Technical Report

FPolicy Solution Guide for Clustered Data ONTAP: Northern Storage Suite (NSS)

Brahmanna Chowdary Kodavali and Saurabh Singh, NetApp
Anette Lawless and Robert Dahlquist, Northern
December 2015 | TR-4479

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Introduction

The NetApp® FPolicy® component is a file access notification system that enables an administrator to monitor file access in storage configured for Network File System (NFS) and CIFS. Introduced for the scaled-out architecture in the NetApp clustered Data ONTAP® 8.2 operating system, FPolicy enables a rich set of use cases working with selected NetApp partners. FPolicy requires all nodes in a cluster to run Data ONTAP 8.2 or later. The system supports all SMB versions, including SMB 1.0 (CIFS), SMB 2.0, SMB 2.1, and SMB 3.0. FPolicy also supports major NFS versions, including NFSv3 and NFSv4.0.

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

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

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

1.1 Audience

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

1.2 Purpose and Scope

This document explains the FPolicy framework. It also describes the steps required to deploy the Northern Storage Suite (NSS) software for management of user-generated data. 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 have 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.

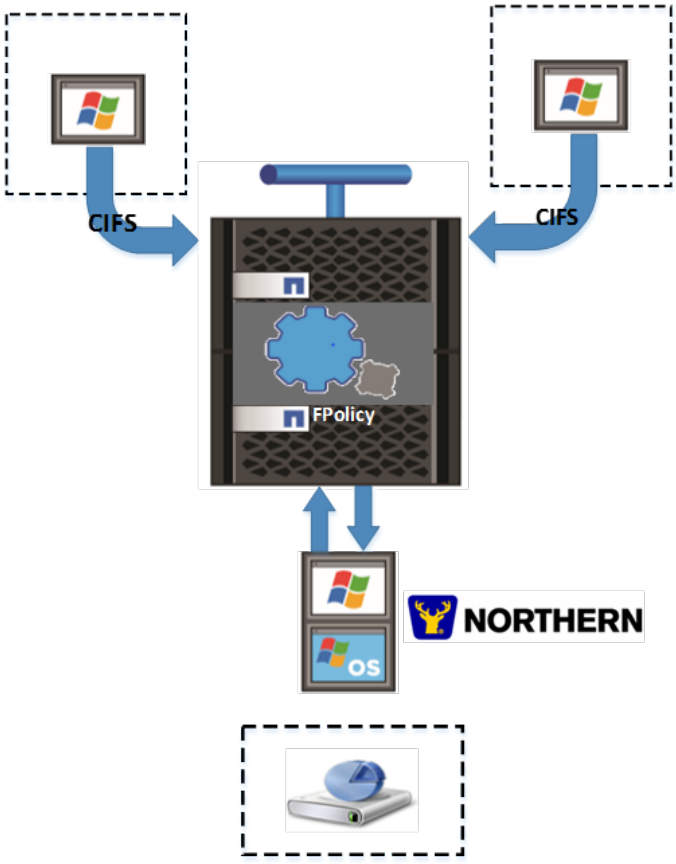
- Ability to bypass any FPolicy checks so that file access over a privileged data path does not generate an FPolicy notification

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 NSS application. 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: Northern Storage Suite (NSS)

Northern's user data management (UDM) offering lets organizations manage their user-generated data proactively to help increase efficiency and reduce risk.

The NSS software solution provides three primary capabilities in its policies for managing user data:

- Top-level insight into how file systems are being used:
  - Exposing and quantifying enterprise-wide opportunities for increased cost efficiency and risk reduction
  - Consistently monitoring data creation activities to identify changing trends and needs
- Ability to affect change in storage practices:
  - Using hard or soft quotas to monitor growth in file shares and trigger actions when predetermined sizes are reached
  - Preventing specific file types from being saved in specific shares
  - Creating cost awareness or billing for storage use in a service delivery model
- Delegation of data management activities into the business:
  - Delivering actionable reports to share custodians and data owners to guide efficient and compliant file service use
  - Allowing responsibility for data to be placed firmly in the hands of those who create and use it

For DAS and SAN management, the NSS software package is installed directly on file servers. For solutions that include NAS platform management, the NSS software package can also be installed on dedicated application servers. The software is platform agnostic, and it manages environments in the petabyte range. For integration with NetApp clustered Data ONTAP, the software uses the FPolicy API to enable synchronous enforcement of data management policies.

4 Installing and Configuring NSS

4.1 NSS Software Requirements and Installation

For system requirements and installation procedures, see Getting Started with Northern Storage Suite.

