Technical Report

FPolicy Solution Guide for Clustered Data ONTAP: NTP Software QFS

Brahmanna Chowdary Kodavali and Saurabh Singh, NetApp
September 2015 | TR-4453

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 SMB1.0 (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

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

1.2 Purpose and Scope

The purpose of this document is to provide an understanding of the FPolicy framework. The document also describes the steps needed to deploy a file-access auditing solution by using the data-governance software NTP Software QFS for NAS, NetApp Edition. The scope of the document encompasses the 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 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 the FPolicy framework expects a notification response from the FPolicy server.

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.

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.

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 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 context 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 admin SVM can be leveraged in all data SVMs.
- **Data LIFs.** Connections to the FPolicy servers 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, FPolicy framework manages the following tasks:

- Controls the flow of file notifications through the correct LIF to the FPolicy server
- Load-balances notifications to the FPolicy server when 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 of the 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 removed immediately.

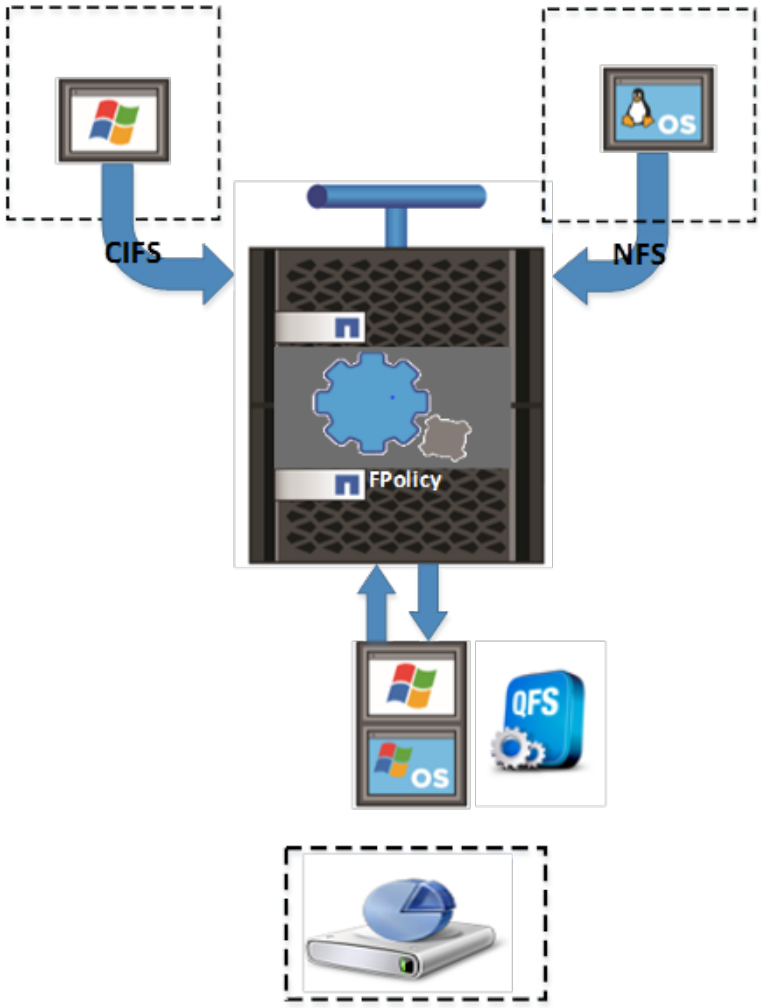
- Ability to bypass any FPolicy checks so that file access over a privileged data path does not generate an FPolicy notification

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 NTP Software QFS for NAS, NetApp Edition. 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 within clustered Data ONTAP. The FPolicy framework connects to external FPolicy servers and 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 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.

3.2 FPolicy Application Software: NTP Software QFS

NTP Software QFS for NAS, NetApp Edition, enables you to create quota and file-blocking policies that are configurable and granular. This application allows you to:

- Manage with disk quota policies to limit user consumption.
- Reduce your risk and storage growth with advanced file blocking.
- Provide tools for users to understand and clean up unneeded data.
- Make controlling data and storage easy without creating additional headaches.

NTP Software QFS enables the near-instantaneous ability to check against a policy when an end user requests saving a file. And because you can apply policies at both the share level and the directory level, you can tailor your file blocking and quotas based on the specific needs of your end users.

NTP Software QFS for NAS, NetApp Edition, does its job remotely as part of the NTP Software QFS family of products. NTP Software QFS for NAS, NetApp Edition, uses a connector service to create a bridge and include storage controllers as full participants in storage environments controlled by NTP Software QFS.

You can use NTP Software QFS for NAS, NetApp Edition, to manage NetApp storage controllers, NetApp vFiler® units, and NetApp clusters or any combination of these systems. NTP Software QFS imposes no restrictions on the way you organize or manage your storage. You can design policies for individual directories, for individual users, and/or for groups of users.

4 Installing and Configuring NTP Software QFS

4.1 NTP Software QFS Software Requirements and Installation

For system requirements and installation procedures, see the NTP Software document Installation Guide - NTP Software QFS for NAS, NetApp Edition.

