SailPoint IdentityIQ

Version 8.1

File Access Manager

DFS Connector Installation Guide

Table of Contents

Chapter 1: Connector Installation & Configuration

Overview

Installation Flow

1. Configure all the prerequisites.
2. Add a new application to the IdentityIQ File Access Manager Administrative Client.
3. Run a Crawl task.

Chapter 2: General

Terminology

- DFS Namespace – A virtual view of shared folders on servers provided by DFS. A DFS namespace consists of a root and many links and targets. The namespace starts with a root that maps to one or more root targets. Below the root are links that map to their own targets.
- Domain-based DFS namespace – A DFS namespace whose configuration information is stored in Active Directory.
- DFS Link (folder with targets) – A component in a DFS path that lies below the root and maps to one or more link targets.
- DFS Link Target (folder target) – The mapping destination of a link. A link target can be any UNC path, such as (for example) a shared folder or another DFS path.
- Figure 1 contains the following link folders:
  - "Tools" which has two targets: "\\LDN-SVR-01\Tools London" and "\\NYC-SVR-01\Tools New York".
  - "Training Guides" which has one target: "\\NYC-SVR-02\Training New York"

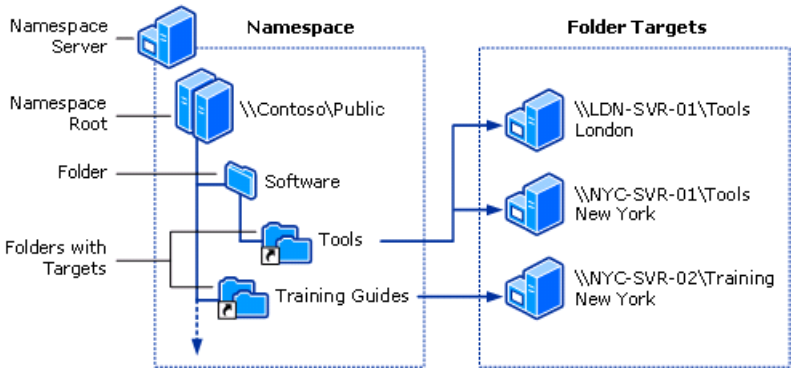

Figure 1. DFS Technology Elements

Connector Operation Principles

- IdentityIQ File Access Manager Windows DFS application differs from other IdentityIQ File Access Manager connectors in that it does not actively monitor activities, collect permissions, or classify data. Instead, it acts as a logical representation of multiple physical applications. It fetches data by mapping DFS logical shares to their corresponding physical target applications shares.
- The crawler service creates mapping between DFS applications and physical applications.

Note: Windows DFS applications only supports domain-based DFS namespaces.

Note: An application must be configured in IdentityIQ File Access Manager for each DFS domain.

Crawler Responsibilities

- The crawler works with native API calls that communicate with the domain controller and the DFS namespace servers.
- The crawler:
  - Creates the DFS resources tree
  - Creates mapping between the DFS links resources and physical applications resources.
  - The crawler can only map DFS links to physical shares in the IdentityIQ File Access Manager database. Therefore, before the DFS crawler runs, the shares in the physical applications must have already been found. If a physical share is not found for a DFS link, the crawler will issue an “unfound target” warning in the task details.

Monitored Activities

Any activities on shares that are targets of DFS links are “tagged” with an additional field with the logical DFS path and an indication that they are DFS-related. This allows activities to be queried via a DFS application and business resources and to have its DFS logical path displayed.

Any activity type monitored by a physical application, mapped to the DFS application, can also be displayed via the DFS application.

Permission Collection

There is no need to collect DFS resource permissions, as they are logical resources that only point to the physical folders in which actual data are located. Windows DFS applications do not have a Permission Collection service.

To display permissions, DFS applications redirect their link folders to their mapped targets and display the results collected by their physical applications.

For example:
Given the DFS structure in Figure 1, if we query the “Training Guides” DFS resource for permissions, the query will redirect itself to the physical “\\NYC-SVR-02\Training New York” resource and its permissions.

Data Classification

There is no need to collect DFS data classifications, as they are logical resources that only point to the physical folders in which actual data are located. Windows DFS applications do not have a Data Classification service.

To display Data Classification results, DFS applications redirect their link folders to their mapped targets and display the results which were collected by their physical applications.

For example:
Given the DFS structure in Figure 1, if we query the “Training Guides” DFS resource for classified data, the query will redirect itself to the physical “\\NYC-SVR-02\Training New York” resource and its Data Classification results.

