Technical Report

# FPolicy Solution Guide for Clustered Data ONTAP: PeerSync from Peer Software

Brahmanna Chowdary Kodavali, Saurabh Singh, NetApp
Matt Marsala, Peer Software
May 2019 | TR-4472

NetApp®

TABLE OF CONTENTS



## LIST OF TABLES



## LIST OF FIGURES



# 1 Introduction

The NetApp® FPolicy® feature is a file-access notification system that allows an administrator to monitor file access in storage configured for Network File System (NFS and CIFS). Introduced for the scaled-out architecture of 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. FPolicy supports all SMB versions, including SMB 1.0 (CIFS), SMB 2.0, SMB 2.1, and SMB 3.0. It also supports major NFS versions, including NFSv3 and NFSv4.0.

FPolicy natively supports simple file-blocking use cases, which enables administrators to restrict end users' unwanted files. For example, an administrator can block audio and video files from being stored in data centers, saving storage resources. This feature blocks files only based on extension; for more advanced features, partner solutions have to be considered.

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

- File screening
- File-access reporting
- User and directory quotas
- Hierarchical storage management (HSM) and archiving solutions
- File replication
- Business file sharing and collaboration
- Data governance

## 1.1 Audience

The primary audience for this document is:

- Clustered Data ONTAP customers and prospective clients who want to implement a CIFS/SMB real-time file replication solution
- Data ONTAP operating in 7-Mode or Windows customers looking to transition to clustered Data ONTAP

## 1.2 Purpose and Scope

The purpose of this document is to provide an understanding of the FPolicy framework and to discuss various solutions that are built around PeerSync. 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 asynchronous or synchronous.

The use of asynchronous or synchronous communication depends on whether or not the FPolicy framework expects a notification response from the FPolicy server.

- Asynchronous notification is suitable for use cases such as monitoring and auditing of file-access activity that do not require Data ONTAP to take action based on the FPolicy server's notification response. In these cases, Data ONTAP does not need to wait for a response from the FPolicy server. Monitoring and auditing file-access activity, file replicating, and file collaborating require asynchronous notification.

- Synchronous notification is suitable for use cases in which Data ONTAP must allow or deny client access based on the notification response from the FPolicy server. Use cases such as quotas, file screening, and file archiving recall require synchronous notification.

**Role of Clustered Data ONTAP Components in FPolicy Configuration**

The following components play a role in FPolicy configuration:

- **Administrative SVM (cluster).** The administrative storage virtual machine (SVM, formerly 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 SVM.** 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 admin SVM can be leveraged by 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 FPolicy configuration. The data LIFs used for these connections can fail over in the same manner as data LIFs used for normal client access.

## 2.1 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 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 over an authenticated session
- Establishes a connection with the data LIFs on all nodes participating in the SVM

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 the permissions 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 the privileged data path does not generate an FPolicy notification.

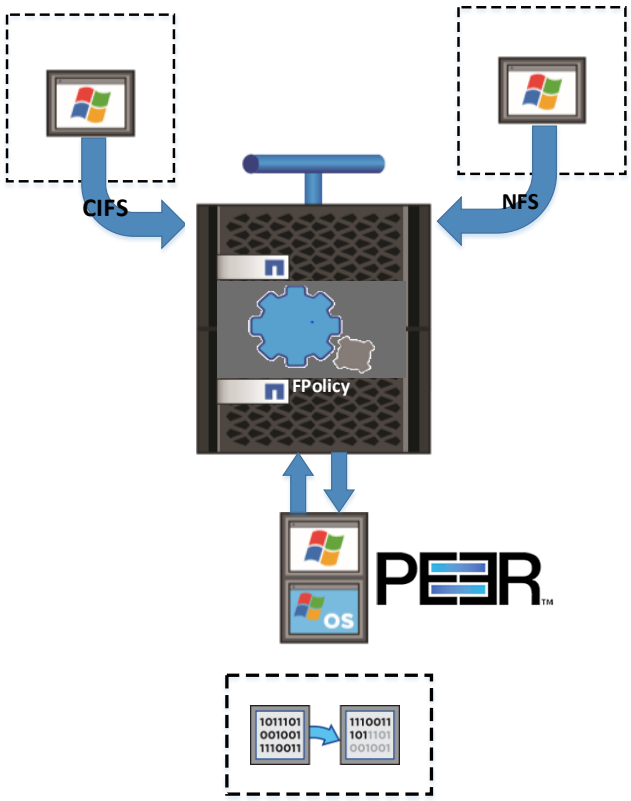
For more information about FPolicy functionality, see Clustered Data ONTAP 8.3 File Access Management Guide for CIFS on the NetApp Support site.