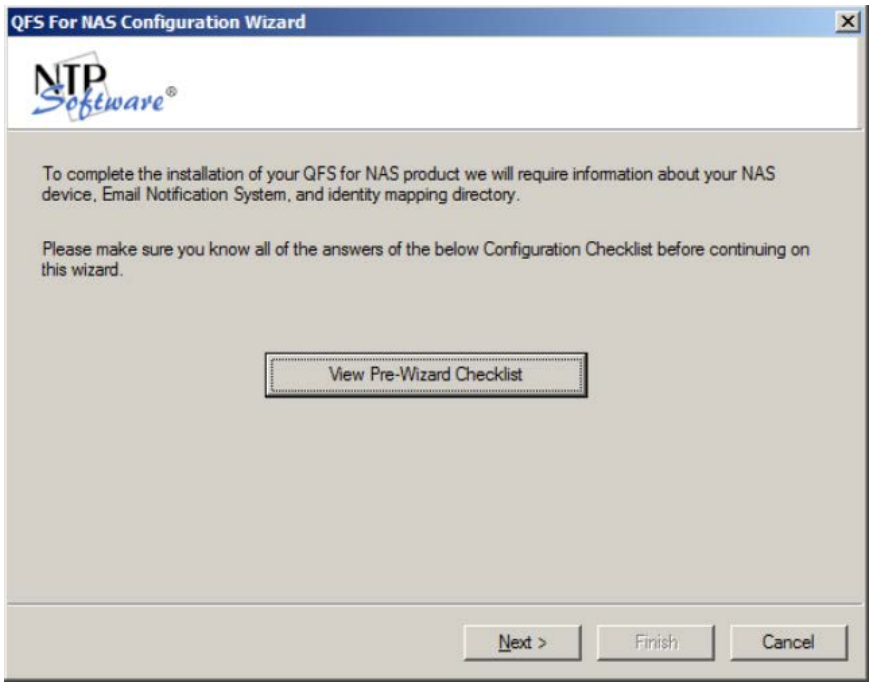
4.2 Configuring NTP Software QFS for NetApp

The following procedures explain how to use the configuration wizard, add a storage controller to NTP Software QFS for NAS administration, and verify the registration of a storage controller.

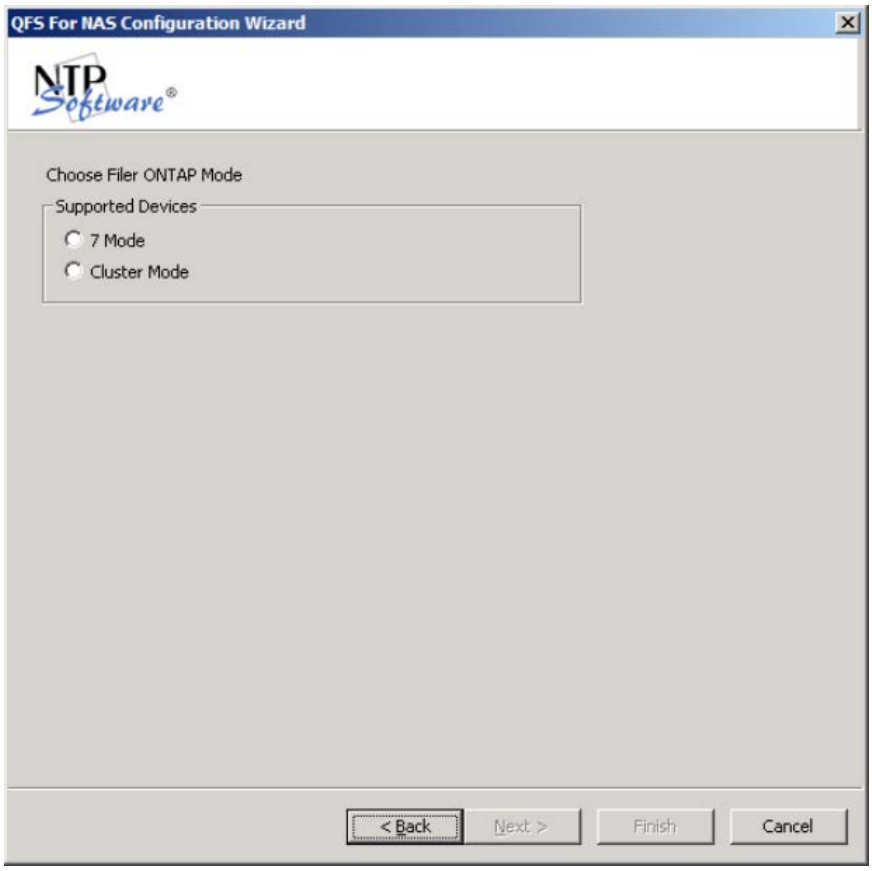
Use NTP Software QFS for NAS Configuration Wizard

When NTP Software QFS installation is complete, the QFS for NAS configuration wizard appears. To use the wizard, complete the following steps:

