SailPoint IdentityIQ

Version: 8.0

File Access Manager EMC Celerra and VNX NAS Connector Installation Guide

Table of Contents

List of Figures

List of Tables

Table of Revisions

Ver. #	Description	Author	Date
5.0	Final Version	Jonathan Rappeport	10 Jan 2017
5.1	First Draft	Jonathan Rappeport	08 Feb 2017
5.1	Second Draft	Jonathan Rappeport	13 Jun 2017
5.1	Third Draft	Jonathan Rappeport	26 Sep 2017
6.0	First Draft	Jonathan Rappeport	10 May 2018
6.1	Formatting changes only	Josh Lewin	11 Dec 2018
8.0	• Formatting • Adding command to enable CEPA on the data mover for NFS • Rebranding – IdentityIQ File Access Manager 8.0	Josh Lewin	28 Jul 2019

Chapter 1: Connector Installation & Configuration

Overview

Installation Flow

1. Configure all the prerequisites.
2. Add a new application to the IdentityIQ File Access Manager Admin Client.
3. Install the Activity Monitor/Permissions Collector/Data Classification Collector services.

Note: Permissions Collector and Data Classification services installation is optional and should only be installed by someone with a full understanding of IdentityIQ File Access Manager deployment architecture. The IdentityIQ File Access Manager Administrator Guide has additional information on IdentityIQ File Access Manager architecture.

Chapter 2: General

Activity Monitor Operation Principles

- IdentityIQ File Access Manager Connector for EMC uses EMC CEPA over the Common Event Enabler Framework (or CEE, formerly known as CAVA) infrastructure for getting audit events from the Celerra/VNX NAS for both CIFS and NFS file access.
- The Activity Monitor supports different architectures and can work with either a single or multiple, remote, or local CEE services.

Permissions Collector Operation Principle

CIFS Shares

- IdentityIQ File Access Manager connects using EMC administrative shares and analyzes folder permissions.
- Local groups and users are collected from the CIFS server during the Permission Collector process.

NFS Exports

- IdentityIQ File Access Manager connects using standard NFSv3 access to analyze UNIX-style folder permissions.
- A NIS Identity Collector is used to resolve UIDs/GIDs permissions discovered during the Permissions Collection process.

Monitored Activities

Table 1. Monitored Activities

Action	Meaning
Create File	A new file was created.
Create Folder	A new folder was created.
Create from Move	A “Create Folder” event generates this event on the newly created folder.
Create from Rename	A “Rename Folder” event generates this event on the newly created folder.
Delete File	A file was deleted.
Delete Folder	A folder was deleted.
Move File	A file was moved.
Move Folder	A folder was moved.
Permission Change File	A file’s permissions were changed.
Permission Change Folder	A folder’s permissions were changed.
Read File	A file was read.

Action	Meaning
Rename File	A file was renamed.
Rename Folder	A folder was renamed.
Write File	A file was modified.

Supported Versions

- EMC Celerra 6.0 and above (including Virtual Data Mover and Aliases).

Chapter 3: Celerra/VNX Components Overview

For more information and a deep technical understanding of the EMC architecture and CEE, refer to the EMC CEE version 7.0 using the Common Event Enabler for Windows

https://www.emc.com/collateral/TechnicalDocument/docu48055.pdf

Physical & Virtual Data Mover

Celerra/VNX architecture is based on physical components named data movers.

A physical data mover can host multiple virtual data movers (VDMs).

Note: Audit facility (CEPA) is single for each physical data mover, and must be configured separately for each physical data mover.

CIFS Server

A CIFS server is an EMC component that corresponds to a file server (\\cifs_server_name).

You can configure a CIFS server on a physical Data Mover or on a VDM. Typically, the CIFS servers are configured on a VDM.

Every CIFS server requires an Application definition in IdentityIQ File Access Manager.

CIFS Servers Aliases

An alias is a synonym name of the CIFS server. It is defined in the CIFS server itself and is visible in the EMC Unisphere.

Every CIFS server can have one or more aliases.

You must configure the aliases as well in the Application configuration. Failure to do so results in losing the events of users accessing the aliases.

However, all the activities are always saved in IdentityIQ File Access Manager with the real name of the filer.

Notes:

- **The filer name configured in the application must be the real name only.**
- **A DNS alias is not an EMC alias.**

NFS Exports

An NFS export is an EMC component that can be associated with any existing network interface to expose a UNIX-style NFS file server.

Every NFS network interface that exposes NFS exports requires an Application definition in File Access Manager.

CEE

A CEE service is the EMC gateway for communicating and receiving events notifications from the data movers.

All data movers send notifications on CIFS/NFS events to the CEE service. The service in the data mover responsible for sending the events to the CEE is called CEPA (Celerra Event Publishing Connector).