# 3 FPolicy Solution Architecture

The FPolicy solution consists of the clustered Data ONTAP FPolicy framework and the FPolicy application PeerSync, as shown in Figure 1.

**Figure 1) FPolicy solution architecture.**




The FPolicy application software is installed on 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 FPolicy framework.

## 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: PeerSync

PeerSync application software was created to efficiently keep two or more file servers in sync and in real time, whether in the same data center or across the globe. Developed over 20 years of continuous refinement and customer input, the PeerSync file-based replication engine works across platforms between Windows file servers, clustered Data ONTAP, Cloud ONTAP® solutions, and Data ONTAP 7-Mode systems. It can be deployed between any number of file servers, from two to a few thousand:

- Bidirectional real-time replication of user home directories
- General file replication and distribution for NetApp environments

## 3.3 Main Features

Some of the main features of the PeerSync application software are:

- Real-time file replication
- Cross-platform support for Windows, clustered Data ONTAP, Cloud ONTAP solutions, and Data ONTAP 7-Mode
- Multiple connectivity options
- Bandwidth optimization for WAN links
- Multithreading support for high-speed scan and sync operations
- Centralized management and monitoring using a web-based management console
- Byte-level replication
- NFSv3 support for clustered Data ONTAP and Data ONTAP 7-Mode environments
- Easy software-based installation and unobtrusive operation
- E-mail and admin reporting and alerts
- Full support for DFS namespaces
- Unicode compliance

## 3.4 Components

The main components of PeerSync are:

- **PeerSync profiler/engine.** Handles configuration, monitoring, management, and all actual replication.
- **PSListener.** A lightweight agent that enables two features of PeerSync: namely, its byte-level replication technology and its TCP communication mechanism between sites using WAN-based connectivity.
- **Peer Management Center (PMC).** Designed to manage and monitor multiple instances of PeerSync applications deployed across a company's infrastructure, from a single Windows and web-based console.

## 3.5 Solutions

PeerSync's engine is the centerpiece of several different solutions that offer value to clustered Data ONTAP customers and prospective clients. Some of these solutions are:

### Solution 1: Continuous Data Protection for Data ONTAP 7-Mode and Clustered Data ONTAP (a NetApp SnapMirror Alternative)

PeerSync's integration with FPolicy allows it to perform real-time file-level replication for continuous data protection between any combination of Data ONTAP 7-Mode and clustered Data ONTAP. This replication

can be efficiently performed locally within a single data center or between locations through a WAN, VPN, or dedicated link.

PeerSync's real-time replication capability allows it to help with phased clustered Data ONTAP transition projects that involve multiple Data ONTAP 7-Mode controllers. Here PeerSync can be used as a SnapMirror® deployment alternative until all controllers have been transitioned to clustered Data ONTAP.