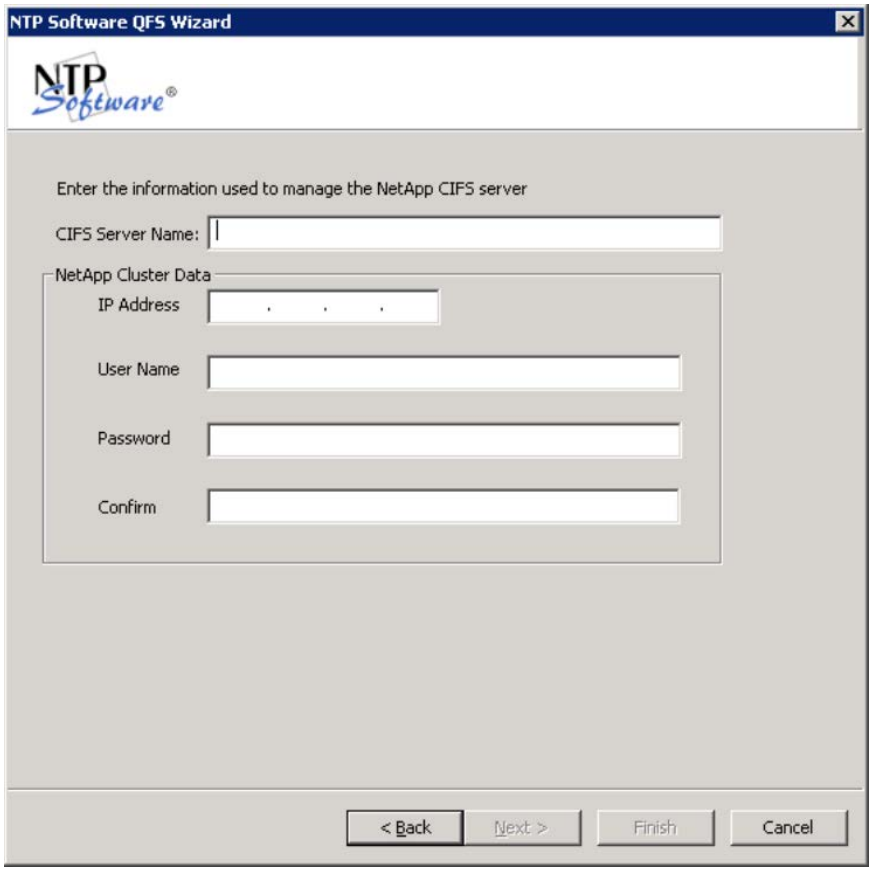
1. Click Start > All Programs > NTP Software QFS for NAS > NTP Software QFS for NAS Configuration Wizard.
2. Click View Pre-Wizard Checklist and gather the required information before continuing. Click Next.



3. Select either 7-Mode or Cluster-Mode, as appropriate for your version of Data ONTAP. Click Next.

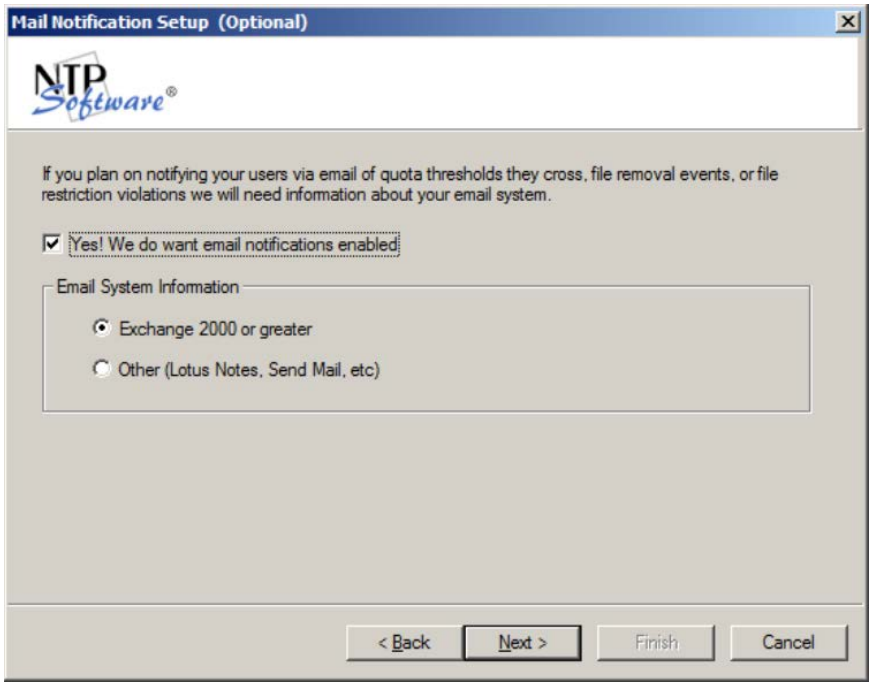


4. For clustered Data ONTAP storage controllers, enter the name of the CIFS server. Also enter the cluster IP address and the user name and password for the account on the cluster that has permission to execute some NetApp APIs (called the ONTAPI® library) required by QFS. Click Next.

