Technical Report

FPolicy Solution Guide for ONTAP: STEALTHbits File Activity Monitor

Brahmanna Chowdary Kodavali, NetApp
Paul Shmakov and Robin Stefani, STEALTHbits Technologies, Inc.

May 2019 | TR-4696

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Introduction

NetApp® FPolicy™ is a file access notification framework that allows users to monitor file access over NFS and CIFS protocols. This feature was introduced in NetApp clustered Data ONTAP® 8.2, a scale-out architecture that enables a rich set of use cases working with partners. The FPolicy framework requires that all the nodes in the cluster are running Data ONTAP 8.2 or later. FPolicy supports all SMB versions such as SMB 1.0 (also known as CIFS), SMB 2.0, SMB 2.1, and SMB 3.0. It also supports major NFS versions such as NFS v3 and NFS v4.0.

The FPolicy framework natively supports a simple file-blocking use case, which enables administrators to restrict end users from storing unwanted files. For example, an administrator can block audio and video files from being stored in data centers, which saves precious storage resources. This feature blocks files based on only extension. For more advanced features, partner solutions must be considered.

The FPolicy framework enables partners to develop applications catering to a diverse set of use cases. The use cases include, but are not limited to, the following:

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

1.1 Audience

The target audience for this document is customers implementing a file access auditing solution based on FPolicy for ONTAP® using STEALTHbits File Activity Monitor for ONTAP.

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 access auditing solution using the data governance software STEALTHbits File Activity Monitor. The scope of the document includes the required deployment steps and best practices for the solution.

2 FPolicy Overview

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

Asynchronous or synchronous communication depends on whether the FPolicy framework expects a notification response from the FPolicy server:

- Asynchronous notification is suitable for use cases for which ONTAP does not act based on the notification response from the FPolicy server. Therefore, it won’t wait for the response from the FPolicy server.

  Monitoring and auditing file access activities are examples of asynchronous notification use cases.
- In contrast to asynchronous notification, synchronous notification is suitable for the use cases for which ONTAP must allow or deny the client access based on the notification response from the FPolicy server.

  Quotas, file screening, file archiving recall, replication, and so on are examples of synchronous notification use cases.

2.1 Role of ONTAP Components in an FPolicy Configuration

The administrator storage virtual machine (SVM) (cluster), data SVMs, and data LIFs associated with SVMs play a role in an FPolicy configuration.

Administrator SVM (Cluster)

A cluster contains the FPolicy management framework and maintains and manages the information about all FPolicy configurations in the cluster.

Data SVMs

FPolicy configuration can be defined at the cluster or the SVM. The scope option in the FPolicy configuration defines the resources that are monitored in the SVM context; the scope option operates on only the SVM resources. One SVM configuration cannot monitor and send notifications for the data (shares) that belongs to another SVM.

FPolicy configurations defined on the administrator SVM can be leveraged in all data SVMs.

Data LIFs

Connections to the FPolicy servers are made through data LIFs belonging to the data SVM with 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

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

- Make sure that file notification flows through the correct LIF to the FPolicy server.
- Load balances the notifications to the FPolicy server when multiple FPolicy servers are associated with a policy.
- Attempts to reestablish the connection when a connection to an FPolicy server is broken.
- Sends the notifications to FPolicy servers over an authenticated session.
- Establishes the connection with the data LIFs on all the nodes participating in the SVM.

For synchronous use cases, the FPolicy server accesses data on the SVM through a privileged data access path. To make this privileged data access path secure, ONTAP uses a combination of user credentials and the IP address of the FPolicy server configured as part of the FPolicy configuration on ONTAP. After the FPolicy server is enabled, the user credentials used in the FPolicy configuration are granted the following special privileges on the file system:

- The ability to bypass permissions checks while accessing the data. The user avoids checks on files and directory access.
- Special locking privileges. ONTAP allows the FPolicy server to read, write, or modify access to any file regardless of existing locks.

  Note: If the FPolicy server takes byte range locks on the file, it results in immediate removal of existing locks on the file.

- The ability to bypass any FPolicy checks. File access over a privileged data path does not generate FPolicy notification.

