Technical Report

FPolicy Solution Guide for Clustered Data ONTAP: dg file

Brahmanna Chowdary Kodavali, Saurabh Singh, NetApp
Dr. Rainer Pollak, Traian Matei, DataGlobal
October 2015 | TR-4465

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Introduction

The NetApp® FPolicy® feature is a file-access notification system that allows an administrator to monitor file access in storage configured for Network File System (NFS and CIFS). Introduced for the scaled-out architecture of the NetApp clustered Data ONTAP® 8.2 operating system, FPolicy enables a rich set of use cases working with selected NetApp partners. FPolicy requires all nodes in a cluster to run Data ONTAP 8.2 or later. FPolicy supports all SMB versions, including SMB 1.0 (CIFS), SMB 2.0, SMB 2.1, and SMB 3.0. It also supports major NFS versions, including NFSv3 and NFSv4.0.

FPolicy natively supports simple file-blocking use cases, which enables administrators to restrict end users' unwanted files. For example, an administrator can block audio and video files from being stored in data centers, saving storage resources. This feature blocks files only based on extension; for more advanced features, partner solutions have to be considered.

This system enables partners to develop applications that cater to a diverse set of use cases, including but not limited to the following:

- File screening
- File-access reporting
- User and directory quotas
- Hierarchical storage management (HSM) and archiving solutions
- File replication
- Data governance

1.1 Audience

The target audience for this document is customers who want to implement virus scanning for clustered Data ONTAP storage systems that use the CIFS protocol.

1.2 Purpose and Scope

The purpose of this document is to provide an understanding of FPolicy framework and define steps to deploy a file-archiving solution using a DataGlobal dg file. The scope of the document encompasses the deployment procedures and best practices for the solution.

2 FPolicy Overview

The Data ONTAP FPolicy framework creates and maintains the FPolicy configuration, monitors file events that result from client access, and sends notifications to external FPolicy servers. Communication between the storage node and the external FPolicy servers is either asynchronous or synchronous.

The use of asynchronous or synchronous communication depends on whether or not the FPolicy framework expects a notification response from the FPolicy server.

- Asynchronous notification is suitable for use cases such as monitoring and auditing of file-access activity that do not require Data ONTAP to take action based on the FPolicy server's notification response. In these cases, Data ONTAP does not need to wait for a response from the FPolicy server. Monitoring and auditing file-access activity, file replicating, and file collaborating require asynchronous notification.
- Synchronous notification is suitable for use cases in which Data ONTAP must allow or deny client access based on the notification response from the FPolicy server. Use cases such as quotas, file screening, and file-archiving recall require synchronous notification.

2.1 Role of Clustered Data ONTAP Components in FPolicy Configuration

The following components play a role in FPolicy configuration:

- **Administrative SVM (cluster).** The administrative storage virtual machine (SVM, formerly called Vserver in the Data ONTAP CLI and GUI) contains the FPolicy management framework and maintains and manages the information about all FPolicy configurations in the cluster.
- **Data SVM.** FPolicy configuration can be defined at the cluster or at the SVM. The scope defines the resources to be monitored within the context of an SVM and operates only on SVM resources. One SVM configuration cannot monitor and send notifications for the data (shares) belonging to another SVM. However, FPolicy configurations defined on the admin SVM can be leveraged by all data SVMs.
- **Data LIFs.** Connections to the FPolicy servers are made through data logical interfaces (LIFs) that belong to the data SVM containing the FPolicy configuration. The data LIFs used for these connections can fail over in the same manner as data LIFs used for normal client access.

2.2 How FPolicy Works with External FPolicy Servers

FPolicy runs on every node in the cluster and is responsible for establishing and maintaining connections with external FPolicy servers. As part of its connection management activities, FPolicy framework manages the following tasks:

- Controls the flow of file notifications through the correct LIF to the FPolicy server
- Load-balancing notifications to the FPolicy server when multiple FPolicy servers are associated with a policy
- Tries to reestablish the connection when a connection to an FPolicy server is broken
- Sends notifications to FPolicy servers over an authenticated session
- Establishes a connection with the data LIFs on all nodes participating in the SVM

The FPolicy server accesses data on the SVM through a privileged data-access path. Data ONTAP secures this path by combining specific user credentials with the FPolicy server IP address that was assigned during FPolicy configuration. After FPolicy is enabled, the user credentials included in the FPolicy configuration are granted the following special privileges in the file system:

- Ability to bypass the permissions checks when accessing data, enabling the user to avoid checks on files and directory access
- Special locking privileges through which Data ONTAP allows the FPolicy server to read, write, or modify access to any file, regardless of existing locks

Note: If the FPolicy server creates byte-range locks on the file, existing locks on the file are removed immediately.

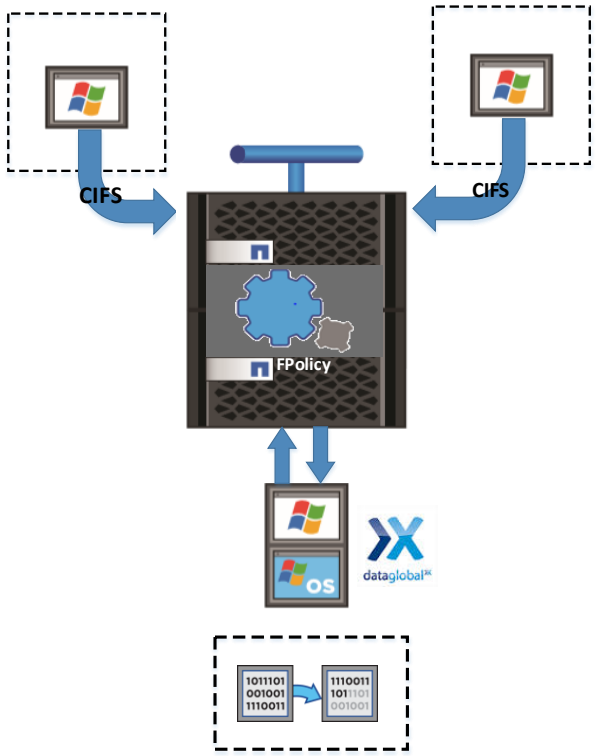
- Ability to bypass any FPolicy checks so that file access over the privileged data path does not generate an FPolicy notification

For more information about FPolicy functionality, see Clustered Data ONTAP 8.3 File Access Management Guide for CIFS on the NetApp Support site.