**Figure 2) Continuous data protection for Data ONTAP 7-Mode (graphic supplied by Peer Software).**

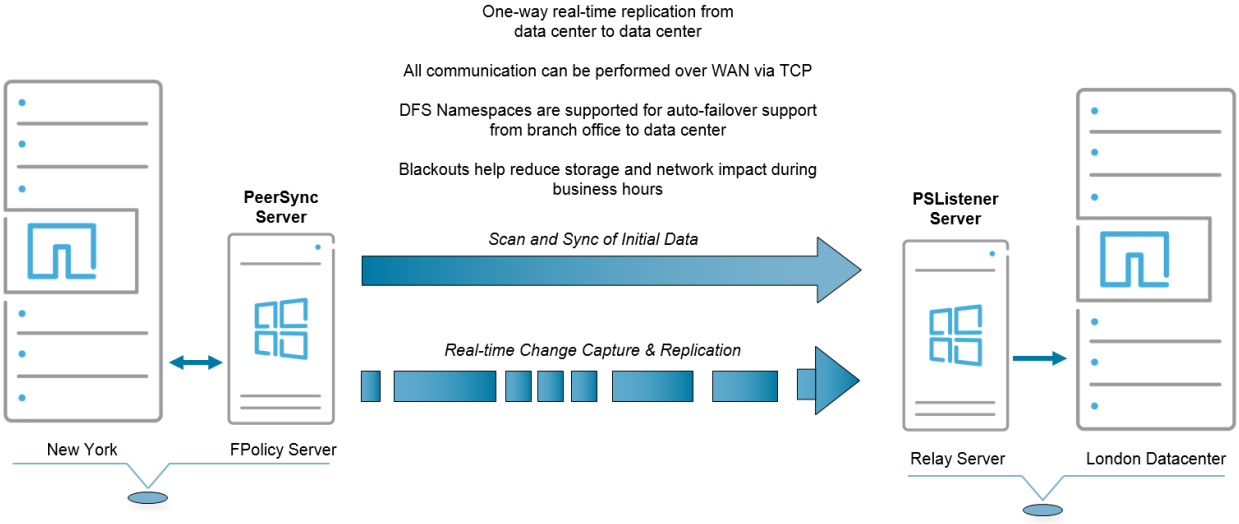



Figure 2 shows simple WAN-based real-time replication architecture, representing a standard two-controller deployment of PeerSync as a SnapMirror alternative.

- The NetApp device in New York is fronted by an FPolicy server running PeerSync.
- The NetApp device in London is fronted by a Windows relay server running the PSListener.
- When started, PeerSync performs an initial scan and sync of all files and folders from the New York NetApp device to the London NetApp device. If a SnapMirror relationship existed in this direction, PeerSync can be set to simply use this content after breaking the relationship.
- PeerSync uses FPolicy to stay up-to-date on activity that occurs on the NetApp device in New York. As changes are reported to PeerSync, it replicates those changes to the NetApp London device.
- Data ONTAP 7-Mode could be running on the NetApp device in New York and clustered Data ONTAP in London, or vice versa.

## Solution 2: Continuous Data Protection from Windows to Clustered Data ONTAP (an OSSV Alternative)

PeerSync's real-time replication engine also integrates directly with Windows file servers. It offers continuous data protection from branch office Windows file servers to a clustered Data ONTAP system deployed in a central data center.

PeerSync offers a solution for environments that need remote Windows file server backup to a central data center that has transitioned to clustered Data ONTAP. PeerSync can also be paired with ImageX/DISM to replicate a full system state on a scheduled basis, in addition to continuous data protection offered by its real-time engine.