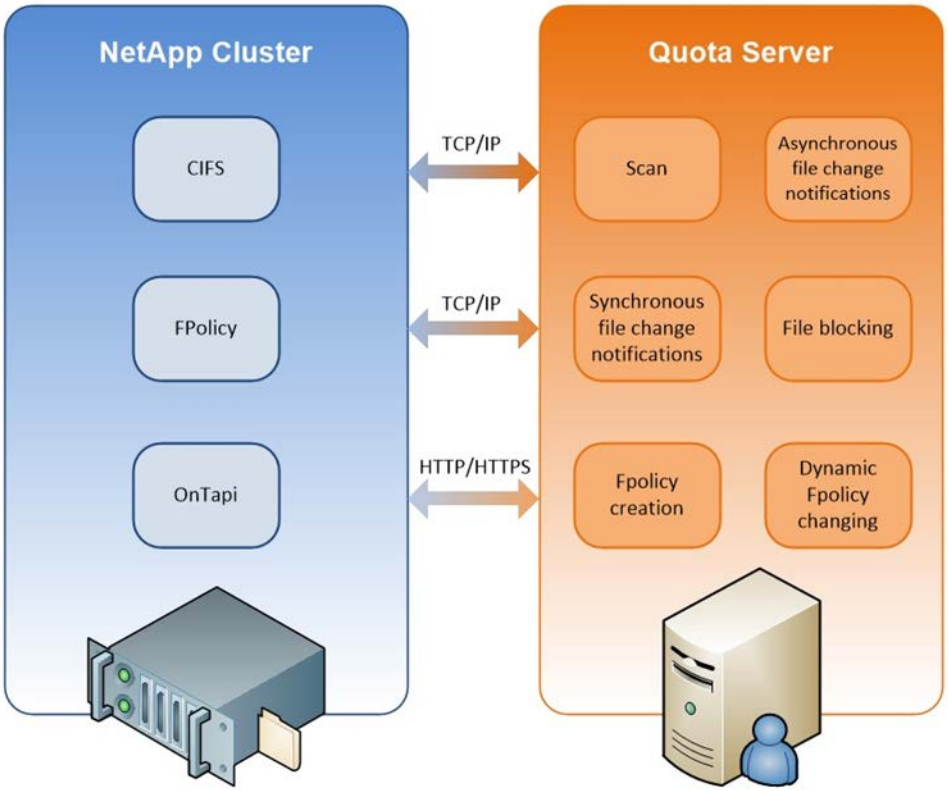
4.2 Configuring NSS for NetApp Storage

This section covers the essential steps needed to integrate NetApp clustered Data ONTAP with the quota server functionality in NSS. This integration requires NSS version 9.6 or later to be installed. Version 9.61 SR1 or later is required if the Data ONTAP version is 8.3 or later.

As Figure 2 shows, NSS communicates with NetApp clusters through three types of protocols:

- CIFS
- TCP/IP
- HTTP/HTTPS

Figure 2) NSS communication with NetApp cluster (graphic supplied by Northern).



CIFS for Quotas and Reports

The NSS services must access the CIFS shares on which quotas or reports are applied. Using CIFS gives NSS access to the SVM allowed by the user account that is used for the NSS core server and NSS quota server services.

When they are run under administrator groups, both services claim backup rights for scanning operations.

TCP/IP for Requests and Responses

The NSS quota server uses the TCP/IP protocol to retrieve and answer FPolicy requests. FPolicy requests and responses are sent on one TCP/IP port per SVM.

HTTP/HTTPS for Connection and Object Creation

The HTTP/HTTPS channel is used to manage the FPolicy connection. NSS uses this configuration to connect to Data ONTAP and create the required FPolicy object. It also removes the object upon exit.

4.3 Prerequisites and Configuration

The FPolicy object is created or updated as soon as a quota or a file block is added or removed. This can happen only if the following three prerequisites are met:

- The NSS quota server service account is an administrator on each managed SVM.
- The quota server is connected to the SVM with the `vsadmin-account` or its equivalent (ONTAPI® rights required). For more information, see section 6, “Security Login Configuration for FPolicy Server.”

- A settable TCP/IP port is opened for each managed SVM (the default port is 9000).

For more information about FPolicy configuration in NSS quota server, see How to Integrate with NetApp Clustered Data ONTAP.

4.4 Adding NSS Quota Server Service Account to SVM Administrator Group

Add the account used by the NSS quota server functionality in `BUILTIN\Administrators` on each managed SVM. It is necessary to add this account because the service must have permission to perform operations on the SVM.

