Integrating a Generic Table with File Access Manager

Version: 8.3 Revised: March 30, 2022

Contents

Contents ..... **iii**

Capabilities **4**

Connector Overview **5**

Prerequisites **6**

Software Requirements 6

Communications Requirements 6

Generic Table Installation Flow Overview **7**

Collecting Data Stored in an External Application **8**

Adding a Generic Table Application **9**

Select Wizard Type 9

General Details 9

Connection Details 9

Configuring Activity Monitoring 11

Configuring Data Enrichment Connectors 11

Installing Services: Activity Monitor and Collectors **12**

Verifying the Generic Table Connector Installation **14**

Installed Services 14

Log Files 14

Monitored Activities **15**

Capabilities

This connector enables you to use File Access Manager to access and analyze data stored in Generic Table and do the following:

- Analyze the structure of your stored data.
- Monitor user activity in the resources.

See the File Access Manager documentation for a full description.

Connector Overview

File Access Manager connector for Generic Table queries a database table (either SQL Server or Oracle) for activity monitoring.

Prerequisites

Make sure your system fits the descriptions below before starting the installation.

Software Requirements

File Access Manager requires the latest ASP.NET Core 3.1.x Hosting Bundle. This bundle consists of .NET Runtime and ASP .NET Core Runtime. You can download the latest 3.1.x Hosting Bundle version from here .

Communications Requirements

Communications Requirements

Requirement	Source	Destination	Port
File Access Manager Access	Activity Monitor	File Access Manager servers	8000-8008
Activity Monitoring	Activity Monitor	Monitored database table	Database port

Generic Table Installation Flow Overview

To install the Generic Table connector:

1. Configure all the prerequisites.
2. Add a new Generic Table application in the Business Website.
3. Install the relevant services:
    - Activity Monitor - This is the activity collection engine, used by all connectors that support activity monitoring.

Collecting Data Stored in an External Application

Terminology:

Connector

The collection of features, components and capabilities that comprise File Access Manager support for an end-point.

Collector

The “Agent” component or service in a Permission Collection architecture.

Engine

The core service counterpart of this architecture.

Identity Collector

A logical component used to fetch identities from an identity store and holds the configuration, settings for that identity store, and the relations between these identities.

The identity collector has no “physical” manifest.

- The actual work is done by the Collector Synchronizer.

The list below describes the high level installation process required to collect and analyze data from an external application. Most of these should already be set up in your File Access Manager installation. See the server Installation guide for further details.

Install a Permission Collection central engine

One or more central engines, installed using the server installer

Create an Application in File Access Manager

From the Business Website. The application is linked to central engines listed above.

Add an Activity Monitor

To collect activities for this application - run the Collector Installation Manager and add an application under Activity Monitoring.

Optionally, you can install collectors that will run on a separate server and take some of the work from the central PC and DC engines (Where supported). When installing a collector, you attach it to an engine. If no collectors are installed, the central services act as both the engine and the collector.

To install a collector, you must have the **RabbitMQ** service installed for communication between the central engines and the collectors. RabbitMQ is installed

> For further details, see section **Application > Central Service > Collector Relations** in the File Access Manager Administrator Guide

Adding a Generic Table Application

In order to integrate with Generic Table, we must first create an application entry in File Access Manager. This entry includes the identification, connection details, and other parameters necessary to create the link.

To add an application, use the **New Application Wizard**.

1. Navigate to *Admin* > *Applications*
2. Click **Add New** to open the wizard.

Select Wizard Type

1. Click **Standard Application**
2. Click **Next** to open the **General Details** page.

General Details

Application Type

Generic Table

Application Name

Logical name of the application

Description

Description of the application

Tags

Select tags for the application from the dropdown menu, and / or type a new name, and press **Enter** to create a new tag. The dropdown list of tags filters out matching tags as you type and displays up to 50 tags.

> The **tags** replace the **Logical container** field that was used when creating applications in releases before 8.2

Event Manager Server

This option is available if there are more than one event manager servers configured in the system.

Select an event manager from the drop down menu.

Click **Next**. to open the Connection Details page.

Connection Details

Complete the Connection Details fields:

Database Type

The type of database, either SQL Server or Oracle.

SQL Server Only Fields

Server Name

The SQL Server

Database Name

The SQL database

Use Windows Authentication

The default is not to use Windows authentication

Oracle Only Fields

Oracle Data Source Name

The Oracle data source to connect to

Username / Password

The user to connect to the database

Activities Query

This query will periodically run to fetch new activities

Activity ID Column Name

The column name in the *Activities Query* which identifies the unique id of the activity. This column is used to query for new activities periodically

Business Resource Column Name

The column name in the *Activities Query* which will be displayed to the user as the Business Resource Full Path in the Activities Forensics

Username Column Name

The column name in the *Activities Query* which will be displayed to the user as the User Name in the Activities Forensics

Action Column Name

The column name in the *Activities Query* which represents the action

Activities Timestamp Column Name

The column name in the *Activities Query* which represents the time the activity occurred

Sample Event Column Name

Either by Event ID or by date

> The Generic Table connector adds a condition for each query to fetch only new events. This condition is created with the Sample Event Column.

Query Timeout (min)

In minutes, the default being 0, which means wait indefinitely

Click **Next**

Configuring Activity Monitoring

Configure the activity monitoring processes frequency.

Polling Interval (sec)

Activity fetching interval [in seconds]). Default is set to 60 seconds,

Report Interval (sec)

Activity Monitor Health reporting interval [in seconds]). Default is set yo 60 seconds.

