGS files |
| * Opened files in temp directories |
| * Documents and Settings |
| * Native SQL database files at  C:\ (default Master, MSDB, …) H:\ (MII database files) L:\ (MII database transaction log files) |

**Installation media**

It is not necessary to back up regularly the copy of installation media /from the MII installation USB flashdisk/. Take care that those media must be stored at a fireproof place to ensure availability in case of needs

**System high-availability concerns**

High availability system of MII servers (DoubleTake solution) is not intended to protect from system, MII application or database data failures. That is because – all those kind of errors will be also replicated to the secondary failover server on the disk data content layer.

## MII SQL database backup set

The system backup set will be controlled by the Simpana SQL Agent.

SAP database called **<SID>** (site id specific name of database - equals to the Faurecia 3-digit site code used, e.g. ORE, MER, MBO, PUE… = the MII trigram) and MII application database called **MES\_FAURECIA** have to be included into different backups sets.

**Database backup Configuration**

Set up the Recovery Model FULL for MES\_FAURECIA database in the MSSQL server configuration to achieve the Transaction Log backup with point-in-time recovery possibility of all transactions!

With FULL Recovery Model also the dedicated backup of Transaction Log files must be configured and scheduled accordingly. This is the only way to keep the size of transactional log files maintained within MSSQL scope. Otherwise there is a risk of filling up the limited L: disk space, where the transaction log file is located resulting in stopping the database.

You can leave SIMPLE Recovery model for <SID> database, as recommended by SAP.

**MSSQL system databases concerns**

The system databases “master”, “model” and “msdb” must be backed up too because they are needed in the case full restore has to be done. The “master” database contains the master configurations of the SQL server and user logins and passwords. This database allows full backups only, so all scheduled transaction log or differential backup jobs on this master database are automatically converted to full backups.

The “msdb” database contains job definitions and logs for the SQL agent and also the backup catalog.

The “model” database is simply an empty database used as a template when creating new databases.

(Database backup and restore logs are always created and are available also within MSSQL server logs/reports.)

## MII Backup Schedule Policy

Backup schedule planning should consider production load on MII server together with user activity factors, as well as other schedules configured in the centralized backup solution Simpana.

**It is recommended to schedule the Transactional LOG backup start after the database backup (full or incremental / differential) ended.**

**No other database backup must be scheduled (e.g. in a SQL maintenance plan) in parallel to a Simpana SQL database backup to avoid conflicts!**

File system backup schedule:

|  |
| --- |
| The schedule of MII system backup: |
| * **File system backup – follow Faurecia standards, additional requirement is:** |
| * 2 x daily Incremental backup |
| * 1 x weekly FULL backup |

Database backup schedule:

|  |
| --- |
| The MII database backup schedule: |
| * **All databases FULL backup** * **Weekly** * **All databases DIFF backup** * **Once a day** |
| * **All databases LOG backup (or DIFF for SIMPLE recovery mode)** |
| * **Every 2 hours** |

Caution – the backup Schedule is when the backup effectively runs, it is not the retention time !

**Monitoring the Backup**

All data backup jobs must be checked for errors and failed items after its creation. This could be performed in MSSQL or by automated reporting provided by CommVault Simpana.

(See CommVault documentation how to achieve a suitable backup monitoring / reporting / verification.)

At the monitoring report, take care of the successfully completed backup jobs and that there is no failed item shown at the backup log. In case of detection of failed items, check for reason and solve the issue appropriately.

## Storage Policy – Retention Times

Retention times for MII backups are not defined by SAP so far. As a consequence, retention time for MII backups must correspond to the needs of the location concerned, defined by the owner of MII data.

Follow up Corporate Data Backup Policy in this definition.

[Corporate Data Backup Policy](http://group.intranet.faurecia/sites/fes/fcp/Lists/FCP/DispForm.aspx?ID=3557)- [FAU-I-LSG-5250/EN](http://group.intranet.faurecia/sites/fes/fcp/Lists/FCP/DispForm.aspx?ID=3557).

