Technical Report

FPolicy solution guide for ONTAP: SPHEREboard

Brahmanna Chowdary Kodavali, NetApp
Douglas Yochim and Douglas Bayne, SPHERE Technology Solutions

December 2021 | TR-4916

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Introduction

NetApp® FPolicy® is a file access notification framework that allows an administrator to monitor file access over NFS or CIFS protocols. This feature was introduced in NetApp clustered Data ONTAP® 8.2. The FPolicy framework requires that all the nodes in the cluster run Data ONTAP 8.2 and 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.

FPolicy support for FlexGroup was added in ONTAP 9.4. FPolicy is transparent to the type of volume (FlexGroup or FlexVol®). The configuration parameters with volume option refer to both FlexGroup and FlexVol volumes.

FlexGroup volumes can be included or excluded in the FPolicy policy scope by using the volumes-toinclude/-volumes-to-exclude option.

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 to save storage resources. This feature blocks files based only on extension. For more advanced features, you can consider partner solutions.

This system enables partners to develop applications that cater to a diverse set of use cases, including:

- File screening
- File-access reporting
- User and directory quotas
- Hardware security module and archiving solutions
- File replication
- Data governance

Audience

The target audience for this document is individuals who would want to implement an FPolicy-based file access auditing solution for storage systems running ONTAP software.

Purpose and scope

The purpose of this document is to provide an understanding of FPolicy and describe the steps needed to deploy a file-access auditing solution by using the data governance software SPHEREboard. The scope of the document encompasses the deployment steps and best practices for this solution.

FPolicy overview

The ONTAP framework creates and maintains the FPolicy configuration, monitors file events that result from client access, and sends notifications to external FPolicy servers. Communication between the storage node and the external FPolicy servers is either synchronous or asynchronous. The use of synchronous or asynchronous communication depends on whether FPolicy expects a notification response from the FPolicy server.

Asynchronous notification is suitable for use cases when ONTAP does not need to take any action based on the notification response from the FPolicy server. This notification can be used for monitoring and auditing file-access activity.

Synchronous notification is suitable for use cases when ONTAP must allow or deny client access depending on the notification response from the FPolicy server. Quota, file screening, file archiving recall, replication, and so on require synchronous notification.

Role of ONTAP components in FPolicy configuration

The following components play a role in FPolicy configuration:

- **Administrative storage virtual machine (administrative SVM, called Vserver in ONTAP CLI and GUI).** The administrative SVM 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 at the SVM. The scope defines the resources to be monitored within the context of an SVM and operates only on SVM resources. One SVM configuration cannot monitor and send notifications for the data (shares) belonging to another SVM. However, FPolicy configurations defined on the administrative SVM can be leveraged in all data SVMs.
- **Data logical interfaces (data LIFs)**. Connections to the FPolicy servers are made through data 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.

How FPolicy works with external FPolicy servers

FPolicy runs on every node in the cluster and is responsible for establishing and maintaining connections with external FPolicy servers. As a part of connection management, FPolicy controls the:

- Flow of file notifications through the correct LIF to the FPolicy server
- Load balancing of notifications to the FPolicy server when multiple FPolicy servers are associated with a policy
- Reestablishment of broken connections to an FPolicy server
- Sending of notifications to FPolicy servers during an authenticated session
- Establishment of a 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 privileged data access paths secure, ONTAP uses a combination of specific user credentials and the IP address of the FPolicy server set as a part of the FPolicy configuration. After FPolicy is enabled, the user credentials used in the FPolicy configuration grant the following privileges to the file system:

- Bypassing permissions checks when accessing data, enabling avoiding 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.

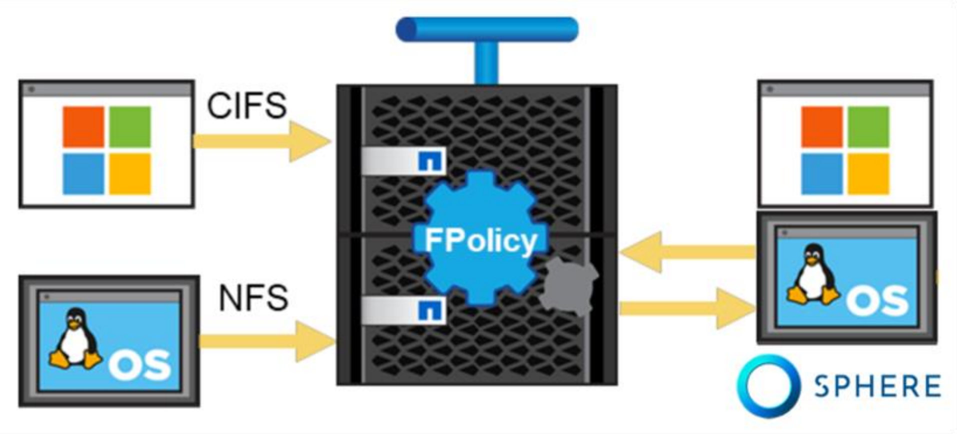
  Note: If the FPolicy server creates byte-range locks on the file, existing locks on the file are removed immediately.
- Bypassing any FPolicy checks. File access over a privileged data path does not generate FPolicy notification.

