Integrating Azure Files with File Access Manager

Version: 8.3 Revised: March 30, 2022

Contents

Capabilities

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

- Analyze the structure of stored data
- Classify the data being stored
- Verify user permissions on the resources and compare them against requirements

Supported Versions

The File Access Manager Azure Files Connector supports the following versions of MS Windows Server:

- 2012 R2, 2016, 2019
- 32 and 64-bit support for all versions

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 .

AD DS Authentication

This connector requires identity-based authentication over Server Message Block (SMB) through on-premises Active Directory Domain Services (AD DS).

Permissions

File Access Manager requires different permissions, based on the tasks that require those permissions. The user configured in the Application configuration wizard must have the following permissions on the Azure Files storage:

- Read share-level RBAC permissions for the desirable shares
- Read NTFS permissions to all folders on the share

Why do we need this access?

In order to get the following information from the Azure Files Storage, File Access Management uses the SMB/CIFS protocol. This requires permissions both on the share level (Azure role-based access control - Azure RBAC) and on the directory level (New Technology File System - NTFS).

The following detailed explanation describes required permissions by each File Access Manager task:

Crawling

The user must have Read permissions to the requested shares and all its folders on the Azure Files storage.

Permission Collection

The user must have Read permissions to the requested shares and all its folders on the Azure Files storage.

Data Classification

The user must have Read permissions to the requested shares and all its folders on the Azure Files storage.

Communications Requirements

Requirement	Source	Destination	Port
File Access Manager Message Broker	Permission Collector / Data Classification Collector	RabbitMQ	5671
Permissions Collector /Data Classification Analysis	Permissions Collector/Data Classification Server	Monitored Azure Files Storage	CIFS/SMB (139, 445)

Connector Installation Flow Overview

To install the Azure Files connector:

1. Configure all the prerequisites.
2. Add a new Azure Files application in the Business Website.
3. Install the relevant services:
    - Permission Collector
    - Data Classification Collector

> Installing the permissions collector and data classification services is optional and should only be installed by someone with a full understanding of File Access Manager deployment architecture. The File Access Manager Administrator Guide has additional information on the architecture.

Collecting Data Stored in an External Application

Connector / Collector 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 Data Classification and/or 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 Data Classification central engine

One or more central engines, installed using the server installer

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.

Install Permission Collectors and/or Data Classification Collector (optional)

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, 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 an Azure Files Application

In order to integrate with Azure Files, 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

Azure Files

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

Identity Collector

Select from the Identity Collector dropdown menu.

You can create identity collectors in the administrative client be navigating to **Applications > Configuration > Permissions Management > Identity Collectors**.

See OOTB Identity Collection in the Collector Installation Manager File Access Manager Administrator Guide for further details.

If adding a new identity collector, click the **Refresh** button to update the Identity Collector dropdown list.

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

Connection Details

Server Name

Name of the Azure Files storage account which is monitored

The correct format is: <storageAccountName>.file.core.windows.net

Domain Name

Credentials which will be used by the Permission Collector, Crawler, and Data Classifications

Username

Credentials which will be used by the Permission Collector, Crawler, and Data Classifications

Password

Credentials which will be used by the Permission Collector, Crawler, and Data Classifications

Click **Next**

Configuring and Scheduling the Permissions Collection

Permissions can be analyzed to determine the application permissions of an out-of-the-box application, provided you have defined an identity store for File Access Manager to use in its analysis, and you have run a crawl for the application.

The permission collector is a software component responsible for analyzing the permissions in an application.

The Central Permission Collector Service is responsible for running the Permission Collector and Crawler tasks.

If the File Access Manager Central Permission Collector wasn't installed during the installation of the server, this configuration setting will be disabled.

To configure the Permission Collection

- Open the edit screen of the required application.
  a. Navigate to **Admin > Applications**.
  b. Scroll through the list, or use the filter to find the application.
  c. Click the edit icon on the line of the application.
- Press **Next** till you reach the **Crawler & Permissions Collection** settings page.

  The actual entry fields vary according to the application type.

When entering this page in edit mode, you can navigate between the various configuration windows using the **Next** and **Back** buttons.

Central Permissions Collection Service

Select a central permission collection service from the dropdown list. You can create permissions collection services as part of the service installation process. See section "Services Configuration" in the File Access Manager Administrator Guide for further details.

Calculate Effective Permissions

Calculate effective permissions during the permissions collection run

Calculate Riskiest Permissions

Calculates the riskiest permission on a resource, for example, Full Control is riskier than Read permissions if both are on a resource.

This option is available when selecting **Calculate Effective Permissions**.

Skip Identities Sync during Permission Collection

Skip identity synchronization before running permission collection tasks when the identity collector is common to different connector.

This option is checked by default.

Scheduling a Task

Create a Schedule

Click on this option to view the schedule setting parameters.

Schedule Task Name

A name for this scheduling task

When creating a new schedule, the system generates a default name in the following format:

{appName} - {type} Scheduler

You can override or keep this name suggestion.

Schedule

Select a scheduling frequency from the dropdown menu.

