Integrating NetApp with File Access Manager

Version: 8.4

Revised: March 27, 2023

Copyright and Trademark Notices

Contents

Capabilities

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

- Analyze the structure of your stored data.
- Monitor user activity in the resources.
- Classify the data being stored.
- Verify user permissions on the resources, and compare them against requirements.
- Manage access fulfillment - automated granting and revoking of access - according to rules set in File Access Manager.

See the File Access Manager documentation for a full description.

Supported Versions

- ONTAP 7.3 7-mode and above
- ONTAP Cluster mode 8.2 and above, including all 9.x versions.

> Earlier versions of ONTAP may be affected by the following:
>
> - Confirmed NetApp bug id 800390: Panic during SCSI compare and write. This issue is resolved in the following ONTAP version and all later releases:
> - 7-mode 7.3 and above
> - 8.2.1P1
> - 8.2.1P2
> - 8.2.2RC1
> - 8.2.2RC2

Connector Overview

Activity Monitor

- SailPoint is a NetApp security alliance partner.
- To monitor activities on a NetApp filer, File Access Manager Connector for NetApp uses the NetApp FPolicy mechanism and registers as an FPolicy server.

Permissions Collector

CIFS Shares

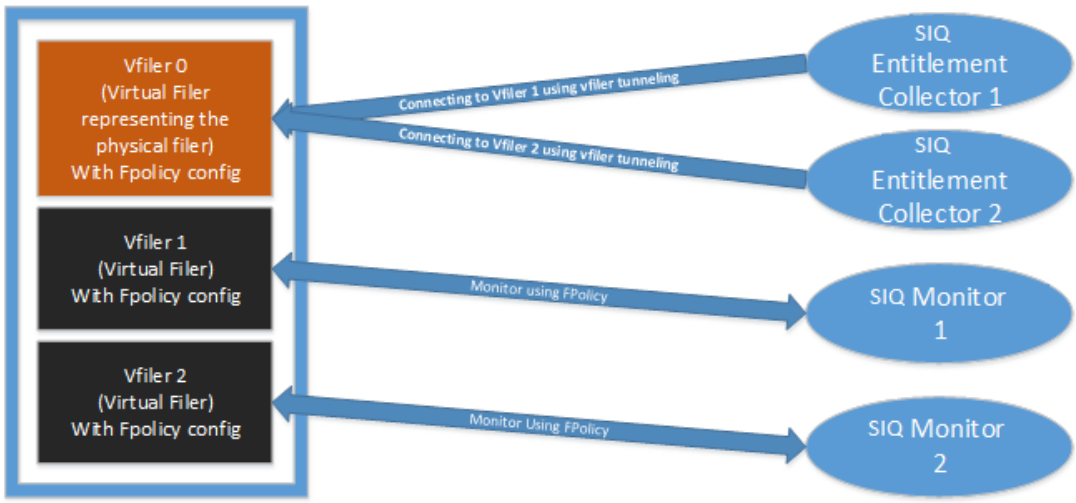
- File Access Manager connects to CIFS shares using backup semantics (‘seBackup’ privilege).
- During the Permissions Collection process - local groups and users are retrieved using the NetApp Ontapi Web API.

NFS Exports

- 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.
- The NIS Identity Collector is the only selectable option and is required.
- Volume information is retrieved using the NetApp Ontapi web API.

NetApp Architecture and File Access Manager

7-mode ONTAPI NetApp

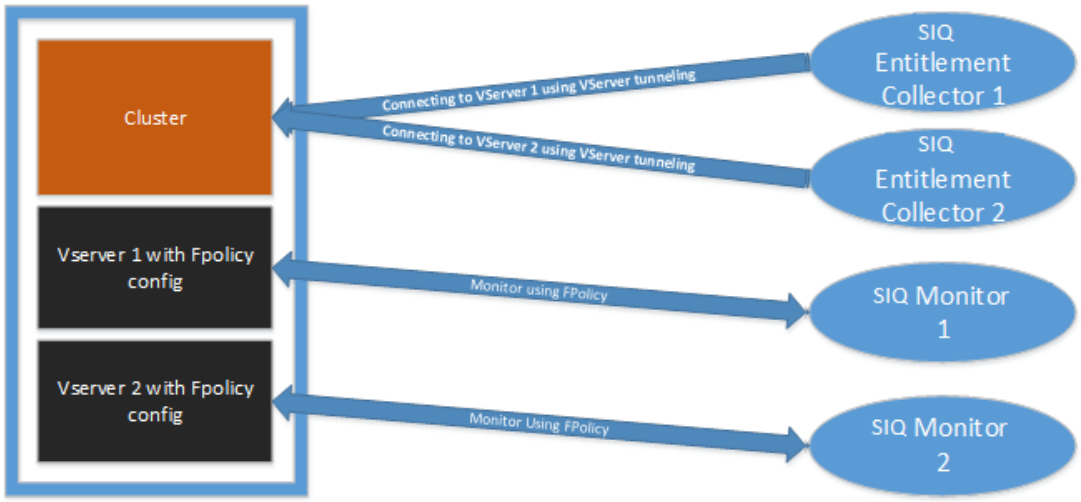


- A 7-mode ONTAPI NetApp can work in one of two architectures, a single physical file server or multiple virtual filers hosted on the same physical machine (by using the Multistore feature).
- The virtual architecture filers enable hosting multiple virtual file servers on single physical machine, with all the benefits included in a virtualized environment.
- In a physical architecture, there will be a single CIFS server configured on the NetApp. The physical filer will be represented by 2 Applications in File Access Manager, one for CIFS, and another for NFS, each with its own set of Activity Monitor / Permissions Collector / Data Classification services.
- For both CIFS/NFS, the File Access Manager connector will communicate directly with CIFS server or the filer IP configured on the physical filer for registering with the FPolicy and calling the Web Ontapi API.
- In a virtual architecture, each virtual file server is called Vfiler, and there is a CIFS server configured on every Vfiler. The name of the CIFS server does not have to match the name of the Vfiler.
- On a Vfiler architecture, Vfiler0 is the default Vfiler. It represents the physical filer.

- Each Vfiler is represented in File Access Manager by two Applications, one for CIFS, and another for NFS, each with its own set of Activity Monitor / Permissions Collector / Data Classification services.
- In a virtual architecture, the FPolicy communication as well as the permissions collection and data classification go directly to the CIFS server configured on the Vfiler or the IPaddress configured for NFS. The Ontapi API calls go to the management IP(the Vfiler 0 IP), and with a destination of the Vfiler name – this mechanism is called **Vfiler tunneling**.
- The FPolicy communication between the Activity Monitor service and the NetApp is based on the RPC protocol, and both the Activity Monitor must be installed on a server in the same Active Directory domain as filer/vfiler CIFS server.
- File Access Manager can be configured to run multiple Activity Monitor services for a single NetApp application. Each Activity Monitor service implements an FPolicy server. For highly loaded environments it is possible to install multiple Activity Monitors, on different servers, which act together as a single logical Activity Monitor in File Access Manager. This architecture is aimed to increase the number of concurrent events that the NetApp machine can handle by distributing the events between multiple FPolicy servers.

> This architecture is not recommended unless instructed by File Access Manager professional services.