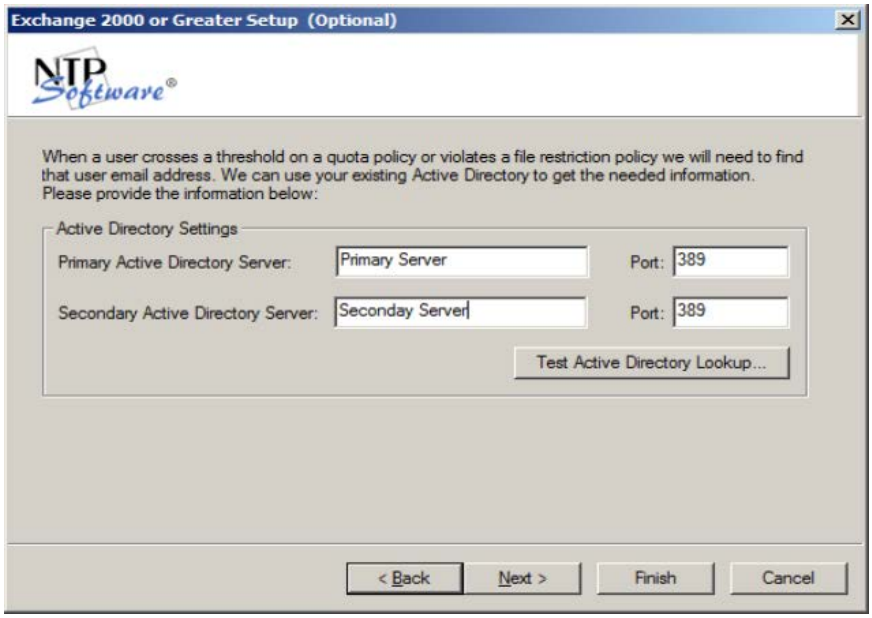


5. Select the e-mail system your environment uses and click Next.

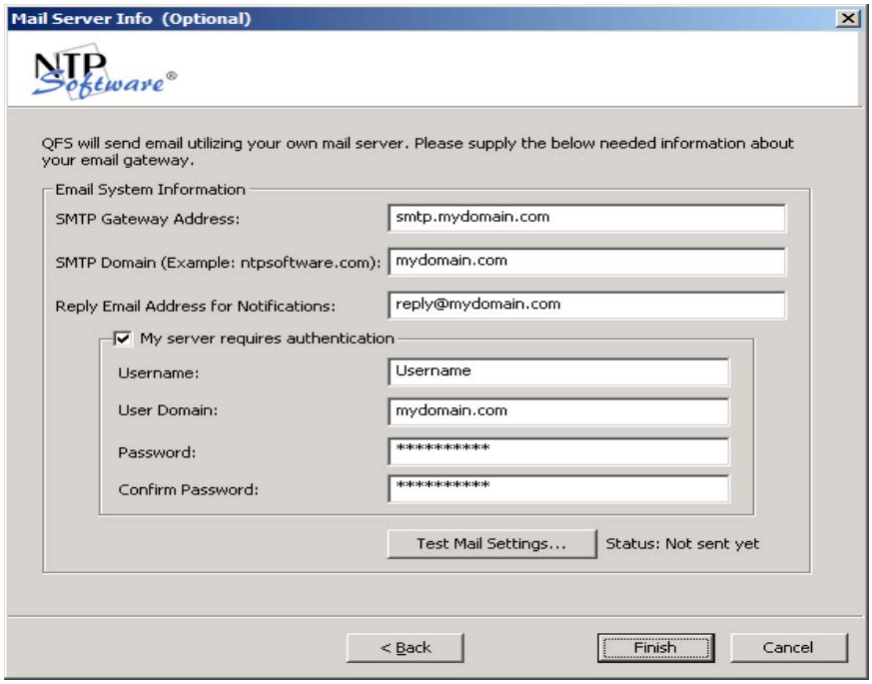
   Note: If you do not want to send e-mail notifications to users when a quota status changes, clear the checkbox for enabling e-mail notifications.



6. Enter the name of your Active Directory server. (Optional: Enter a second server, if desired.) Click Test Active Directory Lookup and test at least one e-mail address to verify connectivity. Click Next.



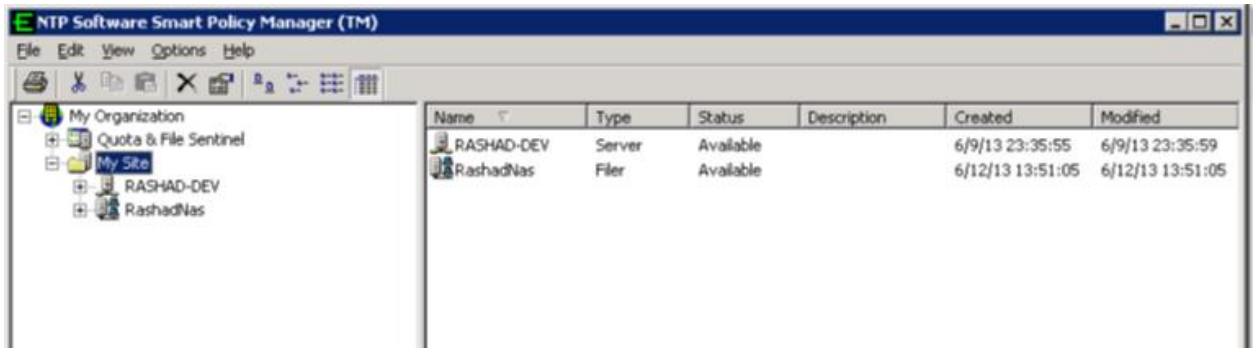
7. Enter the SMTP gateway, the SMTP domain, and the e-mail address to use for notifications. If your SMTP server requires authentication, enter the required user name, domain, and password. Confirm the password to be used to authenticate with your SMTP server. Click Test Mail Settings to verify that the information is correct. Click Finish.