3 FPolicy Solution Architecture

The FPolicy solution consists of the clustered Data ONTAP FPolicy framework and the FPolicy application dataglobal dg file, as shown in Figure 1.

Figure 1) FPolicy solution architecture.



FPolicy application software is installed on a Windows Server; the FPolicy framework exists within clustered Data ONTAP. The FPolicy framework connects to external FPolicy servers and sends notifications for certain file system events to the FPolicy servers when these events occur as a result of client access. The external FPolicy servers process the notifications and send responses back to the FPolicy framework.

3.1 FPolicy Components in Clustered Data ONTAP

The FPolicy framework in clustered Data ONTAP includes the following components:

- **External engine.** This container manages external communication with the FPolicy server application.
- **Events.** This container captures information about protocols and file operations monitored for the policy.
- **Policy.** This is the primary container that associates different constituents of the policy and provides a platform for policy-management functions, such as policy enabling and disabling.
- **Scope.** This container defines the storage objects on which the policy acts; examples include volumes, shares, exports, and file extensions.

3.2 FPolicy Application Software: dg File

The DataGlobal product suite includes modules for analyzing, classifying, managing, and archiving information enterprise wide. DataGlobal sets benchmarks for unified storage and information management and includes the revolutionary unified archiving approach.

The dg file is an important addition to the dg ControlCenter. The dg ControlCenter enables analysis and selection of files on a storage resource that is a likely candidate for archiving.

The replacement of the migrated files with reference files results in a significant reduction of storage space on the primary storage. When there is a user or application access to a reference file, the dg file migration adapter automatically initiates a recall operation, and the reference file is replaced with the original file.

3.3 Benefits

The main benefits of using dg file are that it:

- Reduces complexity by providing a common code basis of dg files for both platforms (NTFS and NetApp)
- Allows selected files to be migrated to archive
- Frees storage space on primary storage
- Provides a transparent solution for the individual user
- Seamlessly integrates with all other functionalities of the dg ControlCenter
- Provides high scalability because from one to any number of file servers can be managed in a single instance of the dg ControlCenter
- Is compatible with all major backup and antivirus solutions

3.4 Glossary

The following terms are important:

dg File Migration Adapter for NetApp

dg file migration adapter is a software product providing archiving functionality for NetApp storage systems.

CC Node

CC node is a server system that is responsible for all dg file migration adapter operations and communication with the dg ControlCenter. It contains an installed dg file migration adapter and a dg file analysis agent in remote configuration mode. The FPolicy server on this system is installed but is configured to be inactive.

FPolicy Node

FPolicy node is responsible only for file recalls using the FPolicy server. The dg file migration adapter is installed but is configured to be inactive on this system.

FPolicy Server

FPolicy server is responsible for detecting access to files residing on the Data ONTAP file system of the NetApp file server. If a reference file is accessed, the dg file migration adapter initiates a recall from secondary storage. The FPolicy server resides on the dg file migration adapter system and is added during the installation process. NetApp recommends using a minimum of two FPolicy nodes for load-balancing reasons. Dg file supports operating up to *n* FPolicy nodes in parallel.

dg File Analysis Agent

dg file analysis agent is the analyzing component of the dg ControlCenter and is required to be installed on the CC node. It needs to be configured in remote mode for NetApp migration.

dg File Analysis Agent in Remote Mode

Because the dg file analysis agent accesses the NetApp file server remotely, the configuration requires read/write credentials to analyze and access the files located on the NetApp file server.

Remote Analysis Agent Group

Multiple dg file analysis agents can be combined into a logical group for work load balancing and failover purposes.

Primary Storage

The HSM source is represented a managed volume on the NetApp file server.

Secondary Storage

The HSM target is represented by either a CIFS archive or another supported archive type such as TSM or ERSArchive.

Reference File

Reference file is also known as stub file or link. The reference file acts as a placeholder for the original file and initiates a recall from the secondary storage in case of access.

Logical Node Manager

The logical node manager (LNM) maintains the primary and secondary storage configuration as well as all global configuration settings.

Physical Node Manager

The physical node manager (PNM) provides configuration data for primary and secondary storage.

3.5 Components

The dg file software contains the following components that can be selected during the installation process:

- dg analysis agent
  - File, capacity, and database analysis
  - End-to-end measurements
  - Classification functionality in different modes (external metadata and content based)
  - Communication with the dg ControlCenter
  - Communication to migration agents or the migration adapter
- dg file migration adapter for Windows
  - File migration, release, and recall for Windows file server
- dg file migration adapter for NetApp
  - File migration, release, and recall for NetApp file server
- NetApp file server environment architecture

1. Functions of one NetApp CC node:
   a. Gets storage configurations from ControlCenter (using the analysis agent).
   b. Stores storage configurations and distributes configurations to FPolicy servers (using LNM).
   c. Running services: dg file analysis agent, dg file LNM, dg file PNM.
   d. Running processes: analysis agent, LNM, PNM, primary storage manager (PSM), secondary storage manager (SSM).
2. Functions of one or multiple FPolicy nodes:
   a. Requests and gets storage configuration from LNM process that is running on the CC node.
   b. Running services: dg file PNM.
   c. Running processes: PNM, FPolicy server, PSM, SSM.
   d. Configuration for CC node and FPolicy nodes: see section 4.2.