There are two ways to add the NSS quota server service account to the `BUILTIN\Administrators` group on the managed SVM:

- Through the NetApp CLI
- Through the OnCommand GUI

Adding Account Through NetApp Command Line Interface

To add an account through the NetApp CLI, complete the following steps:

1. At the NetApp command prompt, enter `vserver cifs users-and-groups local-group`. In this example, the NetApp cluster is named `NorthernCDOT`:

```
NorthernCDOT::vserver cifs users-and-groups local-group>
```

2. Inside this section of the NetApp client, type the following command to add the NSS quota server service account to the `BUILTIN\Administrators` group on the SVM:

```
add-members -group-name BUILTIN\Administrators -member-names DOMAIN\service_account -vserver
XXXXX
```

Note: Use your NSS quota server service account as the value for `DOMAIN\service_account`. Use the name of the SVM as the value for `XXXXX`. Make sure the domain and the account name are set correctly in the credentials. The following example shows how the command looks in the NetApp command prompt. In this example, the name of the SVM is `SNV-FieldCDOT`.

3. The account is now a member of the `BUILTIN\Administrators` group. Repeat this process for all managed SVMs.

Adding Account Through OnCommand Interface

Another approach to adding an account is to use the NetApp OnCommand interface. This software enables the administrator to manage the NetApp cluster from a GUI. To add an account through the OnCommand interface, complete the following steps:

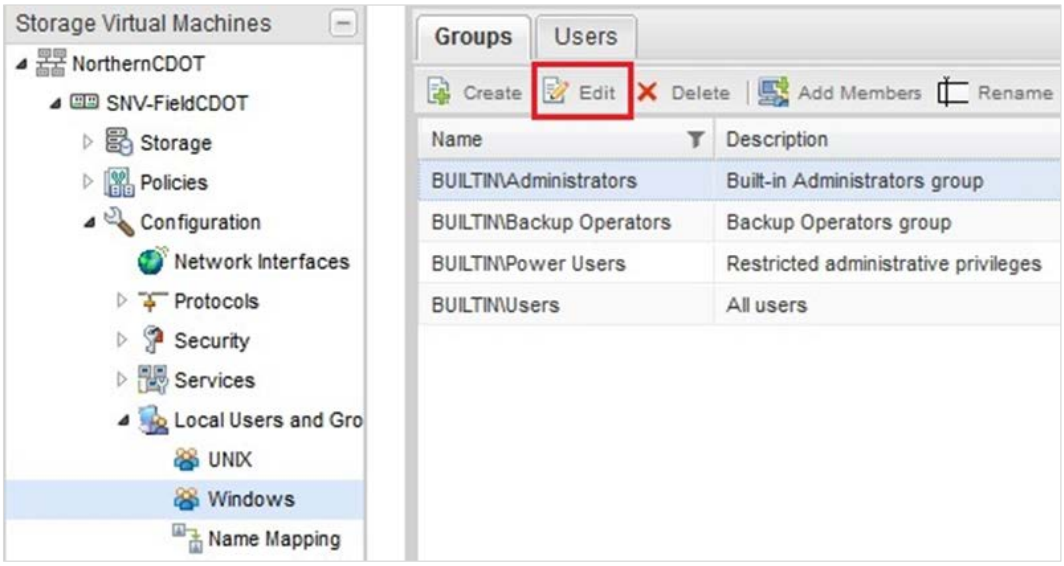
1. Open the OnCommand interface and navigate to the following location:

```
Storage Virtual Machines\Cluster Name\Vserver Name\Configuration\Local Users and Groups\Windows.
```