**Figure 3) Remote office backup on clustered Data ONTAP (graphic supplied by Peer Software).**

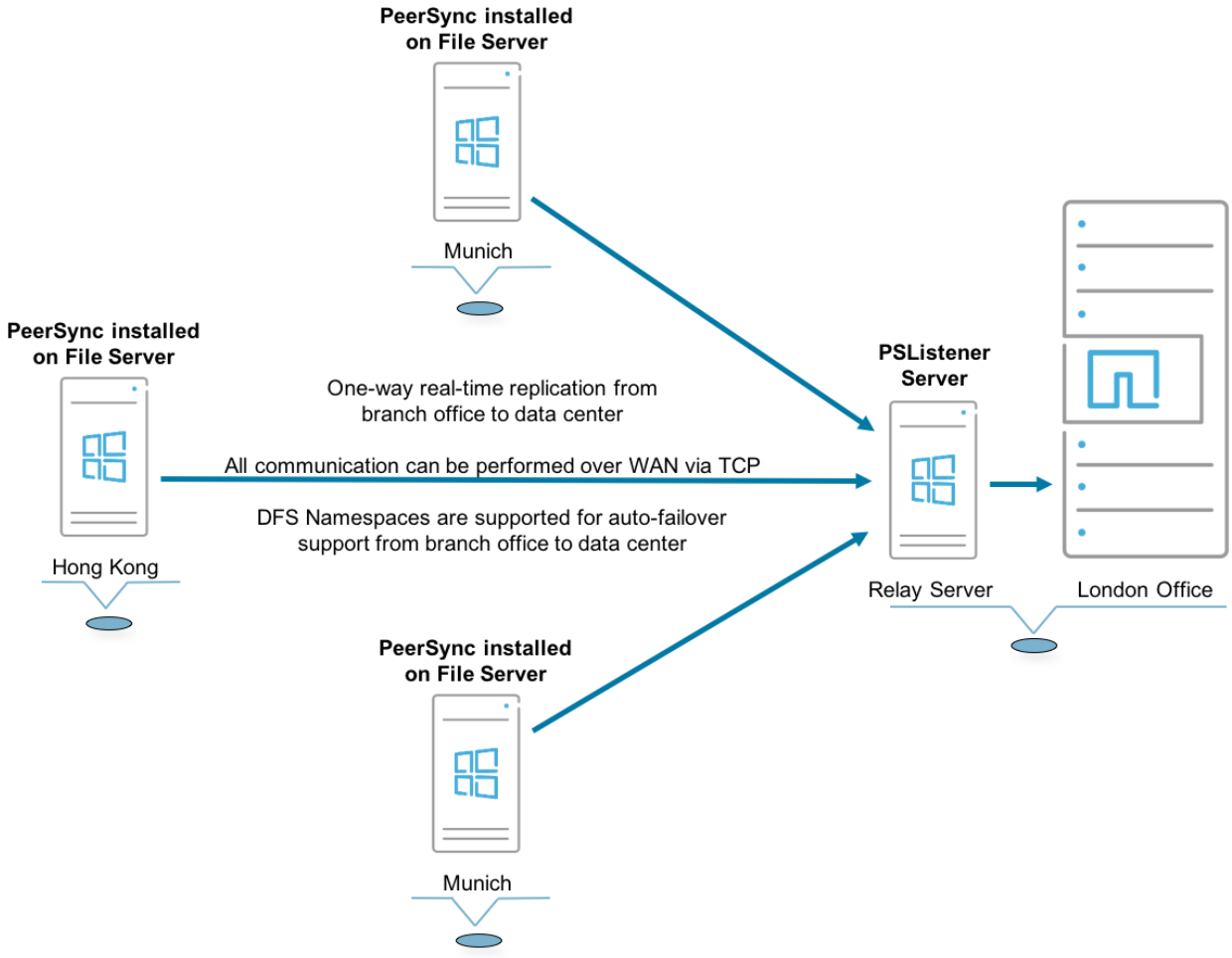



Figure 3 shows a simple PeerSync backup architecture covering three remote office Windows file servers:

- Each copy of PeerSync performs an initial scan and sync of files and folders as depicted in Figure 2, using the PSListener server in London to relay the changes to the London NetApp device as the backup target.
- PeerSync listens for and replicate changes in real time both during and after the initial scan.
- In the event that backups of full system state are required, PeerSync can work with ImageX/DISM to generate a full image of the remote file server on a scheduled basis and then replicate changes to that image to London.

## Solution 3: Cross-Platform File Migration Enabling Streamlined Data Reorganization

PeerSync's replication engine is well suited for file-level migration projects, whether it is from Data ONTAP 7-Mode to clustered Data ONTAP or Windows to clustered Data ONTAP. Its real-time capabilities minimize the final cutover window by eliminating the requirement for a final scan. Because PeerSync works directly with files and folders, data reorganization is easily accomplished as part of the migration itself. In addition, PeerSync can help with subvolume transitions (such as qtree breakouts), controller consolidation, and fan-in/fan-out.

**Figure 4) Data reorganization example: qtree breakout.**

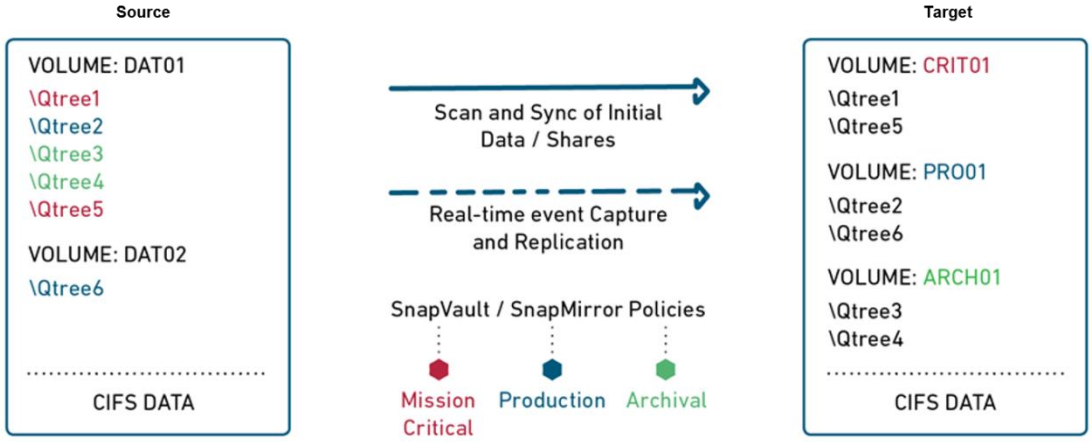



Figure 4 illustrates Data ONTAP 7-Mode to clustered Data ONTAP migration that involves the reorganization of qtrees (subvolume transition):

