Technical Report

FPolicy Solution Guide for Clustered Data ONTAP: Veritas Enterprise Vault

Brahmanna Chowdary Kodavali and Saurabh Singh, NetApp
Bhushan Pandit and David Scott, Veritas
May 2019 | TR-4488

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 that is 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 that involve 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 that are required to deploy a file-archiving solution that uses Veritas Enterprise Vault File System Archiving (FSA) software. 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 have roles in the 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 that are 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) that belong to another SVM. However, FPolicy configurations that are 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 that contains the central FPolicy configuration. The data LIFs used for these connections can fail over in the same manner that data LIFs used for normal client access do.

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. This framework:

- 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 if 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 that participate 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 that are 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.

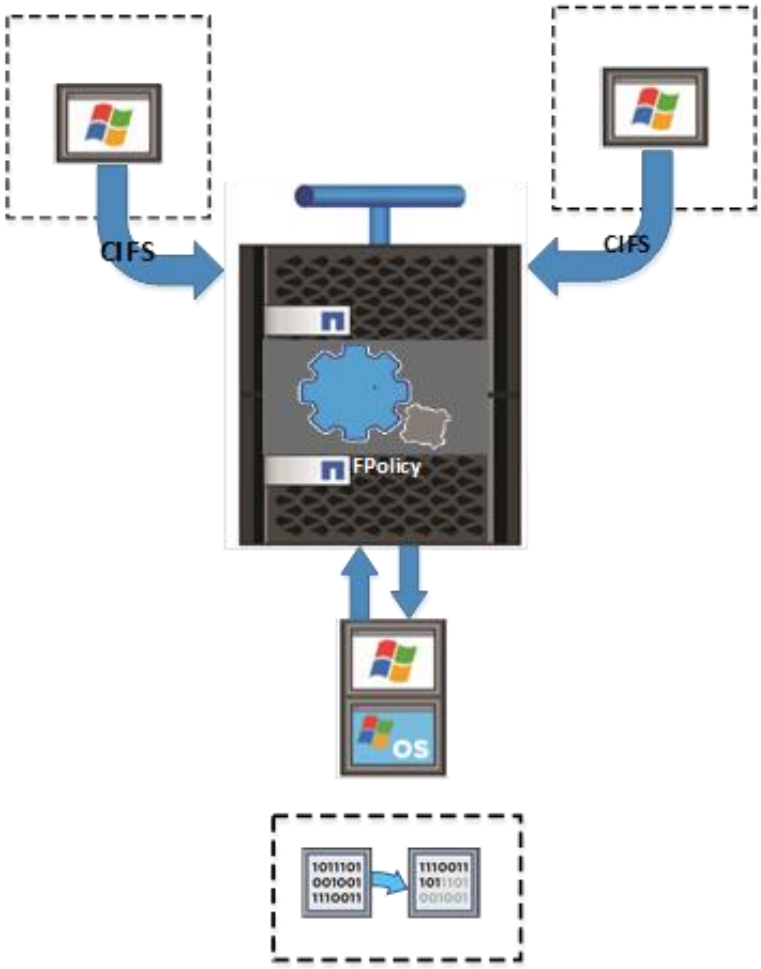
- Ability to bypass any FPolicy checks so that file access over a privileged data path does not generate an FPolicy notification

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 Enterprise Vault. Figure 1 shows the architecture of the solution.

Figure 1) FPolicy solution architecture.



The FPolicy application software is installed on a server that runs 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 if 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 that are 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 Enterprise Vault for File Archiving

Veritas Enterprise Vault is the industry leader in integrated content archiving. It provides the ability to easily store, manage, and discover unstructured information across the organization.

Enterprise Vault's FSA agent addresses storage costs and resource issues by providing an automated and integrated solution for archiving file server content. This solution can lower storage costs and manage file lifecycles while also capturing content for e-discovery and compliance purposes.

4 Installing and Configuring Veritas Enterprise Vault FSA

4.1 Veritas Enterprise Vault Hardware Requirements

Table 1 lists both minimum and recommended hardware specifications for an Enterprise Vault server.

Table 1) Hardware specifications for an Enterprise Vault server.

Item	Minimum and Recommended Specifications
Number of processor cores	Minimum: 4 Recommended: 8 **Note:** You can achieve the total number of cores through any combination of physical CPUs and their cores.
Power of CPUs	2GHz
Memory	Minimum: 8GB Recommended: 16GB
Disk space	1GB **Note:** Enterprise Vault 11.0 prevents installation on a partition with less than 1GB of free disk space.

