Technical Report

FPolicy Solution Guide for Clustered Data ONTAP: PoINT Storage Manager

Brahmanna Chowdary Kodavali, Saurabh Singh, NetApp
Michael Cyrys, Detlef Golze, PoINT Software & Systems GmbH
March 2016 | TR-4497-0316

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 a HSM and archiving solution for clustered Data ONTAP storage systems.

1.2 Purpose and Scope

This document explains the FPolicy framework. It also describes the steps required to deploy an HSM and archiving solution using PoINT Storage Manager. 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.

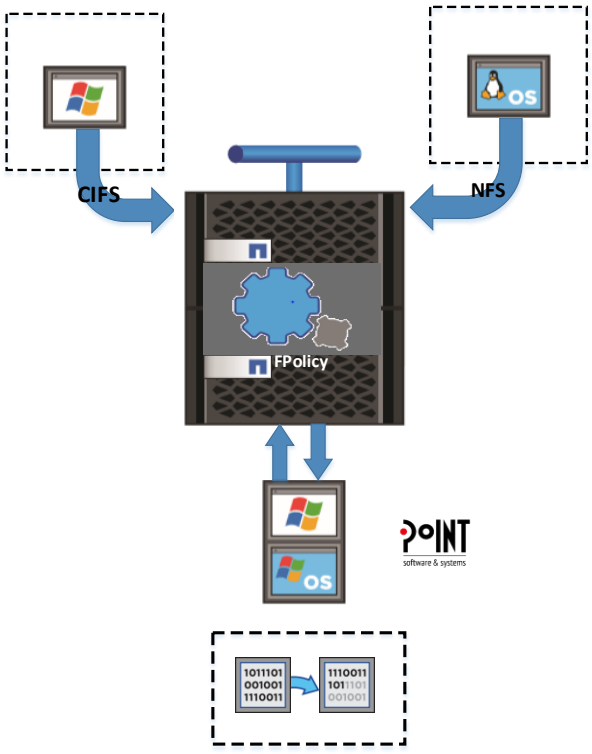
- Ability to bypass any FPolicy checks so that file access over a privileged data path does not generate an FPolicy notification

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—PoINT Storage Manager

PoINT Storage Manager is a universal storage management software solution that supports an automated tiered storage architecture, and it incorporates the capabilities and advantages of different storage technologies. The software provides a solution for automated and secure long-term archiving of data that is stored in a company's IT infrastructure. The product was also especially designed for the seamless data migration from obsolete "legacy" storage systems to new systems with state-of-the-art technologies.

4 Installing and Configuring PoINT Storage Manager

4.1 PoINT Storage Manager Requirements and Installation Procedure

PoINT Storage Manager requires the following hardware and software:

- x86-based system with at least one quad-core processor and at least 8GB RAM
- Operating systems: Windows Server 2012 and 2012 R2 (Standard, Datacenter), Windows Server 2008 R2 SP1

For additional information, see the PoINT Storage Manager manual and the `ReadMe.html` file that are included with the distribution package of PoINT Storage Manager.

To install PoINT Storage Manager, run the `setup.exe` from the root folder of the distribution package and follow the instructions. After installation, the setup wizard starts and guides you through the basic configuration. For more information about the basic configuration, see the PoINT Storage Manager manual.

Depending on the device that you configured as the archival device, you must install a corresponding connector for this device. The connectors are located in the `Connectors` folder of the distribution package. For example, to use a NetApp StorageGRID® Webscale appliance, you must install the connector from the `Webscale` subdirectory.

To install a connector, double-click the `.exe` file and follow the instructions.

You also must install the PoINT NetApp FPolicy Server for Cluster Mode module, which is provided separately from the PoINT Storage Manager distribution package. To install this module, double-click the corresponding `.exe` file and follow the instructions.

