Installation – EK Process Intelligence

Extension Kit Process Intelligence · https://extensionkit.unitfly.com/documentation/installation-ek-process-intelligence/

Extension Kit Process Intelligence serves for ETL process (Extraction, Transformation, and Load) from M-Files to a specific database. There are three options: **Data Export**, **Audit Log Export**, and **Logging**. Data Export serves for exporting M-Files log data to a database, Audit Log Export serves for exporting M-Files audit to a database, and Logging serves for sending M-Files logs.

System Requirements

To ensure proper installation and functionality of Extension Kit Process Intelligence in an on-premise environment, the server must have **.NET Framework version 4.7.2 or higher** installed.

Configuration

Data Export

- Export vault data to a database
  - Object changes, state and assignment changes

1. Configure database connection
   – Create an empty database in SQL Server
2. Configure PI Kit
3. Execute the *Setup database* command to generate required SQL objects
4. When the database has been set up, data can be exported in two ways:
   – **Manually**, by pulling it from the vault – reconstructing events from object histories
   – **On a schedule**, by reading events from M-Files Log

5. The recommended approach is first to pull from the vault manually, and then configure periodic export from M-Files Event Log

Buttons:

- Stop running task -> Stopping task to run while it is in progress
- Cancel pending tasks -> Canceling tasks that were meant to be executed afterward
- Setup database -> Connecting to a configured database
- Pull data – Generating data
- Update data

Audit Log Export

- Periodical audit event export in a database
- Export audit log data to a database
  - Login, logout

1. Configure database connection
   – Create an empty database in SQL Server
2. Configure PI Kit
3. Execute the *Setup database* command to generate required SQL objects
4. When the database has been set up, data can be exported in two ways:
   – Manually, by pulling it from the vault – reconstructing events from object histories
   – On a schedule, by reading events from M-Files Log
   The recommended approach is first to pull from the vault manually, and then configure periodic export from M-Files Event Log
5. When the database has been set up, configure periodic export of audit events from M-Files Event Log

Button:

- Cancel pending tasks
- Setup database

Configuring EK Process Intelligence

Data Export

Field	Value	Description
Enabled	Yes / No	Whether the operation is enabled or not
Export destination		Export destination database
Database type	SQL Server	A type of database for export
Database type -> Connection string		Database connection string
Value		Example: Data Source=[SERVER_NAME];Initial Catalog=[DATABASE_NAME];Persist Security Info=True;User ID=[USER];Password=[PASS]
Use the secure password	Yes / No	Set password to use in the connection string. Any password value specified in the connection string above will be overridden with a value specified in the secured Password field.
Password		Password to use in the connection string.
Export frequency		Frequency for exporting events from M-Files Event Log
Type	Unknown, Interval, Schedule	
Type -> Configuration (Interval)		When Type = Interval

Configuration -> Interval		Choose interval, numeric-
Configuration -> Run on vault start	Yes / No	If true, runs when the vault starts. If false, the first run is scheduled to be after the interval has elapsed.
Type -> Schedule		When Type = Schedule
Configuration -> Enabled	Yes / No	Whether the configuration is enabled or not
Configuration -> Triggers	Unknown / Daily / Weekly / Monthly	
Configuration -> Triggers -> Daily	Time	
Configuration -> Triggers -> Weekly -> Trigger Days	Add DayOfWeek	
Configuration -> Triggers -> Weekly -> Trigger Times	Add time	
Configuration -> Triggers -> Weekly -> Unrepresentable Date Handling		How to handle dates that cannot be represented – e.g. 29 February
Configuration -> Triggers -> Weekly -> Trigger Days	Add number	
Configuration -> Triggers -> Weekly -> Trigger Times	Add time	

Configuration ->Run on vault start	Yes / No	
Included object types	All / Selected	This setting controls whether all events will be exported, or only those that occurred on selected object types
Object types filter	Object type	(if Included object types = Selected) – only those events that occurred on objects of selected types will be exported
Ignored login accounts	Login account	Events caused by login accounts specified here will be ignored
Data enrichment rules		These rules are used for the enrichment of exported data. You can define multiple rules to configure which metadata properties will be exported for any given object.
Rule group -> Name		Group name.
Rule group -> Rules		Rules are used for the enrichment of exported data. You can define multiple rules to configure which metadata properties will be exported for any given object.
Rule -> Name		Rule name.
Rule -> Description		Rule description.
Rule -> Enabled		Specifies whether a rule is in use.
Rule -> Filter conditions		Filter conditions define objects that this rule applies to. Multiple conditions inside a filter are combined with AND operator, while multiple filters are combined with the OR operator.
Filter conditions -> Seach conditions		