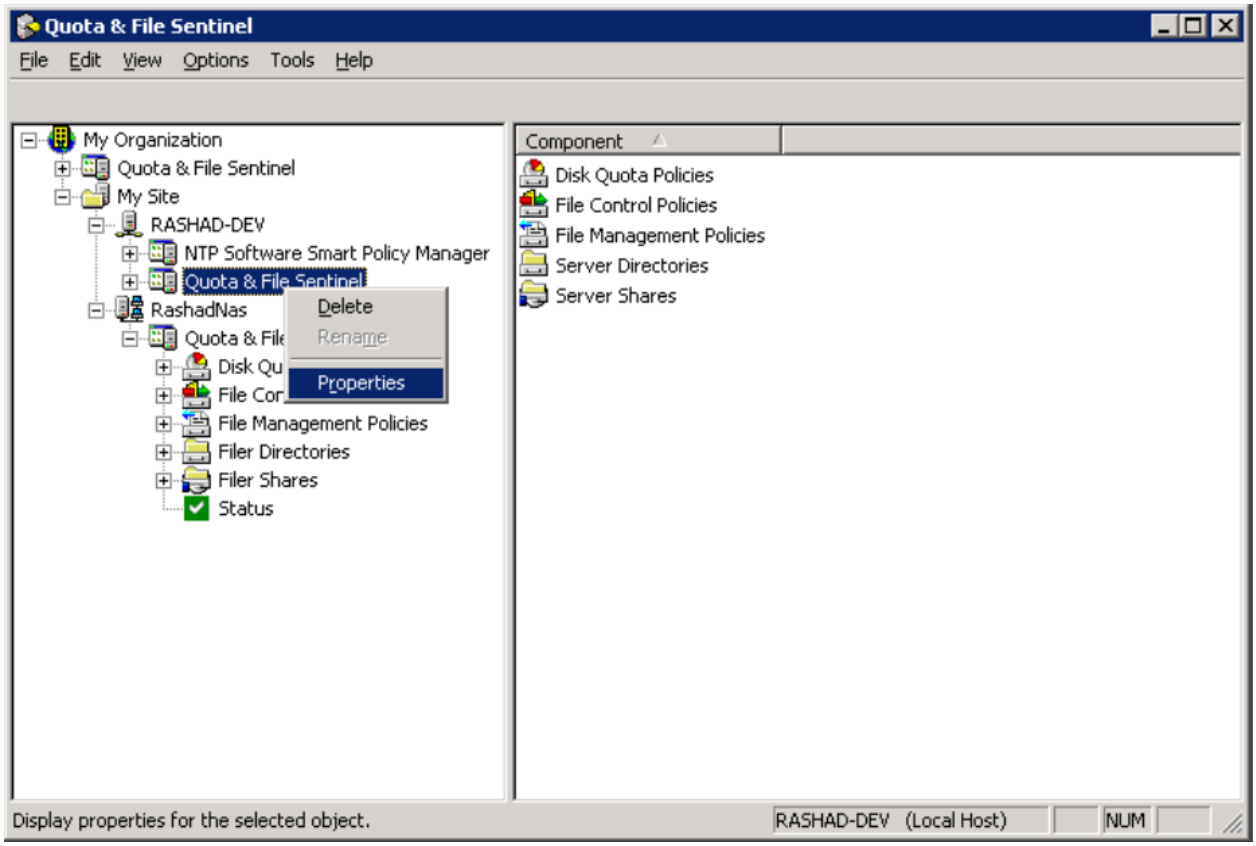
Add Storage Controller to NTP Software QFS for NAS Administration

Before you can use NTP Software QFS for NAS, you must add the storage controller to the NTP Software Smart Policy Manager hierarchy. To add the storage controller, complete the following steps:

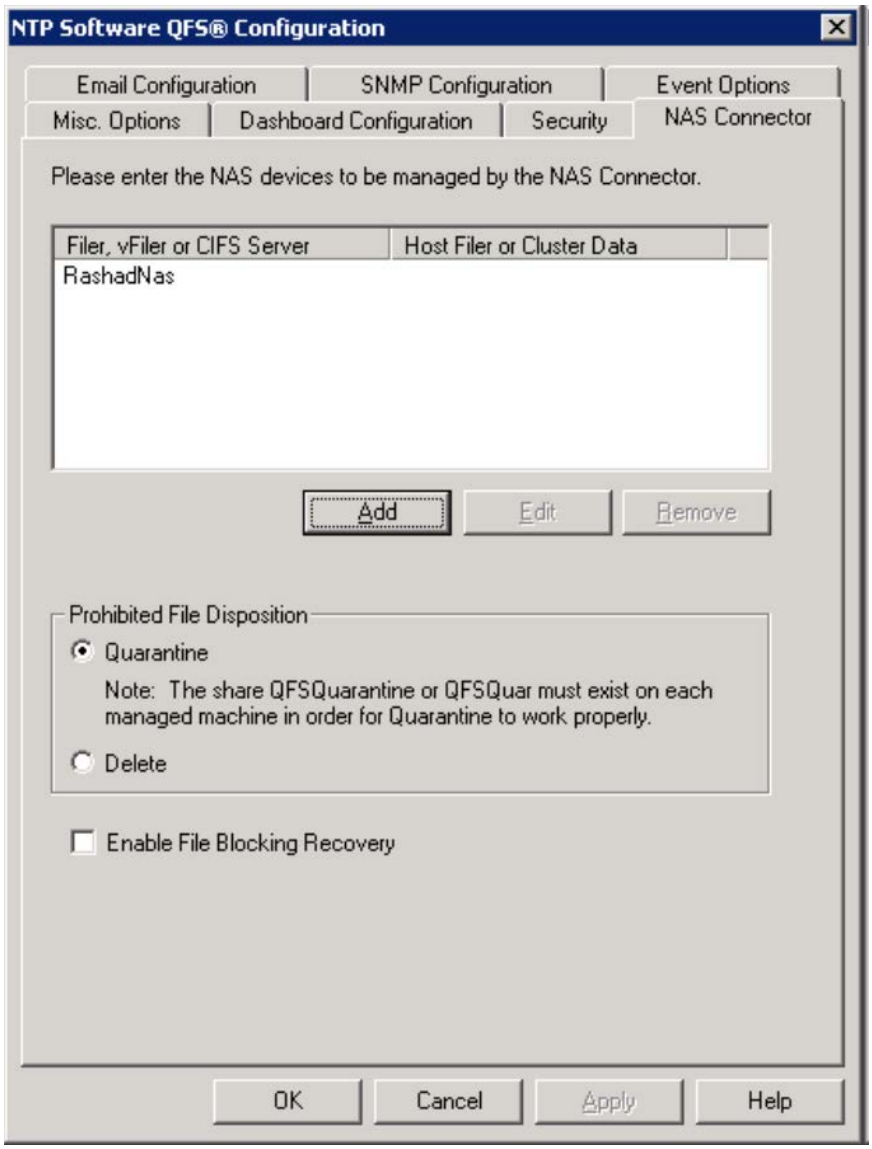
1. Click Start > All Programs > NTP Software QFS for NAS > NTP Software QFS for NAS Admin.
2. In the hierarchy presented, expand the location name you entered while installing the Smart Policy Manager. The default location is My Site. Your storage controller is listed in the right pane, below the server on which NTP Software QFS is installed.