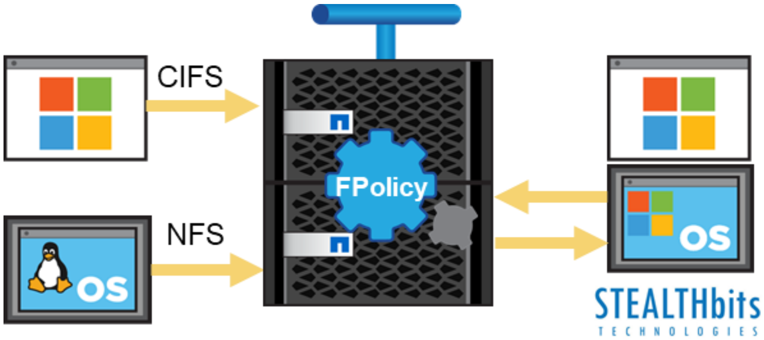
For more information about FPolicy functionality, see “File Access Management Guide for CIFS” on the NetApp Support site.

3 FPolicy Solution Architecture

The FPolicy solution consists of the following components, as shown in Figure 1:

- ONTAP FPolicy framework
- FPolicy application: STEALTHbits Activity Monitor

Figure 1) FPolicy solution architecture.



FPolicy application software runs on an external server. The FPolicy framework is part of ONTAP software. The FPolicy framework connects to external FPolicy servers and sends notifications for certain file system events to the FPolicy servers when these events occur because of client access. The external FPolicy servers process the notifications and send responses back to the node.

3.1 Components of FPolicy on Clustered Data ONTAP

The FPolicy framework on ONTAP includes the following components:

- **External engine.** This container manages external communications with the FPolicy server application, the STEALTHbits File Activity Monitor.
- **Events.** This container captures information about protocols and file operations monitored for the policy.
- **Policy.** This main container associates different constituents of the policy and provides the platform for policy management, such as policy enabling and disabling.
- **Scope.** This container defines the storage objects on which the policy acts: for example, volumes, sharers, exports, and file extensions.

3.2 FPolicy Application Software: STEALTHbits File Activity Monitor

The STEALTHbits File Activity Monitor is a simple-to-install and easy-to-use solution that which monitors and stores file activity for NetApp devices. The solution is designed to provide users with the ability to collect all or specific file activity for specific values or specific combinations of values. The clean, simple user interface enables users to view the results of queries executed against the data. The STEALTHbits Activity Monitor Console is the framework that manages the FPolicy events for the other STEALTHbits products: StealthINTERCEPT, StealthAUDIT, and StealthDEFEND. Through this solution integration, users can generate permission/access, sensitive data, and activity auditing reports; send event alerts; and assist in defending against advanced threats. The STEALTHbits File Activity Monitor ca also feed file activity data to alternative technologies such as SIEM and/or export data in formats that are easy to understand and work with.

The following components comprise the STEALTHbits File Activity Monitor:

- **STEALTHbits Activity Monitor console.** Enables users to deploy agents, configure monitoring settings, send event data to other products, and search event data.
- **STEALTHbits Activity Monitor agent.** Employs FPolicy to monitor file system activity from a Windows proxy server.

4 Installing and Configuring STEALTHbits File Activity Monitor

4.1 Software Requirements and Installation

This document features the FPolicy application for STEALTHbits File Activity Monitor. For software requirements and installation process, see the STEALTHbits Activity Monitor Installation and Console User Guide. This document can also be viewed as an interactive guide through the STEALTHbits website.

4.2 Configure STEALTHbits File Activity Monitor for NetApp

Prior to configuring the STEALTHbits File Activity Monitor for NetApp, make sure that you meet the prerequisites described in this section.

Provision User Account

The credential associated with the FPolicy used to monitor activity must be provisioned with the following CLI commands:

- `version` (read-only access)
- `volume` (read-only access)
- `vserver` (read-only access)
- `vserver fpolicy` (all access)
- `security certificate install` (all access, if FPolicy uses a TLS connection)

Configure Firewall

The following firewall settings are required for communication between the STEALTHbits Activity Monitor activity agent server and the NetApp file server:

- HTTP protocol from the agent server to NetApp: 80
- HTTPS protocol from the agent server to NetApp: 443
- From NetApp to the agent server: TCP 9999

The following firewall setting is required for communication between the activity agent server and the STEALTHbits Activity Monitor console:

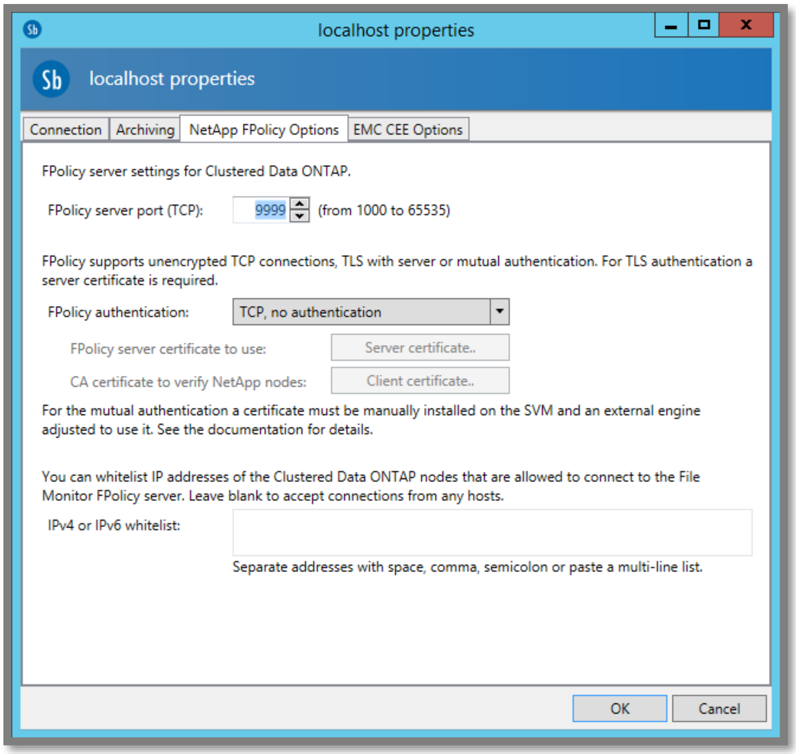
- From STEALTHbits Activity Monitor console server to the agent server: TCP 4498

Configure Agent to Monitor NetApp

After installing the STEALTHbits Activity Monitor console and deploying an activity agent to Windows server, follow the steps in this section to begin monitoring NetApp file servers.

Enable the Agent for FPolicy

1. From the Agents tab, select the agent and then click Edit to open the Agent Properties window.



localhost properties

FPolicy server settings for Clustered Data ONTAP.

FPolicy server port (TCP): 9999 (from 1000 to 65535)

FPolicy supports unencrypted TCP connections, TLS with server or mutual authentication. For TLS authentication a server certificate is required.

FPolicy authentication: TCP, no authentication

FPolicy server certificate to use: Server certificate..

CA certificate to verify NetApp nodes: Client certificate..

For the mutual authentication a certificate must be manually installed on the SVM and an external engine adjusted to use it. See the documentation for details.

You can whitelist IP addresses of the Clustered Data ONTAP nodes that are allowed to connect to the File Monitor FPolicy server. Leave blank to accept connections from any hosts.

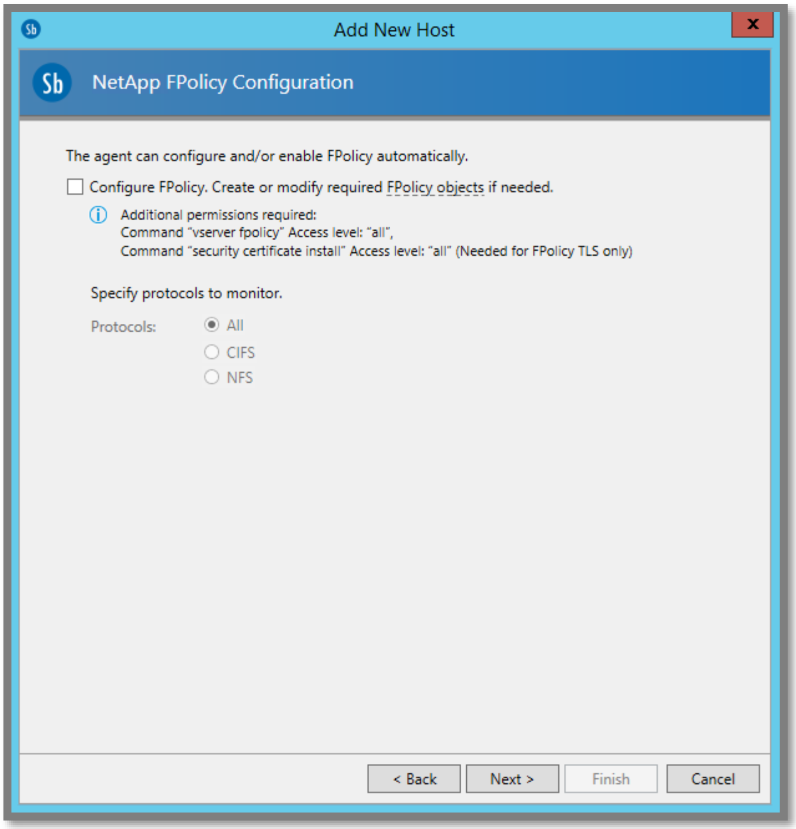
IPv4 or IPv6 whitelist:

Separate addresses with space, comma, semicolon or paste a multi-line list.