NetApp Cluster Mode (cDot) on version 8.2



- On an 8.2 and above cluster mode NetApp, the architecture is the same as in a 7-mode virtual environment hosting multiple Vfilers.
- Each virtual server on a clustered NetApp is called Vserver, and there will be a single CIFS server configured on each Vserver.
- Each Vserver is represented in File Access Manager by two Applications, one for CIFS, and another for NFS, each will have its own set of Activity Monitor/Permissions Collector/Data Classification services.
- In a virtual architecture, the FPolicy communication, permission collection, and data classification all go directly to the CIFS server configured on the Vserver or to the IP address configured for NFS.
  The ONTAPI API call options are:
  - Using the cluster management IP, with the Vserver name as the destination (a mechanism called **Vserver tunneling**).
  - Using the Vserver management IP directly.
- The FPolicy communication between the Activity Monitor service and the NetApp is based on XML over TCP, where the Activity Monitor acts as the server, each of the cluster nodes act as the clients. A dedicated unique port must be configured for each Application if multiple Activity Monitor services are on the same server.
- File Access Manager can be configured with to run multiple Activity Monitor services for a single NetApp application. Each Activity Monitor service implements an FPolicy server. For highly loaded environments it is possible to install multiple Activity Monitors, on different server, which will act together as a single logical Activity Monitor in File Access Manager. This architecture is aimed to increase the number of concurrent events that the NetApp machine can handle by distributing the events between multiple FPolicy servers.

  > This architecture is not recommended unless instructed by File Access Manager professional services.

Prerequisites

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

Software Requirements

File Access Manager requires the latest ASP.NET Core 6.0.x Hosting Bundle. This bundle consists of .NET Runtime and ASP .NET Core Runtime. You can download the latest 6.0.x Hosting Bundle version from here .

Permission Requirements

File Access Manager requires different permissions, based on the tasks performed.

The following listing describes the required permissions by File Access Manager task, in addition to the permissions described in sections 4.3, 54 or 6.3:

Activity Monitoring

See additional information in the Permissions section of the relevant configuration (Physical 7-Mode/Virtual 7-Mode/Cluster Mode)

CIFS Access Permissions

Crawling

Requires a user with Share Read permission to all shares

Permission Collection

Requires a user with Share Read permission to all shares

Enumeration of CIFS Share-Level Permissions - See additional information in the Permissions section of the relevant configuration (Physical 7-Mode/Virtual 7-Mode/Cluster Mode)

Enumeration of local Users and Groups - See additional information in the Permissions section of the relevant configuration (Physical 7-Mode/Virtual 7-Mode/Cluster Mode)

Data Classification

Requires a user with Share Read permission to all shares

NFS Access Permissions

Crawling

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

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

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

NetApp Physical Filer 7-Mode Requirements

1. The monitor server is required to be in the same segment and AD Domain of the NetApp. No firewalls can be in the middle.
2. The Activity Monitor service must run with the dedicated user described in section Physical Filer 7-Mode Permissions.

Physical Filer 7-Mode Policy Definitions

> The configuration below is for CIFS filers.

1. To configure monitoring for NFS, repeat step 2 and replace whitebox_cifs with whitebox_nfs
2. Run the following commands in the NetApp:

```
options fpolicy.enable on
```

```
fpolicy create whitebox_cifs screen
```

```
fpolicy options whitebox_cifs required off
```

```
fpolicy options whitebox_cifs cifs_disconnect_check on
```

```
fpolicy options whitebox_cifs serverprogress_timeout 1
```

```
fpolicy options whitebox_cifs reqcancel_timeout 1
```

```
fpolicy options whitebox_cifs cifs_setattr on
```

```
fpolicy enable whitebox_cifs
```

3. It is recommended to include only the required volumes to the monitored by fpolicy to reduce load from the NetApp machine.
4. To include only specific volumes to be monitored, run the following command:

```
      fpolicy volume include add whitebox_cifs <vol name>
```

> <vol name> must be the short volume name as shown in the 'volume status' command, without the /vol/ prefix

Physical Filer 7-Mode Permissions

Perform the following steps to configure required permission for all File Access Manager tasks:

1. Create a dedicated domain user for the filer (for example, SIQ_<filername>). This user will be used in the application configuration, and must also be the user running the Activity Monitor service.
2. This user must be a member of the Backup Operators and Power Users groups on the NetApp and an administrator on the server running the Activity Monitor service.
3. Run the following commands in the NetApp physical filer to grant the File Access Manager user permissions to access the Ontapi web API.
   Replace *<DOMAIN>* with the domain name and *siq_<filername>* with the correct user name:

```
      useradmin role add siq_netapp_role -a login-http-admin,api-nfs-exportfs-list-
rules,api-cifs-share-list-iter-start,api-cifs-share-list-iter-next,api-cifs-share-list-
iter-end,api-cifs-share-acl-list-iter-start,api-cifs-share-acl-list-iter-next,api-cifs-
share-acl-list-iter-end,api-qtree-list,api-useradmin-group-list,api-useradmin-user-
list,security-api-vfiler,api-system*,api-useradmin-domainuser-list, api-fpolicy-list-
info,api-fpolicy-get-policy-options,api-volume-list-info,api-fpolicy-volume-list-info
```

```
      useradmin group add siq_group -r siq_netapp_role
```

```
      useradmin domainuser add <DOMAIN>\siq_<filername> -g siq_group,"Backup
Operators","Power Users"
```

Physical Filer 7-Mode Communications Requirements

Requirement	Source	Destination	Port
File Access Manager Message Broker	Permissions Collector/Data Classification Collector	RabbitMQ	5671
File Access Manager Access	Activity Monitor	File Access Manager Servers	8000-8008
NetApp CIFS Access	Activity Monitor	NetApp	RPC (135 + Dynamic)
NetApp fpolicy	NetApp filer	Activity Monitor	MSRCP (139)
NetApp fpolicy	Activity Monitor	NetApp	MSRPC (139)
NetApp Web API	Activity Monitor/Permissions Collector	NetApp	443 (https)
NetAPP NFS Access	Permissions Collector/Data Classification	NetApp	UDP/TCP 111, 2049 (NFSv3)

NetApp Virtual Filer 7-Mode Requirements

1. The activity monitor server is required to be in the same segment and AD Domain of the NetApp. No firewalls can be in the middle.
2. The Activity Monitor service must run with the dedicated user described in section Virtual Filer 7-Mode Permissions.

Ontapi API Configuration Options

When working with 7-mode, there are two configuration options, which affect how the connector communicates with the NetApp ONTAPI API:

1. A single physical filer: there are no vFilers defined on NetApp, and there's only one filer. In this configuration, communications are made directly with the filer.
2. vFilers (Multiple logical filers): there is more than one logical filer defined on the NetApp storage, with the original named vFiler0 (vFiler Zero).

With vFilers, ONTAPI communications pass through vFiler0, and targeted at the correct vFiler using its name.

Virtual Filer 7-mode FPolicy Definitions

1. The configuration below is for CIFS filers. To configure monitoring for NFS, repeat step 2 and replace whitebox_cifs with whitebox_nfs
2. Run the following commands in the NetApp vfiler:

```
vfiler context vfilername
options fpolicy.enable on
fpolicy create whitebox_cifs screen
fpolicy options whitebox_cifs required off
fpolicy options whitebox_cifs cifs_disconnect_check on
fpolicy options whitebox_cifs serverprogress_timeout 1
fpolicy options whitebox_cifs reqcancel_timeout 1
fpolicy options whitebox_cifs cifs_setattr on
```

3. To start fpolicy, run:

```
fpolicy enable whitebox_cifs
```

4. It is recommended to include only the required volumes to the monitored by FPolicy to reduce load from the NetApp machine.
   To include only specific volumes to be monitored, run the following command:

```
fpolicy volume include add whitebox_cifs <vol name>
```

> <vol name> must be the short volume name as shown in the ‘volume status’ command, without the /vol/ prefix

Virtual Filer 7-Mode Permissions

Perform the following to configure the required permission for all File Access Manager tasks:

1. When monitoring a vfiler, File Access Manager uses vfiler tunneling for the NetApp Web API.
2. The tunneling can work if the vfiler and vfiler0 (the physical filer is called vfiler0. "vfiler zero") are in the same domain or vfiler0 can resolve users from the vfiler domain.

