Integrating NetApp with File Access Manager

Version: 8.1 Revised: February 23, 2021

Contents

Capabilities

This connector enables you to use IdentityIQ 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 IdentityIQ File Access Manager

See the IdentityIQ File Access Manager documentation for a full description.

Supported Versions

- ONTAPI 7.3 7-mode and above
- ONTAPI Cluster mode 8.2 and above under these specific constraints by NetApp:
    - Confirmed NetApp bug id 800390: Panic during SCSI compare and write is solved in the following specific versions and up:
        - 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, IdentityIQ File Access Manager Connector for NetApp uses the NetApp FPolicy mechanism and registers as an FPolicy server.

Permissions Collector

CIFS Shares

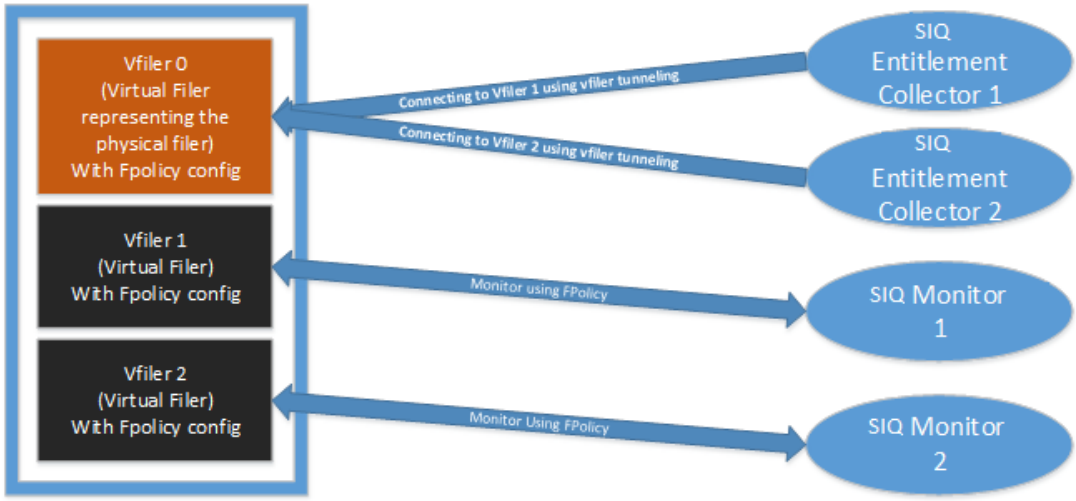
- IdentityIQ File Access Manager connects to CIFS shares using backup semantics ('seBackup' privilege).
- During the Permissions Collection process - local groups and users are retrieved using the NetApp Ontapi Web API.

NFS Exports

- 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.
- 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 IdentityIQ File Access Manager

7-mode ONTAPI NetApp



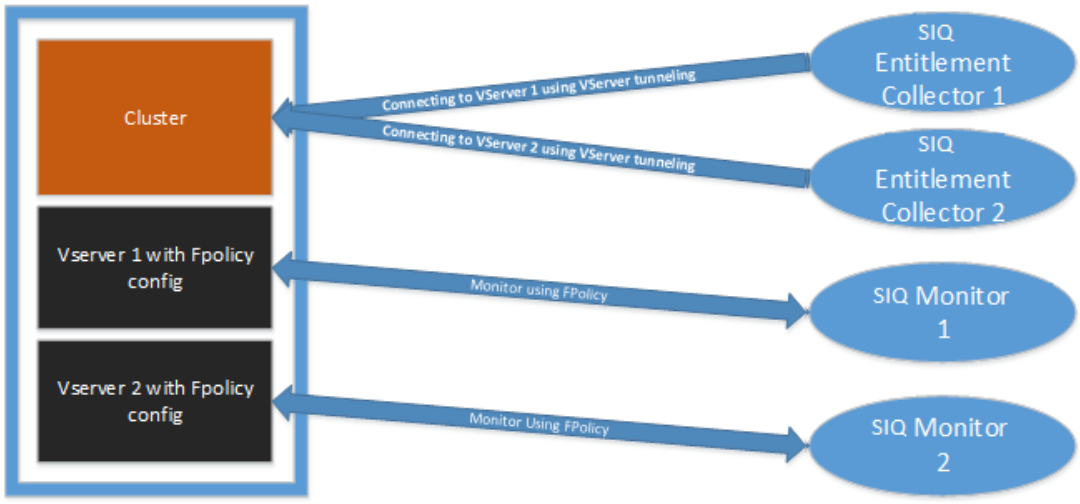
- A 7-mode ONTAPI NetApp can work in one of two architectures, a single physical file server or multiple virtual filers hosted on the same physical machine (by using the Multistore feature).
- The virtual architecture filers enable hosting multiple virtual file servers on single physical machine, with 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 IdentityIQ 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 IdentityIQ 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 IdentityIQ 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.