2. Select the NetApp FPolicy Options tab. Make sure that the following parameters are configured for the target NetApp file server:
   - FPolicy server port (TCP): By default, TCP 9999, for communication between the STEALTHbits Activity Monitor console and the activity agent server.
   - FPolicy authentication: Select the authentication protocol.
   - IPv4 or IPv6 whitelist: To whitelist the IP addresses of the clustered Data ONTAP nodes that can connect to the File Monitor FPolicy server, enter them in the box.

Add the Monitored Host

1. From the Monitored Hosts tab, click Add. The Add New Host window opens.
2. On the Choose Agent page, specify the agent to monitor a storage device. Click Next.
3. On the Add Hosts page, select NetApp and enter the NetApp storage system/SVM device. Click Next.
4. On the NetApp Mode and Credentials page, enter the credentials configured as the provisioned FPolicy account (case-sensitive). Click Connect to validate the connection with NetApp. Then click Next.



NetApp FPolicy Configuration

The agent can configure and/or enable FPolicy automatically.

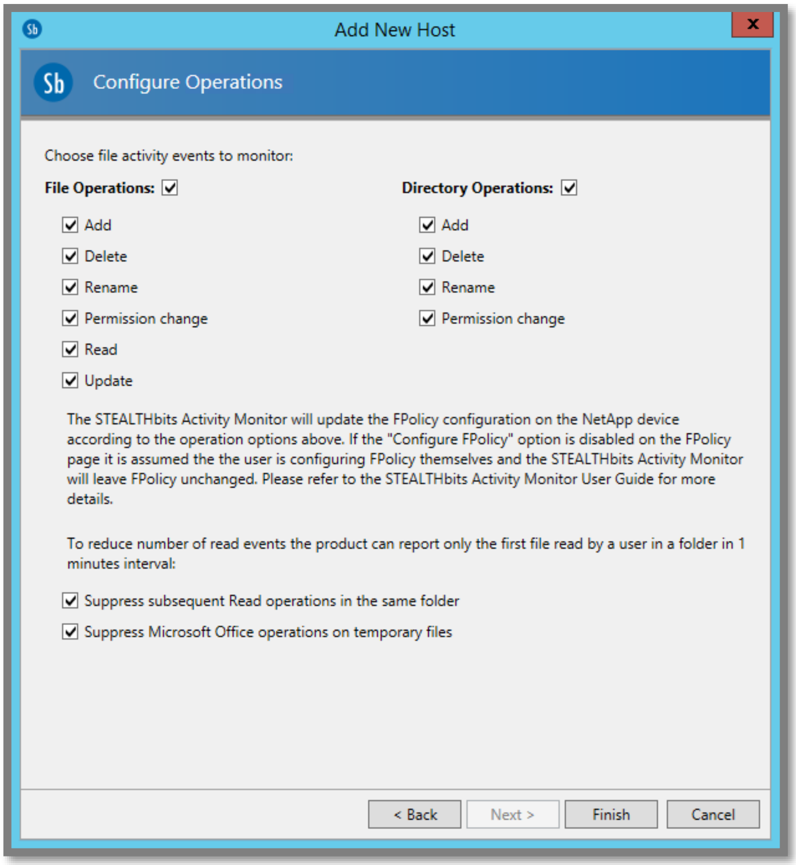
□ Configure FPolicy. Create or modify required FPolicy objects if needed.

Additional permissions required:
Command "vserver fpolicy" Access level: "all",
Command "security certificate install" Access level: "all" (Needed for FPolicy TLS only)

Specify protocols to monitor.

Protocols: ● All ○ CIFS ○ NFS

5. On the NetApp FPolicy Configuration page, select the Configure FPolicy option. Be sure to select the appropriate file protocol. Click Next.
6. On the NetApp FPolicy Enable and Connect page, select the Enable and connect FPolicy option. Provide the cluster node names either manually or using the Discover option. Click Next.
7. On the Configure Basic Options page, set the logging options as desired. Click Next.