3. If vfiler0 is not in any domain or cannot resolve the domain user, create a local user on vfiler0, and follow the steps described in section Configuring a Local NetApp User for the Ontapi API after the Activity Monitor and Permissions Collector installation.
4. Create a dedicated domain user for the filer. This user will be used later in the application configuration, and must also be the user running the Activity Monitor service.
    - siq_<filername> must be part of the domain.
    - In the commands below, replace **<DOMAIN>** with the domain name and **siq_<filername>** with the correct username.
    - This user must be a member of the Backup Operators and Power Users groups in the NetApp (the command to add the user to the group is part of the sequence below).
    - This user must be an administrator on the server running the Activity Monitor service.
5. Decide if a local user is required on vfiler0 according to the previous sections. If you are not sure, consult with your File Access Manager technical support.
6. If a local user is required, name it SIQ_VFILER0
7. These commands need to run only once, when the first vfiler is configured. For subsequent vfilers, the role and group will be present and this step can be skipped.
8. Run the following commands in the NetApp vfiler0 (vfiler zero) to grant the File Access Manager user permissions to access the Ontapi Web API.
   Replace **<DOMAIN>** with the domain name and **siq_<filername>** with the correct user name:

```
useradmin role add siq_netapp_role -a login-http-admin,api-nfs-exportfs-list-rules,api-cifs-share-list-iter-start,api-cifs-share-list-iter-next,api-cifs-share-list-iter-end,api-cifs-share-acl-list-iter-start,api-cifs-share-acl-list-iter-next,api-cifs-share-acl-list-iter-end,api-qtree-list,api-useradmin-group-list,api-useradmin-user-list,security-api-vfiler,api-system*,api-useradmin-domainuser-list, api-fpolicy-list-info,api-fpolicy-get-policy-options,api-volume-list-info,api-fpolicy-volume-list-info
```

```
useradmin group add siq_group -r siq_netapp_role
```

```
vfiler context vfiler0
```

```
useradmin domainuser add <DOMAIN>\siq_<filername> -g siq_group,"Backup Operators","Power Users"
```

9. If this is the first vfiler added for monitoring, a local user is needed. Run the following command:

```
useradmin user add siq_VFILER0 -g siq_group
```

> If this is NOT the first vfiler added for monitoring then the user is present and is associated with the group. This step can be skipped.

10. After the command is completed, assign a password for the local user.

Configuring a Local NetApp User for the Ontapi API

> Make sure you have the password for the NetApp local user created as explained in the Permissions section

1. Navigate to the File Access Manager installation folder on one of the File Access Manager central servers.
2. Open the folder "%SAILPOINT_HOME%\FileAccessManager\Server Installer-\Tools\EncryptStringForService"
3. Copy the content of the folder to the server on which the Activity Monitor service is installed
4. Run: **EncryptStringForService.exe** [password to encrypt]
5. Copy the output of the command

Activity Monitor

1. Navigate to the Activity Monitor installation folder
2. Edit the Activity **BAMFramework.exe.config**
3. Enter the name of the user in the alternativeUserName key:

```
<add key="alternativeUserName" value="local user name"/>
```

4. Paste the output of the command copied in Section 5 into the value of the alternativeUserPassword key:

```
<add key="alternativeUserPassword" value="encrypted password from step 4"/>
```

5. Restart the Activity Monitor service.

Permission Analysis

1. Navigate to the Permission Analysis installation folder.
2. Edit the **RoleAnalyticsServiceHost.exe.config**.
3. Enter the name of the user in the netAppApiPassword key:

```
<add key="netAppApiUser" value="local user name"/>
```

4. Paste the output of the command copied in Section 5 into the value of the netAppApiPassword key:

```
<add key="netAppApiPassword" value="encrypted password from step 4"/>
```

Required Data for Creating a NetApp Application

CIFS Server name

VFILER IP address

VFILER name

An internal name, usually the same as the normal vfiler host name

Local user name and password

If the vfiler0 (vfiler zero) is not in any domain or cannot resolve the user

Virtual Filer 7-Mode Communications Requirements

Requirement	Source	Destination	Port
File Access Manager	Permissions Collector/Data Classification Collector	RabbitMQ	5671
File Access Manager Access	Activity Monitor	File Access Manager Servers	8000-8008
NetApp Access	Activity Monitor / Permissions Collector / Data Classification	NetApp VFILER	MSRPC (135 + Dynamic)
NetApp fpolicy	NetApp VFILER	Activity Server	MSRCP (139)
NetApp fpolicy	Activity Monitor	NetApp VFILER	MSRPC (139)

Requirement	Source	Destination	Port
NetApp Web API	Permissions Collector / Activity Monitor	NetApp VFILER ZERO	443 (https)
NetApp NFS Access	Permissions Collector	NetApp VFILER	UDP/TCP 111, 2049 (NFSv3)

NetApp 8.2+ Cluster Mode Requirements

According to the NetApp Architecture and File Access Manager section, each Vserver is represented as a single Application in File Access Manager. If multiple Activity Monitor services are installed on the same server, each Application must be configured with a unique dedicated port, which is the port the Activity Monitor receives the FPolicy communication.

> The monitor server is required to be in the same segment. No firewalls can be in the middle.

1. Create a domain user for the monitor: For example, *siq_vservername* (small lowercase is recommended).
2. Verify the case in which the user name is written AD (This field is case sensitive).
3. Each Vserver requires its own monitor installed.

Cluster Mode FPolicy Definitions

In the commands below, replace the parameters with the required values:

[vserver_name]

The name of the vserver

[monitors server ip]

The ip address of the server where the Activity Monitor service is installed

[port number]

The port number configured in the Application configuration wizard in section 7

[volume names to include]

Replace with * if all volumes need to be monitored, or enter a list of volumes to monitor

[running number]

A sequential number of the policy in the policy hierarchy. If no FPolicy is defined, this should be 1.

To configure FPolicy for CIFS:

```
fpolicy policy event create -event-name siq_cifs_events -protocol cifs -file-operations create, create_dir, delete, delete_dir, read, write, rename, rename_dir, setattr, open -vserver [vserver_name] -filters first-read, first-write, open-with-delete-intent
```

```
fpolicy policy external-engine create -vserver [vserver_name] -engine-name siq_cifs_engine -primary-servers [monitors server ip] -port [port_number] -extern-engine-type asynchronous -ssl-option no-auth
```

```
fpolicy policy create -vserver [vserver_name] -policy-name wbx_cifs_policy -events siq_cifs_events -engine siq_cifs_engine -is-mandatory false
```

```
fpolicy policy scope create -vserver [vserver_name] -policy-name wbx_cifs_policy -volumes-to-include [* or volume names to include]
```

```
fpolicy enable -vserver [vserver_name] -policy-name wbx_cifs_policy -sequence-number [running_number]
```

To configure FPolicy for NFS:

```
fpolicy policy event create -event-name siq_nfs3_events -protocol nfsv3 -file-operations create, create_dir, delete, delete_dir, read, write, rename, rename_dir, setattr -vserver [vserver_name]
```

```
fpolicy policy event create -event-name siq_nfs4_events -protocol nfsv4 -file-operations create, create_dir, delete, delete_dir, read, write, rename, rename_dir, setattr -vserver [vserver_name]
```

```
fpolicy policy external-engine create -vserver [vserver_name] -engine-name siq_nfs_engine -primary-servers [monitors server ip] -port [port_number] -extern-engine-type asynchronous -ssl-option no-auth
```

```
fpolicy policy create -vserver [vserver_name] -policy-name wbx_nfs_policy -events siq_nfs3_events, siq_nfs4_events -engine siq_nfs_engine -is-mandatory false -allow-privileged-access yes -privileged-user-name [domain\user_name]
```

```
fpolicy policy scope create -vserver [vserver_name] -policy-name wbx_nfs_policy -volumes-to-include [* or volume names to include]
```

```
fpolicy enable -vserver [vserver_name] -policy-name wbx_nfs_policy -sequence-number [running_number]
```

> If multiple activity monitors are installed on the same server, set a unique port per vserver, and replace [port_number] with the value configured in the Application.

