Technical Report

FPolicy Solution Guide for Clustered Data ONTAP: Veritas Data Insight

Brahmanna Chowdary Kodavali and Saurabh Singh, NetApp
Himanshu Ashwani, Veritas Data Insight
May 2019 | TR-4473

NetApp®

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Introduction

The NetApp® FPolicy® component is a file-access-notification system that enables an administrator to monitor file access in storage configured for Network File System (NFS) and CIFS. Introduced for the scaled-out architecture in 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. The system supports all SMB versions, including SMB 1.0 (CIFS), SMB 2.0, SMB 2.1, and SMB 3.0. FPolicy also supports major NFS versions, including NFSv3 and NFSv4.0.

FPolicy natively supports a simple file-blocking use case that enables administrators to restrict end users from storing unwanted files. For example, an administrator can block the storage of audio and video files in data centers and thus save precious storage resources. This feature blocks files based only on extension; for more advanced features, partner solutions should be considered.

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

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

1.1 Audience

This document is for customers who want to implement FPolicy for clustered Data ONTAP storage systems that use the CIFS/SMB protocol.

1.2 Purpose and Scope

This document explains the FPolicy framework. It also describes the steps required to deploy a file-access auditing solution that uses the data-governance software Veritas Data Insight. The scope of the document encompasses 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 resulting from client access, and sends notifications to external FPolicy servers. Communication between the storage node and the external FPolicy servers is either synchronous or asynchronous. The use of synchronous or asynchronous communication depends on whether the FPolicy framework expects a notification response from the FPolicy server.

Synchronous notification is suitable for use cases in which Data ONTAP allows or denies client access based on the notification response from the FPolicy server. Use cases such as quotas, file screening, file-archiving recall, and replication require synchronous notification.

Asynchronous notification is suitable for use cases such as monitoring and auditing file-access activity that do not require Data ONTAP to take action based on the notification response from the FPolicy server. In these cases, Data ONTAP does not need to wait for a response from the FPolicy server.

2.1 Role of Clustered Data ONTAP Components in FPolicy Configuration

The following components play a role in FPolicy configuration:

- **Administrative SVM.** The administrative storage virtual machine (SVM, called Vserver in the Data ONTAP CLI and GUI) contains the FPolicy management framework. It maintains and manages the information about all FPolicy configurations in the cluster.
- **Data SVMs.** FPolicy configuration can be defined at the level of the cluster or the SVM. The scope defines the resources to be monitored in the context of an SVM. It 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 administrative SVM can be leveraged in all data SVMs.
- **Data LIFs.** FPolicy server connections are made through data logical interfaces (LIFs) that belong to the data SVM containing the central 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. It is responsible for establishing and maintaining connections with external FPolicy servers. As part of its connection management activities, the FPolicy framework handles many management tasks:

- Controls the flow of file notifications through the correct LIF to the FPolicy server
- Load-balances notifications to the FPolicy server if 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 during an authenticated session
- Establishes a connection with the data LIFs on all nodes participating in the SVM

For synchronous use cases, 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 permission 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 immediately removed.

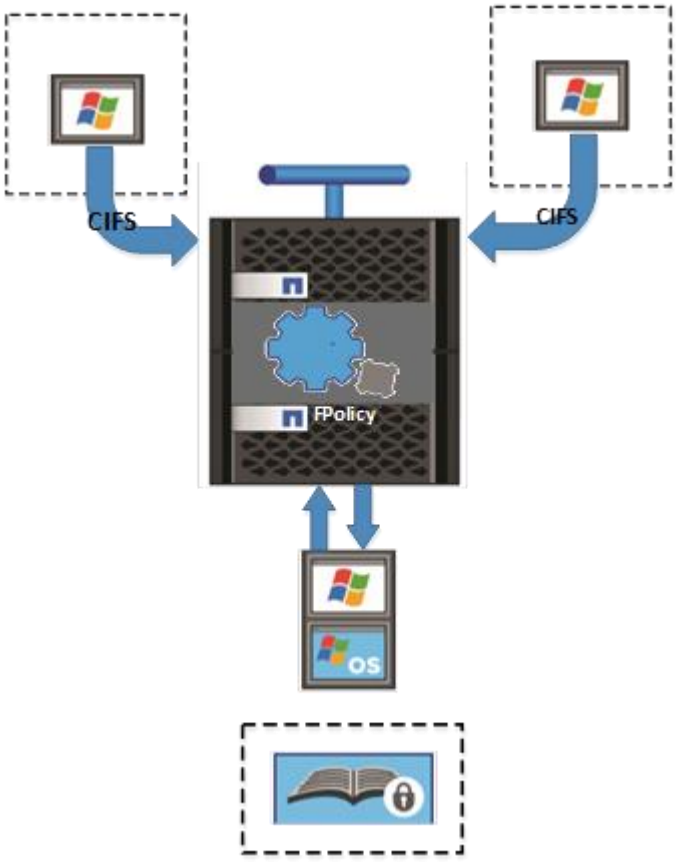
- Ability to bypass any FPolicy checks so that file access over a privileged data path does not generate an FPolicy notification