For more information about FPolicy functionality, see the Product Documentation site.

FPolicy solution architecture for SPHEREboard

Figure 1 illustrates the FPolicy solution for SPHEREboard.

Figure 1) FPolicy for SPHEREboard solution architecture.



SPHERE's FPolicy server (or Receiver) runs on Linux, and the FPolicy framework exists within ONTAP. The FPolicy framework connects to external FPolicy servers and sends notifications to the FPolicy servers for certain file-system events that occur because of client access. The external FPolicy servers process the notifications and return the responses to the node.

Components of FPolicy on ONTAP

FPolicy on ONTAP consists of the following components:

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

FPolicy Application Software—SPHEREboard

SPHEREboard provides customers with a single view to all of their access related issues. SPHEREboard consists of three components:

- SPHEREboard connectors.
- SPHEREboard UDM. SPHEREboard UDM provides customers with all the tools required to manage unstructured data including collection, reporting, ownership, entitlement reviews and remediation.
- Receivers. Messages and information sent from the FPolicy engine are sent to the receiver which is the FPolicy server. The receiver then accepts the information, processes it and stores it for analysis and retrieval.
- Workers. When it is time to remediate, the workers interact with the asset being remediated such as updating permissions on a filesystem or updating an AD group.

Installing and configuring SPHEREboard

SPHEREboard software requirements and installation

The FPolicy server application featured in this document is part of SPHEREboard. For instructions on how to set up the SPHEREboard application in your environment, see the SPHEREboard Installation Guide.

Configuring SPHEREboard for ONTAP

To configure SPHEREboard for use with ONTAP, complete the steps outlined in this section.

Prerequisites

- SPHEREboard requires the manual configuration of FPolicy in ONTAP before adding the file server to the SPHEREboard Receiver's config file. For configuration steps, see section "Configuring FPolicy on ONTAP."
- The SPHERE application sends NetApp ONTAPI calls over HTTP to the SVM through the data LIF to manage FPolicy. This requires the IP address of the SPHERE application server to be added in to the firewall policy allow list.

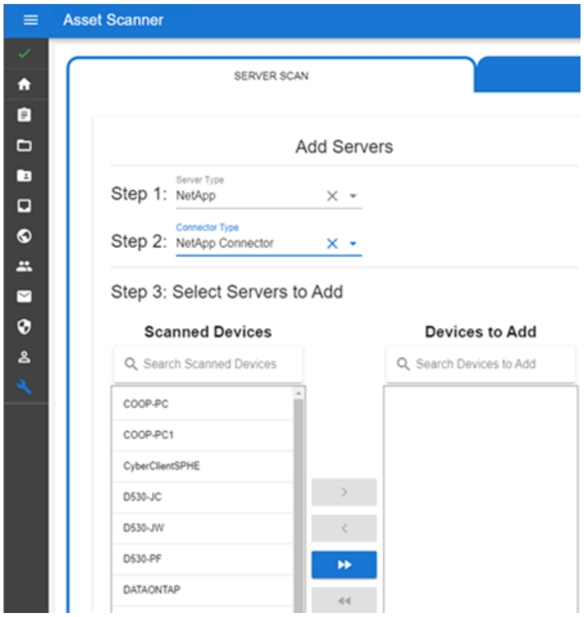
```
system services firewall policy clone -policy data -new-policy-name fp_sphere system services
firewall policy create -policy fp_sphere -service http action allow -ip-list 10.10.160.131/32
```

- When configuring the data LIF for SVM, use the `fp_sphere` firewall policy.

For details about configuring the firewall policy, see the Network Management guide for your ONTAP version on the ONTAP 9 Documentation page.