Cluster Mode Permissions

1. Create a new role for File Access Manager.

```
      security login role create -role siq_netapp_role_82 -cmddirname "vserver cifs
share access-control" -access readonly -vserver <vserver_name>
```

```
      security login role create -role siq_netapp_role_82 -cmddirname "vserver cifs
share" -access readonly -vserver <vserver_name>
```

```
      security login role create -role siq_netapp_role_82 -cmddirname "vserver cifs
users-and-groups local-group" -access readonly -vserver <vserver_name>
```

```
      security login role create -role siq_netapp_role_82 -cmddirname "vserver cifs
users-and-groups local-group show-members" -access readonly -vserver <vserver_name>
```

```
      security login role create -role siq_netapp_role_82 -cmddirname "vserver cifs
users-and-groups local-user" -access readonly -vserver <vserver_name>
```

```
      security login role create -role siq_netapp_role_82 -cmddirname "vserver fpolicy
engine-connect" -vserver <vserver_name>
```

```
      security login role create -role siq_netapp_role_82 -cmddirname "vserver fpolicy
engine-disconnect" -vserver <vserver_name>
```

```
      security login role create -role siq_netapp_role_82 -cmddirname "vserver fpolicy
show-engine" -access readonly -vserver <vserver_name>
```

```
      security login role create -role siq_netapp_role_82 -cmddirname "vserver services
name-service unix-group" -access readonly -vserver <vserver_name>
```

```
      security login role create -role siq_netapp_role_82 -cmddirname "vserver services
name-service unix-user" -access readonly -vserver <vserver_name>
```

```
      security login role create -role siq_netapp_role_82 -cmddirname "volume qtree" -
access readonly -vserver <vserver_name>
```

```
      security login role create -role siq_netapp_role_82 -cmddirname "volume" -access
readonly -vserver <vserver_name>
```

```
      security login role create -role siq_netapp_role_82 -cmddirname "vserver fpolicy
policy scope" -access readonly -vserver <vserver_name>
```

```
      security login role create -role siq_netapp_role_82 -cmddirname "vserver fpolicy
show" -access readonly -vserver <vserver_name>
```

```
      security login role create -role siq_netapp_role_82 -cmddirname "vserver fpolicy
policy" -access readonly -vserver <vserver_name>
```

```
security login role create -role siq_netapp_role_82 -cmddirname "vserver fpolicy policy external-engine" -access readonly -vserver <vserver_name>
```

> <vserver_name> = The Vserver name configured in NetApp settings.

> If the File Access Manager Application is configured to use Vserver Tunneling, run these commands at the cluster level without the -vserver parameter. However, if the File Access Manager Application is configured to use the Vserver directly, run these commands at the Vserver level without the -vserver parameter, or at the cluster level with the -vserver parameter.

2. Create a new user for File Access Manager, and assign to the newly created role:

```
security login create -vserver <vserver_name> -username <domain\user_name> -application ontapi -authmethod domain -role siq_netapp_role_82
```

> Domain and user_name must be configured with the same case as configured in the Application configuration.

> The username must be in the same case as defined in Active Directory. This is a known NetApp issue.

3. Add the new user to the “Backup Operators” security group on each virtual CIFS server.
4. Add the new user to the “Power Users” security group on each virtual CIFS server.
5. If no domain-tunnel is configured, run the following command (this command should be run only once, and not for each vserver):

```
security login domain-tunnel create -vserver [vserver_name]
```

> If the domain-tunnel cannot be configured, authentication to the NetApp Web API will fail with the Active Directory user configured in the Application configuration.

> It is possible to define an alternative local NetApp user to use instead of the user defined in the application configuration. Section Configuring a Local NetApp User for the Ontapi API for detailed instructions.

Communications Requirements

Requirement	Source	Destination	Port
File Access Manager Message Broker	Permissions Collector / Data Classification Collector	RabbitMQ	5671
File Access Manager Access	Activity Monitor	File Access Manager Servers	8000-8008
NetApp Access	Each NetApp Cluster Nodes	Activity Monitor	MSRPC + The port defined in the FPolicy definition (12000, or the specific port defined)
NetApp Web API	Activity Monitor / Permissions Collector	NetApp Cluster Management IP	443 (https)
NetApp NFS Access	Permissions Collector / Data Classification	NetApp	UDP/TCP 111, 2049 (NFSv3)

NetApp OnTap 9.X Command Template

1. Create a new role for File Access Manager for the CIFS vserver. For example, fam_netapp_role.

   Replace (v_server) with CIFS vserver from cluster.

   Replace (cluster) with cluster name.

```
security login role create -role fam_netapp_role -cmddirname "vserver cifs share access-control" -vserver (v_server) -access readonly
```

```
security login role create -role fam_netapp_role -cmddirname "vserver cifs share" -vserver (v_server) -access readonly
```

```
security login role create -role fam_netapp_role -cmddirname "vserver cifs users-and-groups local-group" -vserver (v_server) -access readonly
```

```
security login role create -role fam_netapp_role -cmddirname "vserver cifs users-and-groups local-group show-members" -vserver (v_server) -access readonly
```

```
security login role create -role fam_netapp_role -cmddirname "vserver cifs
users-and-groups local-user" -vserver (v_server) -access readonly
```

```
security login role create -role fam_netapp_role -cmddirname "vserver fpolicy
engine-connect" -vserver (v_server)
```

```
security login role create -role fam_netapp_role -cmddirname "vserver fpolicy
engine-disconnect" -vserver (v_server)
```

```
security login role create -role fam_netapp_role -cmddirname "vserver fpolicy
show-engine" -vserver (v_server) -access readonly
```

```
security login role create -role fam_netapp_role -cmddirname "vserver services
name-service unix-group" -vserver (v_server) -access all
```

```
security login role create -role fam_netapp_role -cmddirname "vserver services
name-service unix-user" -vserver (v_server) -access readonly
```

```
security login role create -role fam_netapp_role -cmddirname "volume qtree" -
vserver (v_server) -access readonly
```

```
security login role create -role fam_netapp_role -cmddirname "volume" -vserver
(v_server) -access readonly
```

```
security login role create -role fam_netapp_role -cmddirname "vserver fpolicy
policy scope" -vserver (v_server) -access readonly
```

```
security login role create -role fam_netapp_role -cmddirname "vserver fpolicy
show" -vserver (v_server) -access readonly
```