- IdentityIQ 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 IdentityIQ 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 IdentityIQ 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 IdentityIQ 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.
- IdentityIQ 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 IdentityIQ 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 IdentityIQ File Access Manager professional services.

Prerequisites

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

Software Requirements

.NET 4.5 is required on servers where the Activity Monitor / Permissions Collector / Data Classification service is installed.

Permission Requirements

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

The following listing describes the required permissions by IdentityIQ 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 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 IdentityIQ File Access Manager tasks:

1. Create a dedicated domain user for the filer (for example, SIQ_<filename>). 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 IdentityIQ File Access Manager user permissions to access the Ontapi web API.
   Replace <*DOMAIN*> with the domain name and *siq_<filename>* 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_<filename> -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
IdentityIQ File Access Manager Access	Activity Monitor	IdentityIQ File Access Manager Servers	8000-8008
NetApp CIFS Access	Activity Monitor	NetApp	RPC (135 + Dynamic)
NetApp fpolicy	NetApp filer	Activity Monitor	MSRCP (139)
NeApp 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 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 IdentityIQ File Access Manager tasks:

1. When monitoring a vfiler, IdentityIQ 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 IdentityIQ 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 IdentityIQ 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 IdentityIQ File Access Manager installation folder on one of the IdentityIQ 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
IdentityIQ File Access Manager	Permissions Collector/Data Classification Collector	RabbitMQ	5671
IdentityIQ File Access Manager Access	Activity Monitor	IdentityIQ 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)
NetApp Web API	Permissions Collector / Activity Monitor	NetApp VFILER ZERO	443 (https)
NetApp NFS Access	Permissions Collector	NetApp VFILER	UDP/TCP 111, 2049 (NFSv3)

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.