Local Buffer Size (MB)

Local buffer size for activities [in MB]). Default is set to 200MB.

This cyclic buffer is used to store activities on the Application Monitor's machine in case of network errors that prevent the activities from being sent.

Configuring Data Enrichment Connectors

The Data Enrichment Connectors (DEC) configuration enables us to select data enrichment sources. These can be used to add information from other sources about identities.

An enrichment source could be a local HR database that is used to combine users' job descriptions or departments to the information stored in the identity store.

Select the data enrichment connectors to enrich monitored activities from the Available DECs text box.

Use the > or >> arrows to move the selected DECs to the Current DECs text box.

The user can select multiple DECs. Simply select each desired DEC.

You can create a new DEC in the Administrative Client(Applications>Configuration>ActivityMonitoring>DataEnrichmentConnectors).

After creating a new DEC, click **Refresh** to refresh the dropdown list.

The chapter Connectors of the File Access Manager Administrator Guide provides more information on Data Enrichment Connectors, including what they are, how to configure them, and how they fit in the Activity Flow.

Installing Services: Activity Monitor and Collectors

The Collector Installation Manager is part of the File Access Manager installation package. This tool is used to install the activity monitor, permission collector, and data classification collector.

Activity Monitor

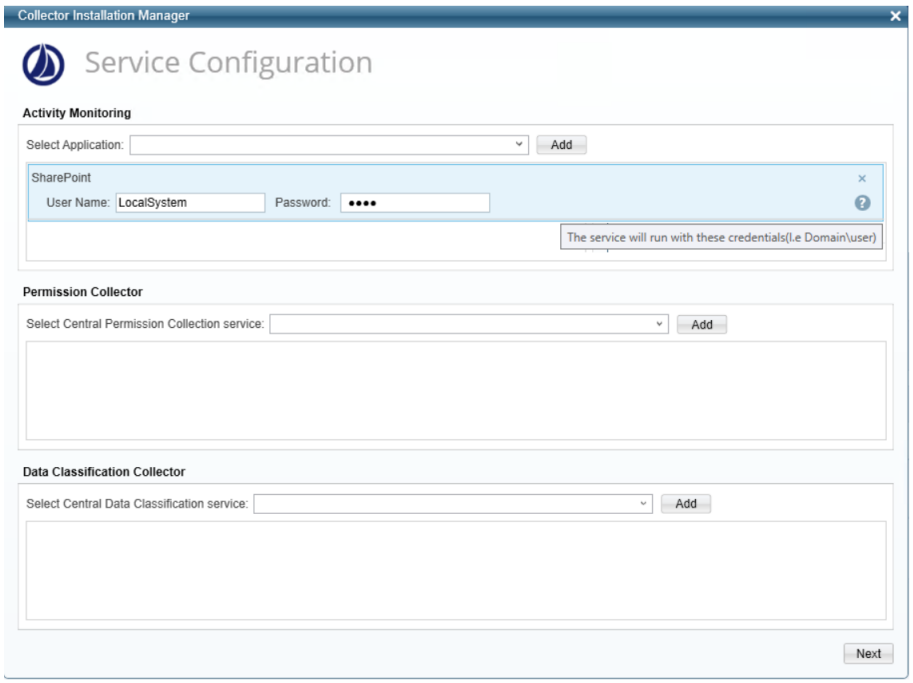
The activity monitor is installed per application, and collects SharePoint Audit entries and IIS activity logs.

1. Run the **Collector Installation Manager** as an Administrator.
   The installation files are in the installation package under the folder **Collectors**.

   The Collector Installation Manager window displays.

2. Enter the credentials to connect to File Access Manager.
   a. ServerName/IP should be pointed to the Agent Configuration Manager service server.
   b. An File Access Manager user with Collector Manager permission (permission to install collectors). For Active Directory authentication, use the format domain\username.
3. Click **Next**.

   The Service Configuration window displays.



4. If you are installing the Activity Monitor, select the application, and click **Add.**
5. When installing a SharePoint Activity Monitor, you will be prompted for service account credentials. This service account will be used by the Activity Monitor service to run the service and authenticate against the SharePoint IIS servers to fetch the logs (“Log on as”). Make sure the service account provided has local administrator privileges on the local server (hosting the Activity Monitor service) and can access the activity logs on the IIS servers.
6. Click **Next**.

   The Installation Folder window displays.

   > If this is the first time you are installing collectors on this machine, you will be prompted to select an installation folder, in which all future collectors will also be installed.

7. Browse and select the location of the target folder for installation.
8. Browse and select the location of the folder for system logs.
9. Click **Next**.
10. The system begins installing the selected components.
11. Click **Finish**

    The Finish button is displayed after all the selected components have been installed.

> The *File Access Manager Administrator Guide* provides more information on the collector services.

Verifying the Generic Table Connector Installation

Installed Services

Verify that the services installed for the connector are available and active. Using windows Service manager, or other tool, look for the File Access Manager services, and see that they are running.

for example:

- File Access Manager Central Activity Monitor - <Service Name> service is running.

Log Files

Check the log files listed below for errors

- “%SAILPOINT_HOME_LOGS%\GenericDBTable-<Application_Name>.log" .

Monitored Activities

1. Simulate activities by inserting them into the Generic Table on the database selected during the connector configuration.
2. Wait a minute (approximately).
3. Verify that the activities display in the File Access Manager website under *Forensics* > *Activities*