In smaller environments, you can install all Enterprise Vault core services on the same server. In larger environments, however, you might consider deploying individual services such as storage and indexing on dedicated Enterprise Vault servers.

For more information about distributing Enterprise Vault services, see Enterprise Vault Introduction and Planning.

4.2 Veritas Enterprise Vault Software Requirements

Enterprise Vault FSA supports NetApp clustered Data ONTAP 8.2.x and 8.3.x. Future versions of clustered Data ONTAP will be officially supported after testing.

4.3 Configuring Enterprise Vault FSA for NetApp Clustered Data ONTAP File Servers

Grant Required Permission on Each SVM

Before you add a NetApp clustered Data ONTAP SVM as an FSA target, you must grant a domain user permission to register the FPolicy server on the SVM.

Important Note

Only one user account can be configured per Enterprise Vault site for all the SVMs. If you change the user account details, you must make sure that the user has NetApp ONTAPI® permissions on all the SVMs. In addition, the data LIF associated with the SVM must have both data and management access.

For more information, see section 5, “Security Login Configuration for FPolicy Server.”

Configure FPolicy Server Details

To configure the FPolicy server details, you must provide the following information:

- The credentials of the domain user account that is used to register the FPolicy server on the SVM. This user account is granted ONTAPI access permission on the SVM.
- The port number for Enterprise Vault FPolicy servers. The SVM’s FPolicy engine tries to establish a connection with the Enterprise Vault FPolicy server through the specified port.

To configure the FPolicy user account credentials, complete the following steps:

1. In the administration console, expand the Enterprise Vault site until the Targets container is visible.
2. Expand Targets.
3. Right-click the File Servers container.
4. In the shortcut menu, click Properties.
5. Click the NetApp C-Mode tab.
6. In the Account text box, enter the user account credentials in the format `DomainName\UserName`.

   Where:

   – `DomainName` is the name of the Active Directory domain of the user account.

   Note: The value that you enter in this text box is case-sensitive. When you create the login and grant ONTAPI permission for this user on the NetApp clustered Data ONTAP SVM, be sure to use the correct case.
7. Enter the password.
8. In the Port Number text box, enter the FPolicy server port number.

   Note: The port number should not be greater than 65,535.
9. Click OK.

Add NetApp Clustered Data ONTAP SVM as Archiving Target

To add a NetApp SVM as an archiving target, complete the following steps:

1. In the administration console, expand the Enterprise Vault site until the Targets container is visible.
2. Expand Targets.
3. Right-click the File Servers container.
4. In the shortcut menu, click New and then File Server to start the new file server wizard.
5. Work your way through the wizard. Do not select the option to install the FSA agent.

   Note: You must provide the fully qualified DNS name of the NetApp clustered Data ONTAP SVM. You can browse to select this server.

Important Note

A NetApp restriction prevents archiving from a NetApp clustered Data ONTAP SVM if the path to the files exceeds 512 characters.

For more information about the default values, see the following Veritas Enterprise Vault documents:

- Adding a NetApp C-Mode Vserver as an Archiving Target
- Installing and Configuring Guide
- Setting Up File System Archiving

5 Security Login Configuration for FPolicy Server

5.1 Grant Permissions on Each NetApp Server

To grant ONTAPI privileges to a domain user on the NetApp SVM, complete the following steps:

1. Log in to the NetApp cluster console as a cluster administrator.
2. Grant the required permission by running the following command:

```
security login create -vserver VSERVER –username DomainName\UserName -application ontapi -
authmethod domain
```

Where:

- `VSERVER` is the name of the NetApp SVM in the clustered Data ONTAP cluster setup.
- The value of `–username` must be specified in the format `DomainName\UserName`. `DomainName` is the domain of the CIFS server, and `UserName` indicates a domain user.

Important Note

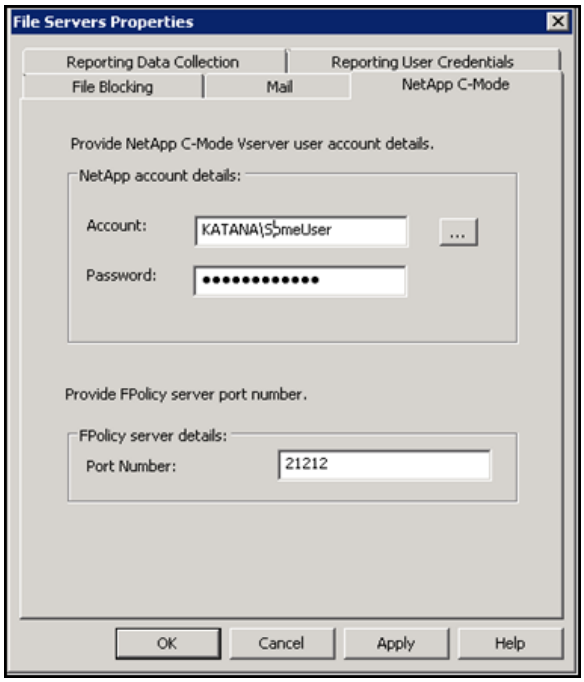
The value specified in `–username` is case sensitive. You must enter the user name with the correct case when configuring the NetApp details in the File Servers Properties dialog box. (See section 5.2, “Grant Domain User Permission to Allow Communication with NetApp Server.”) This requirement applies even though the Windows Active Directory domain treats user names as case-insensitive.