Choose file activity events to monitor:

File Operations: ☑

- ☑ Add
- ☑ Delete
- ☑ Rename
- ☑ Permission change
- ☑ Read
- ☑ Update

Directory Operations: ☑

- ☑ Add
- ☑ Delete
- ☑ Rename
- ☑ Permission change

The STEALTHbits Activity Monitor will update the FPolicy configuration on the NetApp device according to the operation options above. If the "Configure FPolicy" option is disabled on the FPolicy page it is assumed the the user is configuring FPolicy themselves and the STEALTHbits Activity Monitor will leave FPolicy unchanged. Please refer to the STEALTHbits Activity Monitor User Guide for more details.

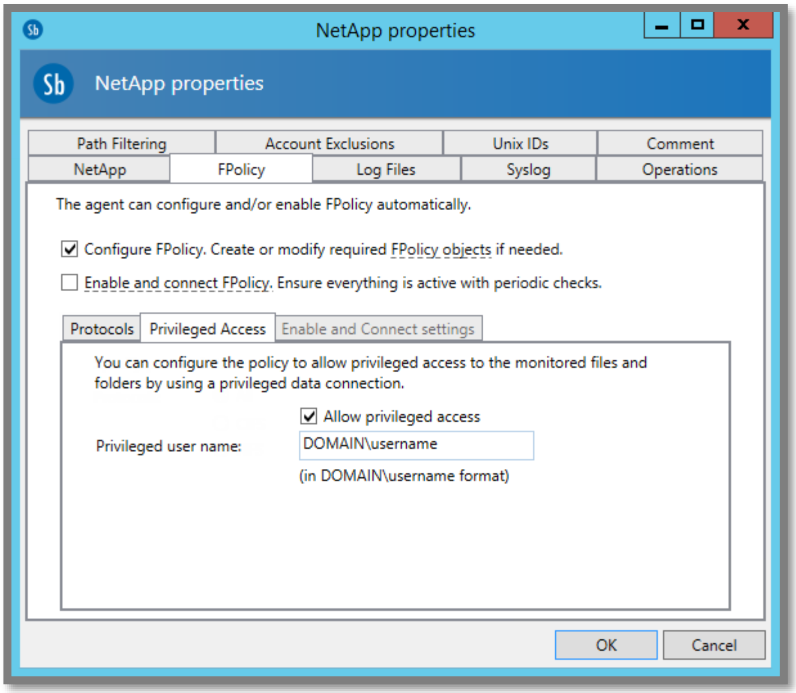
To reduce number of read events the product can report only the first file read by a user in a folder in 1 minutes interval:

- ☑ Suppress subsequent Read operations in the same folder
- ☑ Suppress Microsoft Office operations on temporary files

8. On the Configure Operations page, select the file operations and directory operations that need to be monitored. Click Finish. The Add New Host window closes.

Configure Privileged Access

1. From the Monitored Hosts tab, select the host and click Edit. The Host Properties window opens.
2. From the FPolicy tab, select the Privileged Access section at the bottom and select the All Privilege Access option for the credential associated with the FPolicy policy.



The agent can configure and/or enable FPolicy automatically.

☑ Configure FPolicy. Create or modify required FPolicy objects if needed.

□ Enable and connect FPolicy. Ensure everything is active with periodic checks.

You can configure the policy to allow privileged access to the monitored files and folders by using a privileged data connection.

☑ Allow privileged access

Privileged user name: DOMAIN\username

(in DOMAIN\username format)

See the STEALTHbits File Activity Monitor User Guide for additional NetApp configuration options. This document can also be viewed as an interactive guide through the STEALTHbits website.

5 Configuring FPolicy on ONTAP

This section provides instructions for configuring FPolicy policies for NetApp file servers operating in cluster mode.

The FPolicy structure is defined as follows:

- **Event.** Defines which operations and protocol types the FPolicy audits.
- **External engine.** Defines the endpoint to which the FPolicy sends notification information.
- **Policy.** 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. You can also include and exclude all relevant filters.