See standard Simpana documentation and search for “configure storage policy”. That will provide detailed information how to configure a storage policy at Simpana.

# Virtual Machine file copy backup

Local IT has to create a copy of the primary MII virtual machine (in stopped status) within VMWare vSphere Client and download it to his local storage as a backup every half a year.

It is recommended to use the secondary host server \*\_DATA datastore space to create a copy of productive virtual machine, download from it to a local storage and remove the copy. Proceed this action out of production time only!

The VM copy backup will be important in case of a total hardware failure to have a quick possibility to restore the full MII system without new installation and then update it to the last live state by a regular application change management procedure and the most recent database restore.

# Restore & Disaster Recovery

Inconsistencies of the database can be solved by a restore with CommVault Simpana.

(In other cases - for advanced users – restore will be done by 9TechSF team supervision with MSSQL tools, refer how to Appendix 1.

Further refer also to related MSSQL documentation: [Backing up and Restoring databases in MS SQL Server )](http://msdn.microsoft.com/en-us/library/ms187048(v=sql.90))

Never overwrite user´s data by restore !

It is recommended to restore database under a different name with a different data file, check its content and then backup and delete old database and set name of the restored new one.

**Prior to any restore action, inform 9TechSFAdmin team in advance to get the L2 support !**

**L2 will cooperate also with L3 to solve more complex problems.**

## RPO requirements

The term defines maximum accepted data loss in case of failure:

**MII servers RPO for the database** recovery will be **2 hours** due to the defined schedule of the differential or incremental backup.

**MII servers RPO for the file system** will be **half day** due to the configured schedule of the file system backup 2 per day.

However with FULL recovery model on, it is possible to restore complete data - if a so called “tail transaction log backup” is created just after the db failure. Then all transactions “logged” on the database server till time of db failure can be recovered and there would be no data loss. Such action is called “Point-in-time” restore.

( By similar way it is even possible to go back in time with data restore to any other point in time if necessary.)

## RTO requirements

The term defines how long a recovery could last at maximum.

RTO definition is to be distinguished in different cases. RTO definition presumes that most current backup copies are on a local magnetic disk (that is a standard recommendation for Simpana backup) and that Windows OS and VMWare install medium would be available immediately in case of complete server failure.

**MII servers RTO definitions:**

1. **Database recovery** = **less than 1 hour** due to the small size of the database, using last full backup and differential / incremental backups. In case of selecting the point in time to restore the transactional log would be rolled forward, which is more time-consuming.
2. **Full system recovery** **due to a crashed OS** or application at both primary and secondary systems = about **1,5 hours**, where the setup of the OS could be achieved by VMWare clone within 30 minutes and the full system recovery with Simpana would take about 1 hour.
3. **Full system recovery at a crashed infrastructure** on a blank server = about **4 hours**, where the setup of the file system at a blank windows server would take about 3 hours and the full system recovery with Simpana would take about 1 hour.

Full system recovery and all restore processes are documented at CommVault online documentation. 2nd level skills for Windows OS, VMWare, SQL database and Simpana is recommended to perform the right steps for recovery.

In general restore tests are strongly recommended to be performed regularly to validate functionality of the backup configuration.

# Appendix 1

**Backup and Restore without Simpana**

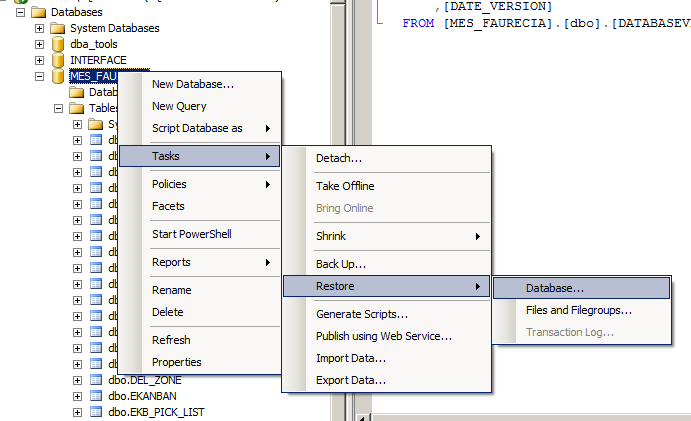
In situations, where Simpana solution is not in place yet or there is a different legacy solution used (e.g. Backup Exec) - it is recommended use backup jobs created optionally with following procedure:

<http://group.shareplace.faurecia/sites/itio_cc/bo/Shared%20Documents/DBA/SQL%20SERVER/GIS-I-LSG-3718_V3_EN_sql%20server%20maintenance.docx>

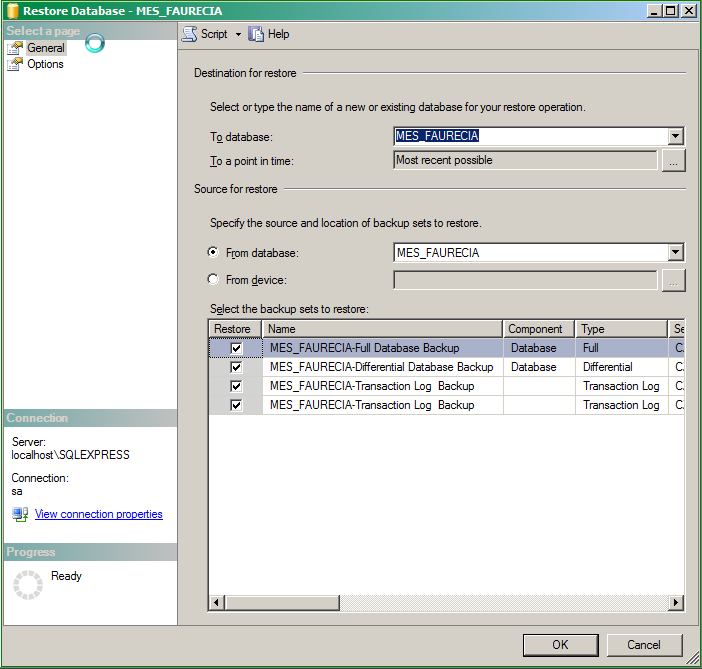
**Proceed ONLY with L2 - 9TECH\_SF Admin team PARTICIPATION!!!**

Following you can find a step by step sample of various types of backup restore for db MES\_FAURECIA. It is possible to proceed same actions with command line tool (SQLCMD). Please refer to product documentation for more help.

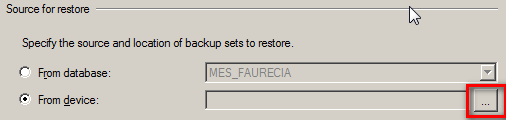
**Restore with MS SQL Management Studio (advanced users)**



On the Restore screen you can see, which backup sets are available to be restored. Be aware that after every backup, the target file is usually moved to the storage location and another backup created a new file. Copy the backup file to be restored on the server. H: drive usually has a spare space for temporary copies of backup files, but be sure to keep at least 30% free space of the volume.