4 Installation and Configuration of the dg File

4.1 dg File Software Requirements and Installation

Hardware Requirements

- Intel/AMD x86 or x64 processors, minimum 4GHZ, four cores recommended
- RAM memory minimum 4GB
- The complete installation of dg file requires 20MB

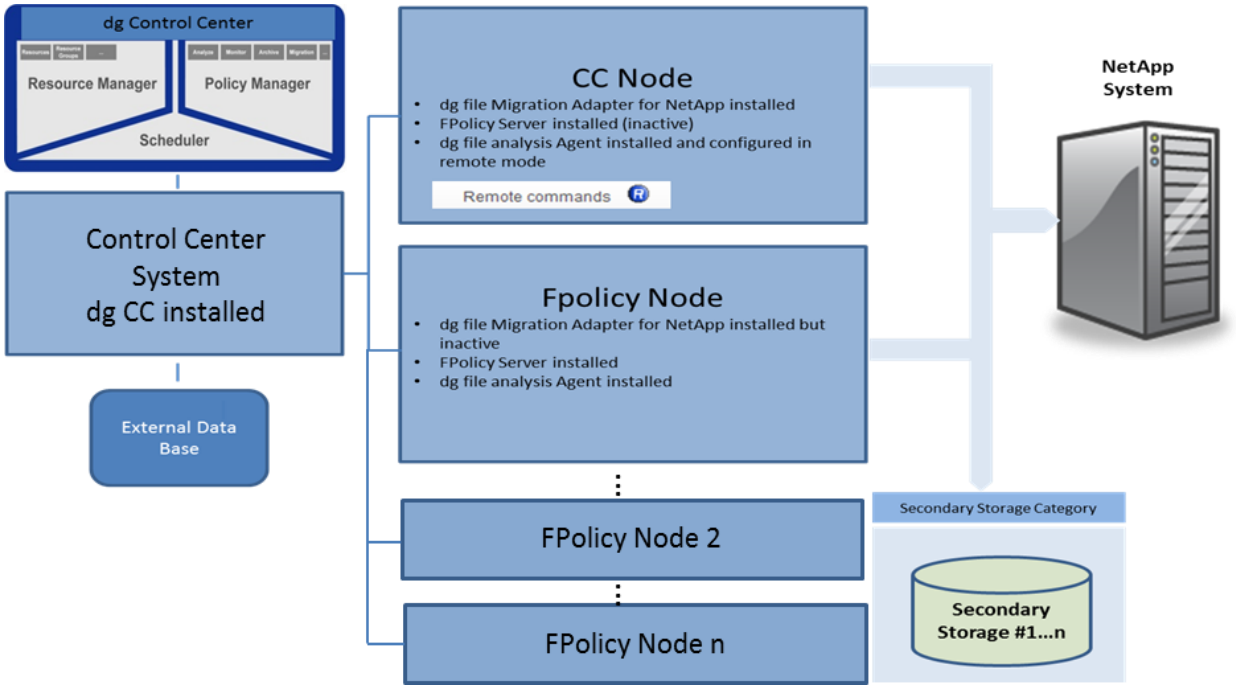
Other Requirements

- The dg analysis agent and the migration feature require local administrator rights.
- Full access/read write credentials required for accessing the secondary storage.
- Operation of dg file NTFS requires the dg analysis agent to have a license module type dg file Windows assigned in the dg ControlCenter.
- Operation of the dg file netapp requires the dg analysis agent to be configured in remote mode and to have a license module type dg file netapp assigned in the dg ControlCenter.
- For dg file migration in a NetApp environment, a minimum of two FPolicy nodes is recommended for load-balancing reasons. dg file migration adapter for NetApp supports operating up to *n* FPolicy nodes in parallel.
- The presence of a dg ControlCenter for configuration of:
  - Primary storage
  - Secondary storage category
  - Secondary storage
  - dg file uses the Transport Layer Security (TLS) 1.0 communication protocol between the dg file agent and the dg ControlCenter

  The dg file Installation Guide (as well as all other technical literature) can be downloaded after registration from http://www.dataglobal.com/en/dg-world.html.

4.2 Configuring the NetApp dg File

Figure 2) Deployment scenario overview.



Prerequisites

- A valid license containing the modules `dg file netapp` and `dg analyze`.
- A configured and enabled FPolicy instance for the managed NetApp volumes.
- CIFS needs to be licensed and enabled for the managed NetApp volumes.
- Both systems (CC node and FPolicy node) require the dg file migration adapter to be installed.
- A user account for the dg file agent in remote mode with sufficient credentials to access primary storage resources must be included in the NetApp administrator group.

Adding the Remote User to the NetApp Group of Administrators

On your NetApp system, use the following command to add the user account for the dg file agent in remote mode to the NetApp group of administrators:

```
cifs user-and-group local-group add-members -vserver <vservername> -group-name
BUILTIN\Administrators -member-names <domain username>
```

Installation of dg File NetApp on Both Nodes

Install the dg file migration adapter on both systems: the CC node and the FPolicy node. After installation of the dg analysis agent, the following service is added with startup type automatic:

Also check for the other related services such as the dg file PNM and the dg file LNM. These services are mandatory for NetApp migration operations.

After installation of the dg file migration adapter, you will notice the following new processes:

Configuring the FPolicy Node

Editing the Registry of the FPolicy Node

Note: Perform this step only on the FPolicy system. Changing this registry key is used to determine which system is started as the FPolicy node.

1. Open the registry editor to modify the following DWORD value by using the following command:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\dataglobal\EMA\FPolicy-Node]
```

2. The default value after installation is "0." Set the value to "1."

Modifying the Address Setting on the FPolicy Node

1. Use `regedit` to modify the following string value:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\dataglobal\EMA\LNM\Address]
```

   The default value data after installation is 127.0.0.1.

2. Replace this default value data with the IPv4 address of the system used as the CC node (for example, 192.168.123.45).

Note: On the FPolicy system, you're now using the LNM of the CC node, which makes sure that both nodes have synchronized configurations.

Enabling Firewall Rules on the FPolicy Node

On the FPolicy node, navigate to Administrative Tools > Windows Firewall with Advanced Security. Depending on the value of the NetApp console option `cifs.netbios_over_tcp.enable`, enable the following inbound rules:

- If `cifs.netbios_over_tcp.enable on`, enable the inbound rule `File and Printer Sharing (NB-Session-In).`
- If `cifs.netbios_over_tcp.enable off`, enable the inbound rule `File and Printer Sharing (SMB-In).`

Stopping the LNM Service on the FPolicy Node

On the FPolicy node, locate the EMA LNM service, set the startup type to manual, and stop the service.

Note: The FPolicy node does not need a running LNM service.