To add a NetApp storage system, complete the following steps in the SPHEREboard Asset Scanner:

1. Correctly enter the server into SPHEREboard by using the Asset Scanner as follows:
   a. Navigate to the Asset Scanner section of the SPHEREboard Admin page.



Add Servers

Step 1: Server Type: NetApp

Step 2: Connector Type: NetApp Connector

Step 3: Select Servers to Add

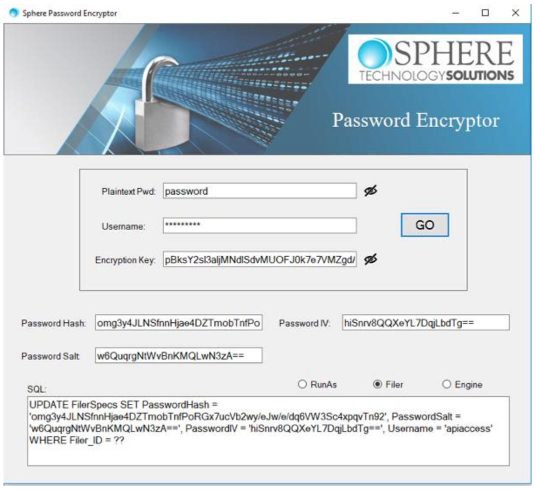
2. Under Step 1, select NetApp
3. Under Step 2, select NetApp Connector

4. Click Import Server List near the bottom of the page.
5. Enter the server name and click Save.
6. Upon setup, provide the following NetApp information:
   a. Do not select the Pass-through Authentication option.
   b. The IP address must include either `http://` or `https://` and then the address with no trailing slash.

   Note: It is not the address of the CIFS share, but the Node Management address that you can get from the NetApp sysadmin.

   c. Locate and run the `.exe` for the Sphere Password Encryptor. In a normal installation, it is located at `C:\Program Files\SPHERE\Utilities\SPHEREPasswordEncryptor`.

   Note: There are no config options in the `.config` file to set.



Plaintext Pwd: password

Username: *********

Encryption Key: pBksY2sl3aljMNdlSdvMUOFJ0k7e7VMZgd/

Password Hash: omg3y4JLNSfnnHjae4DZTmobTnfPo

Password IV: hiSnrv8QQXeYL7DqjLbdTg==

Password Salt: w6QuqrgNtWvBnKMQLwN3zA==

○ RunAs ● Filer ○ Engine

SQL:

```
UPDATE FilerSpecs SET PasswordHash =
'omg3y4JLNSfnnHjae4DZTmobTnfPoRGx7ucVb2wy/eJw/e/dq6VW3Sc4xpqvTn92', PasswordSalt =
'w6QuqrgNtWvBnKMQLwN3zA==', PasswordIV = 'hiSnrv8QQXeYL7DqjLbdTg==', Username = 'apiaccess'
WHERE Filer_ID = ??
```

   d. Provide the program with the following details, then click Go:
   – Plaintext password
   – User name

   Note: The Encryption Key field is optional. If you don’t provide a value, it will be auto-generated for you. Save a copy of this value, you will need it for the `.config` file at `C:\Program Files\SPHERE\Connectors\NetAppSPHERE.Connectors.NetAppConnector.exe.config`.

   Note: Click the eye icons to make those fields visible.

   e. Cut and paste the values generated here into the Details Modal in SPHEREboard and click Save.
7. You should now see the filer that you added in the Devices to Add list. Be sure to hit Save again at the bottom.

SPHEREboard Receiver best practices

To avoid performance issues, deactivate SPHEREboard’s Receiver during the following scenarios:

- When performing large data migrations from one NetApp storage system to another (large write or modification of files).
- When upgrading your release of ONTAP to a newer version.
- When performing a SPHEREboard upgrade.

After performing any of these actions, you can safely activate FPolicy.

To deactivate SPHEREboard’s Receiver, complete this step:

1. From a machine in the whitelisted IPs located in the config file under the value of `SphereMessageAllowedIPs`, navigate a browser to the address and port where the config file specifies that the FPolicy Admin Interface is located like this: `http://IPAddress:SphereMessagePort/stopall`.

   Note: Manage VM datastores or SQL Server datastores with FPolicy with caution, because such stores are not accessed by humans and do not host human-generated data. Activation of an FPolicy can increase the usage of resources on those stores and affect the performance of applications that use them.

Configuring FPolicy on ONTAP

This section provides instructions for configuring FPolicy for NetApp storage systems running ONTAP.