There is an n:n relation between the CEPA service running on the data mover and the CEE service:

Every CEE can communicate with multiple data movers.

Every CEPA service on a data mover can communicate with multiple CEE servers (for high availability and load sharing).

CEPA and Virtual Data Movers

For CEE to work, you need to have a CIFS server configured on the physical Data Mover. This is the global CIFS server or the default CIFS server on the physical Data Mover.

CEE & Activity Monitor

Every Activity Monitor can communicate with one or more CEE servers.

Every CEE service can be configured to work with a multiple Activity Monitor services.

Activity Monitor Service

Each Activity Monitor in IdentityIQ File Access Manager corresponds to a single CIFS server.
The first Activity Monitor installed on a physical server creates the Activity Monitor service. All subsequent Activity Monitors installed will not create additional Activity Monitor services.

Every Activity Monitor that is installed adds a *bamconfig.xml* file under the Activity Monitor to add itself to the same service.

Note: The first installed Activity Monitor must be the last Activity Monitor uninstalled. If you uninstall the first Activity Monitor before uninstalling the other installed Activity Monitors, those Activity Monitors will not work, and it will not be possible to uninstall them.

NFS Event Monitoring Peculiarities

The NFS Event Monitoring peculiarities include:

- EMC Celerra event data for NFS activities does not contain a full path to the target object, but only NFS identifiers (*inode*) regarding the target files and folders. To complete the partial event data File Access Manager event monitor maintains a local cache mapping inode identifiers to physical paths.
- The local cache mapping is based on the results of the crawling process, which collects the inode and file system information required to complete the event details.
- EMC Celerra pushes events into CEE service only if it is online and having at least one connected client. Therefore, any activity occurring when EMC CEE or File Access Manager event monitor services are down will not be registered. A downtime such as this may cause the local inode mapping cache to go out-of-sync with the actual directory structure on the NFS server.
- The only resolution to an out-of-sync state is to resynchronize File Access Manager by running a new crawl task, thus updating the database.

Note: The Activity Monitor service synchronizes the entire folder structure of the monitored NFS environment locally. Plan your configuration with caution regarding network and disk load that may arise.

Sample Architecture

In the schema below, the first physical Data Mover is configured to send events to CEE 1 & 2. CEE 1 & 2 are configured to send events notifications to the Activity Monitor.

The second physical Data Mover is configured to send events to CEE 2 & 3. CEE 2 & 3 are configured to send events notifications to the Activity Monitor.

- CIFS Server 1
- CIFS Server 2
- NFS Export 1

The Activity Monitor monitors using CEE 2 & 3:

- CIFS Server 4
- CIFS Server 5
- NFS Export 2

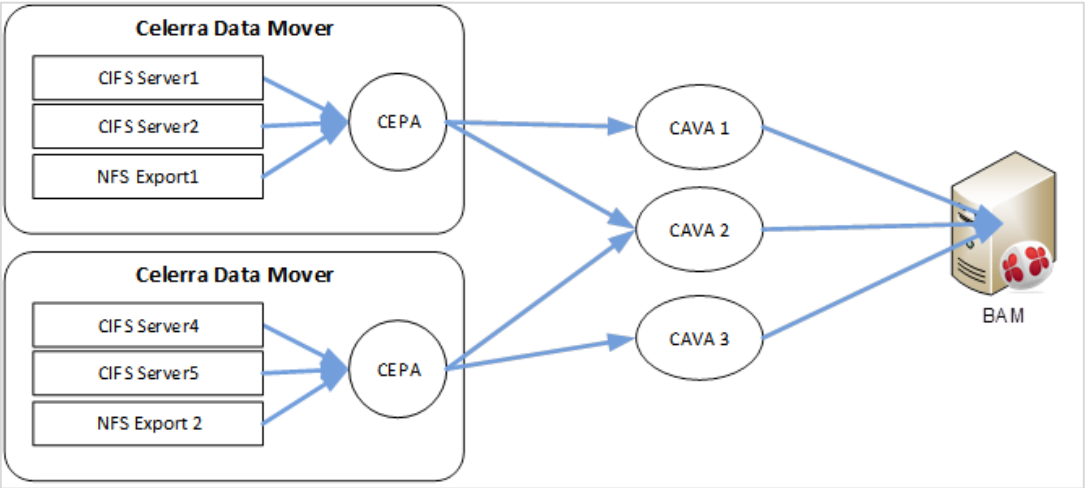

Figure 1. Configuration Drawing

Chapter 4: Prerequisites

Configure the CEE Service

Supported Versions

- EMC CAVA/CEE version 4.9.3 and above

Remote CEE

For enterprises with an existing central CEE infrastructure, where the Activity Monitor will be installed on a different server than the CEE service:

1. On every CEE server, open the registry and perform the following changes:

```
[HKLM\Software\EMC\CEE\CEPP\Audit\Configuration] set
 Endpoint=whitebox@<File Access Manager Activity Monitor server ip address>
 Enabled=1
```

Note: If multiple monitor servers exist, the list should look like: whitebox@ip, whitebox@ip, ...