NetApp 8.2+ Cluster Mode Requirements

According to the NetApp Architecture and IdentityIQ File Access Manager section, each Vserver is represented as a single Application in IdentityIQ 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 IdentityIQ 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>
```

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

> If the IdentityIQ File Access Manager Application is configured to use Vserver Tunneling, run these commands at the cluster level without the -vserver parameter. However, if the IdentityIQ 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 IdentityIQ 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
IdentityIQ File Access Manager Access	Activity Monitor	IdentityIQ 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 Connector Installation Flow Overview

To install the NetApp connector:

1. Configure all the prerequisites.
2. Add a new NetApp application in the IdentityIQ File Access Manager Administrative Client.
3. Install the relevant services:
    - Activity Monitor
    - 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 IdentityIQ File Access Manager deployment architecture. The IdentityIQ File Access Manager Administrator Guide has additional information on the architecture.

Data Collection Configuration Overview

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 IdentityIQ 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 IdentityIQ File Access Manager Administrative Client. 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. 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

> Some application do not support adding a collector to the central engine. (Box, Dropbox, OneDrive, SharePointOnline) . In these applications the task will be done entirely by the engine, and none of the work will be relegated to its collectors.

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

Connector / Collector terminology:

Connector

The collection of features, components and capabilities that comprise IdentityIQ File Access Manager support for an endpoint.

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 It has no “physical” manifest.

- The actual work is done by the Collector Synchronizer.
- There are no collectors other than Data Classification and Permission Collection
- The connector is not synonymic to a collector.

Adding a NetApp Application

In order to integrate with NetApp , we must first create an application entry in IdentityIQ 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 (In New Application Wizard)

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 **Locigal container**field that was used when creating applications in releases before 8.2

Event Manager Server

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*
- 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 (In New Application Wizard)

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 IdentityIQ File Access Manager Professional Services/Support)

Click **Next**.

Permissions Collection

Associate an application with a Central Permission Collector Service. This service is responsible for running the Permission Collector and Crawler tasks

> This page is is part of the New Application Wizard

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

Set up the permission collection filling the following fields.

> The actual fields displayed will vary between application types.

Enable Permissions Collection

Click to enable permission collection for this application. If the "IdnetityIQ FAM Central Permission Collector" wasn't installed during the installation of the server, this checkbox will be disabled

Central Permissions Collection Service

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

Skip Identities Sync during Permission Collection

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

> This setting is not recommended unless required

Calculate Effective Permissions

Calculate effective permissions during the permissions collection run

Calculate Riskiest Permissions

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

Permissions Source

NTFS, Share, Both

Analyze the "Shared Link" permissions on files

Click to collect the permissions of Shared Links. A Resource will be created for each Shared Link with unique permissions, which will display.

Analyze the "Collaborators" permissions on files

Click to collect permissions for files assigned directly to Collaborators. A Resource will be created for each file with Collaborators and its permissions will display.

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.

Configure Activity Monitoring

Configure the activity monitoring process frequency .

> This page is is part of the New Application Wizard

Polling Interval

Activity fetching interval [in seconds])

Report Interval

Activity Monitor Health reporting interval [in seconds])

Local Buffer Size

Local buffer size for activities [in MB])

Monitoring Exclusions:

Excluded File Extensions

List of file extensions that are not monitored. Click **+** on the extension field to add the extension to the list.

Click **Save** or **Cancel** to exit this entry panel.

Exclude Folders

List of folders that are not monitored

Exclude Users

List of users whose activities are not monitored

> Each excluded user must be in the form of Domain\User.

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

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.

Click **Next**.

Crawler Scheduling

To set or edit the Crawler configuration and scheduling, open the appropriate application The Crawler configuration is filled per

> This page is part of the New Application Wizard

Crawl Snapshots Folder

Only for NetApp - CIFS / NetApp - NFS

Calculate Resource size

Select one of the following:

- Never
- Always
- Second crawl and on (default)

This option is not relevant for Active Directory, Exchange, Exchange on-line, Windows DFS

Crawl Scope

Define the resources to scan

Advanced Crawl Scope Configuration

There are two methods to enter the scope (such as folders) to scan:

1. An explicit list of folders to include or exclude in the crawl
2. Using a regex to define the scope.

Exclude Paths by Regex

Type in the names of folders to exclude from the crawling process.

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

Create a Schedule

See Scheduling a Task

Click **Next**.

Data Classification Scheduling

Associate an application with Central Data Classification Service.

> This page is is part of the New Application Wizard

Enable Data Classification

For applications that support data classification, this checkbox appears, and is checked by default.

If the “Central Data Classification” wasn’t installed during the installation of the server, this checkbox is disabled.

Create a Schedule

See Scheduling a Task

> See the chapter “Data Classification” in the IdentityIQ File Access Manager Administrator Guide for more information

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

Data Enrichment Scheduling

> This page is part of the New Application Wizard

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 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.

Access Fulfillment Configuration

Enable Access Fulfillment for Revoking Explicit Permissions

1. Check the relevant fulfillment option.

   Enable Access Fulfillment for removing direct permissions

   Clck this optin to enable access direct permission remediation.

   Enable Access Fulfillment for normalized groups

   Click this option to allow IdentityIQ File Access Managerto add to, and remove permissions from, specific IdentityIQ File Access Manager groups

   > See “Access Fulfillment” in the *IdentityIQ File Access Manager Administrator Guide* For additional information.

2. Domain Name
3. Click **Finish**.

Fulfillment Setup Notes for NetApp

> On the scheduling screens, Fulfillment is only applicable for NetApp CIFS applications.

Adding New Bulk Application(CIFS only)

To add NetApp CIFS applications in bulk, use the **New Application Wizard** in the IdentityIQ File Access Manager Administrative Client.

1. 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: [Application Name] – RoleAnalytics 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

Schedule

Select a scheduling frequency from the dropdown menu.

Schedule Types and Intervals

Schedule Type	Start / End	Comment
Once		Single execution task runs.
Run After		Create dependency of tasks. The task starts running only upon successful completion of the first task.
Hourly	Yes	Set the start time
Daily	Yes	Set the start date and time
Weekly	Yes	Set the day(s) of the week on which to run.
Monthly	Yes	The start date defines the day of the month on which to run a task.
Quarterly	Yes	A monthly schedule with an interval of 3 months.
Half Yearly	Yes	A monthly schedule with an interval of 6 months.
Yearly	Yes	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 IdentityIQ 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 I**nstallation 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: Collector Installation

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

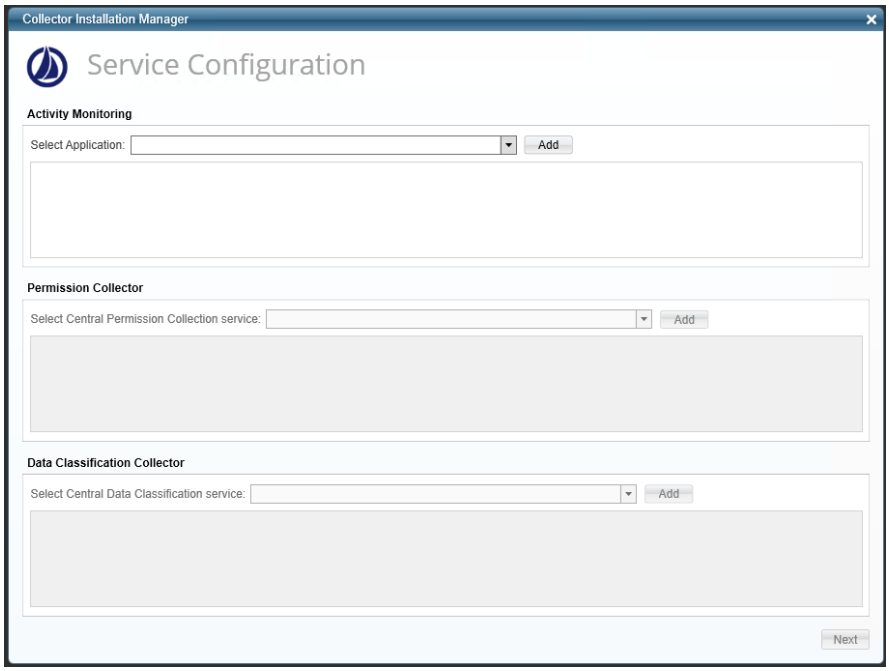
   The Collector Installation Manager window displays.

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 Manageruser 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.



4. If you are installing the Activity Monitoring collector, select the application, and click **Add.**

   > In some applications, additional credentials may be required to allow granting elevated permission for activity monitoring collection. .

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, select the Central Classification Collector to which to connect this service, and click **Add**
7. 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.

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**

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

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

Verifying the NetApp Connector Installation

Installed Services

Verify that the services installed for the connector are available and active. Using windows Service manager, or other tool, look for the IdentityIQ 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%\Netapp_<Application_Name>.log"
- “%SAILPOINT_HOME_LOGS%\RoleAnalytics_<Application_Name>.log"
- “%SAILPOINT_HOME_LOGS%\DataClassification_<Application_Name>.log"

Monitored Activities

1. Simulate activities on NetApp.
2. Wait a minute (approximately).
3. Query for activities in the IdentityIQ File Access Manager Administrative Client by <Application_Name>.
4. Verify that the activities display in the IdentityIQ File Access Manager website under

   Forensics > *Activities*

Permissions Collection

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

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 SMB1 is enabled on the Activity Monitor server by:
     - Using the following PowerShell command (Windows Server 2012 and up):

       `Get-SmbServerConfiguration | Select EnableSMB1Protocol`

     - To enable, use:

```
Set-SmbServerConfiguration -EnableSMB1Protocol $true
```

- Checking the registry value SMB1 under: `HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters` (if it exists and 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

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/app/answers/answer_view/a_id/1075045/~/backups-failing-even-though-user-is-part-of-builtin%5Cbackup-operators-group-

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, perform the following:

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. You should see that there 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, assure that:
   - 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 no more than 5 minutes' difference. This can 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:
10. Make sure all the prerequisites listed in the Permissions section were configured correctly
11. If the Activity Monitor seems to connect successfully to the NetApp, but disconnects a few seconds later, check whether SMB1 is enabled on the Activity Monitor server by:
    - Using the following PowerShell command (Windows Server 2012 and up): Get-SmbServerConfiguration | Select EnableSMB1Protocol
    - To enable, use: Set-SmbServerConfiguration -EnableSMB1Protocol $true
    - Checking the registry value SMB1 under: HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters (if it exists and 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 assure 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. Make sure 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.

6. If you see Authentication Failures to the ONTAP API in the Activity Monitor or Permissions Collector logs:

   a. Make sure all the prerequisites in the Permissions section were configured correctly.
   b. Make sure the Domain case configured in the Application matches the configured domain value for the user configured in the Permissions sections.
   c. Make sure 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 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
     ```