This command grants ONTAPI access to the user for any given SVM. The same account is used for running the archiving task to configure the resident FPolicy policy. The use account that you specify here is referred to as the user name for privileged access, as shown in section 6.4, “Create FPolicy Policy.”

5.2 Grant Domain User Permission to Allow Communication with NetApp Server

This information must be configured before NetApp clustered Data ONTAP is added to the site. Figure 2 shows the NetApp C-Mode tab in the File Servers Properties dialog box. This tab is where you enter the user account credentials that are required to register the FPolicy policy. In this tab, you also enter the TCP port that must be configured on the Enterprise Vault server and the file server.

Figure 2) NetApp C-Mode tab in the File Servers Properties dialog box.



6 FPolicy Configuration in Clustered Data ONTAP

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

- **Events.** Defines which operations and protocol types FPolicy audits.
- **External engine.** Defines the endpoint to which FPolicy sends notification information.
- **Policy.** Provides the aggregation of the 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.

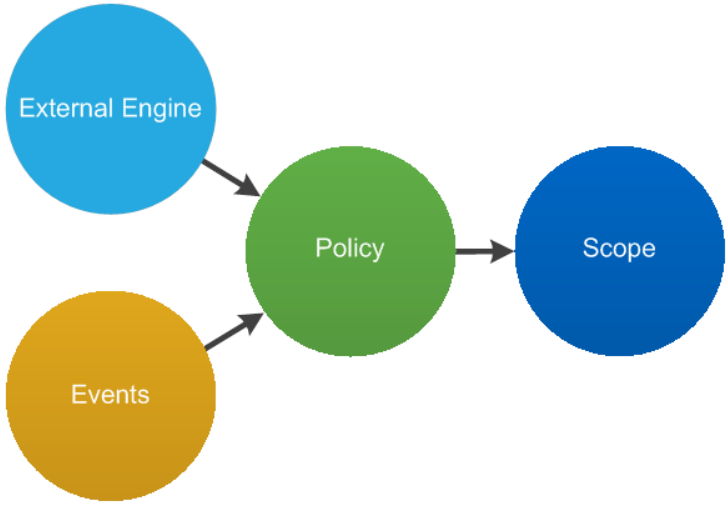
Configuration Requirements
The shares must reside on the volume that is monitored for CIFS events.

6.1 FPolicy Configuration Workflow

Figure 3 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 as the highest priority and 10 as the lowest.

Figure 3) FPolicy configuration workflow.



Important Note

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

Sections 6.2 through 6.6 explain the commands that the application uses in the background to configure the different components. These commands are included strictly for reference.

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

If FPolicy is configured manually on clustered Data ONTAP, the manual configuration might differ from the configuration that is defined in the following sections. If the manual configuration differs, the Enterprise Vault FPolicy server overwrites or recreates the configuration the next time that the service is started.

Veritas Enterprise Vault does not currently support NFS archiving through FPolicy for clustered Data ONTAP.

6.2 Create FPolicy Events

To enable the Enterprise Vault application to connect to a NetApp storage device that runs clustered Data ONTAP, you must configure an FPolicy policy for it. To configure an FPolicy policy, you must be a user with the vsadmin role, and you must 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 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 -event-name cifs -volume-operation false -protocol cifs -file-operations open, read, write,create
```


Table 2 lists the options for the FPolicy event.

Table 2) FPolicy event options.

Option	Description
`-vserver`	The name of the SVM on which you want to create an FPolicy event
`-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, open, read, close, write, 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
```

6.3 Create FPolicy External Engine

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

```
fpolicy policy external-engine create -engine-name engine -primary-servers <ip_address> -port
20248 -extern-engine-type synchronous -ssl-option server-auth
```

Table 3 lists the options for the FPolicy external engine.

Table 3) FPolicy external-engine options.