DFS Link Targets Priority

Some DFS links may point to multiple physical shares that are assumed to be replicated. If so, IdentityIQ File Access Manager selects prioritized results from one or more physical shares, which is different for each of the following scenarios:

- Activities – When a link has multiple targets, all physical target resources are queried for activities, since activities are not necessarily replicated consistently across shares.
- Permissions – When a link has multiple targets, the target with the most recent IdentityIQ File Access Manager permission analysis is selected.
- Data Classification – When a link has multiple targets, the target with the most recent IdentityIQ File Access Manager Data Classification analysis is selected.

Manual Matching of Unknown Target Host Names

During a DFS Crawl, the Crawler tries to match target host names to the host names of existing applications in the IdentityIQ File Access Manager database.

When the Crawler is unable to match specific hosts, it attempts to match hosts via DNS lookups, and to find valid matching alias names (for example, a host name displayed as an IP address).

If a search cannot find host names or cannot match host name aliases to an existing host in the IdentityIQ File Access Manager database, it is possible to configure matching hosts manually.

To manually configure matching hosts, perform the following steps:

1. Create an *.xml file with the following structure:

```
<?xml version="1.0"?>
<mappings>
<key name="hostA">AlternateHostA</key>
<key name="hostB">172.66.12.12</key>
</mappings>
```

   In the above example, “hostA” is a host name of a link target to be matched manually. “AlternateHostA” is the host name to which “hostA” will be matched.

   Note: Note:“AlternateHostA” should be a host name of an existing application in IdentityIQ File Access Manager.

2. Add the following key to the DFS Permissions Collector’s service “app.config”.

```
"<add key="dfsMappings" value="C:\myMappings.xml"/>"
```

3. Replace "C:\myMappings.xml" with the path that points to the configuration file.
4. Restart the DFS Permissions Collector service.

Chapter 3: Prerequisites

Software Requirements

- Microsoft .Net Framework 4.5

Permissions

When the Crawler service runs on a server, which is part of the domain that hosts the domain-based DFS namespaces, neither a user nor a password configuration is required.

If the server is not part of the DFS domain, then the following requirements must be met:

- The server must be able to resolve the DFS domain.
- The Crawler service must be configured with a standard domain user on that DFS domain in order to gain access using impersonation.

Communications Requirements

Table 1—Communications Requirements

Requirement	Source	Destination	Port
Database Access	Permissions Collector	IdentityIQ File Access Manager DB	Per the specific DB definitions

Chapter 4: Add New Application Wizard

1. Navigate to

   Admin Client **Applications >> New >> Application**

2. The **New Application Wizard** window displays under the Welcome tab.
3. Select Standard Application.
4. Select **Windows DFS** from the **Application Type** dropdown menu
5. Click **Next**
   The General Details window of the New Application Wizard displays under the General tab.
6. Type the logical name of the application in the *Name* field.
7. Type a description of the application in the *Description* field.
8. Select a logical container for the application from the **Container** dropdown menu.
9. Click **Next**.
   The first Monitor Configuration window of the New Activity Monitor Wizard displays under the Configuration tab.
10. Complete the Connection Details fields:
    - *Domain Name* (FQDN of the domain) that hosts the domain-based DFS namespaces.
    - *User* (samAccount Name of the User with the required permissions, or the User Principle Name (UPN) if the user is from a trusted domain)
    - *Password* (User's password for this configuration)

    Note: ***Note:*****User, and Password are defined for the user in the prerequisites.**
11. Select the relevant Permissions Collection service:
12. Click **Next**.

    Note: Note:The Windows DFS application supports only crawling, therefore, the scheduling tab will only contain the crawler scheduling window.

    The Crawler window of the New Application Wizard displays under the Scheduling tab.