Configuring a Local Security Policy on the FPolicy Node

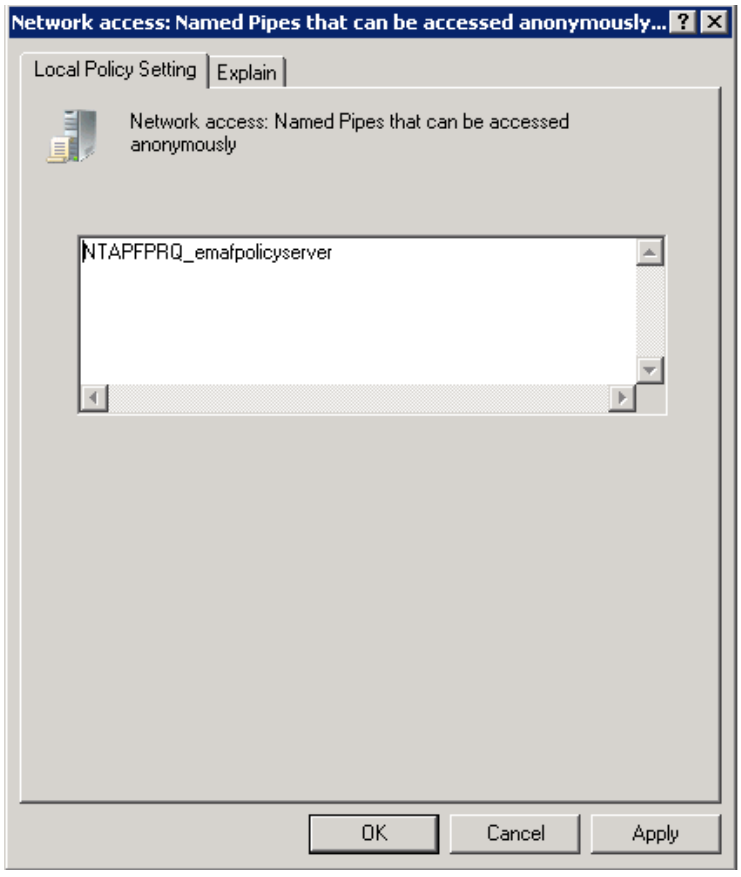
The FPolicy server uses an RPC call to register a file policy on the NetApp storage system and to enable the features of this file policy. This RPC call carries the name of the SMB request named pipe. The FPolicy serve installed on the FPolicy node requires a named network access session (pipe). This security setting determines which communication sessions have attributes and permissions that allow anonymous network access.

Note: The request pipe name must adhere to the following naming convention: `NTAPFPRQ_<application_name>`.

The registration on the NetApp storage system is denied if the SMB pipe name does not follow the naming convention.

1. On the FPolicy node, open Local Security Policy and navigate to Local Policies > Security Options > Network Access > Named Pipes, which can be accessed anonymously.
2. Enter `NTAPFPRQ_emafpolicyserver` for the named pipe.

Figure 3) Local security policy on FPolicy node.



4.3 Typical Configuration of dg File NetApp in the dg ControlCenter

This chapter describes the steps required to configure the dg analysis agent to operate in remote mode. The chapter also contains the steps for the configuration of primary and secondary storage together with at least one second storage category for dg file netapp.

Configuring the Installed dg Analysis Agent for Remote Access

Requirements

- A dg file migration adapter must be installed.
- A dg analysis agent must be locally installed on the CC node system.
- A user account with sufficient credentials to access the primary storage resources should be included in the NetApp administrator group.

Steps

1. Open Services and right-click the dg analysis agent service. Select Properties.
2. Select the tab Log On.
3. Select This account to supply the credentials required to access the NetApp storage system or vFiler® instance remotely.
4. Click Apply Changes.

Important
Stop/restart the dg analysis agent service to take over the changes.

Adding dg Analysis Agent in the dg ControlCenter

Requirements

- A dg ControlCenter must be installed and started.
- Valid license modules such as dg analyze and dg file netapp need to be installed.
- A dg file migration adapter must be installed, and all services should be started.

Steps

1. Navigate to Administration > Agents > Analysis Agent.
2. Select Add to discover and to activate already installed agents.
3. Enter the host name or IP address of the server where the dg analysis agent has been locally installed.
4. Enter the port number for the dg analysis agent (default = 9047).
5. Select and move the available license modules.
6. Select and move the license module dg analyze.
7. Select and move the license module dg file netapp to migrate files.
8. Click Save.

When the dg analysis agent has been configured for remote access, a blue icon called Remote commands appears, as follows: 

The dg analysis agent has to be configured in remote mode to support dg file NetApp HSM commands. The following icon for HSM commands has to appear to support dg file migration adapter operations: 

Note: Make sure you have first installed the dg file migration adapter.

Creating a Remote Analysis Agent Group in the dg ControlCenter

The dg analysis agent provides the analysis ability for the managed volumes of the NetApp storage system. Multiple agents can be combined to form a remote analysis agent group. The dg ControlCenter

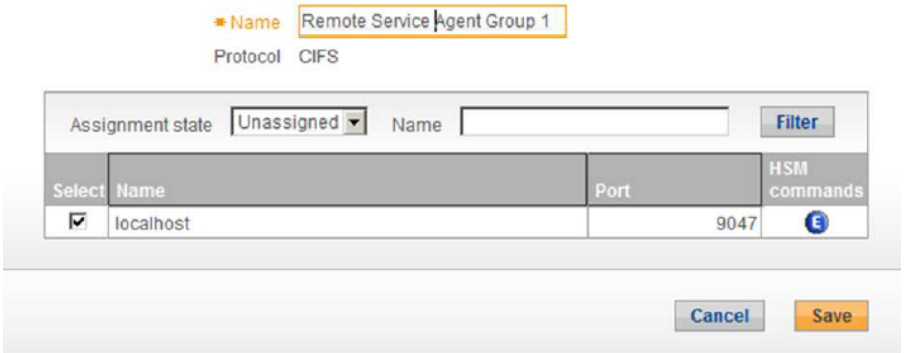
provides the required interface to create and to configure a remote analysis agent group. A remote agent group provides several benefits in addition to increased analyzing speed (for example, load balancing and failover).

Requirements

- A dg file migration adapter must be installed.
- A dg analysis agent must be installed.

Steps

1. Navigate to Administration > Agents > Remote Analysis Agent Groups.
2. Click Add.
3. The list of activated agents is displayed. Enter a name for the remote analysis agent group to be created.
4. Select the server where the dg file migration adapter is installed and running (indicated by the icon HSM for commands).
5. Save the configuration.



Adding a Remote Server in the dg ControlCenter

The NetApp storage system has to be configured as a remote server in the dg ControlCenter because the Data ONTAP operating system does not support local agent installation. The remote server requires an existing remote agent group.