- ***Schedule Types and Intervals***

  Once

  Single execution task runs.

  Run After

  Create dependency of tasks. The task starts running only upon successful completion of the first task.

  Hourly

  Set the start time.

  Daily

  Set the start date and time.

  Weekly

  Set the day(s) of the week on which to run.

  Monthly

  The start date defines the day of the month on which to run a task.

Quarterly

A monthly schedule with an interval of 3 months.

Half Yearly

A monthly schedule with an interval of 6 months.

Yearly

A monthly schedule with an interval of 12 months.

Date and time fields

Fill in the scheduling times. These fields differ, depending upon the scheduling frequency selected.

Active check box

Check this to activate the schedule.

Click **Next**.

Configuring and Scheduling the Crawler

To set or edit the Crawler configuration and scheduling

- Open the edit screen of the required application.
  a. Navigate to **Admin > Applications**.
  b. Scroll through the list, or use the filter to find the application.
  c. Click the edit icon on the line of the application.
- Press **Next** till you reach the **Crawler & Permissions Collection** settings page.

  The actual entry fields vary according to the application type.

Top Level Shares

Add the top-level shares names you would like to analyze:

- To add a share to a list, type in the name in the top field and click **+** to add it to the list.
- To remove a share from a list, find the share from the list and click the trashcan icon on the resource row.

Calculate Resource Size

Determine when, or at what frequency, File Access Manager calculates the resources' size.

Select one of the following:

- Never
- Always
- Second crawl and on (This is the default)

Create a Schedule

Click to open the schedule panel.

Setting the Crawl Scope

There are several options to set the crawl scope:

- Setting explicit list of resources to include and / or exclude from the scan.
- Creating a regex to define resources to exclude.

Including and Excluding Paths by List

To set the paths to include or exclude in the crawl process for an application

- Open the edit screen of the required application.
    a. Navigate to **Admin > Applications**.
    b. Scroll through the list, or use the filter to find the application.
    c. Click the edit icon  on the line of the application.
- Press **Next** till you reach the **Crawler & Permissions Collection** settings page.

  The actual entry fields vary according to the application type.

1. Scroll down to the Crawl configuration settings.
2. Click **Advanced Crawl Scope Configuration** to open the scope configuration panel.
3. Click Include / Exclude Resources to open the input fields.
4. To add a resource to a list, type in the full path to include / exclude in the top field and click **+** to add it to the list.
5. To remove a resource from a list, find the resource from the list, and click the *x* icon on the resource row.

> When creating exclusion lists, excludes take precedence over includes.

Excluding Paths by Regex

To set filters of paths to exclude in the crawl process for an application using regex.

- Open the edit screen of the required application.
    a. Navigate to **Admin > Applications**.
    b. Scroll through the list, or use the filter to find the application.
    c. Click the edit icon  on the line of the application.
- Press **Next** till you reach the **Crawler & Permissions Collection** settings page.

  The actual entry fields vary according to the application type.

1. Click **Exclude Paths by Regex** to open the configuration panel.
2. Type in the paths to exclude by Regex, See regex examples in the section below. Since the system does not collect BRs that match this Regex, it also does not analyze them for permissions.

Crawler Regex Exclusion Example

The following are examples of crawler Regex exclusions:

Exclude all shares that start with one or more shares names:

Starting with \\server_name\shareName

Regex: \\\\server_name\\shareName$

Starting with \\server_name\shareName or \\server_name\OtherShareName

Regex: \\\\server_name\\(shareName|OtherShareName)$

Include ONLY shares that start with one or more shares names

Starting with \\server_name\shareName

Regex: ^(?!\\\\server_name\\shareName($|.)).

Starting with \\server_name\shareName or \\server_name\OtherShareName

Regex: ^(?!\\\\server_name\\(shareName|otherShareName)($|.)).

Narrow down the selection

> To write a backslash or a dollar sign, add a backslash before it as an escape character.

> To add a condition in a single command, use a pipe character “|” .

Special Consideration for Long File Paths in Crawl

If you need to support long file paths above 4,000 characters for the crawl, set the flag

`excludeVeryLongResourcePaths`

in the Permission Collection Engine App.config file to true.

By default this value will be commented out and set to false.

This key ensures, when enabled, that paths longer than 4000 characters are excluded from the applications’ resource discovery (Crawl), to avoid issues while storing them in the SQLServer database.

When enabled, business resources with full paths longer than 4000 characters, and everything included in the hierarchical structure below them, will be excluded from the crawl, and will not be collected by File Access Manager. This scenario is extremely rare.

> You should not enable exclusion of long paths, unless you experience an issue.

Background

File Access Manager uses a hashing mechanism to create a unique identifier for each business resource stored in the File Access Manager database. The hashing mechanism in SQLServer versions 2014 and earlier, is unable to process (hash) values with 4,000 or more characters.

Though resources with paths of 4000 characters or longer are extremely rare, File Access Manager is designed to handle that limitation.