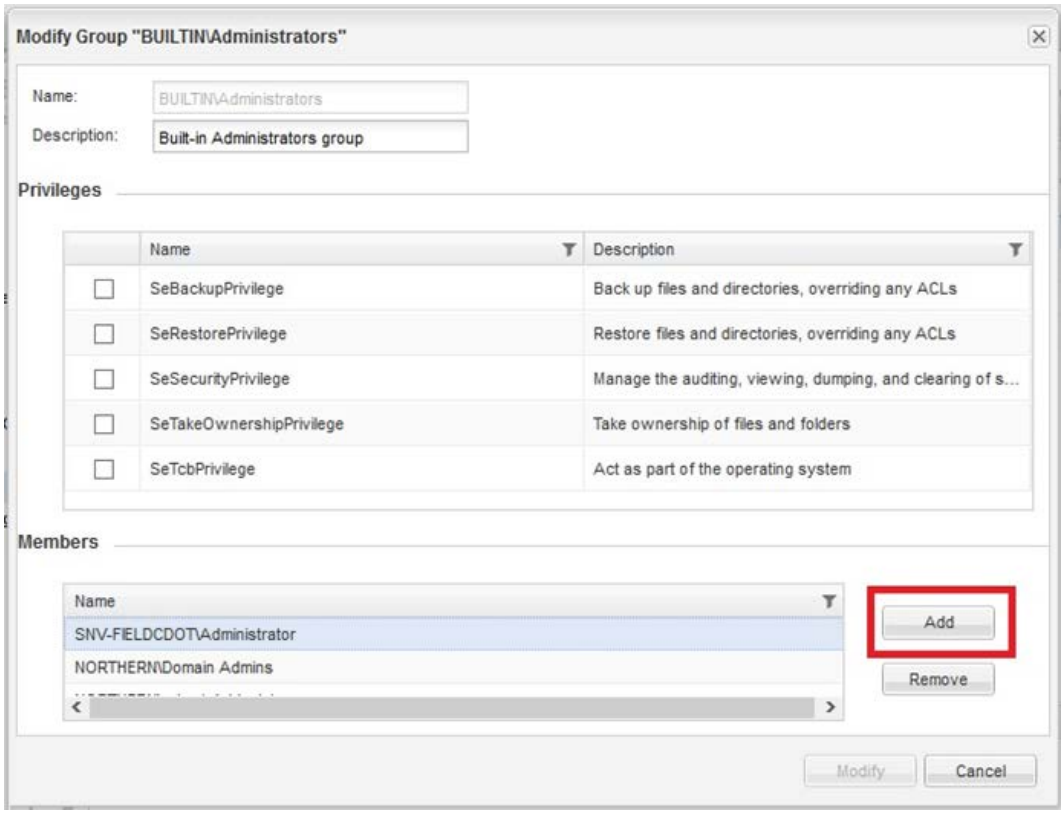
Note: The pathway in this example uses the following specific names:

```
Storage Virtual Machines\NorthernCDOT\SNV-FieldCDOT\Configuration\Local Users and Groups\Windows.
```