2. Create a new role for file access manager for the cluster (use cluster name for -vserver switch).

```
security login role create -role fam_netapp_role -cmddirname "vserver cifs
share access-control" -vserver (cluster) -access readonly
```

```
security login role create -role fam_netapp_role -cmddirname "vserver cifs
share" -vserver (cluster) -access readonly
```

```
security login role create -role fam_netapp_role -cmddirname "vserver cifs
users-and-groups local-group" -vserver (cluster) -access readonly
```

```
security login role create -role fam_netapp_role -cmddirname "vserver cifs
users-and-groups local-group show-members" -vserver (cluster) -access readonly
```

```
security login role create -role fam_netapp_role -cmddirname "vserver cifs
users-and-groups local-user" -vserver (cluster) -access readonly
```

```
security login role create -role fam_netapp_role -cmddirname "vserver fpolicy
engine-connect" -vserver (cluster)
```

```
security login role create -role fam_netapp_role -cmddirname "vserver fpolicy
engine-disconnect" -vserver (cluster)
```

```
security login role create -role fam_netapp_role -cmddirname "vserver fpolicy
show-engine" -vserver (cluster) -access readonly
```

```
security login role create -role fam_netapp_role -cmddirname "vserver services
name-service unix-group" -vserver (cluster) -access all
```

```
security login role create -role fam_netapp_role -cmddirname "vserver services
name-service unix-user" -vserver (cluster) -access readonly
```

```
security login role create -role fam_netapp_role -cmddirname "volume qtree" -
vserver (cluster) -access readonly
```

```
security login role create -role fam_netapp_role -cmddirname "volume" -vserver
(cluster) -access readonly
```

```
security login role create -role fam_netapp_role -cmddirname "vserver fpolicy
policy scope" -vserver (cluster) -access readonly
```

```
security login role create -role fam_netapp_role -cmddirname "vserver fpolicy
show" -vserver (cluster) -access readonly
```

3. Assign the newly created role to the domain user created for fam (Upper and lower case are important.)

```
security login create -vserver (cluster) -username domain\domainAccountFam -
application ontapi -authmethod domain -role fam_netapp_role
```

```
security login create -vserver (v_server) -username domain\domainAccountFam -
application ontapi -authmethod domain -role fam_netapp_role
```

4. Domain user must be a member of the “Backup Operators” group on the VServer. Execute the below command for the Vserver you intend to on-board.

```
vserver cifs users-and-groups local-group add-members -vserver (v_server) -
group-name "BUILTIN\Backup Operators" -member-names domain\domainAccountFam
```

5. Domain user to be a member of the “Power Users” group on the Vserver. Execute the below command for the Vserver you intend to on-board

```
vserver cifs users-and-groups local-group add-members -vserver (v_server) -
group-name "BUILTIN\Power Users" -member-names domain\domainAccountFam
```

6. If no domain-tunnel is configured, run the following command (this command should be run only once, and not for each vserver):

```
security login domain-tunnel create -vserver (v_server)
```

7. CIFS Access:

   User account should have Share Read permission to all shares.

   Requires a user with Share Read permission to all shares

   Should be able to enumerate CIFS Share-Level Permissions

   Should be able to enumerate local Users and Groups

8. Domain user must be an administrator (local administrator) on the server running the Activity Monitor service.

9. Execute the commands to configure a fpolicy for CIFS server.

```
fpolicy policy event create -event-name fam_cifs_events -protocol cifs -file-
operations create,create_dir,delete,delete_dir,read,write,rename,rename_dir,-
setattr,open -vserver (v_server) -filters first-read,first-write,open-with-
delete-intent
```

> IP for the SailPoint Activity Mornitor server should be used in place of x.x.x.x.

```
fpolicy policy external-engine create -vserver (v_server) -engine-name fam_
cifs_engine -primary-servers x.x.x.x  -port 12000 -extern-engine-type asyn-
chronous -ssl-option no-auth
```

```
fpolicy policy create -vserver (v_server) -policy-name wbx_cifs_policy -events
fam_cifs_events -engine fam_cifs_engine -is-mandatory false
```

10.
```
fpolicy policy scope create -vserver (v_server) -policy-name wbx_cifs_policy -
volumes-to-include *
```

11.
```
fpolicy enable -vserver (v_server) -policy-name wbx_cifs_policy -sequence-num-
ber 1
```

NetApp Installation Flow Overview

To install the NetApp connector:

1. Configure all the prerequisites.
2. Add a new NetApp 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.
    - Permissions 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

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.

Add an Activity Monitor

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

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, 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 NetApp Application

In order to integrate with NetApp, 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

Select NetApp Type

- NetApp CIFS
- NetApp DFS

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.

Identity Collector

Select from the Identity Collector dropdown menu.

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

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

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

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

Connection Details

Filer Name

The CIFS server name or the NFS IP address to which users connect.

Domain Name, Username and Password

The user defined in the prerequisites

When working with NetApp 7-mode

If there is only one filer (no vFilers):

Management IP

- Empty.

Use Management IP for tunneling

Unchecked.

Is Cluster-Mode?

Unchecked.

If there is more than one filer (working with vFilers):

Management IP

vFiler0's (vFiler Zero) IP address.

Use Management IP for tunneling

Checked.

vFiler/Vserver name

The target vFiler's name in NetApp settings.

Is Cluster-Mode?

Unchecked.

When working with NetApp Cluster-Mode:

If communicating directly with the Vserver:

Management IP

The Vserver's management IP. If it's the same as the data access IP, leave empty.

Use Management IP for tunneling

Unchecked.

Is Cluster-Mode

Checked.

Port

The port used by the FPolicy Server as configured in NetApp.

If using Vserver Tunneling:

Management IP

The cluster management IP.

Use Management IP for tunneling

Checked.

vFiler/Vserver name

The target Vserver's name in NetApp settings.

Is Cluster-Mode

Checked.

Port

The port used by the FPolicy Server as configured in NetApp.

Multiple FPolicy Servers?

(Check this checkbox if more than one FPolicy server need to be installed for performance reasons. This should be used only with File Access Manager Professional Services/Support)

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 "IdentityIQ FAM 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

Valid for NetApp-CIFS only

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**

Valid for NetApp-CIFS only

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.

Permission Collection Setup Notes for NetApp

> The permissions are managed either on the NTFS level, or on the Share Level.

> When the shares are configured with Full Control to Everyone, and all the permissions are defined in the folders, you should select NTFS, which is the 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.

Crawl Snapshot Folders

Only for NetApp CIFS / NetApp DFS

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. See Scheduling a Task

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 which 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 which 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:

Include ONLY the C$ drive shares: \\server_name*C$* `Regex: ^(?!\\\\server_name\\C\$($|\\.*)).*`
Include ONLY one folder under a share: \\server\share*folderA* Regex: `^(?!\\\\server_name\\share\$($|\\folderA$|\\folderA\\.*)).*`
Include ONLY all administrative shares Regex: ^(?!\\\\server_name\\[a-zA-Z]\$($|)).*

> 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 “|” .

Excluding Top Level Resources

Use the top level exclusion screen to select top level roots to exclude from the crawl. This setting is done per application.

To exclude top level resources from the crawl process

1. Open the application screen

   Admin > Applications

2. Find the application to configure and click the drop down menu on the application line. Select **Exclude Top Level Resources** to open the configuration panel.

3. ***Run Task***

   The Run Task button triggers a task that runs a short detection scan to detect the current top level resources.

   Before running the task for the first time, the message above this button is:

   "Note: Run task to detect the top-level resources"

   If the top level resource list has changed in the application while yo u are on this screen, press this button to retrieve the updated structure.

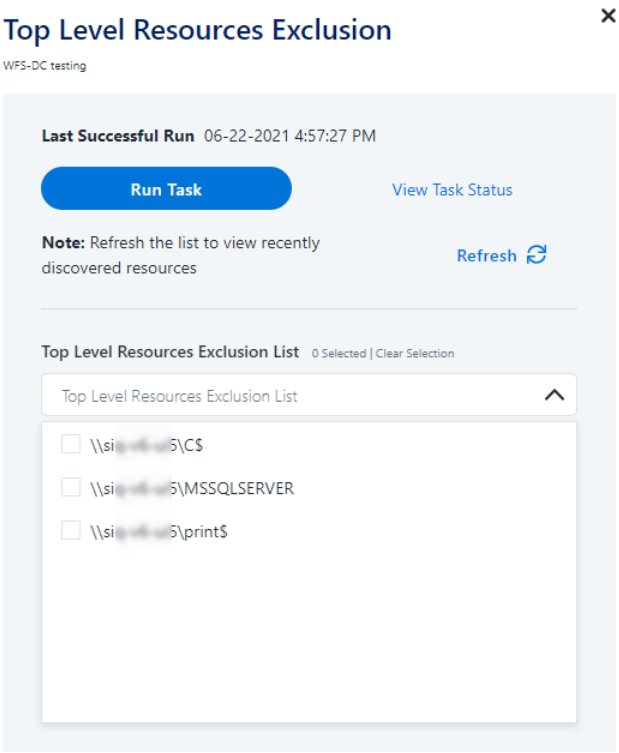
   Once triggered, you can see the task status in

   Settings > Task Management > Tasks

> This will only work if the user has access to the task page

When the task has completed, press **Refresh** to update the page with the list of top level resources.