4.2 Configuration of PoINT Storage Manager for NetApp

The configuration of PoINT Storage Manager consists of the following steps:

1. Configuration of an archival device
2. Creation of a storage vault and an archival policy

Configure an Archival Device

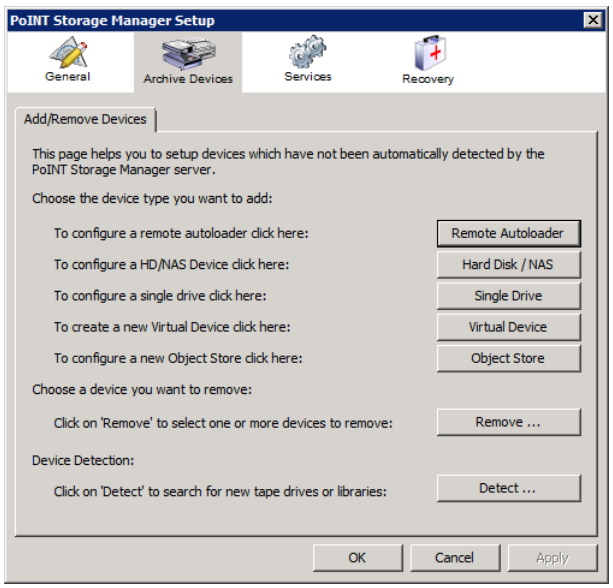
To configure an archival device, complete the following steps:

1. Select Setup PoINT Storage Manager and click Archive Devices. The Add/Remove Devices dialog box appears.
2. Select the type of archival device by clicking the corresponding button.

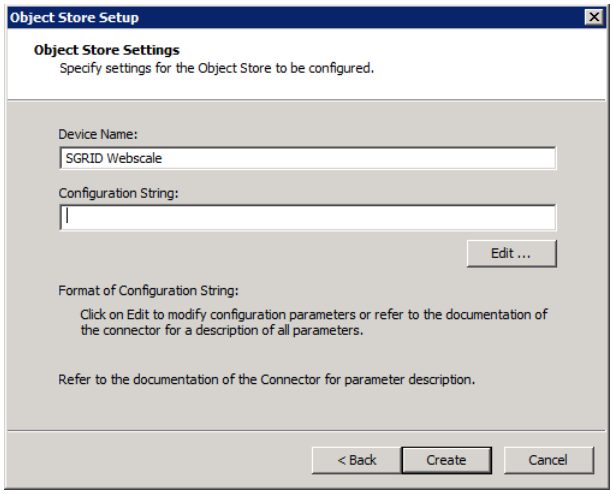
   For example, if you want to add a network share on a NetApp FAS system as archival storage, select Hard Disk/NAS in this dialog box. Select NetApp Storage in the next dialog box and then specify the network share to use.

The following steps demonstrate how to configure NetApp StorageGRID Webscale as an archival device:

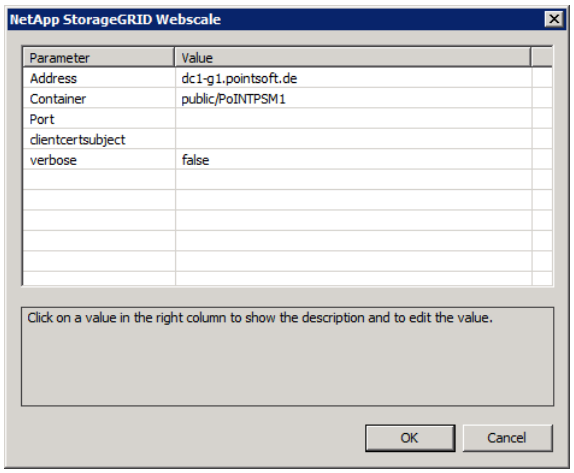
1. In PoINT Storage Manager Setup, under Archive Devices, click Object Store.
2. Select NetApp StorageGRID Webscale from the Advanced Connectors drop-down menu and click Next.