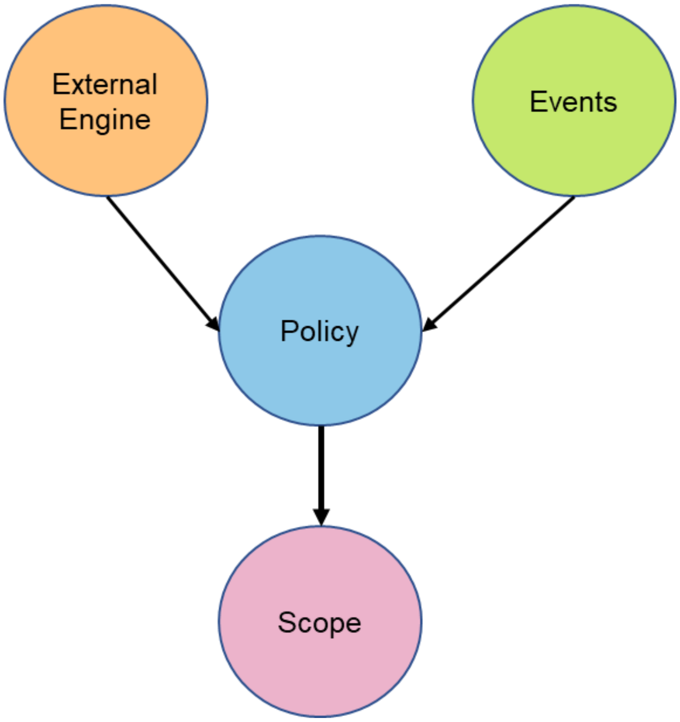
The FPolicy configuration requirements include:

- The shares must reside on the volume monitored for CIFS events.
- The export policy must be created on and applied to the volume monitored for NFS events.

5.1 FPolicy Configuration Workflow

Figure 2 shows a workflow that specifies the high-level steps that you must perform to configure and manage FPolicy.

Figure 2) FPolicy configuration workflow.



The workflow for creating a resident policy is as shown in Figure 2. You should create the external engine and event before you create a policy. After the policy is defined, you must associate it with a scope.

After the scope is created, you must enable a policy with the sequence number. The sequence number helps to define the priority of the policy in a multipolicy environment. The sequence of 1 has the highest priority, and 10 has the lowest.

5.2 Create an FPolicy Event

To connect to a NetApp file server operating in cluster mode, you must configure an FPolicy event. You must be a user with the `vsadmin` role and have a user name that is associated with the `ontapi` application. The order in which you create an FPolicy event is important.

To create an FPolicy event using TCP:

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

```
fpolicy policy event create -vserver <Vserver Name>
-event-name <event name> -file-operations
create, create_dir, delete, delete_dir, read, write, open, rename, rename_dir, setattr -protocol
cifs -filters first-read, first-write, open-with-delete-intent
```

3. To create and verify an FPolicy event object for NFS protocol, run the following command:

```
fpolicy policy event create -vserver <Vserver Name>
-event-name <event name> -file-operations
create, create_dir, delete, delete_dir, read, write, rename, rename_dir, setattr -protocol nfsv3
```

Where:

- `-vserver` is the name of the SVM (formerly known as Vserver) on which you want to create an FPolicy external engine.

- `-event-name` is the name of the FPolicy event that you want to create.

Note: The recommended name is `StealthAUDITScreeningCifs` for CIFS protocol and `StealthAUDITScreeningNfsV3` for NFS protocol.

- `-file-operations` is the file operations for the FPolicy event.

  The values are:

  - Create: `create_dir`
  - Delete: `delete_dir`
  - Read
  - Close
  - Rename: `rename_dir`
- `-protocol` is the name of the protocol for which the event is created. The protocol value is `cifs`.
- `-filters` specifies the filters used with a given file operation for the protocol specified in the `-protocol` parameter. For example, `first-read, first-write, open-with-delete-intent`.

4. To view and verify an FPolicy event object, run the following command:

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

5.3 Create an FPolicy External Engine

1. 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 <port no> -extern-engine-type asynchronous -ssl-
option no-auth
```

Where:

- `-vserver` is the name of the SVM on which you want to create an FPolicy external engine.
- `-engine-name` is the name of the external engine that you want to create; the recommended name is `StealthAUDITEngine`.
- `-primary-servers` is the IP addresses for the primary FPolicy servers.
- `-port` is the port number for the FPolicy service; the default port number is 9999.
- `-extern-engine-type` is the type of external engine; only asynchronous type is supported.
- `-ssl-option` is the SSL option for external communication with the FPolicy server.

  Possible values include:

  - `server-auth` provides STEALTHbits File Activity Monitor authentication.
  - `mutual-auth` provides both STEALTHbits File Activity Monitor and NetApp authentication.

Note: For details about SSL and TLS options, refer to the STEALTHbits File Activity Monitor User Guide.

2. To view and verify the external engine, run the following command:

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

5.4 Create an FPolicy Policy

To create an FPolicy policy, complete the following steps:

1. Run the following command:

```
fpolicy policy create -vserver <Vserver Name> -
policy-name <policy name> -events <event names>
-engine <engine name> -is-mandatory false –allow-privileged-acces yes –privileged-user-name <User
Name>
```

Where:

- -vserver is the name of the SVM on which you want to create an FPolicy external engine.
- -policy-name is the name of the FPolicy policy that you want to create; the recommended name is StealthAUDIT.
- -events is a comma-separated list of events to monitor for the FPolicy policy.
- -engine is the name of the external engine that you want to create.
- -is-mandatory determines whether the FPolicy object is mandatory.
- -allow-privileged-access enables privileged direct access from the SVM to the user specified in the -privileged-user-name parameter.
- -privileged-user-name is the name of a privileged user in DOMAIN\username format. The specified user accesses files on the SVM using a separate data channel with privileged access.

2. To view the policy, run the following command:

```
FPolicy policy show
```

5.5 Create an FPolicy Scope

To create an FPolicy scope, complete the following steps:

1. Run the following command:

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

Where:

- -vserver is the name of the SVM on which you want to create an FPolicy external engine.
- -policy-name is the name of the FPolicy policy that you want to create.
- -volumes-to-include is a comma-separated list of volumes to be monitored.
- -export-policies-to-include is a comma-separated list of export policies for monitoring file access. Wildcards are supported.

2. To view the FPolicy scope, run the following command:

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

5.6 Enable an FPolicy Policy

When the Enable and Connect FPolicy option is selected, starting the STEALTHbits Activity Monitor activity agent enables the new FPolicy policy automatically. To enable the FPolicy policy manually, run the following command:

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

6 Configuring Security Login for FPolicy Server

The STEALTHbits File Activity Monitor requires access to the ONTAP API. The permissions for operations depend on the features enabled for the monitored host.

6.1 STEALTHbits File Activity Monitor Configures FPolicy

The STEALTHbits File Activity Monitor can be configured to automatically configure FPolicy. If the Configure FPolicy option is enabled, then the credential requires the following permissions to enable FPolicy, connect to FPolicy, and collect events:

- `version` (read-only access)
- `volume` (read-only access)
- `vserver` (read-only access)
- `vserver fpolicy` (all access)
- `security certificate install` (if FPolicy uses a TLS connection, then all access)

6.2 STEALTHbits File Activity Monitor Enables/Connects to FPolicy

The STEALTHbits File Activity Monitor can be configured so that everything is actively monitoring with periodic checks on FPolicy. If the Enable and Connect FPolicy option is enabled, then the credential requires the following permissions to enable FPolicy, connect to FPolicy, and collect events:

- `version` (read-only access)
- `volume` (read-only access)
- `vserver` (read-only access)
- `vserver fpolicy disable` (all access)
- `vserver fpolicy enable` (all access)
- `vserver fpolicy engine-connect` (all access)

Note: It is necessary to create the FPolicy policy manually if this less-privileged access model is employed.

6.3 STEALTHbits File Activity Monitor Only Collects Activity

The following minimum permissions are required for the STEALTHbits File Activity Monitor to collect activity events:

- `version` (read-only access)
- `volume` (read-only access)
- `vserver` (read-only access)

Note: It is necessary to create and enable the FPolicy policy manually if this least-privileged access model is employed.

6.4 Include Permission, Access, and Sensitive Data Auditing

Through integration with other STEALTHbits products, FPolicy can also be employed to collect information about permissions, access, and sensitive data from the NetApp file servers. In additional to those employed by STEALTHbits File Activity Monitor, the following permissions are required:

- `vserver fpolicy` (read-only access)
- `security login role show-ontapi` (read-only access)

Note: To bypass NTFS on the NetApp file servers, the credential must have group membership in the Power Users group on the target host.

7 ONTAP Best Practices

NetApp recommends the FPolicy best practices described in this section for server hardware, operating systems, patches, and so on.

7.1 Policy Configuration

FPolicy External Engine for SVM

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

FPolicy Events for SVM

Monitoring file operations influences 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 recommended filters, refer to the section "Create an FPolicy Event."

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 `is-file-extension-check-on-directories-enabled` is set to true, directory objects are subjected to the same extension checks as regular files.

7.2 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: In a scenario where the LIF for FPolicy traffic is configured on a different port than the LIF for client traffic, the FPolicy LIF might fail over to another node due to a port failure. This situation can make the FPolicy server not reachable from the node and can also make the FPolicy notifications for the file operations on the node fail.

Make sure that the FPolicy server is reachable through at least one LIF on the node to process FPolicy requests for the file operations 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, irrespective of the sequence number. Decision-altering policies have a higher priority than others. Policy priority depends on use cases. To determine the appropriate priority, NetApp recommends working with partners.

7.5 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 do not configure FPolicy to monitor `read` and `getattr` file operations. Monitoring these operations in 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. A slow AV scanner could affect overall performance, so AV solutions must be sized properly.

When defining the scope, add all the shares you want to monitor or audit into the share/include list. Turn off monitoring on the file server if you do not want to monitor the shares. Disabling FPolicy on the SVM is not helpful because the STEALTHbits Activity Monitor activity agent periodically checks on the file server and automatically disables or enables FPolicy if it notices a disconnection (if the Enable and connect FPolicy option was selected).

7.6 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, workload characteristics such as operations per user, data size, and network latency.

8 STEALTHbits File Activity Monitor Best Practices

The following best practices are recommended when using the STEALTHbits File Activity Monitor with a NetApp file server:

- Restrain the FPolicy configuration to specific volumes, shares, and operations to decrease the impact on the SVM.
- Consider deploying multiple STEALTHbits Activity Monitor activity agents for load balancing and fault tolerance.
- Use the Enable and Connect FPolicy option to keep the SVM connected and consistently sending events to the STEALTHbits Activity Monitor activity agents.

9 Troubleshooting

The STEALTHbits File Activity Monitor generates a debug log file that helps to diagnose FPolicy issues. The verboseness of the file, the trace level, is controlled in the STEALTHbits Activity Monitor console. NetApp recommends increasing the trace level to Trace when troubleshooting.

The debug the log file, `FPolicyServerSvc.log`, is located on the STEALTHbits Activity Monitor activity agent server in the following installation directory: …`\STEALTHbits\StealthAUDIT\FSAC`.

9.1 Problem 1: The FPolicy Server Is Disconnected

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

Example command:

```
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 2: The FPolicy Server Does Not Connect

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

Example command:

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

Potential cause number 1: There are issues with routing.

Potential solution: Check the routing table entries by running the `routing-groups route show` command to verify whether a route is available for the SVM. If not, add a route by running the `routing-groups route create` command.

Example command:

```
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 number 2: The FPolicy server is not listening on the port specified.

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

Example command:

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

Potential cause number 3: The security options for the external engine are not the same as for the FPolicy server.

Potential solution: Run the `fpolicy policy external-engine show –instance` command. If the FPolicy server is using 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 on the level of security needed.

Example command:

```
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 number 4: The LIF dedicated for the FPolicy traffic has failed over to a different node.

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

Example command:

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

Potential cause number 5: A firewall is blocking connection to the FPolicy server.

Potential solution: Configure the firewall to allow connections to the FPolicy server.

9.3 Problem 3: The External Engine Is Not Native for the Policy

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

Example command:

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

9.4 Problem 4: Notifications Are Not Received for the 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 verify 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.

Example command:

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

10 Performance Monitoring

FPolicy is a notification-based system. Notifications are sent to an external server for processing, and a response is then sent back to the ONTAP software. This roundtrip process adds latency to client access.

Monitoring the performance counters on the FPolicy server and ONTAP helps to identify bottlenecks in the solution and allows you 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 ONTAP to set up a workload for each volume or SVM that is enabled for FPolicy.

NetApp recommends displaying workload statistics by running the `statistics show –object workload` command. NetApp also recommends that you monitor the average read and write latencies, the total number of operations, and the read and write counters. You can also use the ONTAP FPolicy counters described in this section to monitor the performance of FPolicy subsystems.

Note: To collect statistics related to FPolicy, you must be in diagnostic mode.

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 Counters to Monitor

Table 1 and Table 2 contain lists of FPolicy counters that can be monitored.

Table 1) List of FPolicy counters.

Counter	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 2) List of fpolicy_server counters.

Counter	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 Monitoring of STEALTHbits Activity Monitor Agent

The STEALTHbits Activity Monitor activity agent employs the FPolicyServerSvc service to receive and collect activity events from the SVM. Health of this service, the hosting operating system, and network and disk I/O can be monitored to identify bottlenecks on the STEALTHbits File Activity Monitor side.

Where to Find Additional Information

To learn more about the information described in this document, refer to the following website:

- ONTAP 9 Documentation Center
  http://docs.netapp.com/ontap-9/index.jsp

Version History

Version	Date	Document Version History
Version 1.1	May 2019	Refresh date on cover page, footers, and back page.
Version 1.0	June 2018	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.

Copyright Information

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

TR-4696-0519