Requirements

- IP address of the NetApp storage system
- CIFS licensed on the NetApp storage system
- An existing and enabled FPolicy instance

Steps

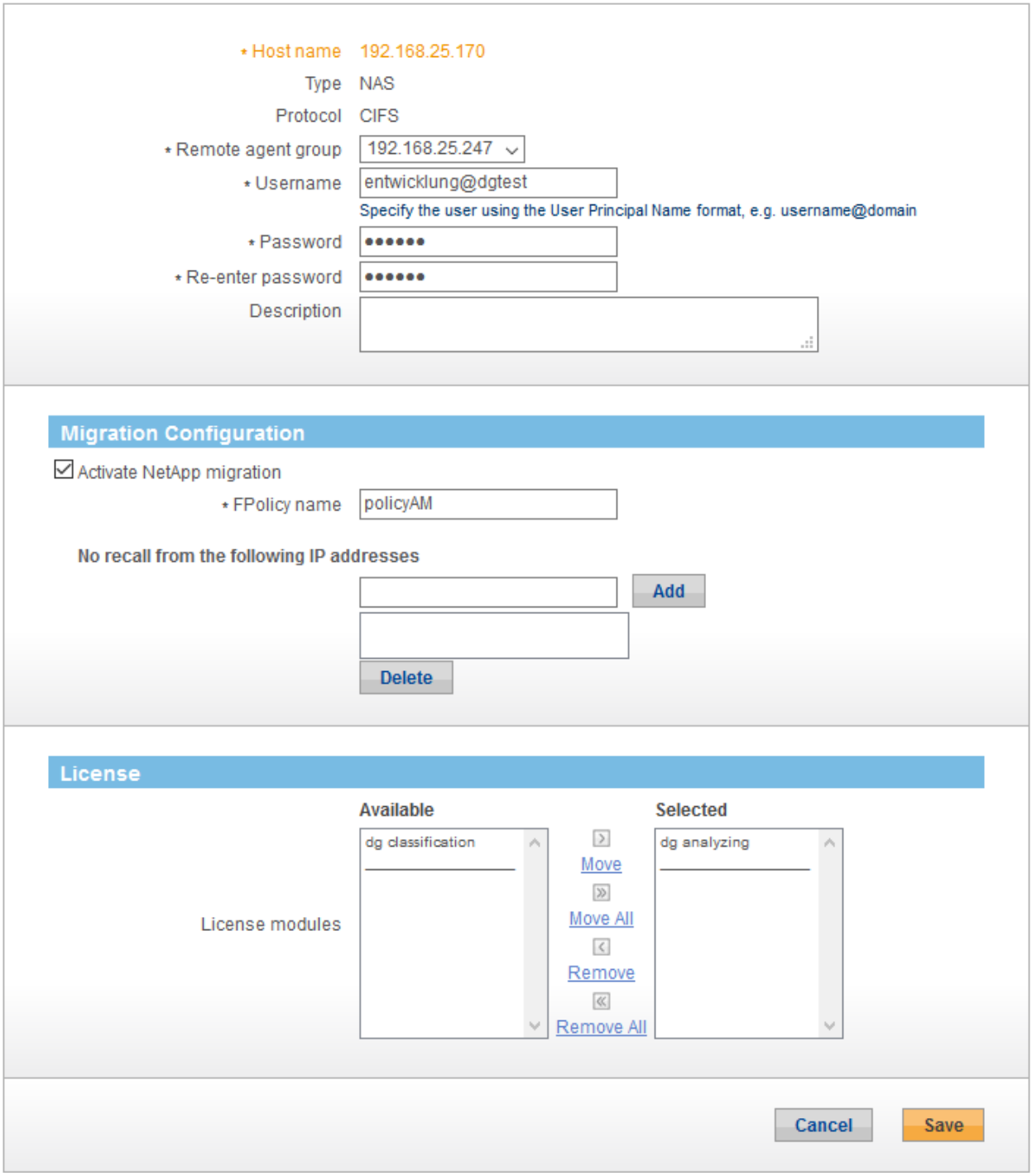
1. Navigate to Resource Manager > Remote Servers.
2. Click Add.
3. Enter host name or IP address of the remote server, which is the NetApp storage system.
   - Remote server type is NAS.
   - Protocol is always CIFS.
4. From the drop-down list, select the remote agent group that is to be used to access the NetApp storage system.

5. Enter the user credentials for accessing the remote server, which in this case is the NetApp storage system.

Note: The user credentials need to be accepted by the Data ONTAP® API for the FPolicy instance, and the user has to be included in the NetApp administrator group. This user needs to access the shares on the NetApp primary storage with read/write permissions and needs permission to log on as a service. This user is usually an existing domain backup user.

6. Optional: enter a description:
   - Migration configuration
   - Activate NetApp migration
   - Enter the FPolicy name
7. Mandatory: add the IP addresses for no recall from the following IP addresses for the following systems:
   - CC node system
   - Backup server
   - Antivirus server
8. Assign the desired license modules to the remote agent.
9. Save the configuration.

Figure 4) Adding a remote server in the dg ControlCenter.



5 FPolicy Configuration in Clustered Data ONTAP

This section provides instructions for configuring FPolicy for NetApp file servers running clustered Data ONTAP. The FPolicy structure includes the following components:

- **Event.** Defines which operations and protocol types FPolicy audits.

- **External engine.** Defines the endpoint to which the FPolicy instance sends notification information.
- **Policy.** Provides the aggregation of events policy, external engine, and scope.
- **Scope.** Defines the volumes, shares, export policies, and file extensions to which the FPolicy policy applies. The scope also allows you to include and exclude all relevant filters.

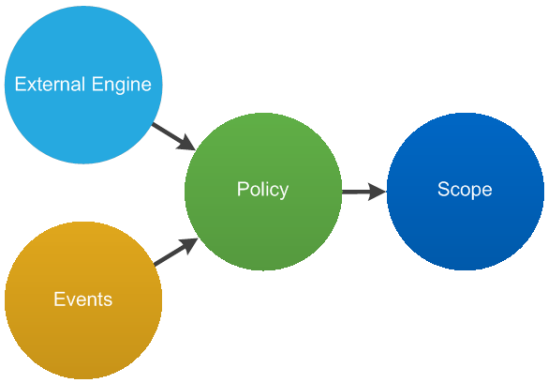
Configuration Requirements
The shares must reside on the volume monitored for CIFS events.