4. Click the top level resource list, and select top level resources to exclude.
5. Click *Save* to save the change.
6. To refresh the list of top level resources, run the task again. Running the task will not clear the list of top level resources to exclude.



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 ealier

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 Scheduling a Task

> 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.

Configuring Activity Monitoring

To configure the activity monitoring polling parameters

- 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 **Activity Configurations & Decs** settings page.

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.

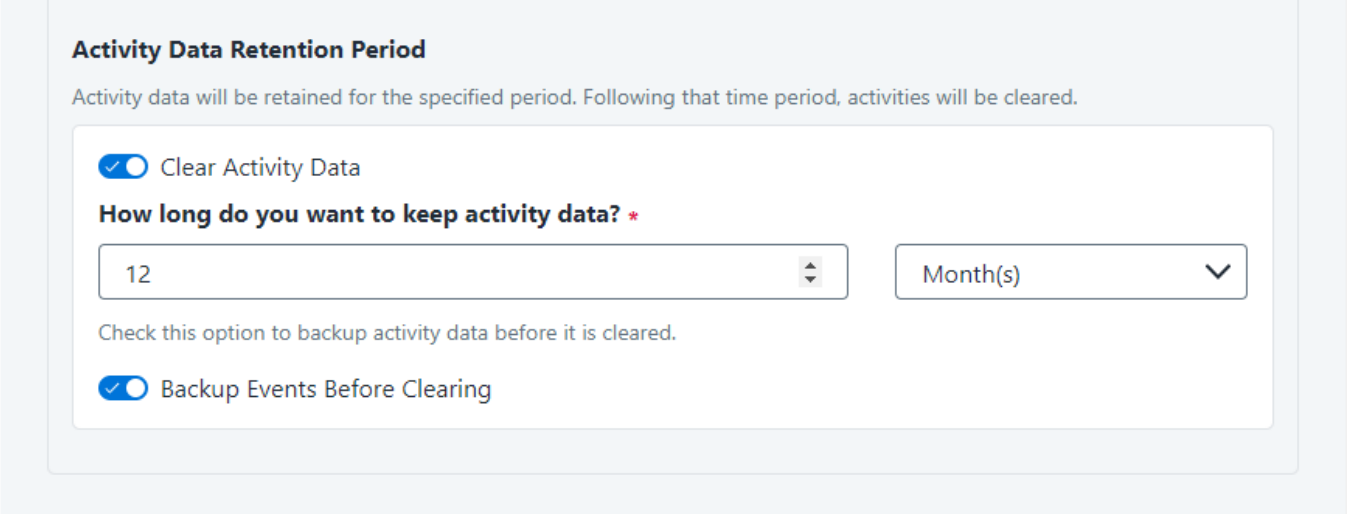
Activity Data Retention Period

> By default, this feature is disabled.

When selecting the Clear Activity Data option, a user is able to provide a time frame (1 to 100) in either months or years for all activity to be retained. Once that time period is met, all data will be removed.

A user can also select to backup the data before it is deleted by selecting the Backup Events Before Clearing option.

> The Backup Before Clearing Option will only be enabled if the backup option is set during the system installation. If a user has not selected the backup option during the installation nor provided a backup path, this option will not be enabled.



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.

Monitoring Exclusions

- To add an exclusion

  Click the dropdown list

  Type in an exclusion (file extension, user, folder, etc. as relevant)

  Click the **+** icon to add this item to the list

  After completing the list, click **Next** or **Cancel** to close the panel

- To edit or remove an exclusion from the list

  Click the dropdown list

  On the extension to edit or remove click the delete or edit icon

  click **Next**or **Cancel** to close the panel

- Click **Clear Selection** to clear the entire list

Excluded File Extensions

List of file extensions that are not monitored, e.g., txt, exe.

Enter one value at a time as described above.

Exclude Folders

List of folders that are not monitored, e.g., \\servername\share1\\folder1.

Enter one value at a time as described above.

Exclude Users

List of users whose activities are not monitored, e.g., user1, domain\user2, user3@domain.com.

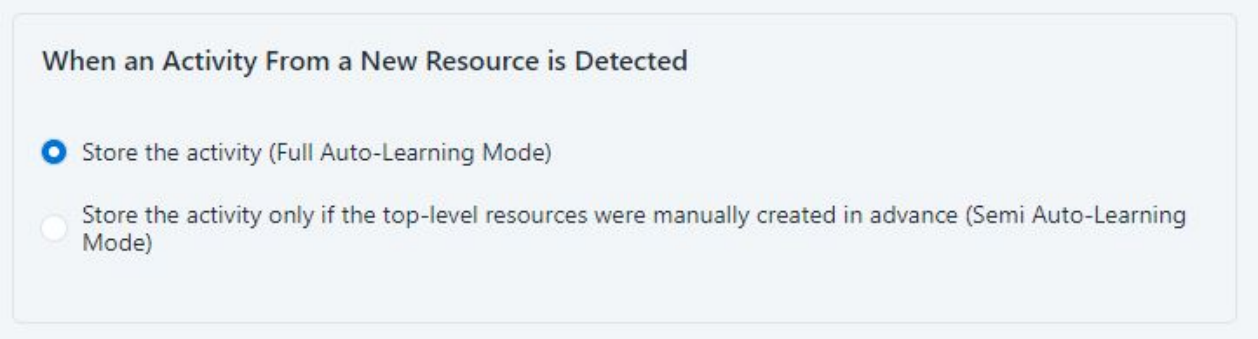
Enter one value at a time as described above.

> The user format to be used depends on how the activity is logged by the endpoint. If you are not sure which of the user formats above to use, either specify all of them, or leave the list empty for now, navigate to the Forensics > Activities screen in the File Access Manager Website after some activities flow in to see how the user is depicted in them and use that depiction in the exclusion list.

When an activity from a new resource is detected:(Modes of Storing Activities)

Full Auto-Learning Mode – Will audit everything (every action) on every resource.

Semi Auto-Learning Mode – Will monitor activities on resources nested under the top-level resources that are marked for Monitoring. This operation mode will also allow the user to select what type of activities are being monitored.



Monitored Actions

The user has the ability set monitored actions within Manage Resources.

1. Navigate to **Admin > Applications**.
2. Under the Actions column, click the ellipsis on the desired application.
3. Click **Manage Resources**.

   The Manage Resources will display with all resources listed.
4. Click **Manage Monitored Actions**.
5. Toggle the **Enable Activity Monitoring for this Resource Hierarchy**.

The user can now select the type of actions they want monitored.

> All actions are automatically selected initially.

Click **Next**.

Enabling Access Fulfillment for an Application

Access fulfillment is enabled per application in the application setting screen, for applications that support fulfillment (See the compatibility table in Compass for the full list)

To enable Access Fulfillment for an application:

1. Open the configuration 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.
2. Press **Next** till you reach the **Access Fulfillment** settings page.

    > The setting pages and entry fields vary according to the application type.

3. For non-normalized resources, you can click **Enable Access Fulfillment for Revoking Explicit Permissions** . See Access Fulfillment for Removal of Explicit Permissions.
4. Click **Enable Access Fulfillment for Normalized Groups**.