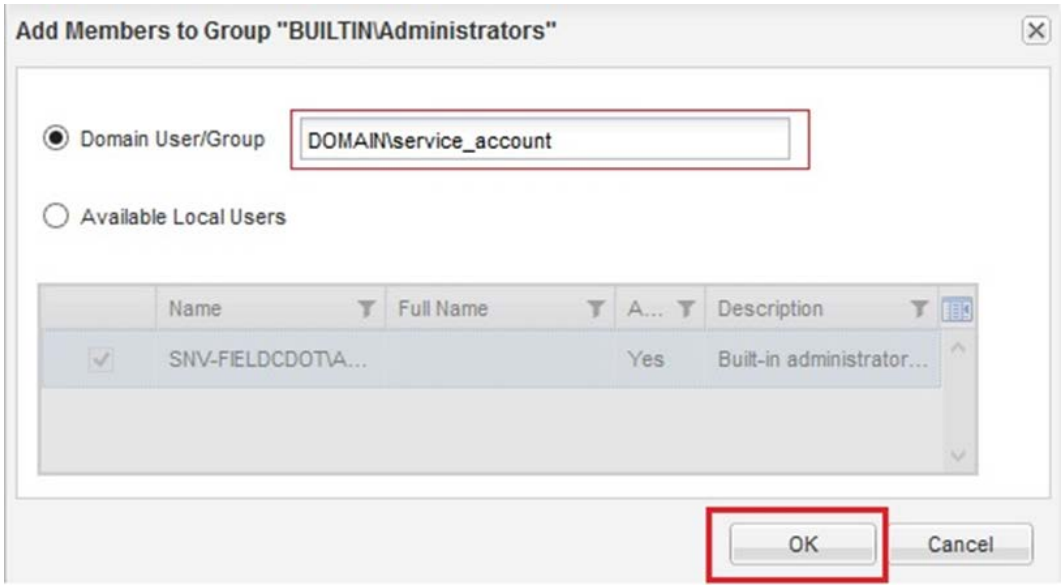

2. From the list, select `BUILTIN\Administrators`. Click Edit to begin modifying the group.



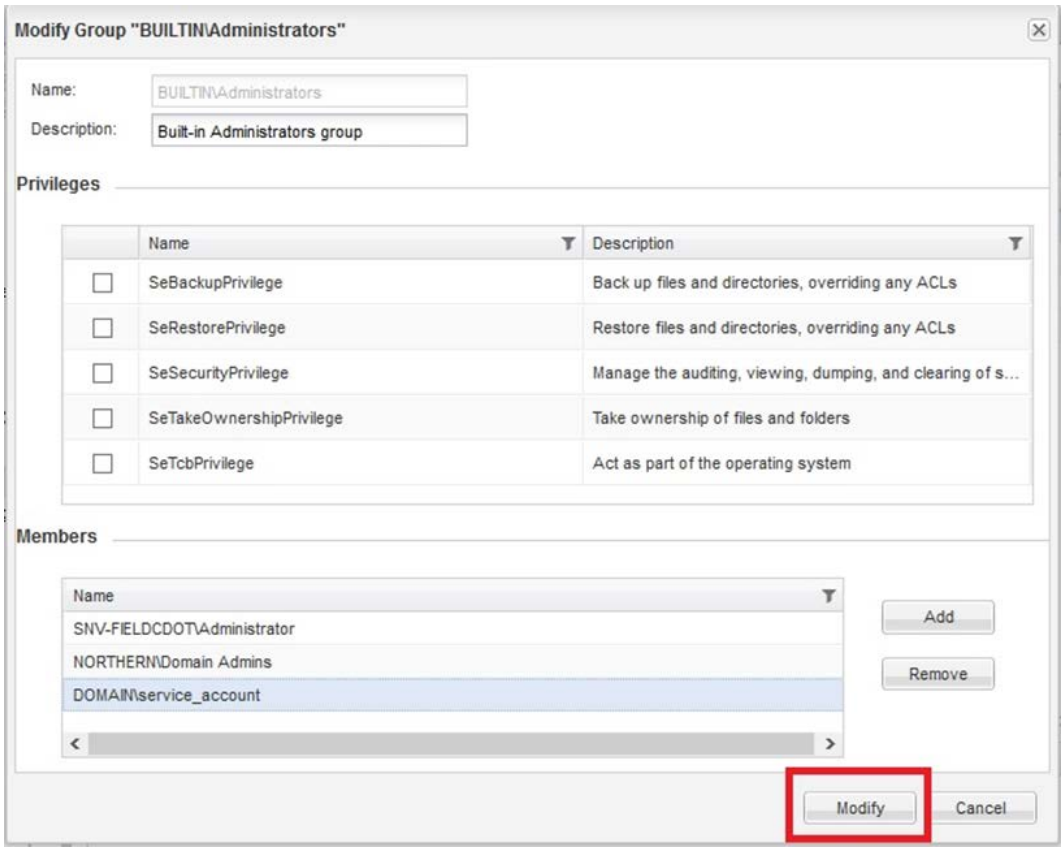
3. In the Members section, click Add.



4. Add the NSS quota server service account.



5. Click Modify to apply the change.

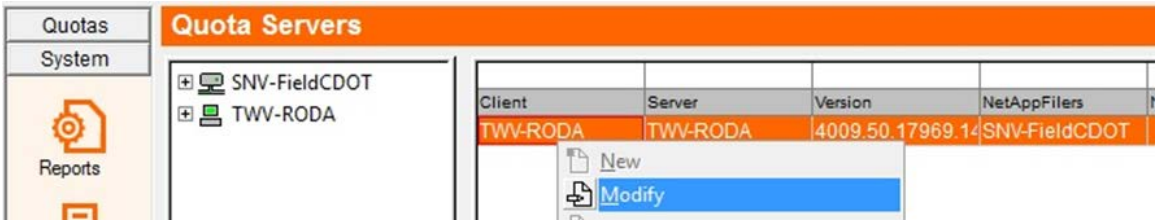


6. The account is now a member of the `BUILTIN\Administrators` group. Repeat this process for all managed SVMs.

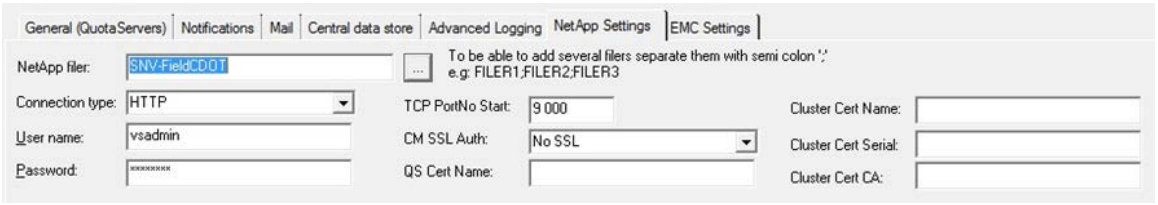
4.5 Establishing FPolicy Connection in NSS Quota Server

After the account is added, the connection can be established. To establish the FPolicy connection, complete the following steps:

1. After you confirm that the account has been added, launch the NSS quota server client.
2. Navigate to System > Quota Servers.
3. Find your quota server and right-click to select it.
4. From the drop-down list, select Modify.