Rule -> Simple properties		Additional simple properties that will be included in data export.
Simple property -> Property		
Rule -> Custom properties		Additional custom properties that will be included in data export.
Custom property -> Column name		Database column name.
Custom property -> Type	Expression / TimelineId	Type of custom property.
Custom property -> Data type	Uninitialized, text, integer, floating, date, time, timestamp, boolean, lookup, multi-select lookup, integer64, file time, multi-line text, ACL	Expression result data type.
Data pull settings		Settings for pulling data from the vault
Events insert health check		Frequency of periodic check if any unprocessed events exist in the database. If such events exist, the operation will be resumed.
Events insert health check -> Type	Unknown / Interval / Schedule	
Configuration (Interval) -> Enabled	Yes / No	
Configuration -> Triggers -> Trigger		
Trigger -> Type	Unknown / Daily / Weekly / Monthly	

Type -> Configuration (Daily) -> Trigger Times	Time	
Type -> Configuration (Weekly) -> Trigger Days	Add DayOfWeek -> Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday	
Type -> Configuration (Weekly) -> Trigger Time	Time	
Type -> Configuration (Monthly) -> Configuration -> Unrepresentable Date Handling		How to handle dates that cannot be represented (e.g. 29 February)
Type -> Configuration (Monthly) -> Trigger Days	Add DayOfWeek -> Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday	
Type -> Configuration (Monthly) -> Trigger Time	Time	
Events insert health check -> Run on vault start	Yes / No	If true, runs when the vault starts. If false, the first run is calculated from the triggers.
Start date (inclusive)		
Start time (inclusive)		
End date (inclusive)		
End time (inclusive)		

Audit Log Export

Field	Value	Description
Enabled	Yes / No	Whether the operation is enabled or not
Export destination		Export destination database
Database type		Type of database for export.
Connection string -> Value		Database connection string. Example: Data Source=[SERVER_NAME];Initial Catalog=[DATABASE_NAME];Persist Security Info=True;User ID=[USER];Password=[PASS]
Connection string -> Use secure password		Set password to use in the connection string. Any password value specified in the connection string above will be overridden with a value specified in the secured Password field.
Password		Password to use in the connection string.
Export frequency	Unknown / Interval / Schedule	
Type (Interval) -> Configuration -> Interval		
Type (Interval) -> Configuration -> Run on vault start	Yes / No	If true, runs when the vault starts. If false, the first run is scheduled to be after the interval has elapsed.
Type (Schedule) -> Configuration -> Enabled	Yes / No	
Type (Schedule) -> Configuration -> Triggers -> Trigger -> Type	Unknown / Daily / Weekly / Monthly	

Trigger -> Type (Daily) -> Configuration -> Trigger Times	Add time	
Trigger -> Type (Weekly) -> Configuration -> Trigger Days	Add DayOfWeek	
Trigger -> Type (Weekly) -> Configuration -> Trigger Times	Add time	
Trigger -> Type (Monthly) -> Configuration -> Unrepresentable Date Handling		How to handle dates that cannot be represented (e.g. 29 February)
Trigger -> Type (Monthly) -> Configuration -> Trigger Days	Add number	
Trigger -> Type (Monthly) -> Configuration -> Trigger Times	Add time	
Ignored login accounts		Events caused by specified login accounts specified will be ignored.
Logging account		

Logging

Field	Value	Description
Enabled	Yes / No	Whether the operation is enabled or not
Minimum log level	Verbose, debug, information, warning, error, fatal	Minimum log event level for sending events to file and event log.

Logging destinations		Logging destinations. Application restart is required for changes to this setting to take effect.
File -> Enabled	Yes / No	Specifies whether logs are sent to a specified destination.
File -> Folder		The folder where log files will be generated. Requires vault restart for changes to take effect.
File -> Logs file size limit (MB)		The approximate maximum size, in bytes, to which a single log file will be allowed to grow. When the file size limit is reached, a new file will be created. Filenames will have a number appended in the format <code>_NNN</code>, with the first filename given no number. Requires vault restart for changes to take effect.
File -> Retention policy		Retention policy for log files. Requires vault restart for changes to take effect.
Retention policy -> Verbose logs retention		The number of verbose log files to retain. Set to 0 to retain all files.
Retention policy -> Debug logs retention		The number of debug log files to retain. Set to 0 to retain all files.
Retention policy -> Information logs retention		The number of information log files to retain. Set to 0 to retain all files.
Retention policy -> Error logs retention		The number of error log files to retain. Set to 0 to retain all files.
Event log -> Enabled	Yes / No	Specifies whether logs are sent to Windows event log.
External dashboard -> Enabled	Yes / No	Specifies whether application logs are sent to the dashboard.