    Identity Collector

    Fulfillment requires an identity collector in order to run. If you did not select an identity collector in the General Details configuration page, you can select one from the drop down list now.

    If there is no identity collector defined for this application, or if you want to use a different identity collector than the ones in the dropdown list, you can create a new identity collector in the Administrative Client (*Applications* > *Configuration* > *Permissions Management* > *Identity Collectors*).

    See Create/Edit an Active Directory Identity Collector for more details on creating an identity collector.

    Managed Group OU (DN)

    The organizational unit in which the managed permission groups will be created. Make sure that the chosen identity collector's user has permissions to create groups under this location (e.g. OU=FileAccessManagerManaged, DC=SailPoint, DC=COM)

    OU refers to an Organizational Unit, and DN refers to a Distinguished Name.

    How to Handle 'List Folder Contents' Permissions

    Not relevant for SharePoint

- Create and manage a dedicated permissions group for it - this is the default value
- Revoke these permissions

How to Handle Inexact Permissions Matches

During the normalization process, the application has to decide what to do with permissions that do not match the normalized permissions.

- Fail the normalization process
- Elevate to the nearest permission match
- Revoke the permission

5. Open the Advanced Settings panel for additional settings:

Group Cache Sync Interval(sec)

This setting will add a pause to the process of setting normalize permissions on the resource. This will allow the endpoint's local AD groups cache to sync the newly created managed groups.

The default Is 0 - signifying the process will not pause by default.

Use Template Permission Group

Template groups are created per application and added as a template to every managed resource. These groups are not managed by File Access Manager, and are usually used to ensure that users who need application-wide access such as backup or archiving users have access.

Select for each permission group whether File Access Manager should create a group or whether to use an existing group, for the following groups:

- List Folder Contents
- Read & Execute
- Modify
- Full Control

If you select **Use an Existing Group**, select the required group to use from the dropdown list.

Once an application is enabled for access fulfillment, you can set specific resources to be normalized using the Manage Normalized Resources page.

Adding New Bulk Application (CIFS only)

To add NetApp CIFS applications in bulk, use the New Application Wizard in the admin client.

1. Log into the File Access Manager admin client and navigate to ***Applications > New > Bulk Application***.

   The New Bulk Application Wizard window displays under the Welcome tab.

2. Select **NetApp CIFS**.

3. Click **Download Template** and download the bulk installation Excel template

   > Each application type has a different template

4. Fill in a new row in the template for each application to be installed.

   In the multiple selection fields, such as **Cluster Mode**, and **Multiple FPolicy Servers**, you can select valid options from the drop down list in the Excel file.

   Save the template file.

5. In the wizard, click **Browse** and select the template you filled

6. Click **Upload** to upload the template

7. Once the template is uploaded, the *Upload Status* table contains a row for each application in the template

8. If there are errors displayed in the *Upload Status* table, correct the parameters and upload the template again.

   - This stage is for validation only.
   - Applications with errors will be ignored, and won't be created

9. Click **Next**.

   > You can navigate among the Permissions Collection and Crawler scheduling windows (under the Scheduling tab) with the Next and Back buttons

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

   > A schedule is created for each application with the name: PermissionsCollection_<Service Name> Task, with the same details.

Scheduling Tasks

In the next configuration screens you can schedule tasks to collect and analyze the BRs in the connected servers.

The scheduling includes

- Permissions Collector
- Crawler - Automatic application crawling to find new resources
- Data Classification - to classify your results

Fill in the scheduling fields for each scheduling screen:

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.

> See the chapter “Crawling” in the File Access Manager Administrator Guide for more information on the crawling mechanism.

Press **Next** and **Back** to navigate between the screens.

Completing the Installation

After the Data Classification screen, click **Next**.

> The applications are created at this stage

The Application Creation Status window of the New Bulk Applications Wizard displays under the Status tab.

A table lists the creation status of each application.

Click **Next**

The **Installation File** window of **New Bulk Applications Wizard** displays.

1. Browse to select the destination for the .zip file, which contains the files required to install the Activity Monitor / Permissions Collector / Data Classification services for each application.
2. A text file with the command line for remote installation of the Activity Monitor connector is also created. This file can be used for unattended installations of the Activity Monitor. See Activity Monitor Bulk/Unattended Installation for further information.
3. Click **Finish**

Installing Services: Activity Monitor and Collectors

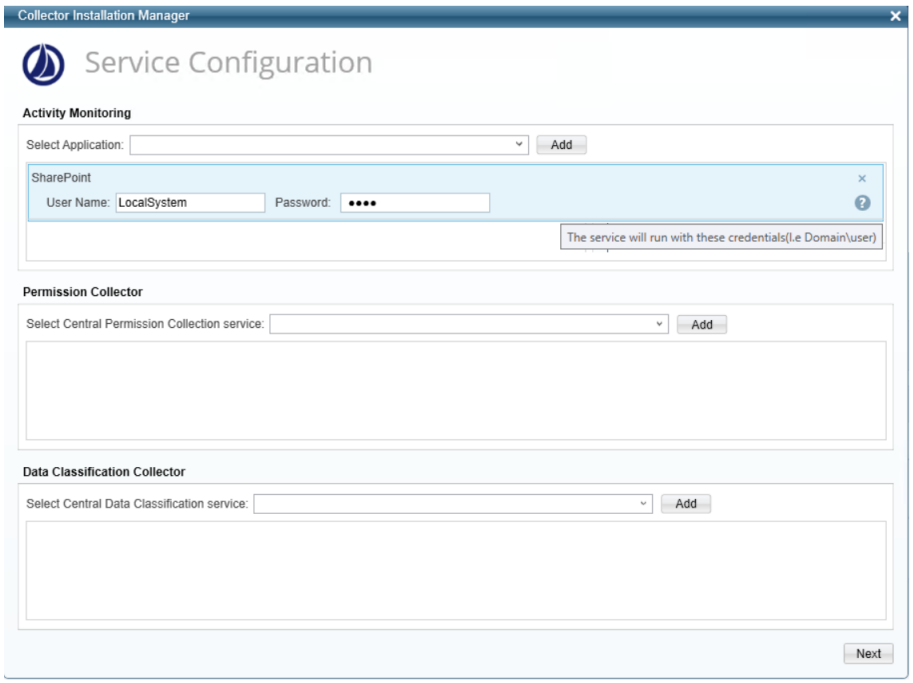
The Collector Installation Manager is part of the File Access Manager installation package. This tool is used to install the activity monitor, permission collector, and data classification collector.

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. If you are installing the Permission Collector, select the Central Permission Collector to which to connect this service, and click **Add**.
7. If you are installing the Data Classification, select the Central Classification Collector to which to connect this service, and click **Add**.
8. 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.

9. Browse and select the location of the target folder for installation.

10. Browse and select the location of the folder for system logs.
11. Click **Next**.
12. The system begins installing the selected components.
13. 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 NetApp Connector Installation

Verifying Application Configuration

After the configuration of one of the following applications is complete, verify it was properly configured by running the Test Connection task.

The Test Connection will run and validate a series of validations to see if the application was configured correctly.

Common NetApp Validations

The following is a list of common validations that run when the test connection is run with a NetApp application.

- Server responsiveness
- Verifying the ability to list shares
- Verifying the ability to read share permissions
- Verifying the membership to the Backup Operators group
- Verifying access to the ONTAP API
- Verifying the FPolicy is configured
- Verifying there is a connection between FPolicy and the Activity Monitor

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>
- File Access Manager Central Permissions Collection - <Service Name>
- File Access Manager Central Data Classification - <Service 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"
- “%SAILPOINT_HOME_LOGS%\Netapp-<Application_Name>.log"

Monitored Activities

1. Simulate activities on NetApp.
2. Wait a minute (approximately).
3. Verify that the activities display in the File Access Manager website under *Forensics* > *Activities*

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*)

Troubleshooting

Check the issues below for common problems and suggested ways of handling them.