5. In the settings menu that displays at the bottom of the screen, click NetApp Settings.



6. In this section, specify the connection type and the logon credentials:
   a. In the NetApp Filer field, specify the name or names of the CIFS servers to be managed.

   Note: If you have multiple CIFS server names, separate them with a semicolon (;). Note that the CIFS server name might or might not be the same as the SVM name, depending on the configuration of your NetApp environment.

   b. Select either HTTP or HTTPS as the connection type you want to use.
   c. In the User Name field, specify the vsadmin account or its equivalent.

   Note: Use the vsadmin account because this account has all of the required rights to establish the FPolicy connection. You can use another account, but it must have the same rights on the SVM as the vsadmin account. ONTAPI login rights are required. For more information, see section 6, “Security Login Configuration for FPolicy Server.”

   d. Type in the password of the account used for authentication.
   e. Specify a starting TCP/IP port for the NSS quota server to use for communicating with the SVM.

   Note: The default port is set to 9000. Each SVM claims a port. You must open an additional port for each managed SVM. For example, if you want to manage three SVMs, you must open ports 9000, 9001, and 9002.

Optional Settings

The following settings are relevant only for encrypting communication to and from an SSL layer:

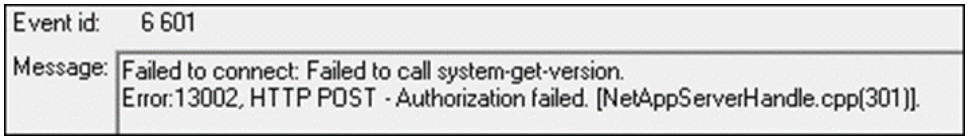
- `CM SSL Auth`: This setting dictates whether to make the connection through SSL. The default value is set to `No SSL`. The other two settings, `Server` and `Mutual`, enable SSL.
- `QS Cert Name`: Specify the name of your NSS QS certificate.
- `Cluster Cert Name`: Specify the name of your cluster certificate.
  - `Cluster Cert Serial`: Specify your cluster certificate serial.
  - `Cluster Cert CA`: Specify the cluster certificate CA.

Apply the changes either by pressing Enter or by right-clicking and selecting Apply from the menu.

Authorization Failure

The `authorization failed` message is shown in Figure 3. This message displays to indicate that the quota server cannot connect to the NetApp cluster.

Figure 3) Authorization-failed message.



The most common cause of authorization failure is incorrect configuration of the account user name and/or password. If authorization fails, verify that the credentials are correct and try again.

Confirming Your Results

Before you test the locking and file blocking, verify that the following requirements are met:

- Is the NSS quota server service account a member of the `BUILTIN\Administrators` group on all managed SVMs?
- Are the login credentials correct in the Quota Server NetApp Settings tab?
- Is the local vsadmin account (or equivalent) properly configured?
- Does the account have ONTAPI login rights?
- Has a TCP/IP port been opened for each managed SVM: 9000, 9001, 9002, and so on?

For further information about FPolicy configuration in NSS quota server, see How to Integrate with NetApp Clustered Data ONTAP.

After this checklist is complete and verified, you can test the locking functionality.

Important Note

Make sure that these tests are carried out with a regular user account on a different machine. File operations performed directly on the NSS server bypass the file policy rules. (This behavior is dictated by FPolicy.)

Test Procedure Example

The following steps provide a typical example of a testing procedure:

1. Create an object quota, selecting NetApp as the platform.
2. Assign a locking action to a threshold (suggested value: `Lock dir`).
3. Copy enough files to the quota path to push the folder over the locking threshold.

   Note: Use a network client for the copy action.
4. Watch for the blocking to take effect.

   Note: The first file passing through the quota activates the associated action, but the system allows it to be saved. If the settings are correct, the next attempt to copy should be blocked.
5. Log in at the `NetApp Cluster Command` prompt.
6. Type `vserver fpolicy show` to verify that the FPolicy server object has been created and registered.

For further information about FPolicy configuration in NSS quota server, see How to Integrate with NetApp Clustered Data ONTAP.

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.