5.1 FPolicy Configuration Workflow

Figure 5 shows the workflow for creating a resident policy. Before you create a policy, you should create an external engine and an event. After you define a policy, you must associate a scope with it.

After the scope is created, the policy must be enabled with a sequence number. The sequence number helps to define the policy's priority in a multipolicy environment, with 1 having the highest priority and 10 having the lowest.

Figure 5) FPolicy configuration workflow.



5.2 Creating an FPolicy Event

To enable the IDU suite to connect to a NetApp file server running clustered Data ONTAP, you must configure an FPolicy instance for it. To do so, you must be a user with the vsadmin role and have a user name that is associated with the NetApp ONTAPI application. The order in which you create an FPolicy event is important.

To create an FPolicy event by using TCP, complete the following steps:

1. Connect to NetApp Data ONTAP management.
2. To create and verify an FPolicy event object, run the following command:

```
fpolicy policy event create -vserver <Vserver Name>
-event-name <event name> -volume-operation false -protocol cifs -file-operations read,write -
filters offline-bit,first-read,first-write
```

The FPolicy event options are described in Table 1.

Table 1) FPolicy event options.

Option	Description
-vserver	The name of the Vserver on which you want to create an FPolicy external engine.

Option	Description
-event-name	The name of the FPolicy event that you want to create.
-file-operations	The file operations for the FPolicy event. Values are create, create_dir, delete, delete_dir, read, close, write, rename, rename_dir
-protocol	The name of the protocol for which the event is created. Value: cif
-filters	Specifies the filters used with a given file operation for the protocol specified in the -protocol parameter. For example: first-read, close-with-modification

To view the event object, run the following command:

```
fpolicy policy event show <event name> –instance
```

5.3 Create FPolicy External Engine

To create and verify an FPolicy external engine, run the following command:

```
fpolicy policy external-engine create -vserver
<Vserver Name> -engine-name <engine name> -primary
servers <IP address of FPolicy server> -port 9876 -extern-engine-type synchronous -ssl-option no-
auth
```

The FPolicy external engine options are described in Table 2.

Table 2) FPolicy external engine options.

Option	Description
-vserver	The name of the Vserver on which you want to create an FPolicy external engine
-engine-name	The name of the external engine that you want to create
-primary-servers	The IP addresses for the primary FPolicy servers
-port	The port number for the FPolicy service
-extern-engine-type	The type of external engine. Only *asynchronous* is supported.
-ssl-option	The SSL option for external communication with the FPolicy server. Possible values include the following: • server-auth: Provides probe authentication • mutual-auth: Provides both probe and NetApp authentication

To view the external engines you created, run the following command:

```
FPolicy policy external-engine show
```

5.4 Create FPolicy Policy

Run the following command to create FPolicy policy:

```
fpolicy policy create -vserver <Vserver Name> -
policy-name <policy name> -events <event name>
-engine <engine name> -is-mandatory true -allow-privileged-access yes -privileged-user-name <user
name>
```

The FPolicy policy options are described in Table 3.

Table 3) FPolicy policy options.

Option	Description
-vserver	The name of the Vserver on which you want to create an FPolicy external engine
-policy-name	The name of the FPolicy policy that you want to create
-events	A list of events to monitor for the FPolicy policy
-engine	The name of the external engine that you want to create
-is-mandatory	Determines whether the FPolicy object is mandatory

To view the policy you created, run `fpolicy policy show`.

5.5 Create FPolicy Scope

To create and verify an FPolicy scope, run the following command:

```
fpolicy policy scope create -vserver <Vserver Name>
-policy-name <policy name> -volumes-to-include *
```

The FPolicy scope options are described in Table 4.

Table 4) FPolicy scope options.

Option	Description
`-vserver`	The name of the Vserver on which you want to create an FPolicy external engine
-policy-name	The name of the FPolicy policy that you want to create
-volumes-to-include	A comma-separated list of volumes to be monitored
-export-policies-to-include	A comma-separated list of export policies for monitoring file access. Wildcards are supported.

To view the FPolicy scope, run the following command:

```
fpolicy policy scope show -vserver <Vserver Name> - policy-name <Policy name>
```

5.6 Enable FPolicy Policy

On startup the probe service enables the new FPolicy policy. The following command is for reference only.

```
fpolicy policy enable -vserver <Vserver Name> -policy-name <FPolicy name> -sequence-number <seq no>
```

6 Security Login Configuration for FPolicy Server

The dg file needs to communicate to the FPolicy instance using Data ONTAP APIs and requires the domain user (designated in section 4.3) to have vsadmin privileges for application ONTAPI and authmode as domain.

Run the following command on the clustered Data ONTAP console:

```
security login create -username <domain username> -vserver <Vserver Name> -application ontapi -
authmethod domain -role vsadmin
```

6.1 Prerequisites

The domain and user name are case sensitive and must be identical to those defined in the management console. Use the following command to list and verify the settings:

```
security login show -vserver <Vserver Name>
```

7 Clustered Data ONTAP Best Practices

NetApp recommends the following FPolicy best practices for server hardware, operating systems, patches, and so on.

7.1 Policy Configuration

Configuration of an FPolicy External Engine for the SVM

Providing additional security comes with a performance cost. Enabling SSL communication has a performance effect on CIFS.

Configuration of an FPolicy Event for the SVM

Monitoring file operations has an effect on the overall user experience. In fact, filtering unwanted file operations on the storage side improves the overall user experience. NetApp recommends monitoring the minimum types of file operations and enabling the maximum number of filters without breaking the use case. The CIFS home directory environment has a high percentage of `getattr`, `read`, `write`, `open`, and `close` operations. NetApp recommends using filters for these operations. For recommended filters, refer to the section “Creating an FPolicy Event.”

Configuration of an FPolicy Scope for SVM

Restrain the scope of the policies to relevant storage objects, such as shares, volumes, and exports, rather than enabling them across the entire SVM. NetApp recommends checking directory extensions. If parameter `is-file-extension-check-on-directories-enabled` is set to true, directory objects are subjected to the same extension checks as regular files.