3. Enter a device name and click Edit to open the configuration string editor.



4. Enter the required information in the Value fields and click OK.

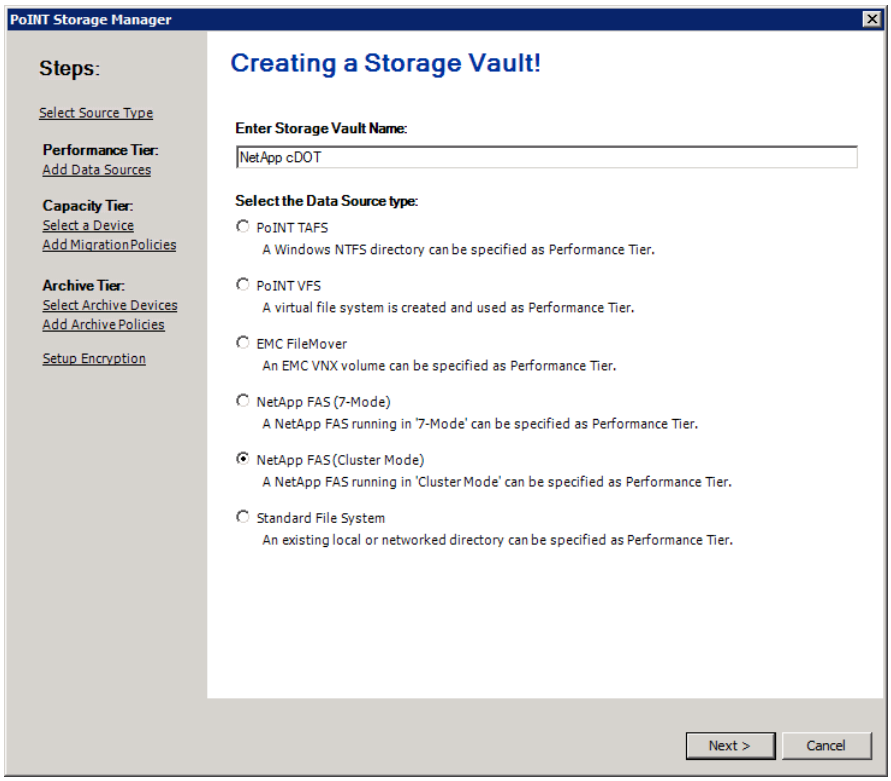


5. Click Create to complete the configuration of the archival device and then click OK to exit the PoINT Storage Manager Setup wizard.

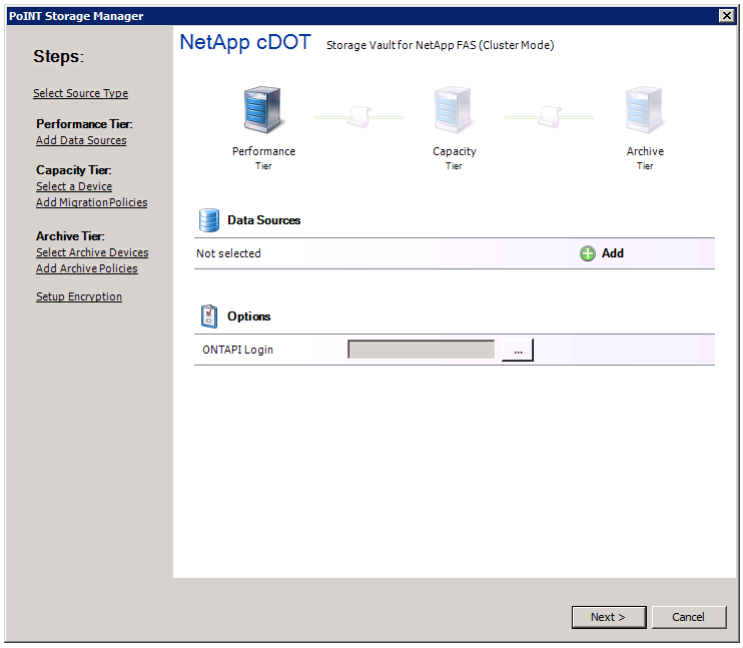
Create a Storage Vault and Archival Policy

To create a storage vault, complete the following steps:

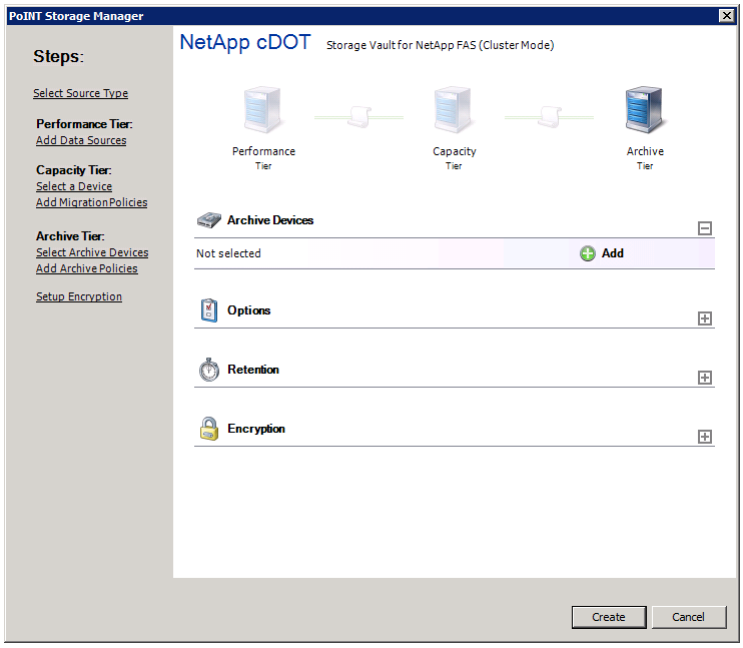
1. Click Create Storage Vault to start the Storage Vault configuration wizard.



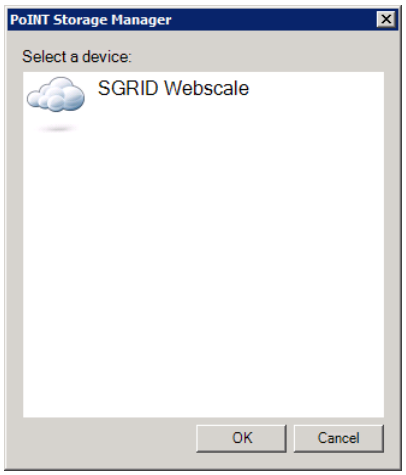
2. Enter a name for the storage vault and select NetApp FAS (Cluster Mode) and click Next.



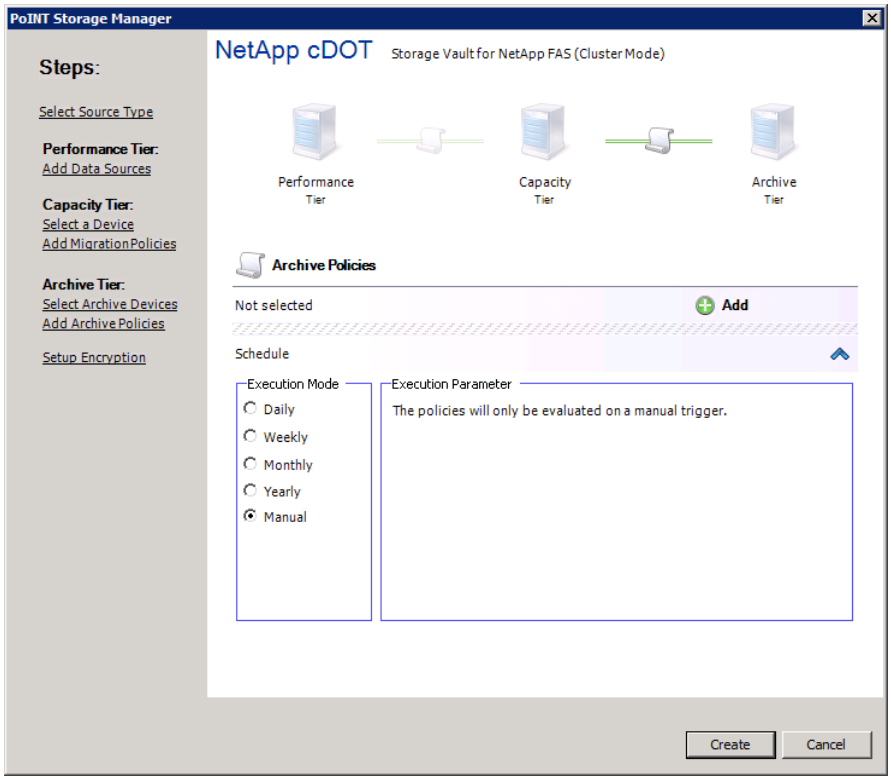
3. In the Performance Tier dialog box, under Data Sources, click Add to specify the folder that contains the data that you want to archive. You are also prompted to enter a NetApp ONTAPI® login. For information about the requirements for the ONTAPI login, see the `ReadMe.pdf` document of the PoINT NetApp FPolicy Server for Cluster Mode module.
4. Click Next twice to skip configuration of a capacity tier and to select the Archive Tier configuration dialog box.