The FPolicy structure is defined as follows:

- **Event.** Defines which operations and protocol types FPolicy audits.
- **External engine.** Defines the endpoint (FPolicy server, also known as the SPHEREboard receiver) 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.

Configuration requirements

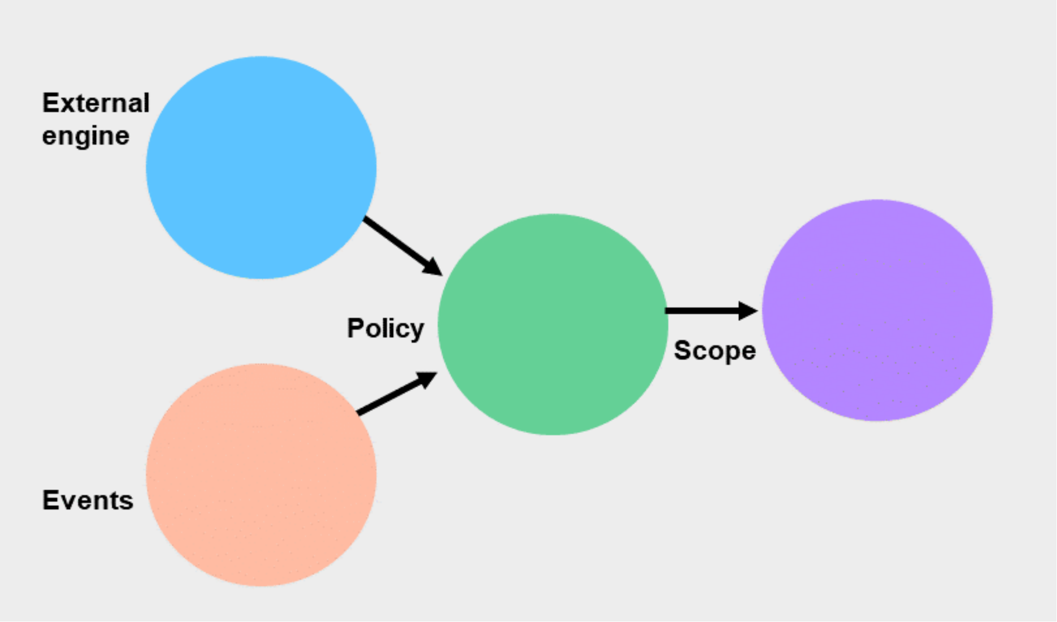
- The shares must reside on the volume monitored for CIFS events.
- The export policy must be created on and applied to the volume monitored for NFS events.

FPolicy configuration workflow

The workflow for creating a resident policy is depicted in Figure 2. Create an external engine and event before you create a policy. After a policy is defined, a scope must be associated with it.

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

Figure 2) FPolicy configuration workflow.



Create an FPolicy event

To enable SPHEREboard to connect to a NetApp storage system running ONTAP, you must configure an FPolicy for it. To do so, you must be a user with the vsadmin role and have a user name that is associated with the NetApp ONTAPI® application. The order in which you create an FPolicy event is important.

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

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

```
vserver fpolicy policy event create -vserver newSVM -event-name eventSPHERE -protocol cifs -
fileoperations create, create_dir, open, delete, delete_dir, read, write, rename, rename_dir,
setattr -filters first-read, first-write, open-with-delete-intent
```

Table 1) FPolicy event options.

Option	Description
`-vserver`	The name of the SVM on which you want to create an FPolicy external engine.
`-event-name`	The name of the FPolicy event that you want to create.
`-file-operations`	The file operations for the FPolicy event. Available values are: `create`, `create_dir`, `open`, `delete`, `delete_dir`, `read`, `write`, `rename`, `rename_dir`, and `setattr`.
`-protocol`	The name of the protocol for which the event is created. Available value `cifs`
`-filters`	The filters used with a given file operation for the protocol specified in the `protocol` parameter (for example, first-read, first-write).

Note: Although use of the first-read filter can improve performance, it may not be used concurrently with the Filter False-Open Events feature.

Additionally, in order that FPolicy captures and provides delete file operation done from clients using SMB3\SMB3.1 protocol, it requires to configure open, file-operation with open-with-deleteintent filter.