- On the Data ONTAP 7-Mode source, various qtrees exist across two volumes, in which each qtree has its own Snapshot® policy.
- When transitioning to clustered Data ONTAP, all qtrees with similar Snapshot copy policies should be colocated on the same volume.
- PeerSync is configured to perform the data reorganization during the initial scan and sync.
- PeerSync's FPolicy integration keeps the qtree and volume structure on the target clustered Data ONTAP system in sync and in real time. Therefore, a final scan is not required during cutover.

## Solution 4: Fallback Coverage for Clustered Data ONTAP Transition

PeerSync can also provide clustered Data ONTAP customers and prospective clients with a posttransition fallback plan. Fallbacks are not desired in a transition process but are still possible. The PeerSync real-time replication engine based on FPolicy provides reliability so that the newly transitioned clustered Data ONTAP system is replicated to the original source system (Data ONTAP 7-Mode or any other source) for as long as is necessary. Fallback becomes as simple as moving user access back to the original source system.

**Figure 5) Transition fallback coverage (graphic supplied by Peer Software).**

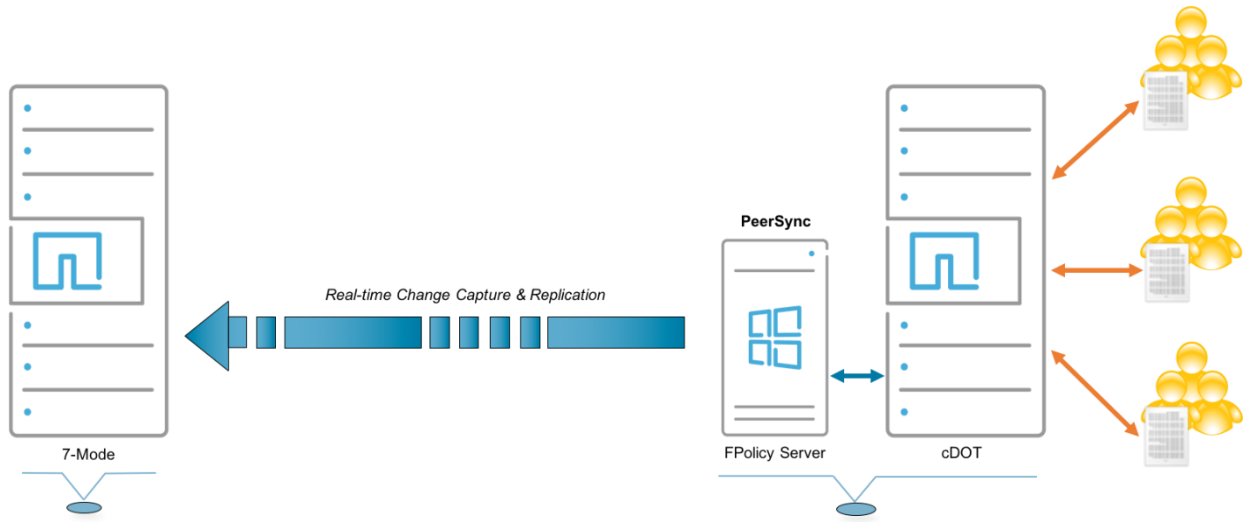


Figure 5 shows the architecture of a simple transition fallback scenario involving clustered Data ONTAP and Data ONTAP 7-Mode:

- The PeerSync FPolicy server fronts the clustered Data ONTAP system and is enabled before access is granted to end users.
- Unlike in Figure 2, this scenario does not require PeerSync to perform an initial scan and sync.
- The FPolicy framework notifies PeerSync as changes occur in real time. PeerSync pushes these changes back to the Data ONTAP 7-Mode system.
- If fallback to the Data ONTAP 7-Mode system is required, it is already in sync and ready for a cutback window.