For more information about FPolicy functionality, see the 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 Veritas Data Insight. Figure 1 shows the architecture of the solution.

Figure 1) FPolicy solution architecture.



The FPolicy application software is installed on a server running Windows Server; the FPolicy framework exists in clustered Data ONTAP. The FPolicy framework connects to external FPolicy servers. It 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 node.

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 primary container 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: Veritas Data Insight

Veritas Data Insight helps organizations improve unstructured data governance to reduce costs and risk through actionable intelligence into data ownership, usage, and access controls. The reporting, analytics, and visualization capabilities in Data Insight shine a light on the data by giving organizations an understanding of what data exists, how it is being used, who owns it, and who has access to it.

In a distributed client-server architecture, a typical Data Insight deployment includes the following components:

- **Management server.** The main component of a Data Insight deployment and the host of the product's web interface.
- **Collector worker nodes.** Host machines that scan metadata from NAS file systems (CIFS or NFS), from SharePoint site collection hierarchies, and from enterprise box repositories in your environment. They also collect user access events from these sources.
- **Indexer worker nodes.** Nodes that store access events and file system metadata that is collected from the storage repositories and periodically uploaded to them. You can choose to have multiple indexers for load-balancing purposes.
- **Self-service portal nodes.** Nodes that provide an interface through which custodians of data can take remedial actions on the data classified by Veritas Data Loss Prevention software.

4 Installing and Configuring Veritas Data Insight

4.1 Veritas Data Insight Software Requirements and Installation

This document features the FPolicy application for Veritas Data Insight. For information about software requirements and installation for Veritas Data Insight, see the Veritas Data Insight installation guide, which can be downloaded from the Veritas Technical Support site.

4.2 Prerequisites for Configuring Clustered Data ONTAP File Servers

Before you can begin using Data Insight to monitor NetApp clustered Data ONTAP file servers, you must verify that the system has the following capabilities:

- The system enables you to access the Data ONTAP cluster management host from the Data Insight Collector by using the short name or the IP address.
- The Data Insight Collector host can communicate with port 80 on the Data ONTAP cluster management host. It is important to have this communication capability so that the Data ONTAP cluster can be automatically configured for use by Data Insight. If port 80 is not accessible, the administrators can configure SSL to enable secure discovery and configuration. For more information about configuring SSL, see the Veritas Data Insight administration guide.
- The Data Insight Collector host can communicate with the CIFS server hosted in the Data ONTAP cluster. This communication capability is important for file system metadata scanning.
- Service accounts are provisioned for use by Data Insight.

Table 1 describes the credentials required for configuring NetApp Data ONTAP file servers to use with Data Insight.

Table 1) Credentials for configuring NetApp Data ONTAP file servers.

Credential Type	Credential Purpose	Credential Owner
Cluster management interface	Required during storage controller configuration through the Veritas Data Insight management console Required for: • Discovering shares • Enabling FPolicy on the NetApp storage controller	Either one of these users: • A NetApp Data ONTAP cluster administration user who is a local user on the Data ONTAP cluster • A Data ONTAP cluster nonadministrator user who has specific privileges For more information, see Preparing a non-administrator local user on the clustered NetApp filer.
Scanner	Required for scanning CIFS shares from the NetApp storage controller	The user in the domain that contains the NetApp storage controller This user must belong to either the power users' group or the administrators' group on the NetApp storage controller. If the credential is not part of one of these groups, the scanner cannot get share-level access-control lists (ACLs) for shares of this storage controller. **Note:** You do not need this privilege if you do not want to get the share-level ACLs. In that case, you need only the privileges for mounting the share and scanning the file system hierarchy. You must have read permission at the share level. In addition, the folder in the share must have the following file system ACLs: • Traverse folder/execute file • List folder/read data • Read attributes • Read extended attributes • Read permissions

4.3 Adding Storage Controllers

You must add the NetApp storage controllers that you want Veritas Data Insight to monitor.