Network Configuration

Network connectivity between the FPolicy server and the controller should be of low latency. NetApp recommends separating FPolicy traffic from client traffic by using a private network.

Note: For a scenario in which the LIF for FPolicy traffic is configured on a different port than the LIF for client traffic, the FPolicy LIF might fail over to other node because of a port failure. This failover would make the FPolicy server unreachable from the node and cause the FPolicy notifications for file operations on the node to fail. Make sure that the FPolicy server can be reached through at least one LIF on the node to process FPolicy requests for the file operations performed on that node.

7.2 Hardware Configuration

The FPolicy server can be on either a physical server or a virtual server. If the FPolicy server is in a virtual environment, be sure to allocate dedicated resources (CPU, network, and memory) to the virtual server. Virtual FPolicy servers must run on enterprise-grade hypervisors and host servers. For environments with high-file activity loads, NetApp strongly recommends a physical server as the FPolicy server.

7.3 Multiple Policy Configuration

The FPolicy policy for native blocking has the highest priority, irrespective of the sequence number. Decision-altering policies have a higher priority than others. Policy priority depends on the use cases. NetApp recommends working with partners to determine the appropriate priority.

7.4 Managing FPolicy Workflow and Dependency on Other Technologies

NetApp recommends disabling an FPolicy policy before making any configuration changes. For example, if you want to add or modify an IP address in the external engine configured for the enabled policy, then first disable the policy.

If you configure FPolicy to monitor NetApp FlexCache® volumes, NetApp recommends that you not configure FPolicy to monitor `read` and `getattr` file operations. Monitoring these operations in Data ONTAP requires the retrieval of inode-to-path (I2P) data. Because I2P data cannot be retrieved from FlexCache volumes, it must be retrieved from the origin volume. Therefore, monitoring these operations eliminates the performance benefits that FlexCache can provide.

When both FPolicy and an off-box antivirus (AV) solution are deployed, the AV solution receives notifications first. FPolicy processing starts only after AV scanning is complete. Because a slow AV scanner can affect overall performance, AV solutions must be sized properly.

Add all shares that you want to monitor or audit into the share-include list during scope definition. Turn off monitoring on the file server if you do not want monitor it.

7.5 Sizing Considerations

FPolicy performs inline monitoring of CIFS operations, sends notifications to the external server, and waits for a response, depending on the mode of external engine communication (synchronous or asynchronous). This process affects the performance of CIFS access and CPU resources. To mitigate any issues, NetApp recommends assessing and sizing the environment before enabling FPolicy. Performance is affected by the number of users, by workload characteristics such as operations per user and the data size, and by network latency.

8 dg File Best Practices

In addition to the FPolicy best practices, the following recommendations are required for the dg file:

- Install, license, and configure dg ControlCenter as described in the technical documentation.
- Activate the dg file agent.
- Select and create primary storage as described in dg file administration guide.
- Create secondary storage for archiving purposes of selected files.
- Create a policy, including a file stream filter with migration task. Select files based on type and last access/last modification date.
- The target for the migration task is the secondary storage for archiving purposes.
- Create a job on primary storage.
- dg file recommends executing jobs manually or on a scheduled basis (productive environment).
- Review the dg file agent logs for potential errors.

9 Troubleshooting

9.1 Problem: FPolicy Server Is Disconnected

Potential solution: If the server is not connected, try to connect it by using the `engine-connect` command. Look for the reason why the FPolicy server disconnected using the command `show-engine -instance` and take appropriate action.

For example:

```
1. fpolicy show-engine
2. fpolicy engine-connect –node <node name> -vserver <vserver name> -policy <policy name> -server
<ip address of FPolicy server>
3. fpolicy show-engine -instance
```

9.2 Problem: FPolicy Server Does Not Connect

Precheck: Verify that the SVM has a data LIF through which the FPolicy server is reachable.

For example:

```
network interface show
                                                                                    2.
network ping -lif <vserver_data_lif> -destination <fpolicy server IP address> -lif- owner
<vserver_name>.
```

Potential Cause 1

There are issues with routing.

Potential solution: Check the routing table entries by using the command `routing-groups route show` to check whether a route is available for the SVM. If no route is available, run the `routing-groups route create` command to add a route.

For example:

```
routing-groups route create -vserver <vserver name> -routing-group d10.X.0.0/18 -destination
0.0.0.0/0 -gateway 10.X.X.X
```

Potential Cause 2

The FPolicy server does not listen on the port specified.

Potential solution: In the FPolicy user space log file (fpolicy.log), look for the log entry `connect failed. errno = 61 Establish TCP connection returned error`. Then, check the port on which the FPolicy server listens and modify the external engine configuration to use the same port.

For example:

```
fpolicy policy external-engine modify -vserver <vserver name> -engine-name <engine name> -port
<tcp port no>
```

Potential Cause 3

The security options for the external engine are not the same as for the FPolicy server.

Potential solution: Run the command `fpolicy policy external-engine show –instance`. If the FPolicy server uses SSL, then the field `SSL Option for External Communication` is either `mutual-auth` or `server-auth`.

Also, check the fields FQDN or Custom Common Name, Serial Number of Certificate, and Certificate Authority to verify that the certificates are properly configured.

To correct this problem, modify `ssl-auth` to `no-auth` if the FPolicy server is not using SSL. Otherwise, use `mutual-auth/server-auth`, depending upon the level of security needed.

For example:

```
fpolicy policy external-engine modify -vserver <vserver name> -engine-name <engine name> -
primary-servers <ip address> -port <tcp port no> -ssl-option no-auth
```

Potential Cause 4

The LIF dedicated for the FPolicy traffic has failed over to a different node.

Potential solution: Make sure that the FPolicy server can be reached through at least one LIF for that SVM on the node to process FPolicy requests for the file operations performed on that node.

For example:

```
network interface show
fpolicy show-engine
```

9.3 Problem: External Engine Is Not Native for the Policy

Potential solution: Run the `fpolicy policy show` command to check whether the `Engine` field is set to `Native`. Then create an external engine for the FPolicy server and attach it to the policy.

For example:

```
fpolicy policy external-engine create
fpolicy policy modify
```

9.4 Problem: Notifications Are Not Received for the File Operations on Volume, Share, or Export

Potential Cause

The FPolicy policy scope is not set properly.