## Solution 5: Bidirectional Real-Time Replication of User Home Directories

PeerSync can be deployed to keep user home directories in sync across two or more data centers running clustered Data ONTAP. PeerSync's FPolicy integration provides the ability to detect and sync changes between data centers in real time, allowing multiple data centers to host active copies of user data. When integrated with DFS namespace, roaming users are always able to access the closest up-to-date copy of their directory.

A common use case for this solution is VDI deployments spanning more than one data center. Virtual user desktops can be hosted out of two or more data centers for load-balancing and/or DR. With PeerSync keeping user home directories in sync between all data centers, a user always has high-speed access to his or her home directory, regardless of where the virtual desktop is running.

**Figure 6) Home directory replication between active data centers (graphic supplied by Peer Software).**

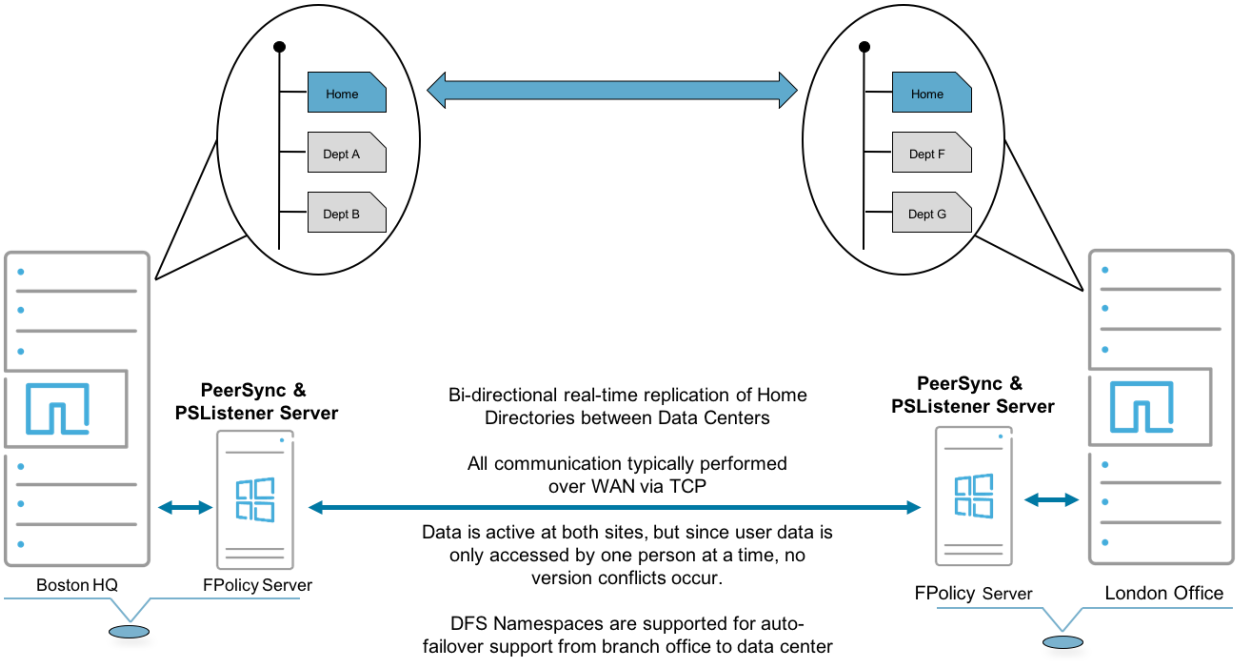



Figure 6 shows a deployment of PeerSync in a home directory replication scenario between two data centers:

- PeerSync and the PSListener are both installed on an FPolicy server fronting both NetApp devices.
- PeerSync works together at both sites to perform the initial scan and sync of the "home" structure between Boston and London.

- If a user is working out of the Boston location and modifies some documents in the home directory, PeerSync in Boston detects this change using FPolicy and syncs just the bytes that have changed in each file to London.
- If the same user then travels to London, the user has local access to the most updated copies of her or his home directory. Any changes made while the user is in London are sent back to Boston automatically.

## Solution 6: General File Replication and Distribution for NetApp Environments

PeerSync's flexible real-time, file-level replication engine can handle many other cross-platform replication scenarios.

As an example, a common use of PeerSync is file distribution. PeerSync's FPolicy integration allows it to push content in real time as it changes from a central clustered Data ONTAP device to several remote file servers, workstations, and/or laptops.