To add a storage controller, complete the following steps:

1. In the Data Insight console, select Settings > Filers to display the list of available storage controllers.
2. Click the Add New Filer drop-down menu and select the type of storage controller you want to add.
3. Select NetApp Cluster File Server.
4. On the Add New NetApp Cluster File Server page, supply the following information:
   a. Supply the NetApp cluster management host IP or host name in the Cluster Management Host field.
   b. From the list of nodes, select Data Insight Indexer.
   c. From the list of nodes, select Data Insight Collector.
   d. Supply the cluster management interface credentials as explained in Table 1.

5. Click Test Credentials. If the test is successful, select the CIFS server discovered from the Data ONTAP cluster.
6. Select Enable File System Event Monitoring and Enable FPolicy Automatically (Recommended).

   When you enable FPolicy from the Data Insight console, Data Insight automatically configures the following items on the NetApp storage virtual machines (SVMs, also known as Vservers) in the Data ONTAP cluster:

   - Creates an FPolicy with a unique name
   - Creates an FPolicy engine by specifying the server IP address and the server port
   - Creates a CIFS event object
7. Select Enable Filer Scanning.
8. Supply scanner credentials as explained in Table 1.
9. Click Test Credentials. If the test is successful, save the new storage controller.

   Note: If this is the first clustered Data ONTAP file server, you are prompted to enable the DataInsightFpolicyCmod service. This is an important step that should be completed before the storage controller is saved.
10. Navigate to Data Insight Servers > Data Insight Chosen Collector > Services.
11. Select DataInsightFpolicyCmod.
12. Specify the following details:
    - An FPolicy name of your choice
    - An FPolicy port of your choice (The NetApp storage controller sends audit events to the Data Insight Collector host on this port. Make sure the firewall rules allow communications on this port on the Data Insight collector.)
    - Data Insight Collector IP address (The host name does not work.)
13. Click Configure.
14. Return to the Add New Filers tab, which should still be open with your earlier details displayed.
15. If you have not already saved the storage controller, save it now.

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 FPolicy 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. It also allows you to include and exclude all relevant filters.

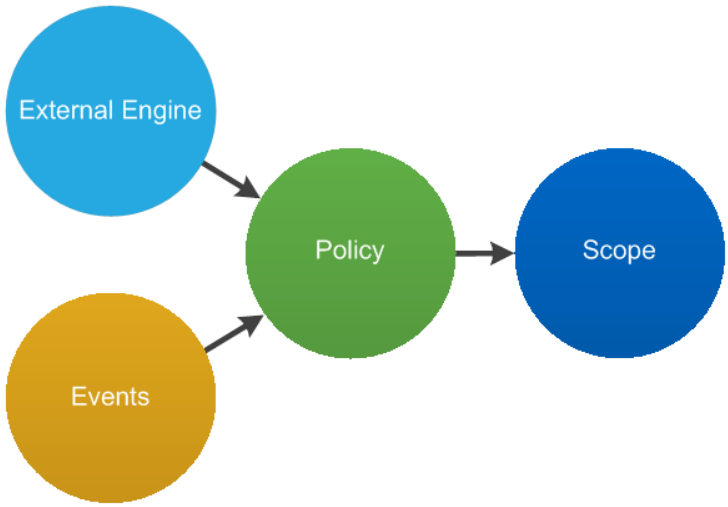
Configuration Requirements
The shares must reside on the volume monitored for CIFS events.

5.1 FPolicy Configuration Workflow

Figure 2 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 2) FPolicy configuration workflow.



Important Note

If Veritas Data Insight is configured to work with clustered Data ONTAP, it automatically configures FPolicy on the SVM.