2. Restart the EMC CEE service.

Local CEE (no central infrastructure)

When installing the CEE service and the Activity Monitor service on the same server:

1. Install CEE Pack on the monitor server.
   The CEE service must be installed on a server in the same domain as the physical data mover CEE server, otherwise the communication between the data mover and the CEE service will fail.

2. Open the registry and perform the following changes:

```
[HKLM\Software\EMC\CEE\CEPP\Audit\Configuration] set
Endpoint=whitebox
Enabled=1
```

3. Set the logon user for the services to a user according to the "required permissions" section.

4. Restart EMC CEE service.

Enable CEPA on the Data Mover

1. The CEPA configuration is separate and must be done for each physical data mover.

2. If you have multiple virtual data movers with CIFS servers, the CEPA configuration must be on the physical data mover (usually server_2 data mover when there is a single physical data mover).

3. If the configuration file (cepp.conf) does not exist, create a new one.

4. Login to the system with your administrative username (nasadmin) and password.

5. Use a text editor to create a new, blank file called *cepp.conf* file in the home folder with the following content:

```
ft level=[0/1] location=<location> size=<size>
pool name=sepapool \
servers=<cee1 FQDN>|<cee2 FQDN>|<cee3 FQDN> \
```

```
preevents= \
postevents=OpenFileRead|CreateFile|FileWrite|FileRead|CreateDir|DeleteFile|DeleteDi
r|CloseModified|RenameFile|RenameDir|SetAclFile|SetAclDir|SetSecFile|SetSecDir
posterrevents= \
option=ignore \
reqtimeout=500 \
retrytimeout=50
```

Notes:

- **The ft level parameter sets the fault tolerance level assigned. Valid values are 0-3, where:**
  - **0 = continue and tolerate lost events (default)**
  - **1 = continue and use a persistence file as a circular event buffer for lost events**
  - **2 = continue and use a persistence file as a circular event buffer for lost events until the buffer is filled and then stop CIFS**
  - **3 = upon heartbeat loss of connectivity, stop CIFS**
    It is recommended that this value be set to 1. If you kept the recommended value, fill in the <location> and <size> parameters, where:
    - **location = directory where the persistence buffer file resides relative to the root of a file system. If a location is not specified, the default location is the root of the file system.**
    - **size = maximum size in MB of the persistence buffer file. The default is 1 MB and the range is 1 MB to 100 MB. It is recommended to set it on 100MB**
- **It is important to verify that all CEE FQDN server names are resolved and reachable from the data mover. You can also fill in the IP address of the server instead of FQDN.**

6. Copy the newly created file to the data mover:

```
server_file <movername> -put cepp.conf cepp.conf
```

♦ If cepp.conf exists, verify that the postevents parameter has the required values.

7. For NFS run the following command:

```
server_mount <data_mover> -o ceppcifs,ceppnfs <file system name> /<file system
path>
```

Synchronize with Domain Watch and Start the Service

```
server_date server_# -timesvc start ntp <domain controller ip>
```

Start the CEPA Service on the Data Mover

```
server_cepp <movername> -service -start
```

Additional Resources

For more information on how to configure the CEPA and CEE refer to the EMC CEE version 7.0 using the Common Event Enabler for Windows

https://www.emc.com/collateral/TechnicalDocument/docu48055.pdf

Permissions

IdentityIQ 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:

Activity Monitoring

- Requires a domain user with administrative privileges on the local machine (on which the CEE service is installed)

Crawling

- CIFS Access
  - Requires a user who is a member of the local Backup Operators group on the virtual CIFS server
  - Requires a user with Share Read access to all the shares on the virtual CIFS server
- NFS Access
  - Requires a user with permission to mount all NFS exports on the virtual NFS server
  - Requires a user with (a) read permission for all files and (b) execute permission for all directories on the virtual NFS server

Permission Collection

- CIFS Access
  - Requires a user with Shared Read access to all CIFS shares on the virtual CIFS server
  - Requires a user who is a member of the local Backup Operators group on the virtual CIFS server
  - Requires a user who is a member of the local Administrators group on the virtual CIFS server to be able to read share permissions and local users and groups
- NFS Access
  - Requires a user with permission to mount all NFS exports on the virtual NFS server
  - Requires a user with (a) read permission for all files and (b) execute permission for all directories on the virtual NFS server

Data Classification

- NFS Access
  - Requires a user with permission to mount all NFS exports on the virtual NFS server
  - Requires a user with (a) read permission for all files and (b) execute permission for all directories on the virtual NFS server
- CIFS Access
  - Requires a user with Share Read access to all CIFS shares on the virtual CIFS server
  - Requires a user who is a member of the local Backup Operators group on the virtual CIFS server