**Figure 7) File distribution from clustered Data ONTAP to remote offices (graphic supplied by Peer Software).**

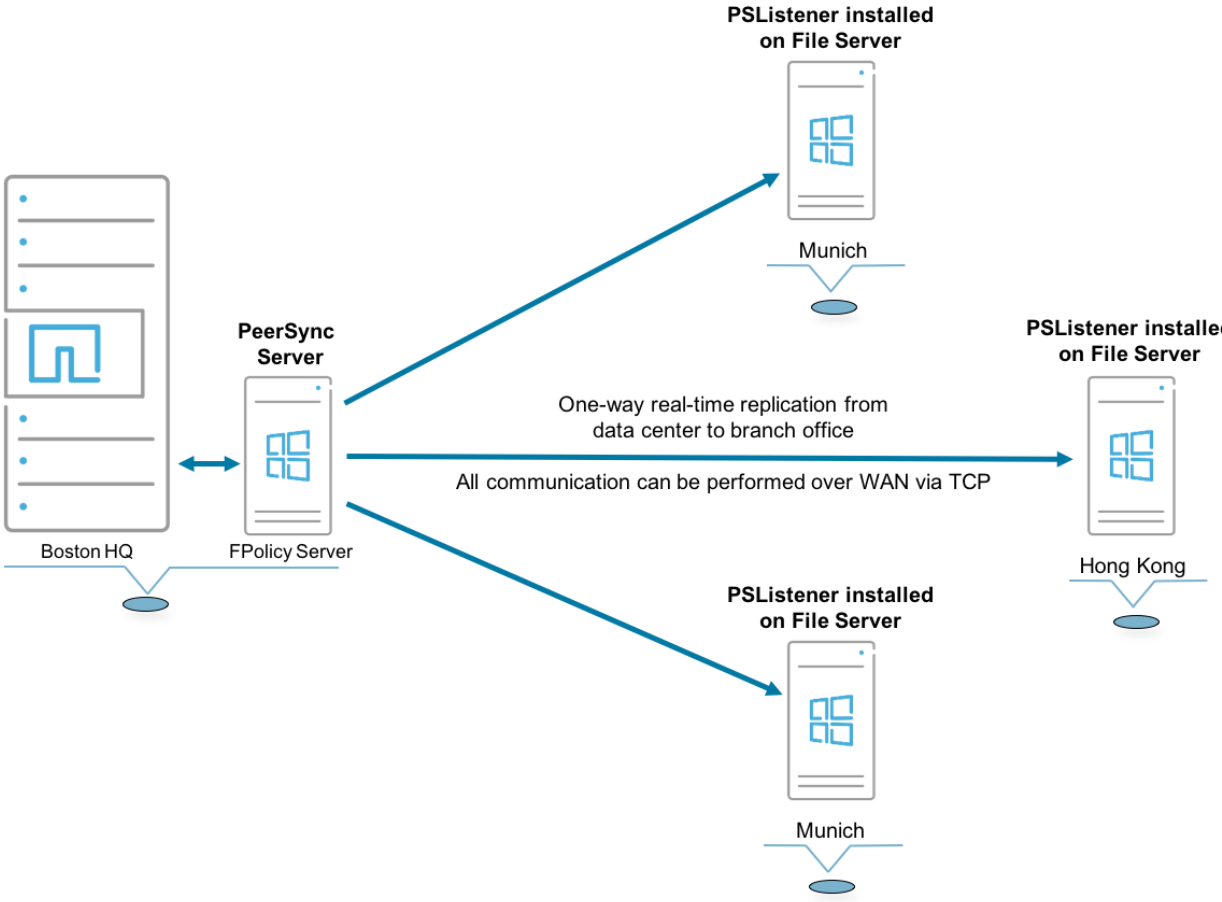



Figure 7 illustrates a file distribution scenario from Boston to remote offices around the globe:

- PeerSync is installed on an FPolicy server fronting the clustered Data ONTAP system in Boston.
- As additions and changes are made to monitored content on the clustered Data ONTAP system, they are detected by FPolicy and replicated to remote offices automatically.

## 3.6 NFSv3 Support

PeerSync now offers its real-time replication engine based on FPolicy for NFSv3 environments based on NetApp. NFSv3 support is available in a majority of the solutions centered on NetApp mentioned in section 3.5, with the exception of “Solution 2: Continuous Data Protection from Windows to Clustered Data ONTAP (an OSSV Alternative).”