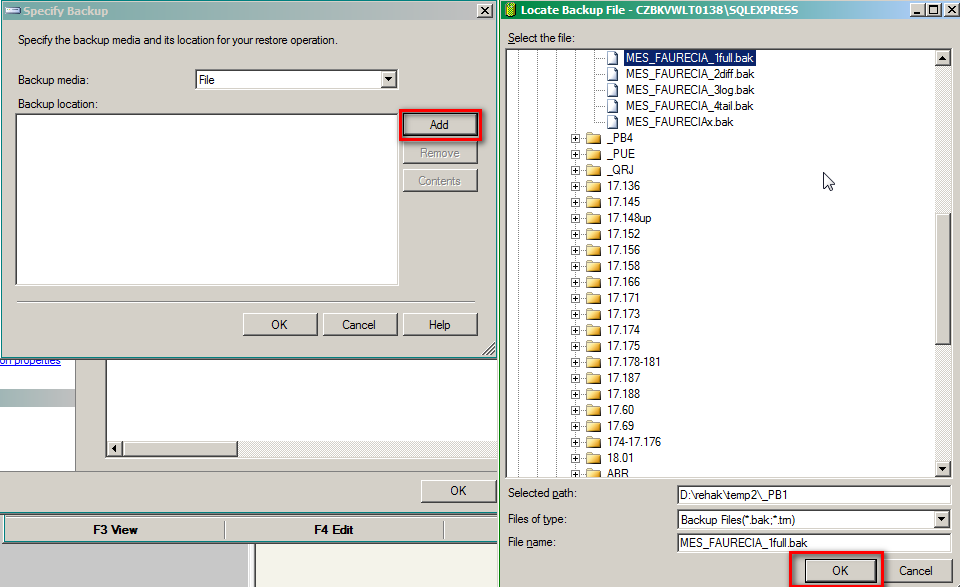


If you want to proceed with a specific backup set go on with option “From device…” to choose a source file.



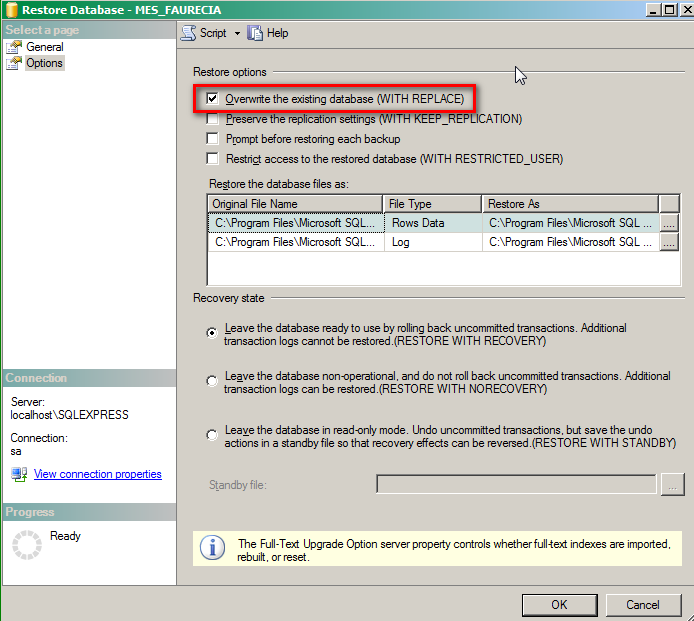
From existing backup files choose the right one to be restored.

It is a good practice to have well defined file name description as on this sample list of files (those files match to backup sets listed on a screen above):



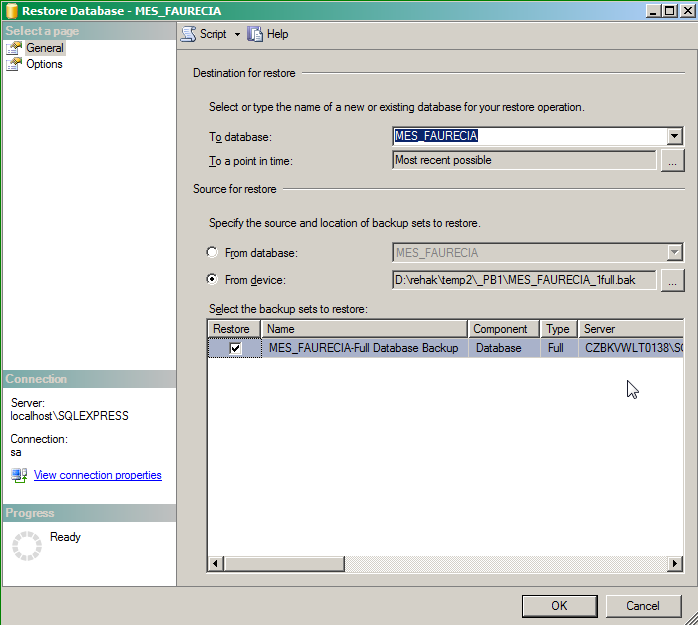
Before any restore, the database should be not used, so it is a possible to bring it offline and online again to clear connections. (Alternatively logoff SSMS and logon again to the server.)