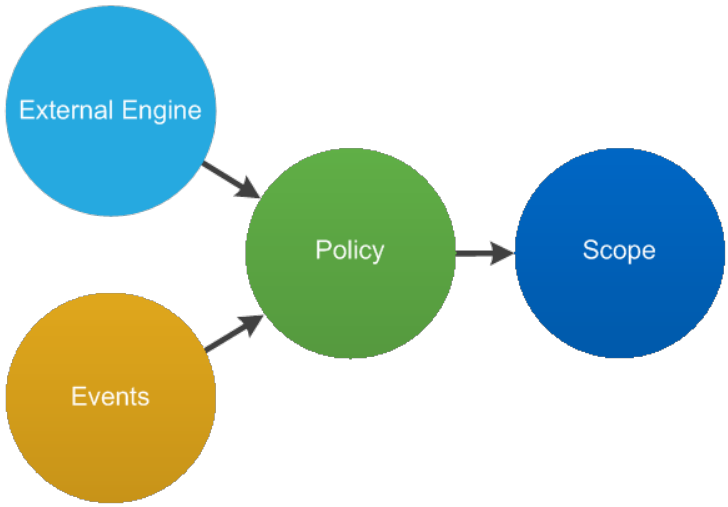
Configuration Requirements
• The shares must reside on the volume monitored for CIFS events. • The export policy must be created on and applied to the volume monitored for NFS events.

5.1 FPolicy Configuration Workflow

Figure 4 shows the workflow for creating a resident policy. Before you create a policy, you should create an external engine and an event. After you define a policy, you must associate a scope with it.

After the scope is created, the policy must be enabled with a sequence number. The sequence number helps to define the policy's priority in a multipolicy environment, with 1 having the highest priority and 10 having the lowest.

Figure 4) FPolicy configuration workflow.



Important Note

The NSS quota server automatically defines the FPolicy configuration in clustered Data ONTAP as soon as a quota or file block is created.

The following sections, 5.2 through 5.6, explain the commands that the application uses in the background to configure the different components. These commands are included strictly for reference; Northern does not support manual FPolicy configuration in the integration of NSS quota server and clustered Data ONTAP.

If necessary, you can use the show commands in each section to review the configuration that has been made automatically by NSS.

5.2 Create FPolicy Event

To enable the NSS quota server to connect to a NetApp storage device running clustered Data ONTAP, you must configure an FPolicy policy for it. To be able to do so, you must be a user with the vsadmin role and have a user name that is associated with the NetApp ONTAPI application. The order in which you create an FPolicy event is important.

Note: NSS does not support NFS events for FPolicy.

To create an FPolicy event by using Transmission Control Protocol (TCP/IP), complete the following steps:

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

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


Table 1 lists the options for the FPolicy event.

Table 1) FPolicy event options.

Option	Description
`-vserver`	The name of the SVM (Vserver) on which you want to create an FPolicy external engine
`-event-name`	The name of the FPolicy event that you want to create
`-file-operations`	The file operations for the FPolicy event Possible values: `create, create_dir, delete, delete_dir, read, close, rename, rename_dir`
`-protocol`	The name of the protocol for which the event is created Possible value: `cifs`
`-filters`	The filters used with a given file operation for the protocol specified in the `-protocol` parameter Examples: `first-read, close-with-modification`

To view the event object, run the following command:

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

5.3 Create FPolicy External Engine

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

```
fpolicy policy external-engine create -vserver
<vserver name> -engine-name <engine name> –primary
servers <ip address of Data Insight fpolicy server>
-port <port used by Data Insight server> -extern-engine-
type asynchronous –ssl-option no-auth
```

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

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

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

5.4 Create FPolicy Policy

To create the FPolicy policy, run the following command:

```
fpolicy policy create -vserver <Vserver Name> -policy-name <policy name> -events <event name>
-engine <engine name> -is-mandatory false
The events attribute may be only one of the events or multiple events separated by commas.
```

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 create an FPolicy external engine
`-policy-name`	The name of the FPolicy policy that you want to create
`-events`	A list of events to monitor for the FPolicy policy
`-engine`	The name of the external engine that you want to create
`-is-mandatory`	Determines whether the FPolicy object is mandatory

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

```
fpolicy policy show
```

5.5 Create FPolicy Scope

To create the FPolicy scope, run the following command:

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

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 create an FPolicy external engine
`-policy-name`	The name of the FPolicy policy that you want to create
`-volumes-to-include`	A comma-separated list of volumes to be monitored
`-export-policies-to-include`	A comma-separated list of export policies for monitoring file access **Note:** Wildcards are supported.

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

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


5.6 Enable FPolicy Policy

The NSS quota server functionality uses the following command to automatically enable the new FPolicy policy at startup:

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

6 Security Login Configuration for FPolicy Server

The NSS quota server functionality uses a local security account on the target SVMs for the FPolicy authorization. Use the existing `vsadmin-account` for this purpose.

If the `vsadmin-account` cannot be used (for example, if it is locked because of a security policy), a new local security account must be created locally on each managed SVM. The new account must have the same rights as the `vsadmin-account` (ONTAPI and SSH rights).