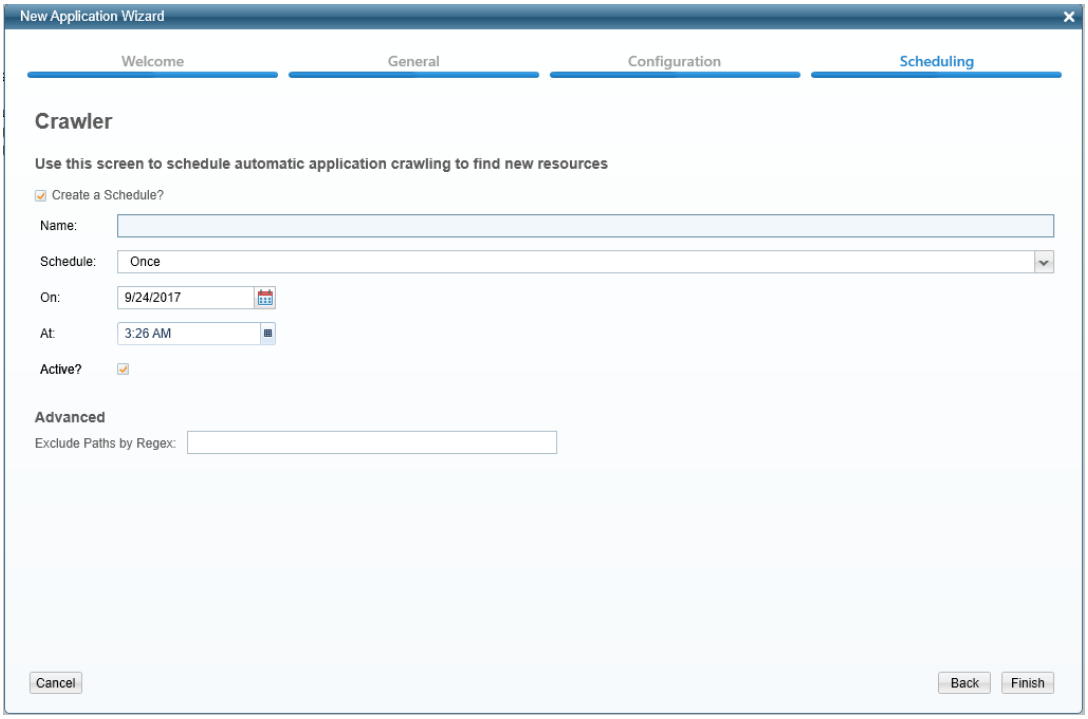

Figure 2. Crawler Window

13. Check the **Create a Schedule** check box.
14. Type a name for the crawling scheduling task in the *Name* field.
15. Select a scheduling frequency from the **Schedule** dropdown menu.
16. Fill in the relevant date and time fields (which differ, depending upon the scheduling frequency selected).
17. Check the **Active** check box if relevant.
18. Type in the distinguished paths to exclude from the crawling process in the *Exclude Paths by Regex* field

    Note: Note:See the chapter "Crawling" of the *IdentityIQ File Access Manager Administrator Guide* for more information.

19. Click **Finish**

Chapter 5: Verification

Crawler

1. Run the Crawler task in the IdentityIQ File Access Manager Administrative Client.
2. Verify that:
   - The tasks completed successfully
   - Business resources were created on the business resource tree
   - DFS is mapped to physical resources

Monitored Activities

1. Assure that activities are received for the physical application, mapped to the DFS share.
2. Run the Crawler task, and verify that the DFS business resource tree has the DFS share and folder to be used for the activity simulations.
3. Simulate activities on physical DFS shares.
4. Wait a for approximately one minute.
5. Query activities in the IdentityIQ File Access Manager Website by selecting the DFS application <Application_Name>.
6. Verify that the activities display in the web Client.

   Note: Note:The activity details should contain a "Logical Paths" field with the DFS logical paths.

Permissions Collection

1. Run a Permissions Collector task on a physical application with DFS target shares.
2. Verify that:
   - The task completed successfully.
   - Permissions display in the Permissions Forensics window for the physical DFS target shares.
   - Permissions display in the Permissions Forensics window for the DFS links which points to the above physical target shares.

Data Classification

1. Run a Data Classification task on a physical application with DFS target shares.

2. Verify that:
    - The task completed successfully.
    - Data Classification results display in the Web Client's Data Classification Forensics window for the physical DFS target shares.
    - Data Classification results display in the Web Client's Data Classification Forensics window for the DFS links that point to the above physical target shares.

Chapter 6: Troubleshooting

If activities are not shown in the Administrative Client:

- Verify that all prerequisites were set.
- Check if the shares on the physical applications have activities.
- If the physical shares do not have activities, this indicates that the monitor on the physical application is not working properly. Please refer to the relevant physical application Connector Troubleshooting guide.
- If the shares on the physical applications have activities, but the DFS shares do not have activities, this indicates that the Windows DFS crawler did not map the DFS shares to physical application shares properly.