Communications Requirements

Table 2. Communications Requirements

Requirement	Source	Destination	Port
File Access Manager Internal Access	Application	File Access Manager Servers	8000-8008
File Access Manager Message Broker	Permissions Collector / Data Classification Collector	RabbitMQ	5671
EMC CEE	EMC Data Mover	CEE Service	RPC (135 + Dynamic)
CEPA Events Push	CEE Service	File Access Manager Application	RPC (135 + Dynamic)
CIFS - Permissions Analysis & Data Classification	Permissions Collection service and/or Data Classification service	CIFS file server	SMB
NFS - Permissions Analysis & Data Classification	Permissions Collection service	NFS file server	NFSv3

Software Requirements

- Activity Monitor/Permissions Collector/Data Classification Collector: .NET 4.5

Chapter 5: Add New Application Wizard

1. Admin Client Navigate to **System** → **Applications**.
2. Select New → Application.

   The **New Application Wizard** window displays under the Welcome tab.
3. Select Standard Application.
1. Select **EMC** as the application type.

   - EMC Celerra – CIFS
   - EMC Celerra – NFS
2. Select EMC Celerra from the Application Type dropdown menu
3. Click Next.

   The General Details window of the New Application Wizard displays under the General tab.
4. Type the logical name of the application in the *Name* field.
5. Type a description of the application in the *Description* field.
6. Select a logical container for the application from the **Container** dropdown menu.
7. Select an identity collector from the **Identity Collector** dropdown menu:

   - EMC Celerra CIFS – Choose an Active Directory identity collector
   - EMC Celerra NFS – Choose a Network Information Service (NIS) identity collector
8. Click **Next**.

   The Configuration window of the New Application Wizard displays under the Configuration tab.

   Note: See below for the description for the NFS configuration.
9. If you are configuring connector for CIFS, complete the Connection Details fields for CIFS:

   - Host Name (The real name of the CIFS server as users connect to it)
   - *User Domain*, *User*, & *Password* (for the user defined in the prerequisites)
   - *Aliases* (aliases defined in the EMC for the CIFS server)
10. If you are configuring connector for NFS Complete the Connection Details fields:

    - *Host Name* (The network address (typically the IP address) of the interface on which the NFS exports are exposed)
    - *User* (A NIS username (or root) to use when connecting to the NFS file server)
    - *Group* (A NIS group name (or root) to use when connecting to the NFS file server
    - *Aliases* (Network aliases to the NFS server (optional))
11. Click to enable Permission Collection, select a Central Permissions Collector and complete the relevant Permissions Collection items:

- *Skip Identities Sync* (Skip identity synchronization before running permission collection tasks when the identity collector is common to many different connectors.)

12. Click to enable Data Classification and select a central data classification service from the list
13. Click **Next**

    The Configuration window of the New Application Wizard displays under the Configuration tab.

14. Select the Monitoring Configuration options.

    - *Excluded File Extensions (*List of file extensions that are not monitored)
    - *Exclude Folders* (List of folders that are not monitored)
    - *Exclude Users* (List of users whose activities are monitored)

    Note: For CIFS, Each excluded user must be in the form of Domain\User. For NFS it must be only the User. When an activity from a new resource is detected:

    - **Store the activity** (Full Auto-Learning Mode) - Monitors all activities from all site collections (automatically creates new folders in the Business Resources Tree).
    - **Store the activity, only if the top-level resource was manually created in advance** (Semi Auto-Learning Mode - Monitor only manually defined resources and their sub-folders to be monitored.
    - **Discard the activity** (No Auto-Learning Mode—Make sure to manually define the resources to be monitored)—Monitor only manually-defined resources to be monitored.

    The Data Enrichment Connectors window of the New Application Wizard displays under the Data Enrichment tab.

15. Select the data enrichment connectors (DECs) to enrich monitored activities from the Available DECs text box and use the > or >> arrows to move them to the Current DECs text box.

    Note: The chapter *Connectors* of the IdentityIQ 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.

16. Click **Next**

Note: The Scheduling tab contains the Permissions Collection, Crawler, and Data Classification (if supported) scheduling windows. You can navigate among those windows, using the Next and Back buttons.