Sections 5.2 through 5.6 explain the commands that the application uses in the background to configure the different components. These commands are included strictly for reference. Veritas Data Insight recommends choosing the Automatically Enable FPolicy option. Veritas Data Insight does not recommend making any manual configurations.

If necessary, you can use the `show` commands in each section to compare the Veritas Data Insight automatic FPolicy configuration.

Veritas Data Insight does not currently support NFS monitoring through FPolicy for clustered Data ONTAP.

5.2 Create FPolicy Event

To enable an external application to connect to a NetApp storage device running clustered Data ONTAP, you must configure an FPolicy policy for it. To be able 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 Transmission Control Protocol (TCP), complete the following steps:

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

```
fpolicy policy event create -vserver <vserver name>
-event-name <event name> -file-operations
create, create_dir, delete, delete_dir, read, close, rename,
rename_dir -protocol cifs -filters first-read, close-with-
modification
```


Table 2 lists the options for the FPolicy event.

Table 2) FPolicy event options.

Option	Description
`-vserver`	The name of the Vserver on which you want to create an FPolicy external engine
`-event-name`	The name of the FPolicy event that you want to create
`-file-operations`	The file operations for the FPolicy event Possible values: `create, create_dir, delete, delete_dir, read, close, rename, rename_dir`
`-protocol`	The name of the protocol for which the event is created Possible value: `cifs`
`-filters`	The filters used with a given file operation for the protocol specified in the `-protocol` parameter Examples: `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 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 Data Insight fpolicy server>
-port <port used by Data Insight server> -extern-engine-
type asynchronous -ssl-option no-auth
```

Table 3 lists the options for the FPolicy external engine.

Table 3) 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 **Note:** Only synchronous external engine communication is supported.
`-ssl-option`	The SSL option for external communication with the FPolicy server Possible values: • `server-auth`. Provides FPolicy server authentication. • `mutual-auth`. Provides both FPolicy server and NetApp authentication.

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

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

5.4 Create FPolicy Policy

Important Note

If FPolicy is configured manually on clustered Data ONTAP (which Veritas Data Insight does not recommend), then you must provide this FPolicy name on the Data Insight configuration console.

To create the FPolicy policy, run the following command:

```
fpolicy policy create -vserver <vserver name> -
policy-name  <policy name> -events <event name>
-engine <engine name> -is-mandatory false
```

Table 4 lists the policy options for FPolicy.

Table 4) 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 the following command:

```
fpolicy policy show
```

5.5 Create FPolicy Scope

To create the FPolicy scope, run the following command:

```
fpolicy policy scope create -vserver <vserver name>
-policy-name <policy name> -volumes-to-include "*" -
export-policies-to-include "*"
```

Table 5 lists the options for the FPolicy scope.

Table 5) 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 **Note:** Wildcards are supported.

To view the FPolicy scope you created, run the following command:

```
fpolicy policy scope show -vserver <vserver name> - policy-name <policy name>
```

5.6 Enable FPolicy Policy

Veritas Data Insight uses the following command to automatically enable the new FPolicy policy at startup:

```
fpolicy policy enable -vserver <vserver name> -policy-name <policy name> –sequence-number <seq no>
```

6 NetApp Clustered Data ONTAP Best Practices

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

6.1 Policy Configuration

Configuration of FPolicy External Engine for SVM

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

Configuration of FPolicy Events for SVM

Monitoring file operations affects the overall user experience. In fact, filtering unwanted file operations on the storage side improves the overall user experience. NetApp recommends monitoring the minimum number 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 a list of recommended filters, see section 5.2, “Create FPolicy Event.”

Configuration of FPolicy Scope for SVM

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

6.2 Network Configuration

The network connectivity between the FPolicy server and the controller should have low latency. NetApp recommends using a private network to separate FPolicy traffic from client traffic.

Note: If the LIF for FPolicy traffic is configured on a different port from that of the LIF for client traffic, a port failure might cause the FPolicy LIF to fail over to the other node. This failover would make the FPolicy server unreachable from the node and cause FPolicy notifications for the 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.

6.3 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.

6.4 Multiple-Policy Configuration

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

6.5 Managing FPolicy Workflow and Dependency on Other Technologies

NetApp recommends disabling an FPolicy policy before making any configuration changes to it. For example, if you want to add or modify an IP address in the external engine configured for the enabled policy, 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 retrieving inode-to-path (I2P) data. Because I2P data cannot be retrieved from FlexCache volumes, it must be retrieved from the original 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 might 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.

6.6 Sizing Considerations

FPolicy performs inline monitoring of CIFS operations and sends notifications to the external server. It might also wait for a response, depending on whether the mode of external engine communication is synchronous or asynchronous. This monitoring process affects the performance of CIFS access and CPU resources. To mitigate problems, 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 data size, and by network latency.

7 Veritas Data Insight Best Practices

By default, Veritas Data Insight does not to monitor `setattr` (permission change) events on clustered Data ONTAP. This default position prevents Data Insight monitoring from adversely affecting Data ONTAP CIFS performance for end users. To turn on the monitoring option, navigate to Data Insight Console > Settings > Filers and select Filer Edit.

Veritas Data Insight also monitors for CIFS latencies from storage controllers running clustered Data ONTAP. Using these latencies as a safeguard, it stops monitoring if the latencies exceed a set threshold. You can configure the thresholds by editing the configuration on the Data Insight console. Navigate to Settings > Scanning and Event Monitoring and change the values in the FPolicy Cluster Mode Safeguard Settings field.

8 Troubleshooting Common Problems

8.1 Problem: FPolicy Server Is Disconnected

Potential solution: If the server is not connected, try to connect it by running the `engine-connect` command. Run the `show-engine –instance` command, look for the message `Reason for FPolicy Server Disconnection`, and take appropriate action.

Command 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
```

8.2 Problem: FPolicy Server Does Not Connect

Precheck: Verify that the SVM has a data LIF through which the FPolicy server can be reached.

Command example:

```
1. network interface show
2. network ping -lif <vserver data lif> -destination <fpolicy server ip address> -lif- owner
<vserver name>.
```

First potential cause: There are problems with routing.

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

Command 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
```

Second potential cause: The FPolicy server is not listening 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 is listening and modify the external engine configuration to use the same port.

Command example:

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

Third potential cause: The security options for the external engine are not the same as those for the FPolicy server.

Potential solution: Run the `fpolicy policy external-engine show –instance` command. If the FPolicy server uses SSL, 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 if the FPolicy server does not use SSL, modify `ssl-auth` to `no-auth`. Otherwise, use `mutual-auth`/`server-auth`, depending on the level of security needed.

Command 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
```

Fourth potential cause: The LIF dedicated to FPolicy traffic has failed over to a different node.

Potential solution: Make sure 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.

Command example:

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

8.3 Problem: External Engine Is Not Native for Policy

Potential solution: Run the `fpolicy policy show` command to verify that the Engine field is set to `Native`. Create an external engine for the FPolicy server and attach it to the policy.

Command example:

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

8.4 Problem: Notifications Are Not Received for File Operations on Volume, Share, and Export

Potential cause: The FPolicy policy scope is not set properly.

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

Command example:

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

9 Performance Monitoring

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

Monitoring the performance counters on the FPolicy server and in Data ONTAP enables you to identify bottlenecks in the solution. It also enables you to tune the parameters as 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. In addition, 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. To monitor the performance of FPolicy subsystems, use the Data ONTAP FPolicy counters listed in Table 6 and Table 7.

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

9.1 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 <instance 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>
```

9.2 Counters to Be Monitored

Table 6 and Table 7 list FPolicy counters that can be monitored.

Table 6) 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 7) `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

Where to Find Additional Information

To learn more about the information that is described in this document, review the following documents and/or websites:

NetApp

- Clustered Data ONTAP 8.3 File Access Management Guide for CIFS
  https://library.netapp.com/ecm/ecm_download_file/ECMP1610207
- NetApp Support site
  http://support.netapp.com/

Veritas Data Insigh:

- Preparing a non-administrator local user on the clustered NetApp filer
  https://sort.symantec.com/public/documents/SDI/4.5/windows/productguides/html/sdi_admin/ch06s05.htm
- Veritas Technical Support site
  https://support.veritas.com/en_US/article.DOC7422.html

Version History

Version	Date	Document Version History
Version 1.1	May 2019	Refreshed the date on the cover page, footers, and back page. Reformatted the cover page to align with the current template.
Version 1.0	November 2015	Initial release

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.

TR-4473-0519