What to do if Events are not Collected

NetApp 7-mode

1. In the relevant vfiler context in the NetApp, run the command

   `FPolicy show [whitebox_cifs_policy]` or `[whitebox_nfs_policy]` depending on the application type.

2. Verify that the Activity Monitor server is connected as an FPolicy server.

3. If the FPolicy server is registered, simulate some activity, run the command again, and look on the counters at the end of the output of the command. They should increase.

4. If they don't increase, there might be something wrong with the definition of the included volumes. If the name of the included volume is wrong, no events will be sent by NetApp.

5. If the Activity Monitor is not registered as an FPolicy server, stop the activity monitor service, wait 60 seconds, and start the activity monitor service again.

   > In some cases, it takes a while to NetApp to de-register the FPolicy server in case of an error.

6. Run the command again and make sure the FPolicy server is registered.

7. If the FPolicy server is not registered, Verify the following:

   - The Activity Monitor service is running with a domain user who is a local administrator on the server running the Activity Monitor
   - The user running the Activity Monitor service is a member of the 'Backup Operators' local group on the filer/vfiler
   - The activity monitor server is in the same domain as the server running the Activity Monitor service

- The clock of the server running the Activity Monitor and the NetApp clock are accurate to within 5 minutes. A larger difference might cause the RPC Kerberos authentication process to fail
- There is no firewall between the NetApp and the server running the Activity Monitor, and that the Windows Firewall is off on the server running the Activity Monitor

8. If all the prerequisites are set, look for errors in the activity monitor which indicates if it cannot connect to the FPolicy server, and look for messages in the NetApp log which indicates if the FPolicy server is trying to register and fails, or disconnected after a while.
9. If there are authenticated failures in the Activity Monitor/Permission Collector logs to the Ontapi API:
    - Make sure all the prerequisites listed in the Permissions section were configured correctly
    - If the Activity Monitor seems to connect successfully to the NetApp, but disconnects a few seconds later, check whether the NetApp filer and the Activity Monitor server use the :same SMB version.

      > SMB1 is no longer supported on most modern systems. The following methods pertaining to that version may not work on any server. Use SMB2 or higher when possible.

        - Run the following command on the NetApp side to see if SMB2 is enabled:

          ```
          options cifs.smb2.enable
          ```

        - If it is not enabled, run the following command to enable it:

          ```
          options cifs.smb2.enable on
          ```

        - If for some internal reason you cannot are are not allowed to enable SMB2, use one of the following methods to enable SMB1 on the Windows side:
        - On Windows Server 2012 up to 2016, you can use the following PowerShell command:
        - ```
          Set-SmbServerConfiguration -EnableSMB1Protocol $true
          ```
          ```

- Windows Server 2016 or lower, you can check the registry value SMB1 under: HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters.
- If it exists and is set to 0, SMB1 is disabled. To enable, set the value to 1.

NetApp Cluster Mode:

If not all events are collected, perform the following:

1. Run the command:

```
fpolicy show-engine
```

2. Locate the line which represents the FPolicy engine for the Vserver you are analyzing and verify that the IP address of the FPolicy server matches the IP address of the server where the Activity Monitor is installed and that the Server Status is connected.
3. If the Server Status is disconnected, run the following command:

```
fpolicy show-engine –node <node-name> -instance
```

   This will indicate the reason for the disconnection.

4. If the disconnect reason is **TCP failure**, make sure the port configured in the Application configuration matches the port configured in the FPolicy configuration, and that the IP address of the external-engine configuration is the same as the IP address of the server running the Activity Monitor.
5. Verify that there is no firewall between the Activity Monitor server and the cluster nodes and that the windows firewall is off on the Activity Monitor server.

   > The firewall should only be off during troubleshooting. Turning off the firewall should not be a permanent solution. Refer to Physical Filer 7-Mode Communications Requirementsfor more information.

6. If you see **Authentication Failures to the ONTAP API** in the Activity Monitor or Permissions Collector logs, check for the following:

a. All the prerequisites in the Permissions section were configured correctly.

b. The domain case configured in the application matches the configured domain value for the user configured in the Permissions sections.

c. The username configured in the Permissions section is with the same as the username in Active Directory, and the user defined in the Application configuration.

7. Make sure the NetApp internal firewall is not blocking communications with the Activity Monitor. Running the following commands in case of a block allows communication with the Activity Monitor:

```
system services firewall policy clone -vserver <vserver_name> -policy data -destination-policy fp_siq1 -destination-vserver <vserver_name>
```

```
system services firewall policy create -vserver <vserver_name> -policy fp_siq -service http -allow-list <am_server_ip_address_with_mask>
```

8. If the Crawler hits unexpected “access denied” errors or misses entire shares because of “access denied” errors, this might be related to a known NetApp bug, which is documented in their knowledgebase (you need a NetApp account to see the entire entry):

   https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/ONTAP_OS/Backups_failing_even_though_user_is_part_of_BUILTIN%5CBackup_Operators_group_for_ONTAP_9

   - The bug affects Data ONTAP 9.x, and according to the document should be fixed in version 9.4. It “causes backup intent permissions to be incorrectly checked”. This means the Backup Operators membership used to gain access to the filesystem doesn’t work, and “access denied” errors are sent back.
   - Fortunately, there’s a workaround provided in the knowledgebase entry, which is to “disable fake open capability” by running the following commands on the NetApp console or an SSH connection to the management interface (replace SVM01 with the relevant Vserver):

```
set diag
```

```
cifs options modify -vserver SVM01 -is-fake-open-enabled false
```

SSL Connection Failure

If an error is received in the Permissions Collector or Activity Monitor about an SSL connection which can’t be established:

- The certificate key length on the NetApp should be verified. In older NetApp versions, the default certificate is created with 512bit length certificate. Use this command to create a certificate with at least 1024bit length key:

```
secureadmin setup ssl
```

- Data ONTAP up to version 8.2.3 operating in 7-mode only supports security protocols up to TLSv1.0, with the following cipher suites supported when using TLSv1.0:
  - TLS_RSA_WITH_RC4_128_MD5
  - TLS_RSA_WITH_RC4_128_SHA
  - TLS_RSA_WITH_3DES_EDE_CBC_SHA
- Removing support for cipher suites using RC4 or 3DES as their block cipher (the algorithm used to encrypt the data) means that the filer has no available cipher suites to use for secure communications.
- Any server trying to communicate securely with the filer must support one of the above cipher suites, preferably 3DES, because it has been deprecated most recently and is still allowed for use). If you have knowledge of these ciphers or TLSv1.0 being blocked in your organization, you must unblock them on the servers running Permission Collection and Activity Monitoring. If you don't know how to unblock them, talk to your organization's security department/team, because those settings are not set that way by default. For further information, check the links below:
  - https://blogs.msdn.microsoft.com/friis/2016/07/25/disabling-tls-1-0-on-your-windows-2008-r2-server-just-because-you-still-have-one/
  - https://www.tbs-certificates.co.uk/FAQ/en/desactiver_rc4_windows.html
- According to a NetApp security advisory, Data ONTAP 8.2.5 operating in 7-mode has the option to turn off TLSv1.0 entirely, and it supports TLSv1.1 and TLSv1.2, plus extra cipher suites that are supported by them, so this version should not be affected by removing support for cipher suites using RC4 or 3DES. The advisory is linked here:

  https://security.netapp.com/advisory/ntap-20160915-0001/
- If no events are collected, See What to do if Events are not Collected.