3. View the event object.

```
fpolicy policy event show eventSPHERE -instance
```

Create an FPolicy external engine

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

```
fpolicy policy external-engine create -vserver<Vserver Name> -engine-name engineSPHERE
-primaryservers <SPHERE_FPolicy_Server> -port 19003 -extern-engine-type asynchronous          -
ssl-option no-auth
```

Table 2) 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-enginetype	The type of external engine. Only asynchronous is supported.
-ssl-option	The SSL option is for external communication with the FPolicy server. Available values include: • server-auth – Provides probe authentication. • mutual-auth – Provides both receiver and NetApp authentication. • When set to mutual-auth, give values to SSL_CertLocation and SSL_KeyLocation in the SPHERE.Recievers.FPolicy_Server.dll.config file. **Note:** SSL is currently not supported.

Note: By default, SPHEREboard Receiver uses TCP/19003 as the port number. You can change this number by configuring another port in the SPHERE.Recievers.FPolicy_Server.dll.config file.

View the external engine or engines that you created.

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

Create an FPolicy policy

To create an FPolicy policy, complete the following steps:

1. To configure FPolicy policy, run the following command:

```
fpolicy policy create -vserver <Vserver Name> - policy-name policySPHERE -events <event names> -
engine  engineSphere -is-mandatory false
```

Table 3) FPolicy policy options.

Option	Description
`-vserver`	The name of the SVM on which you want to create an FPolicy external engine.
`-policy-name`	The name of the FPolicy policy that you want to create. The default policy name, as registered in the management console, is SPHERE.
`-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.

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

```
fpolicy policy show
```

Create an FPolicy scope

To create an FPolicy scope, complete the following steps:

1. To create the FPolicy scope, run the following command:

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

Table 4) FPolicy scope options.

Option	Description
`-vserver`	The name of the SVM on which you want to create an FPolicy external engine.
`-policy-name`	The name of the FPolicy policy that you want to create. The default policy name, as registered in the management console, is SPHERE.
`-volumes-toinclude`	A comma-separated list of volumes to be monitored. SPHERE recommends monitoring all volumes. Wildcards are supported.
`-export-policiesto-include`	A comma-separated list of export policies for monitoring file access. Wildcards are supported.

2. View the FPolicy scope you created.

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

Enable an FPolicy Policy

When the probe service starts, it enables the new FPolicy policy. The following command is for reference only:

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

FPolicy configuration best practices on ONTAP

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

Policy configuration

Configuration of an FPolicy external engine for the SVM

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

Configuration of an FPolicy event for the SVM

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

Configuration of an FPolicy scope for the 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.

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 port different from the LIF for client traffic, the FPolicy LIF might fail over to another node because of a port failure. This scenario renders the FPolicy server unreachable from the node and the FPolicy notifications for file operations on the node fail.

Note: To process FPolicy requests for the file operations performed on that node, make sure that the FPolicy server is reachable through at least one LIF on the node.

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.

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. A policy priority depends on use cases. To determine the appropriate priority, NetApp recommends working with partners.

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, first disable the policy.

When both FPolicy and an offbox 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.

Add all shares that you want to monitor or audit into the share-include list during scope definition. Turn off monitoring on the file server if you do not want monitor it. Disabling FPolicy on the SVM is not helpful, because the SPHEREboard service probes the file server and automatically disables or enables FPolicy if it notices a disconnection.

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 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.

Troubleshooting common problems

Problem: The FPolicy server is disconnected

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

Command example:

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

Problem: The FPolicy server does not connect

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

Command example:

```
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 using the `routing-groups route show` command to check whether a route is available for the SVM. If not, add a route with the `routing-groups route create` command.

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
```

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.

Command example:

```
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 upon 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
```

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.

Command example:

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

Problem: The external engine is not native for the policy

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

Command example:

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

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

Command example:

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

Performance monitoring

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

Monitoring the performance counters on FPolicy server and ONTAP identifies 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 using 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 following ONTAP FPolicy counters to monitor the performance of FPolicy subsystems.

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

Collect and display FPolicy counters

To collect FPolicy counters, run the following command:

```
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 command:

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

Counters to monitor

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

Table 5) List of FPolicy counters.

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

Table 6) List of fpolicy_server counters.

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

Conclusion

File-access reporting has become an integral part of overall infrastructure deployment. The ONTAP and SPHERE Activity Collector solution provides a comprehensive, collaborative, and conclusive approach to file access reporting. With this document, you can efficiently understand, deploy, and manage the solution outlined.

Where to find additional information

To learn more about the information that is described in this document, review the following website:

- NetApp Product Documentation
  https://www.netapp.com/us/documentation/index.aspx

Version history

Version	Date	Document version history
Version 1.0	December 2021	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.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).

Trademark information

TR-4916-1221