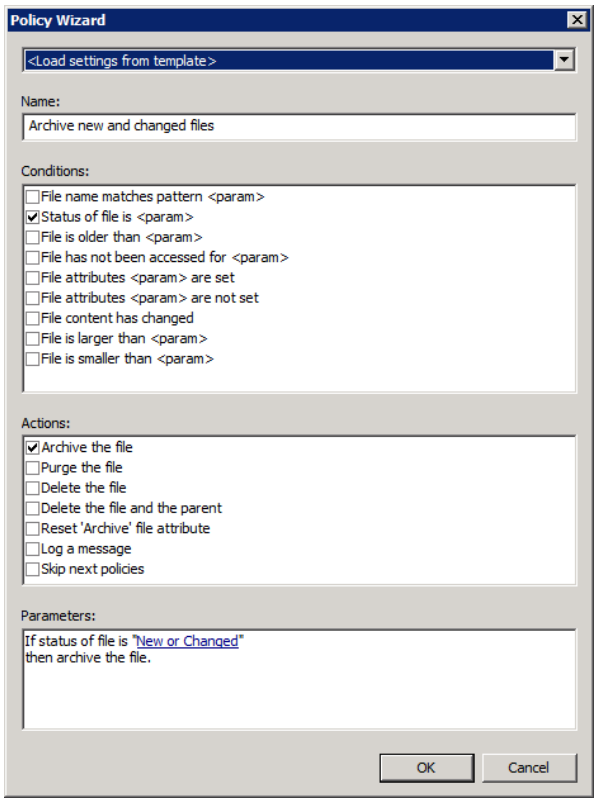
5. Under Archive Devices, click Add to add the archival device that you configured previously.



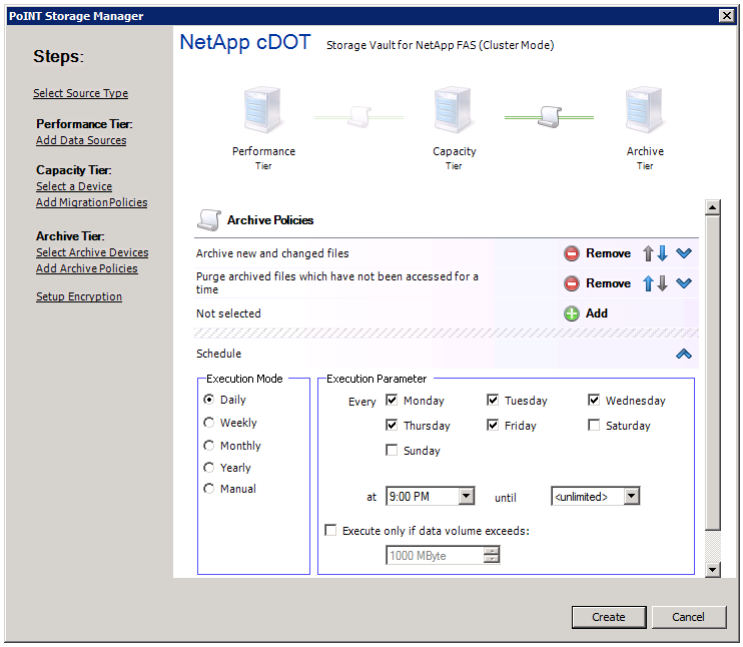
6. Click Next to configure the archival policy.
7. Under Archive Policies, click Add to open the archival polices editor.



8. From the drop-down menu, select Archive New and Changed Files and click OK. This predefined policy archives all new and changed files since the last archiving job cycle.