Option	Description
`-vserver`	The name of the SVM 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 that you created, run the following command:

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

6.4 Create FPolicy Policy

To create the FPolicy policy, run the following command:

```
fpolicy policy create -policy-name evplaceholder -events evplaceholdercmodeCIFSEvent -engine
evplaceholdercmodeExternalEngine -is-mandatory false -allow-privileged-access yes -privileged-
user-name <user name>
```

Table 4 lists the policy options for FPolicy.

Table 4) FPolicy policy options.

Option	Description
`-vserver`	The name of the SVM on which you want to create an FPolicy policy
`-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`	The label that determines whether the FPolicy object is mandatory

To view the policy that you created, run the following command:

```
fpolicy policy show
```

6.5 Create FPolicy Scope

To create the FPolicy scope, run the following command:

```
fpolicy policy scope create -policy-name evplaceholdercmode -volumes-to-include "*"
```

Table 5 lists the options for the FPolicy scope.

Table 5) FPolicy scope options.

Option	Description
`-vserver`	The name of the SVM on which you want to create an FPolicy scope
`-policy-name`	The name of the FPolicy policy for which you want to create the scope
`-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:** Wild cards are supported.

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

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

6.6 Enable FPolicy Policy

The application service uses the following command to enable the new FPolicy policy automatically at start-up:

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


Note: This command is shown for reference only.

7 NetApp Clustered Data ONTAP Best Practices

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

7.1 Policy Configuration

Configure FPolicy External Engine for SVM

Providing additional security comes with a performance cost. Enabling SSL communication affects CIFS performance. The performance cost is due to the security overhead that somes with SSL.

Configure 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 the use of filters for these operations. For examples of filters, see section 6.2, “Create FPolicy Event.”

Configure FPolicy Scope for SVM

Restrain the scope of the policies to include relevant storage objects, such as shares, volumes, and exports, rather than enabling them throughout the SVM. NetApp recommends that you check 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 that regular files are.

7.2 Network Configuration

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

Important 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 would 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 that are performed on that node.

7.3 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, make sure to allocate dedicated resources (CPU, network, and memory) to the virtual server.

7.4 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 do. Policy priority depends on use cases. NetApp recommends that you work with partners to determine the appropriate priority.

7.5 Managing FPolicy Workflow and Dependency on Other Technologies

NetApp recommends that you disable an FPolicy policy before you make any configuration changes to it. For example, if you want to add or modify an IP address in the external engine that is 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.

During scope definition, add all shares that you want to monitor or audit into the list of shares to include.

7.6 Sizing Considerations

FPolicy performs inline monitoring of CIFS operations and sends notifications to the external server. Depending on whether the mode of external-engine communication is synchronous or asynchronous, it might also wait for a response. This monitoring process affects the performance of CIFS access and CPU resources. To mitigate problems, NetApp recommends that you assess and size the environment before you enable FPolicy. Performance is affected by the number of users, by workload characteristics such as operations per user and data size, and by network latency.

8 Veritas Enterprise Vault File System Archiving Best Practices

For a complete list of best practices, see the Veritas document Best Practices for File System Archiving Implementations.

9 Troubleshooting Common Problems

9.1 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
```

9.2 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 that the FPolicy server can be reached through at least one LIF for that SVM on the node. The FPolicy server must be able to process FPolicy requests for the file operations performed on that node.

Command example:

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

9.3 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
```

9.4 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
```

10 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 that you run 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 that are listed in Table 6 and Table 7.

Note: You must be in diagnostic mode to collect statistics that are 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 <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>
```

10.2 Counters to Monitor

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

Table 6) FPolicy counters.

Counters	Description
`max_request_latency`	Maximum latency for screen requests
`outstanding_requests`	Total number of screen requests in process (waiting for a

Counters	Description
	response)
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 screen requests
outstanding_requests	Total number of screen requests in process (waiting for a response)
request_latency	Average latency for screen requests
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

- Adding a NetApp C-Mode Vserver as an Archiving Target
  https://www.veritas.com/support/en_US/article.000045921
- Best Practices for File System Archiving Implementations
  http://www.veritas.com/docs/000015085
- Installing and Configuring Guide
  https://origin-download.veritas.com/library/BUSINESS/DOC6634/11.0-Installing_and_Configuring.pdf
- Enterprise Vault Introduction and Planning
  https://origin-download.veritas.com/library/BUSINESS/DOC6634/11.0-Introduction_and_Planning.pdf
- Setting Up File System Archiving
  https://origin-download.veritas.com/library/BUSINESS/DOC6634/11.0-Setting_up_File_System_Archiving.pdf
- 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 date on the cover page, footers, and back page. Reformatted the cover page to align with the latest template.
Version 1.0	February 2016	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-4488-0519