7 NetApp Clustered Data ONTAP Best Practices

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

7.1 Policy Configuration

Configuration of FPolicy External Engine for SVM

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

Configuration of FPolicy Events for SVM

Monitoring file operations affects the overall user experience. In fact, filtering unwanted file operations on the storage side improves the overall user experience. NetApp recommends monitoring the minimum number of file operations and enabling the maximum number of filters without breaking the use case. The CIFS home directory environment has a high percentage of `getattr`, `read`, `write`, `open`, and `close` operations. NetApp recommends using filters for these operations. For a list of recommended filters, see section 5.2, “Create FPolicy Event.”

Configuration of FPolicy Scope for SVM

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

7.2 Network Configuration

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

Note: If the LIF for FPolicy traffic is configured on a different port from that of the LIF for client traffic, a port failure might cause the FPolicy LIF to fail over to the other node. This failover would make the FPolicy server unreachable from the node and cause FPolicy notifications for the file operations on the node to fail. Make sure that the FPolicy server can be reached through at least one LIF on the node to process FPolicy requests for the file operations performed on that node.

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, be 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. NetApp recommends working with partners to determine the appropriate priority.

7.5 Managing FPolicy Workflow and Dependency on Other Technologies

NetApp recommends disabling an FPolicy policy before making any configuration changes to it. For example, if you want to add or modify an IP address in the external engine configured for the enabled policy, first disable the policy.

If you configure FPolicy to monitor NetApp FlexCache® volumes, NetApp recommends that you not configure FPolicy to monitor `read` and `getattr` file operations. Monitoring these operations in Data ONTAP requires retrieving inode-to-path (I2P) data. Because I2P data cannot be retrieved from FlexCache volumes, it must be retrieved from the original volume. Therefore, monitoring these operations eliminates the performance benefits that FlexCache can provide.

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

Add all shares that you want to monitor or audit into the share-include list during scope definition.

7.6 Sizing Considerations

FPolicy monitors CIFS operations inline and sends notifications to the external server. It might also wait for a response, depending on whether the mode of external engine communication is synchronous or asynchronous. This monitoring process affects the performance of CIFS access and CPU resources. To mitigate potential problems, NetApp recommends assessing and sizing the environment before enabling FPolicy. Performance is affected by the number of users, by workload characteristics such as operations per user and data size, and by network latency.

8 NSS Best Practices

For best practices related to NSS integration with NetApp Clustered Data ONTAP, see How to Integrate with NetApp Clustered Data ONTAP.

9 Troubleshooting Common Problems

9.1 Problem: FPolicy Server Is Disconnected

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

Command example:

```
1. fpolicy show-engine
2. fpolicy engine-connect –node <node name> -vserver <vserver name> -policy <policy name> -server
<ip address of fpolicy server>
3. fpolicy show-engine -instance
```


9.2 Problem: FPolicy Server Does Not Connect

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

Command example:

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

First potential cause: There are problems with routing.

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

Command example:

```
routing-groups route create -vserver <vserver name> -routing-group d10.X.0.0/18 -destination
0.0.0.0/0 -gateway 10.X.X.X
```

Second potential cause: The FPolicy server is not listening on the port specified.

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

Command example:

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

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

Potential solution: Run the `fpolicy policy external-engine show –instance` command. If the FPolicy server uses SSL, the field SSL Option for External Communication is either `mutual-auth` or `server-auth`.

Also check the fields FQDN or Custom Common Name, Serial Number of Certificate, and Certificate Authority to verify that the certificates are properly configured.

To correct this problem if the FPolicy server does not use SSL, modify `ssl-auth` to `no-auth`. Otherwise, use `mutual-auth`/`server-auth`, depending on the level of security needed.

Command example:

```
fpolicy policy external-engine modify -vserver <vserver name> -engine-name <engine name> -
primary-servers <ip address> -port <tcp port no> -ssl-option no-auth
```

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

Potential solution: Make sure 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. Next, 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

Counters	Description
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

10.3 Performance Statistics in NSS

The NSS quota server traces various statistics. For information about performance-monitoring capabilities in NSS, contact Northern Technical Support.

References

This report references the following documents and resources:

From NetApp:

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

From Northern:

- Getting Started with Northern Storage Suite
  http://www.northern.net/en/Training--Support/Knowledge-Base/Concept/Getting-started-with-Northern-Storage-Suite/
- How to Integrate with NetApp Clustered Data ONTAP
  http://www.northern.net/en/Training--Support/Knowledge-Base/Usage/Integrating-NetApp-CDOT-with-Quota-Server/
- Northern Technical Support site
  http://www.northern.net/

Version History

Version	Date	Document Version History
Version 1.0	December 2015	Initial release

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.