9. Click Add again to add the policy and then select Purge Archived Files Which Have Not Been Accessed for a Time. This predefined policy replaces archived files on the performance tier by "stubs" according to the selected conditions.
10. Set a schedule according to your requirements. You can always execute an archiving job cycle manually.



11. Click Create to complete the storage vault configuration. The archiving job cycle will start at the scheduled time or when you manually trigger the job cycle by clicking the green arrow icon.

For information about more advanced functionality of PoINT Storage Manager, see the product documentation in the installation package or on http://www.point.de.

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.

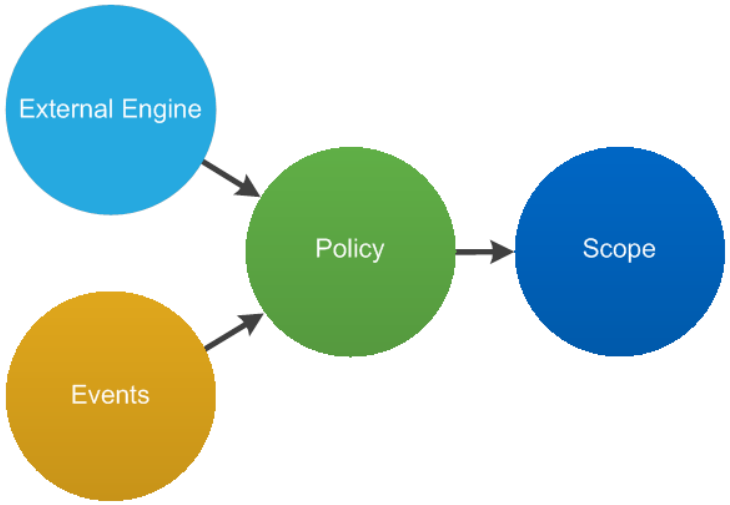
Configuration Requirements
• The shares must reside on the volume monitored for CIFS events. • The export policy must be created on and applied to the volume monitored for NFS events.

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 multi policy environment, with 1 having the highest priority and 10 having the lowest.

Figure 2) FPolicy configuration workflow.



Important Note

PoINT Storage Manager automatically performs the FPolicy configuration. You are not required to modify this configuration, and NetApp does not recommend that you modify it.

Sections 5.2 through 5.6 explain the commands and APIs that the application uses in the background to configure the different components. These commands are included in this TR for reference only. PoINT Storage Manager recommends automatic configuration of the FPolicy options by the application. It does not recommend making any manual configurations.

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

5.2 Create an FPolicy Event

To enable an external application to connect to a NetApp storage device that runs clustered Data ONTAP, you must configure an FPolicy policy for it. To do so, you must be a user with the vsadmin role and must have a user name that is associated with the NetApp ONTAPI application.

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 that monitors CIFS requests, run the following command:

```
fpolicy policy event create -vserver <vserver name> -event-name <event name> -file-operations
close, write, read, setattr -filters offline_bit -protocol cifs
```

Table 1 lists the options for the FPolicy event.

Table 1) FPolicy event options.

Option	Description
`-vserver`	The name of the Vserver on which you want to create an FPolicy
`-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, write, close, rename, rename_dir`
`-protocol`	The name of the protocol for which the event is created Possible value: `cifs, nfsv3, nfsv4`
`-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 an FPolicy External Engine

To manually 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 Fpolicy server> -port <port used by PoINT Storage Manager> -extern-engine-type synchronous –ssl-option no-auth
```

Table 2 lists the options for the FPolicy external engine.

Table 2) FPolicy external engine options.

Option	Description
`-vserver`	The name of the SVM (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 (PoINT Storage Manager uses 8632)
`-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 engine or engines that you created, run the following command:

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

5.4 Create an FPolicy Policy

To manually create an FPolicy policy, run the following command:

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

Table 3 lists the policy options for FPolicy.

Table 3) FPolicy policy options.

Option	Description
`-vserver`	The name of the SVM (Vserver) on which you want to enable FPolicy
`-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 that you created, run the following command:

```
fpolicy policy show
```

5.5 Create an FPolicy Scope

To manually 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 4 lists the options for the FPolicy scope.

Table 4) FPolicy scope options.

Option	Description
`-vserver`	The name of the SVM (Vserver) on which you want to enable FPolicy
`-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 that you created, run the following command:

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

5.6 Enable the FPolicy Policy

Run the following command to manually enable the new FPolicy policy:

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

6 Security Login Configuration for FPolicy Server

During configuration of a Storage Vault in PoINT Storage Manager you will be prompted for the ONTAPI login credentials, which will be used by the PoINT NetApp FPolicy Server to connect to the SVM. This login should be created on the SVM by using the NetApp command shell or NetApp OnCommand® System Manager. It is not necessary to create a related Windows or domain account.

Command example:

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

The login credentials through ONTAPI should be assigned the vsadmin role with its associated password. If there is any restriction in providing vsadmin role to the user, a new role can be created which provides at least the following permissions:

- `version: readonly`
- `volume: readonly`
- `vserver: readonly`
- `vserver fpolicy: all`

Note: Note that all Storage Vaults on a SVM must use the same login credentials.

7 Clustered Data ONTAP Best Practices

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

7.1 Policy Configuration

Configuration of an FPolicy External Engine for the SVM

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

Configuration of FPolicy Events for the SVM

Monitoring file operations has an effect on the overall user experience. In fact, filtering unwanted file operations on the storage side improves the overall user experience. NetApp recommends monitoring the minimum 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 recommended filters, see the section “Create an FPolicy Event.”

Configuration of an FPolicy Scope for the SVM

You should confine 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`, then directory objects are subjected to the same extension checks as regular files.

7.2 Network Configuration

Network connectivity between the NetApp 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 in which the LIF for FPolicy traffic is configured on a different port from the LIF for client traffic, a port failure might cause the FPolicy LIF to fail over to another node. This action makes the FPolicy server unreachable from the node, and 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 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. 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 that you disable an FPolicy policy before you make any configuration changes. For example, if you want to add or modify an IP address in the external engine that is 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 Data ONTAP requires the retrieval of inode-to-path (I2P) data. Because I2P data cannot be retrieved from FlexCache volumes, it must be retrieved from the origin volume. Therefore, monitoring these operations eliminates the performance benefits that FlexCache can provide.

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

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 and the data size; and network latency.

8 PoINT Storage Manager Best Practices

8.1 Changing the FPolicy Configuration

In certain instances, it might be necessary to change the configuration of the FPolicy policies. For example, if the IP address of the computer that runs the FPolicy server has changed or if another local port number should be used by the FPolicy server. When activating a storage vault, the PoINT NetApp FPolicy server verifies the FPolicy configuration and eventually reports that the configuration must be updated.

It does not automatically change the configuration because that change requires deactivating the policy; therefore, the storage system might return the wrong data for purged files. Consequently, the administrator must first make sure that no clients access the storage system and then must manually disable or delete the FPolicy policies that PoINT Storage Manager created. When reactivating the storage vault, the PoINT NetApp FPolicy server automatically creates the new FPolicy policies.

The names of the policies that were created by the PoINT NetApp FPolicy server are logged to the log file for the PoINT storage agent.

8.2 Volume Junction Paths

The PoINT NetApp FPolicy server detects and handles the changes of volume mount points (junction paths). If it detects that a volume has been moved or that a new volume has been mounted, it automatically adjusts the FPolicy scope. However, NetApp recommends that you prevent all file system access and that you deactivate all storage vaults before you change the volume mount points. Also, when you move a volume to outside the scope of a storage vault, you must make sure that the volume does not contain purged files. Access to these files is not possible after you move the volume to outside the scope of the storage vault.

8.3 NetApp Snapshot Copies

The PoINT NetApp FPolicy server supports access to purged files (stubs) in NetApp Snapshot® copies as long as that file version exists in the archive tier.

During job cycles, PoINT Storage Manager ignores hidden directories with the name `~snapshot`, because these directories contain read-only copies of older file versions, which cannot be archived.

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 that is 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 the security options 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` or `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 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 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 5 and Table 6.

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

10.1 Collect and Display FPolicy Counters

To collect FPolicy counters, run the following commands:

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

Table 5 and Table 6 list FPolicy counters that can be monitored.

Table 5) FPolicy counters.

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

Table 6) 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

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.