If necessary choose following option to overwrite existing data. (It is recommended to backup the database before restore, no matter of its last consistence – just in case of need to go back.)

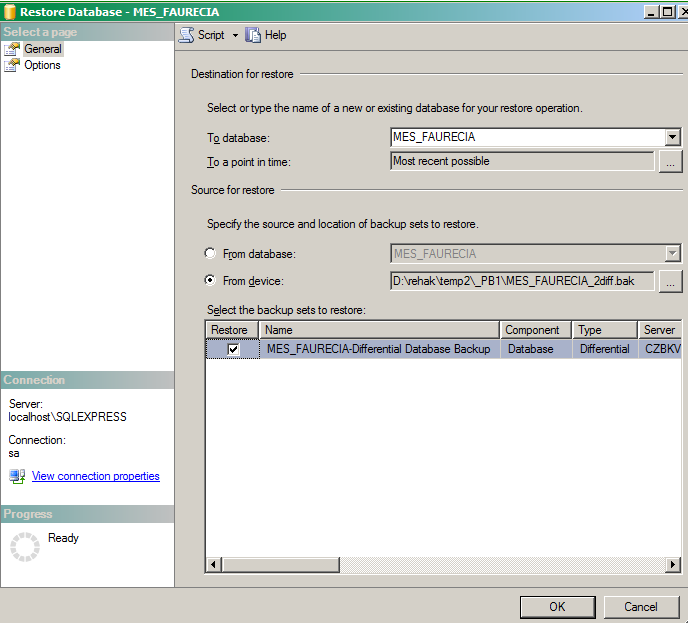


Full backup restore

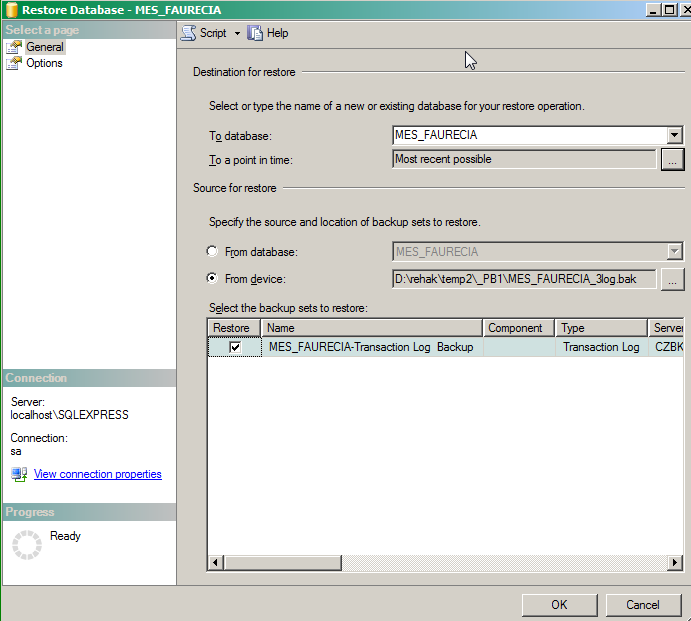
You can check the backup to be restored of the backup set, depending on its type and date/time of creation.