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

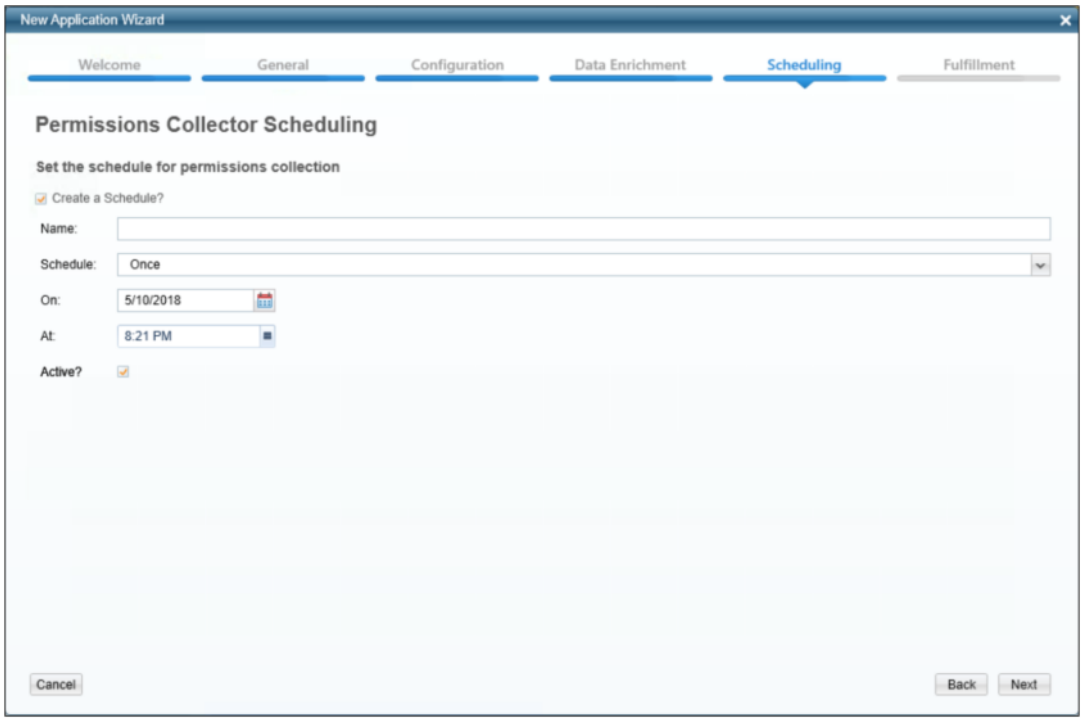

Figure 2. Permissions Collection Window

17. Check the **Create a Schedule** check box.
18. Type a name for the permissions collection scheduling task in the *Name* field.
19. Select a scheduling frequency from the **Schedule** dropdown menu.
20. Fill in the relevant date and time fields (which differ, depending upon the scheduling frequency selected).
21. Check the **Active** check box if relevant
22. Click **Next**

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

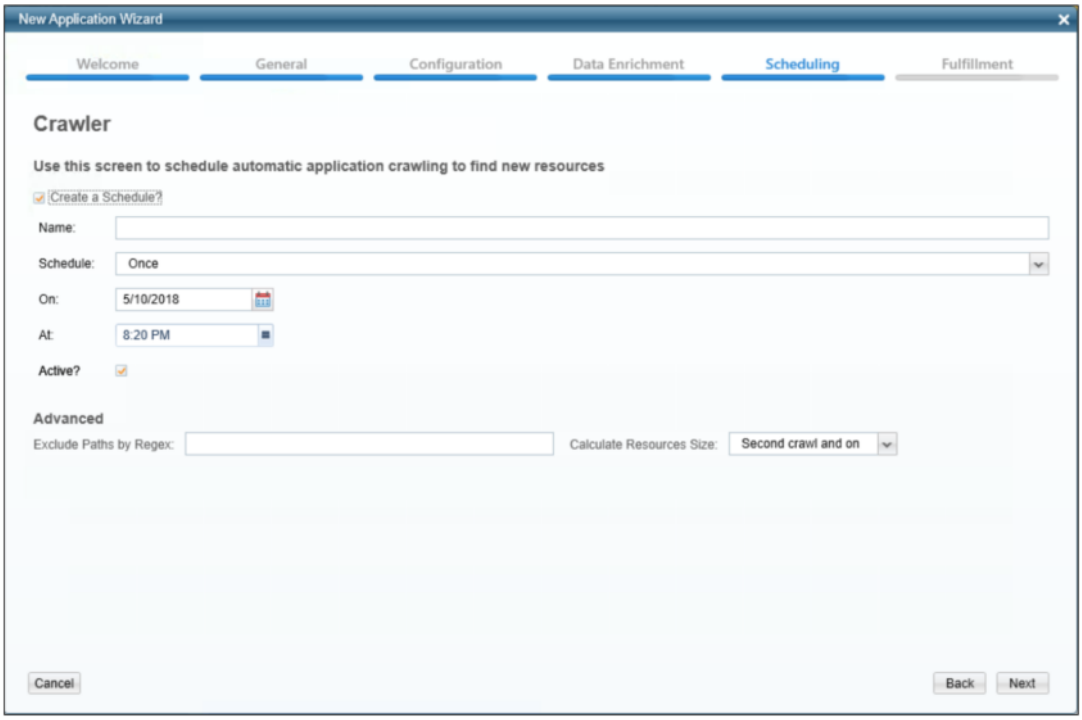

Figure 3. Crawler Window

23. Check the **Create a Schedule** check box
24. Type a name for the crawling scheduling task in the *Name* field
25. Select a scheduling frequency from the **Schedule** dropdown menu
26. Fill in the relevant date and time fields (which differ, depending upon the scheduling frequency selected).
27. Check the **Active** check box if relevant.
28. Type in the names of folders to exclude from the crawling process in the *Exclude Paths by Regex* field.