Identifying the Problem

When using an SQL Server database version 2014 and earlier, the following error message in the Permission Collection Engine log file:

```
System.Data.SqlClient.SqlException (0x80131904): String or binary data would be truncated.
```

In all other cases, this feature should not be enabled.

Setting the Long Resource Path Key

The Permission Collection Engine App.config file is `RoleAnalyticsServiceHost.exe.config`, and can be found in the folder

%SailPoint_Home%\FileAccessManager\[Permission Collection instance]\

Search for the key **excludeVeryLongResourcePaths** and correct it as described above.

Selecting and Scheduling the Data Classification Settings

To associate an application with a data classification service, and set the schedule

- Open the edit screen of the required application
  a. Navigate to **Admin > Applications**
  b. Scroll through the list, or use the filter to find the application
  c. Click the edit icon on the line of the application
- Press **Next** till you reach the **Data Classification** settings page.

  The actual entry fields vary according to the application type

Central Data Classification Service

Associate the application with a Central Data Classification Service. This service is responsible for running the Data Classification tasks.

If the Central Data Classification wasn't installed during the installation of the server, this field is disabled.

Disabling Data Classification

To disable data classification, delete the entry from the central data classification field.

Disabling data classification can also be achieved by setting the scheduler to be inactive (which is the default setting for data classification).

Create a Schedule

This option is enabled only if a central data classification service is selected.

See Configuring and Scheduling the Permissions Collection

> See the chapter "Data Classification" in the File Access Manager Administrator Guide for more information

Click **Next** or **Finish**.

Data Privacy

A user can associate the application with a Central Data Classification Engine Service. This engine will be responsible for executed Data Privacy tasks.

Though using different processes for each, the Data Classification engine service is in charge for both Data Privacy and Data Classification discovery tasks.

You may choose the same service for both, or use a different one for each, to run them in parallel.

> The fields on the Data Privacy step are the same as the Data Classification step.

Installing Services: Collector Installation

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

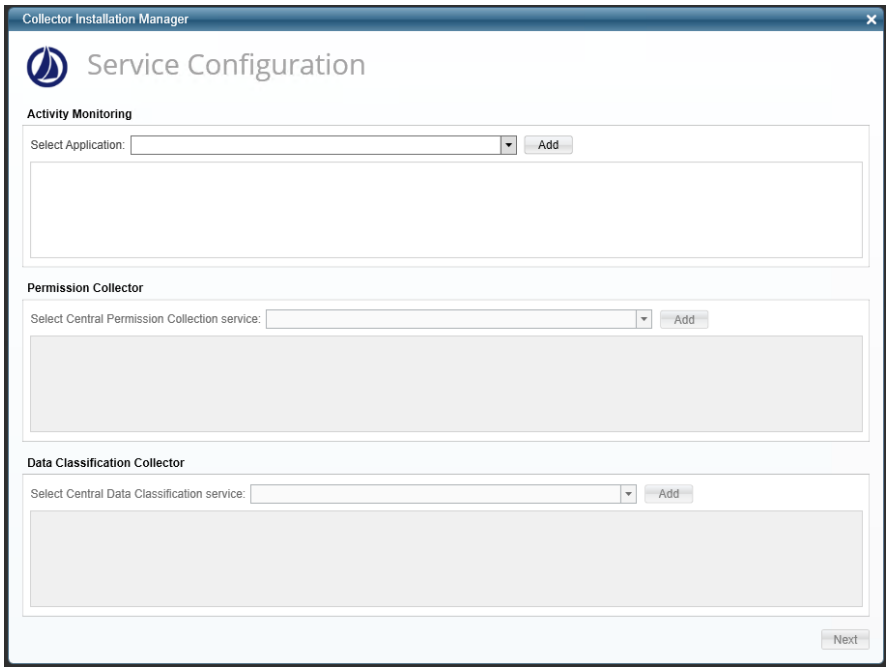
   The Collector Installation Manager window displays.

2. Enter the credentials to connect to File Access Manager.

   a. ServerName/IP should be pointed to the Agent Configuration Manager service server.

   b. A File Access Manager user with Collector Manager permission (permission to install collectors). For Active Directory authentication, use the format domain\username.

3. Click **Next** to open the Service Configuration window.



4. If you are installing the Permission Collector, select the Central Permission Collector to which to connect this service. Click **Add**.
5. If you are installing the Data Classification, select the Central Classification Collector to which to connect this service. Click **Add**.
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. All future collectors will be installed in this folder.

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 Azure Files 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 Permissions Collection - <Application_Name>
- File Access Manager Central Data Classification - <Application_Name>

Log Files

Check the log files listed below for errors

- “%SAILPOINT_HOME_LOGS%\PermissionCollection_<Service_Name>.log"
- “%SAILPOINT_HOME_LOGS%\DataClassification_<Service_Name>.log"

Permissions Collection

1. Run the Crawler and Permissions Collector tasks (**Settings > Task Management > Scheduled Tasks**)
2. Verify that:
    - The tasks completed successfully
    - Business resources were created in the resource explorer (**Admin > Applications > [application column] > Manage Resources**)
    - Permissions display in the Permission Forensics page (**Forensics > Permissions**)