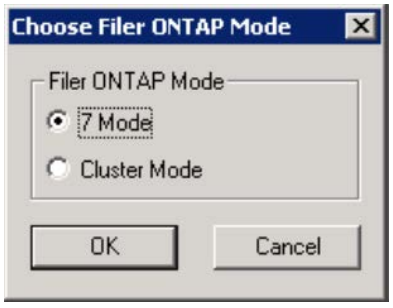
3. In the left pane, expand the server on which NTP Software QFS is installed and right-click Quota & File Sentinel. From the drop-down list, select Properties.



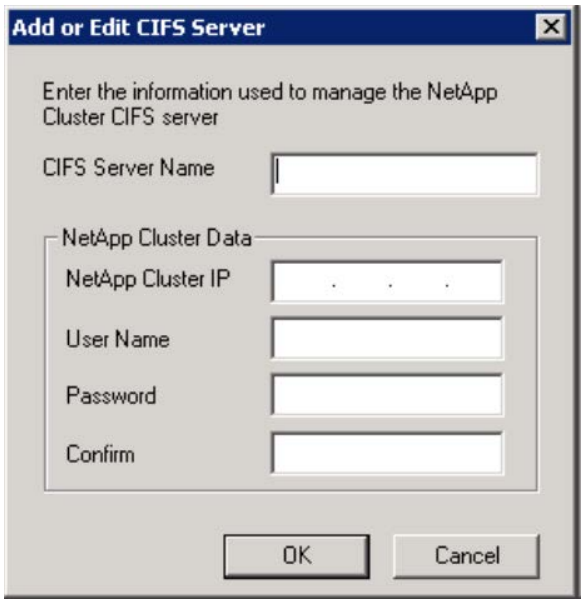
4. Click the NAS Connector tab. Your storage controller should be listed; if it is not, click Add.