    Note: The chapter *Crawling* of the IdentityIQ File Access Manager Administrator Guide provides more information on the Crawling Process.

29. Click **Next**.

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

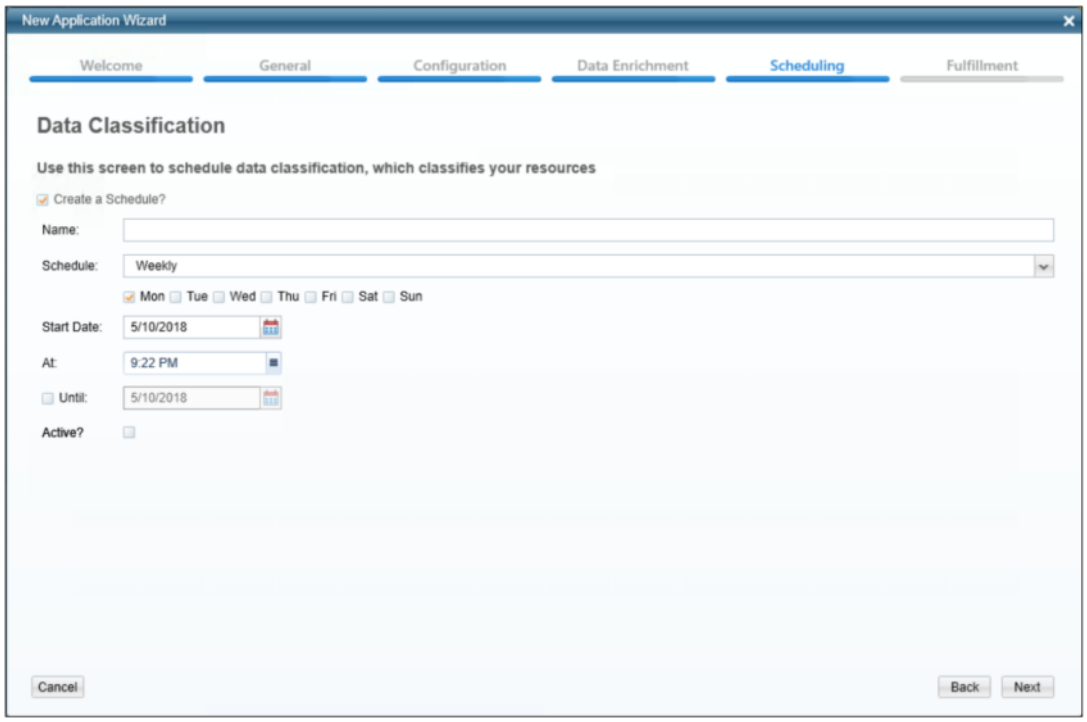

Figure 4. Data Classification Window

30. Check the **Create a Schedule** check box.
31. Type a name for the data classification scheduling task in the *Name* field.
32. Select a scheduling frequency from the **Schedule** dropdown menu.
33. Fill in the relevant date and time fields (which differ, depending upon the scheduling frequency selected).
34. Check the **Active** check box if relevant.

    Note: The chapter *Data Classification* of the IdentityIQ File Access Manager Administrator Guide provides more information on Data Classification.

35. Click **Next**.

The Access Fulfillment window of the New Application Wizard displays (only for CIFS).