Potential solution: Run the `fpolicy policy scope show` command to check whether the scope contains the `vol/share` on which the `ops` are performed. Then create or modify the scope for the policy to add the necessary volume, share, or export.

For example:

```
fpolicy policy scope create/modify
```

10 Performance Monitoring

FPolicy is a notification-based system. Notifications are sent to an external server for processing and for generating a response back to Data ONTAP. This round-trip process adds additional latency to client access.

Monitoring the performance counters on FPolicy server and Data ONTAP allows you to identify bottlenecks in the solution and to tune the parameters necessary for an optimal solution. For example, an increase in FPolicy latency has a cascading effect on CIFS latency. Therefore, you should monitor both workload (CIFS) and FPolicy latency. Also, you can use quality-of-service policies in Data ONTAP to set up a workload for each volume or SVM that is enabled for FPolicy.

NetApp recommends running the `statistics show –object workload` command to display workload statistics. In addition, monitor the average, read, and write latencies; the total number of operations; and the read and write counters. Use the Data ONTAP FPolicy counters mentioned in Table 5 to monitor the performance of FPolicy subsystems.

Note: You must be in diagnostic mode to collect statistics related to FPolicy.

10.1 Collect and Display FPolicy Counters

To collect FPolicy counters, run the following commands:

```
statistics start -object fpolicy -instance <instace name> -sample-id <id>
statistics start -object fpolicy_policy -instance <instace name> -sample-id <id>
```

To display FPolicy counters, run the following commands:

```
statistics show -object fpolicy –instance <instance_name> -sample-id <id>
statistics show -object fpolicy_server –instance <instance_name> -sample-id <id>
```

10.2 Counter Monitoring

Table 5 and Table 6 contain lists of FPolicy counters that can be monitored.

Table 5) List of FPolicy counters.

Counters	Description
max_request_latency	Maximum screen requests latency
outstanding_requests	Total number of screen requests in process
request_latency_hist	Histogram of latency for screen requests
requests_dispatched_rate	Number of screen requests dispatched per second
requests_received_rate	Number of screen requests received per second

Table 6) List of fpolicy_server counters.

Counters	Description
max_request_latency	Maximum latency for a screen request
outstanding_requests	Total number of screen requests waiting for response
request_latency	Average latency for screen request
request_latency_hist	Histogram of latency for screen requests
request_sent_rate	Number of screen requests sent to FPolicy server per second
response_received_rate	Number of screen responses received from FPolicy server per second

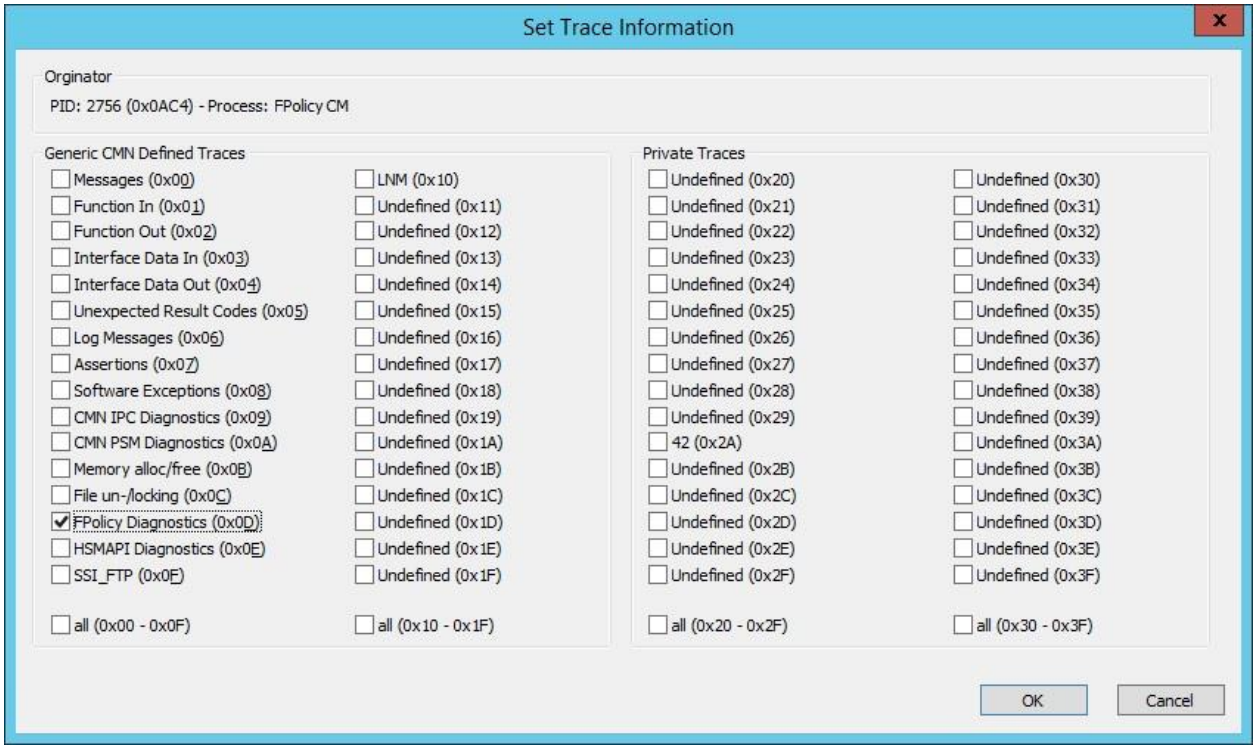
10.3 dg File Monitoring

Each action performed by the dg file FPolicy server can be viewed in the installation folder \Log\EMA.log –. Any errors that occurred during the process are also found there.

Perform the following steps to obtain detailed analysis and diagnostics of the dg file FPolicy server:

1. Open Program Files (x86)\Common Files\dataglobal\CMN\bin\CMNTrcCtrl.exe.
2. Double-click FPolicyCM.exe.

3. Select FPolicy Diagnostics.
4. Click OK.



5. Open a command prompt and type `emacli trc-display`.
6. Press Enter.

References

This report references the following documents and resources:

- dg Installation Guide
  http://www.dataglobal.com/en/dg-world.html
- Clustered Data ONTAP 8.3 File Access Management Guide for CIFS
  https://library.netapp.com/ecm/ecm_download_file/ECMP1610207

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.