5. Select either 7-Mode or Cluster-Mode, as appropriate for your version of Data ONTAP. Click OK.

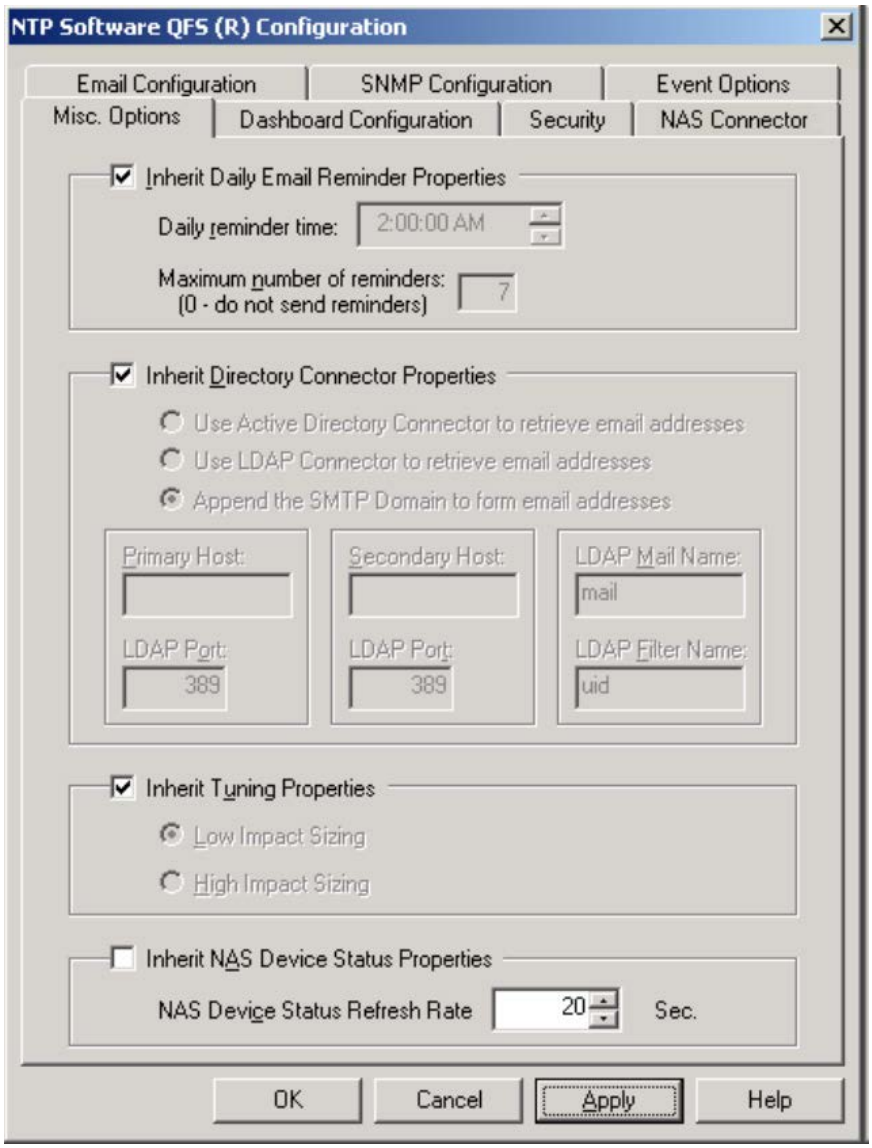


6. For clustered Data ONTAP storage controllers, enter the name of your CIFS server and the IP address of the cluster. Also add the user name and password for the account on the cluster that has permission to execute the ONTAPI APIs required by QFS. Click OK.



7. To configure the NAS device status refresh rate, click the Miscellaneous Options tab in the NTP Software QFS Configuration dialog box. The default refresh rate is 30 seconds, the minimum rate is 10 seconds, and the maximum rate is 3,600 seconds.

   Note: The refresh rate can be inherited from the global Quota and File Sentinel node in the QFS hierarchy.



Verify Registration with Storage Controller

To verify that the clustered Data ONTAP storage controller is associated with NTP Software QFS, complete the following steps:

1. Log in to the storage controller.
2. Run `fpolicy show-engine –vserver <vserver name of your managed CIFS server>` to view the FPolicy settings. The Vserver name of your CIFS server and its associated policies should display with the server status showing as connected:

```
dev-tap82F-cm5::> fpolicy show-engine –vserver vs1-rashad74
  (vserver fpolicy show-engine)
                                        FPolicy          Server         Server
Vserver Policy Name   Node              Server           Status         Type
------- ------------- ----------------- ---------------- -------------- -----------
vs1-rashad74                                             connected      primary
        NTPSoftware_  dev-tap82F-       10.20.2.121
        QFS           cm5-01
```

Note: QFS automatically creates and enables FPolicy for the managed CIFS server on the clustered Data ONTAP SVM. It uses the default sequence number 1 because the sequence number cannot be duplicated. If the sequence number is used by another FPolicy on the same Vserver, QFS does not enable FPolicy on the clustered Data ONTAP SVM.

Inside the connector registry key, QFS creates the `<CifsServerName>_FPolicySeqNum` registry value, which has the default value of `1`. If QFS fails to enable FPolicy because of a redundant sequence number, the user can configure this registry value to any unused sequence number. Then the user can run the diagnostic process on the managed CIFS server from the QFS administrator on the CIFS server-status node. The diagnostic process tries to enable FPolicy automatically by using the new sequence number configured in the registry.

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 the 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.

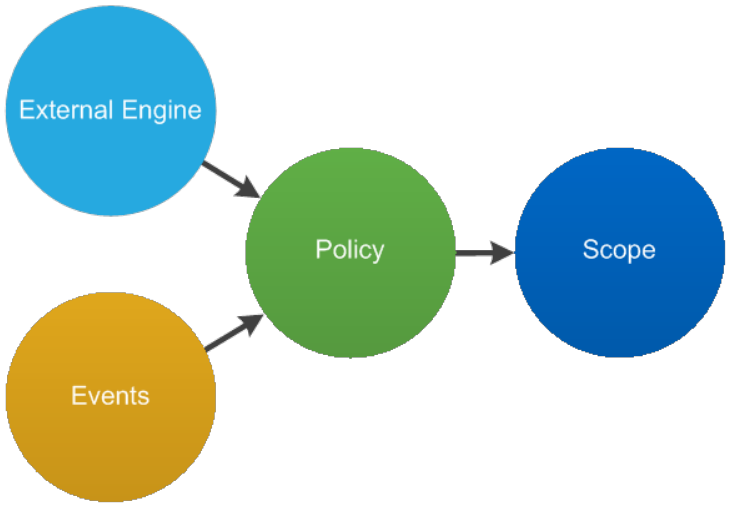
Configuration Requirements
• The shares must reside on the volume monitored for CIFS events. • The export policy must be created on and applied to the volume monitored for NFS events.

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

Figure 2) FPolicy configuration workflow.



Important Note

NTP Software QFS automatically pushes the FPolicy configuration onto clustered Data ONTAP as soon as an SVM is added to it.

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; NTP software QFS does not recommend making manual configurations.

If necessary, you can use the `show` commands in each section to compare the configuration that was pushed automatically.

5.2 Create FPolicy Event

To enable NTP Software QFS for NAS, NetApp Edition, to connect to a NetApp file server running clustered Data ONTAP, you must configure an FPolicy policy 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 Transmission Control Protocol (TCP), complete the following steps:

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

```
fpolicy policy event create -vserver <Vserver Name>
-event-name NTPSoftware_QFSEVT_CIFS -file-operations
create, create_dir, delete, delete_dir, open, close, rename, rename_dir -protocol cifs –volume-
operation true
```

   - For NFSv3, run the following command:

```
fpolicy policy event create -vserver <Vserver Name> -event-name NTPSoftware_QFSEVT_NFSv3 -file-
operations create, create_dir, delete, delete_dir, rename, rename_dir , write, setattr -protocol
nfsv3 –volume-operation true
```