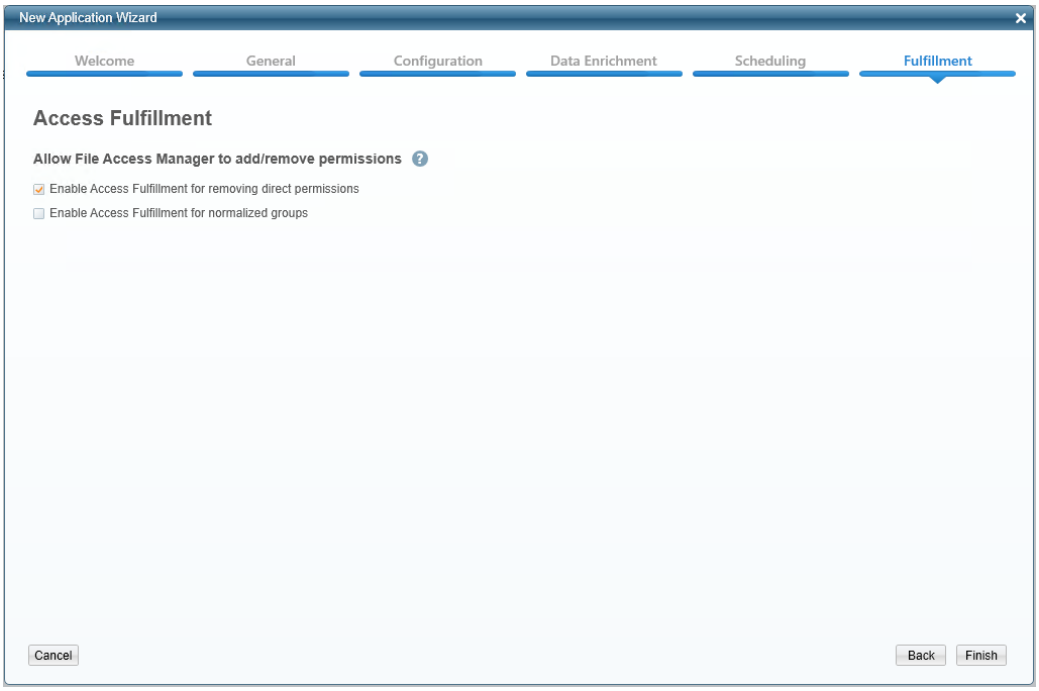

Figure 5. Access Fulfillment Window

36. Check the "Enable Access Fulfillment for removing direct permissions" checkbox to enable access direct permission remediation.

37. Check the "Enable Access Fulfilment for normalized groups" checkbox to allow File Access Manager to add and remove permissions to File Access Manager specific groups.

Note: The chapter *Permissions* of the IdentityIQ File Access Manager Administrator Guide provides more information on access fulfillment.

38. Click **Finish**

Chapter 6: Installation of Services

Collector Installation

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

   The Collector Installation Manager window displays.

Figure 6. Collector Installation Manager

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

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

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

3. Click **Next**

The Service Configuration window displays.

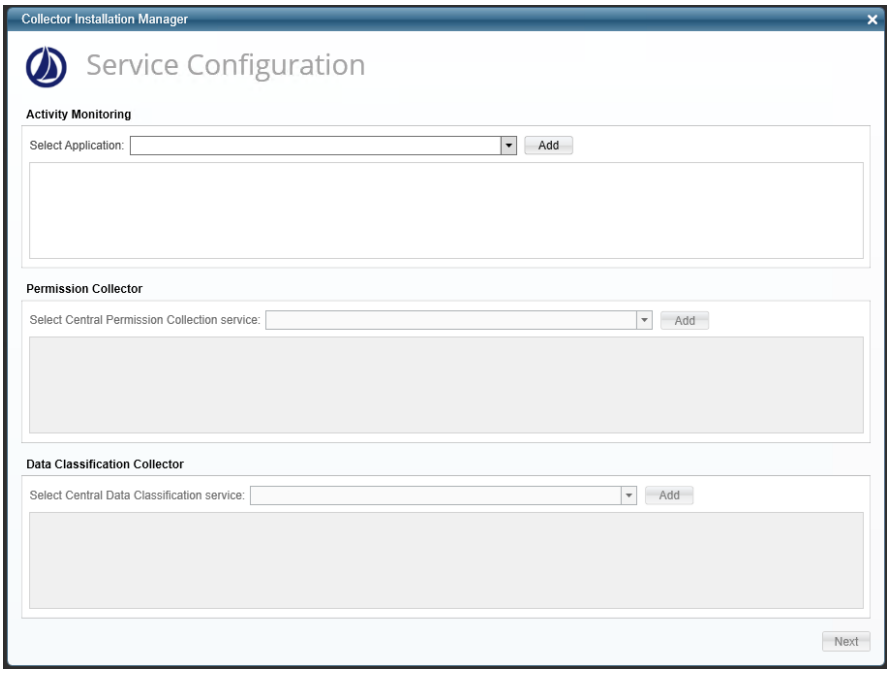

Figure 7. Service Configuration

4. If you are installing the Activity Monitoring collector, select the application and click **Add.**
5. If you are installing the Permission Collector, select the Central Permission Collector to which to connect this service, and click **Add**.
6. If you are installing the Data Classification Collector, select the Central Data Classification to which to connect this service, and click **Add**.
7. Click **Next**

   The Installation Folder window displays.

   Note: 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.

8. Browse and select the location of the target folder for installation.
9. Browse and select the location of the folder for system logs.
10. Click **Next**.
11. The system begins installing the selected components.
12. Click **Finish** (which displays after all the selected components have been installed).