****

Differential backup restore

****

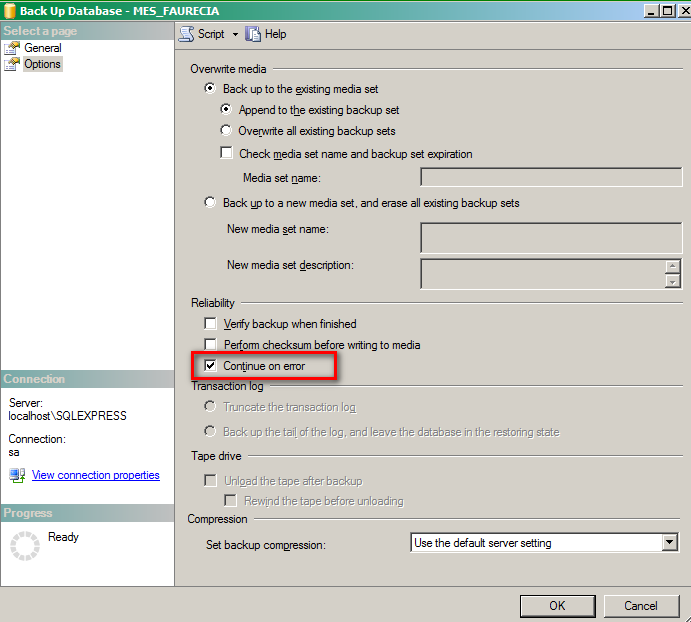
Transactional log backup restore

****

Tail log backup and restore

It is possible to take a backup of log remaining on the server for a broken database, which is not available and use it to restore “The most recent state possible” as an option of “point-in-time” restore. Please refer to next paragraph.

Choose this option to take a Tail-Log backup on creating a Transaction Log backup type:

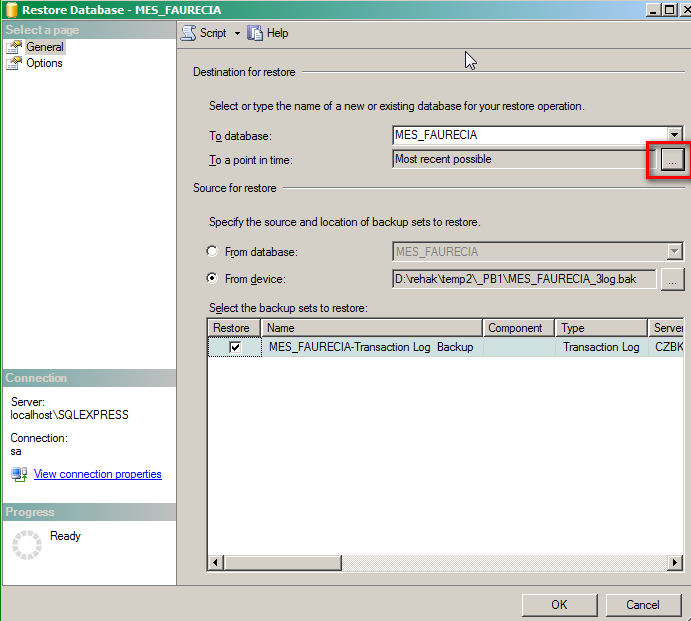
****

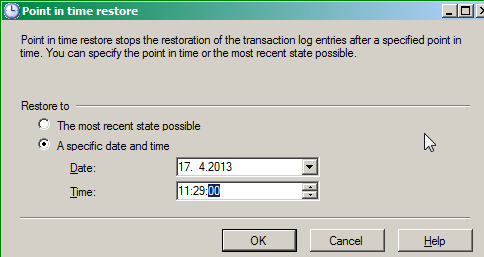
Transactional log point-in-time restore:

This is possible with a proper Transaction Log backup created with FULL Recovery mode enabled.

Such restores could solve an application issue by going back to specific point in time, where application data were still correctly working, just before time when an error occurred.

This however requires an expert knowledge of the MII solution and the qualified determination of the point, when error occurred. Some correct data put in system after the point of error could be lost by this restore. They have to be added manually.

****

****

Appendix 2

Annotations on technical topics

**Recovery Model comparison**

Type SIMPLE **Type FULL**

Restore all data NO YES

Restore to any point in time NO YES

Partial data recovery by page NO YES

Differential backups YES YES

Transactional Log backups NO YES

Last log before failure NO YES

Managing log space 0 log file backup log file

Data loss risk from last backup none

Speed of restore fast from data backup rolling forward transactions

Time of restore will be improved by setting up intermittent differential or incremental backups among log backups and full backups. Differential database backups are also faster to recover than rolling forward a huge Transaction Log.

**RPO**

Accepted maximum time in past when it should be possible to restore working data or it is a maximum time period in which data might be lost

**RTO**

Accepted maximum time in which all services have to be recovered from a failure, in this case it is maximum time when data or files have to be fully restored up to required working status