   - For NFSv4, run the following command:

```
fpolicy policy event create -vserver <Vserver Name> -event-name NTPSoftware_QFSEVT_NFSv4 -file-
operations create, create_dir, delete, delete_dir, rename, rename_dir, write, setattr, open,
close -protocol nfsv4 –volume-operation true
```

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 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`

Option	Description
`-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 and verify an FPolicy external engine, run the following command:

```
fpolicy policy external-engine create -vserver
<Vserver Name> -engine-name NTPSoftware_QFSENG –primary
servers < IP address of FPolicy server> -port <random port no picked by QFS > -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 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 server authentication. • `mutual-auth`. Provides both server and NetApp authentication.

To view the external engine(s) 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  NTPSoftware_QFS -events
NTPSoftware_QFSEVT_CIFS,NTPSoftware_QFSEVT_NFSv3,NTPSoftware_QFSEVT_NFSv4
-engine  NTPSoftware_QFSENG -is-mandatory false –allow-privileged-access true –privileged-user-
name

The events attribute may be only one of the events event 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 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 NTPSoftware_QFS -volumes-to-include "*"
```

Table 4 lists the options for the FPolicy scope.

Table 4) FPolicy scope options.

Option	Description
`-vserver`	The name of the 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

NTP Software QFS uses the following command to automatically enable the new FPolicy policy at startup:

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

6 Security Login Configuration for FPolicy Server

To manage the CIFS server on a clustered Data ONTAP storage controller, you must provide the user name and password for a UNIX user on the clustered Data ONTAP storage controller. You must also give that user specific permissions.

To create a UNIX user account and assign it the permissions required for managing CIFS servers on a clustered Data ONTAP storage controller, complete the following steps:

1. Create a UNIX user on the clustered Data ONTAP storage controller:

```
unix-user create -vserver <vserver name> -user <user name> -id <user id> -primary-gid <primary
group id> -full-name <user full name>
```

2. Create the required role that contains the required permissions:

```
security login role create -role <role name> -cmddirname "network interface show" -access
readonly -query ""
security login role create -role <role name> -cmddirname "version" -access readonly -query ""
security login role create -role <role name> -cmddirname "volume show" -access readonly -query ""
security login role create -role <role name> -cmddirname "vserver show" -access readonly -query
""
security login role create -role <role name> -cmddirname "vserver cifs show" -access readonly -
query ""
security login role create -role <role name> -cmddirname "vserver fpolicy policy" -access all -
query ""
security login role create -role <role name> -cmddirname "vserver fpolicy show-engine" -access
readonly -query ""
security login role create -role <role name> -cmddirname "vserver fpolicy show" -access readonly
-query ""
security login role create -role <role name> -cmddirname "vserver fpolicy enable" -access all -
query ""
security login role create -role <role name> -cmddirname "vserver fpolicy disable" -access all -
query ""
security login role create -role <role name> -cmddirname "vserver fpolicy engine-connect" -access
all -query ""
security login role create -role <role name> -cmddirname "vserver name-mapping" -access all -
query ""
security login role create -role <role name> -cmddirname "vserver services unix-user show" -
access readonly -query ""
```

Note: You must specify the same role name in all of these commands to assign this single role at the end to the UNIX user created by the previous command.

3. Assign the role you created in step 2 to the user you created in step 1:

```
security login create -username <user name> -application ontapi -authmethod password -role <role
name>
```

Note: When you run this command, the storage controller asks you to enter and confirm a password for the user. The password you enter here is used along with the user name in the QFS administrator and wizard UI when you add the CIFS server to be managed by QFS.

7 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 has a performance effect 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. Ensure 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 performs inline monitoring of CIFS operations and sends notifications to the external server. It also 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 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 NTP Software QFS Best Practices

NetApp recommends the following best practices for using NTP Software QFS for NAS, NetApp Edition:

- Enable NetBIOS over TCP/IP on the server running Windows Server.
- When using SMB 2, confirm that it is enabled on storage as well as on the FPolicy server (the QFS machine).
- Disable FPolicy notifications on volumes that do not need to be managed (for example, `vol0`).
- Keep the management server within the same subnet of the SVM being monitored.

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 issues 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, modify `ssl-auth` to `no-auth` if the FPolicy server does not use SSL. 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
```

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 for generating 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 FPolicy-related statistics.

10.1 Collect and Display FPolicy Counters

To collect FPolicy counters, run the following commands:

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

To display FPolicy counters, run the following commands:

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

10.2 Counters to 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) `Policy_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 Monitoring from NTP Software QFS

NTP Software QFS records some statistics about the time required to process file operations on the storage controller. This information is contained in the log file `NCS YYYY-MM-DD.log` in the NTP Software QFS for NAS installation directory. The default path is `C:\Program Files (x86)\NTPSoftware\QFS for NAS`.

The following example excerpt is from log file `NCS 2015-05-17.log`:

```
2015/05/17`16:18:06.868`I`FPolicy stats`1860`FPolicy stats - Requests/sec = `4`Avg time = `97`Min
time = `10`Max time = `20`Avg Qtime = `0`Min Qtime = `0`Max Qtime = `0`Open Files = `138`
```

Note: The `Max time` value displays the performance of NTP Software QFS. Values higher than 500 indicate a problem.

References

This report refers to 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

From NTP Software:

- Installation Guide—NTP Software QFS for NAS, NetApp Edition
  http://www.ntpsoftware.com/downloads/installation-guide-ntp-software-qfs-nas-netapp-edition

Version History

Version	Date	Document Version History
Version 1.0	September 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.