Chapter 7: Verification

Services

Collectors' Installation Status

Verify in windows Service manager or other tool, that the IdentityIQ File Access Manager services are running.

for example,

- **File Access Manager Central Activity Monitor** - <Application_Name> service is running.
- **File Access Manager Permissions Collection** - <Application_Name> service is running.
- **File Access Manager Data Classification** - <Application_Name> service is running.

Logs

- "%SAILPOINT_HOME_LOGS%\EMCCelerra_<Application_Name>.log" does not contain errors.
- "%SAILPOINT_HOME_LOGS%\RoleAnalytics_<Application_Name>.log" does not contain errors.
- "%SAILPOINT_HOME_LOGS%\DataClassification_<Application_Name>.log" does not contain errors.

Monitored Activities

1. Simulate activities on the CIFS/NFS server.
2. Wait a minute (approximately).
3. Query for activities in the Administrative Client by <Application_Name>.
4. Verify that the activities display in the Administrative Client.

Permissions Collection

1. Run the Crawler and Permissions Collector tasks in the IdentityIQ File Access Manager Admin Client.
2. Verify that:
   - The tasks completed successfully
   - Business resources were created on the BRs tree
   - Permissions display in the Permission Forensics window

Chapter 8: Troubleshooting

Activities not collected by the Activity Monitor

If activities are not collected by the Activity Monitor, we need to track the status of the components, starting from the data mover to the Activity Monitor service.

1. Login to the data mover with your administrative user

2. Verify the CEPA facility status on the data mover, type:

```
server_cepp <data mover> -service –status
Output:
server_2 : CEPP Started
```

3. If the CEPA is not started, start it with, type:

```
server_cepp <data mover> -service –start
```

4. Display information about the CEPA service, type:

```
server_2 : CEPP Started
server_cepp <data mover> -pool -info
Output:
server_2 :
pool_name = sepapool
server_required = yes
access_checks_ignored = 0
req_timeout = 5000 ms
retry_timeout = 25000 ms
pre_events =
post_events =
OpenFileRead,CreateFile,FileWrite,FileRead,CreateDir,DeleteFile,DeleteDir,CloseModi
fied,RenameFile,enameDir,SetAclFile,SetAclDir,SetSecFile,SetSecDir
post_err_events =
CEPP Servers:
ip = [ip address of the CEE server], state = ONLINE, status = ONLINE
```

5. Make sure the post events correspond to the definitions described in the prerequisites section

6. Make sure the state and status are both ONLINE

   Note: If they are not ONLINE there is a problem with the connection to the CEE service, or with the connection between the CEE service and the Activity Monitor service.
   The CEPA facility is delicate to communication errors and in some cases the CEE does not recover from a communication failure.

7. Make sure all the prerequisites were set:

8. Make sure the CEE service is running with a domain user who is an administrator on the CEE service server.

9. Make sure the CEE service and the physical data mover CIFS server are joined to the same active directory domain.

10. Make sure the CEPA ip address listed in the output of the command above matches the ip address of the server running the CEE service

11. Make sure there is no firewall between the data mover and the server running the CEE service

12. Make sure the windows firewall is off on the server running the CEE service

13. Stop the CEPA facility with the following command:

14. Server_cepp <data mover> -service -stop
15. Stop the EMC CEE service on the CEE server and the Activity Monitor service.
16. Start the CEPA facility
17. Start the EMC CEE service, wait for 60 seconds
18. Start the Activity Monitor service
19. Wait for 60 seconds, and issue the server_cepp <data mover> -pool –info again

State and status ONLINE, but no events are shown

If the state and status are both ONLINE, but still no events are shown, perform the following:

1. Run the following command on the data mover:

```
server_cepp <data mover> -pool –stats
Output:
server_2 :
pool_name = pool1
Event Name Requests Min(us) Max(us) Average(us)
OpenFileWrite 2 659 758 709
CloseModified 2 604 635 620
Total Requests = 4
Min(us) = 604
Max(us) = 758
Average(us) = 664
```

2. Look at the count of the different events, issue the command a few more times and make sure it increases. Those counters represent the total number of requests for all the CIFS server in all the virtual data movers. If the counters do not increase, it might be that no users are working on the CIFS server at the moment.

Counters increase but no events are collected

If the counters increase, but no events are collected:

1. Check the statistics log file of the Activity Monitor to see if events are received by the Activity Monitor.
2. If no events are received by the Activity Monitor validate the Application configuration:
    a. Make sure the CIFS server name is properly configured in the Application filer name field. This value must be the actual name of the CIFS server name, and not the FQDN or one of the aliases.
    b. If the CIFS server has aliases defined to it (validate that in the EMC management), make sure these aliases are defined under the aliases in the Application configuration.