The majority of PeerSync’s functionality set remains, though the architecture is slightly different. PeerSync is installed on a Windows FPolicy server in front of a NetApp device. However, NFSv3 support requires the addition of at least one Linux-based server alongside the FPolicy server.

**Note:** PeerSync does not currently support NFSv4.

**Figure 8) Migration architecture for NFSv3 (graphic supplied by Peer Software).**

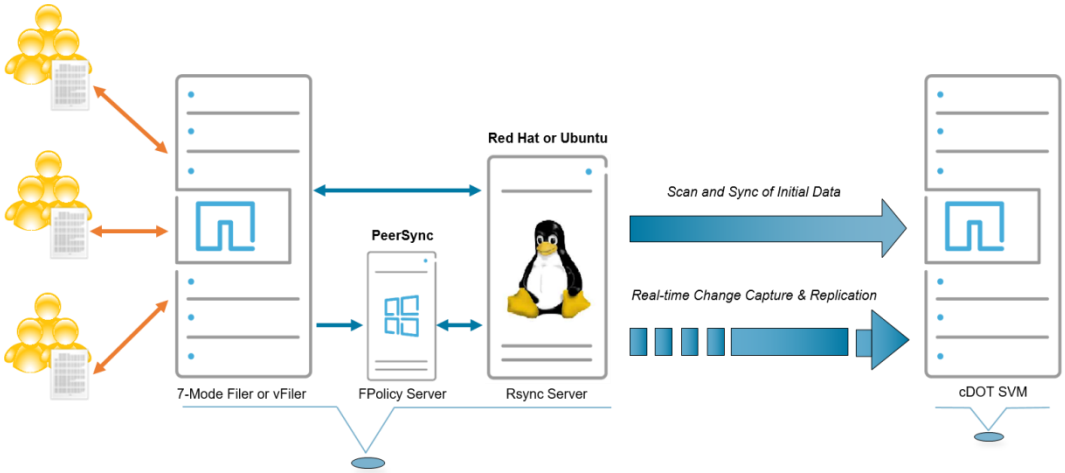



Figure 8 shows the architecture of a Data ONTAP 7-Mode to clustered Data ONTAP migration over NFSv3:

- The PeerSync FPolicy server fronts the Data ONTAP 7-Mode system with a Linux-based Rsync server alongside it.
- The FPolicy framework notifies PeerSync in real time as changes occur. PeerSync offloads all scans and file transfers to the Rsync server and reports when the operations are complete.
- The Rsync server leverages Rsync to perform the actual file replication and directory scans. The use of Rsync also makes sure that permission structures are kept in sync.

**Figure 9) WAN-based CDP architecture for NFSv3 (graphic supplied by Peer Software).**

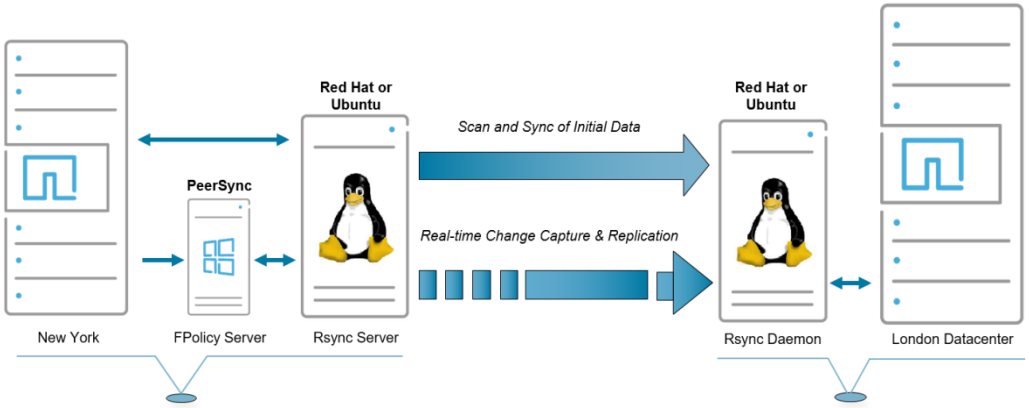


Figure 9 shows a simple WAN-based, real-time NFS replication architecture representing a standard two-controller deployment of PeerSync as a SnapMirror alternative:

- The NetApp device in New York is fronted by an FPolicy server running PeerSync, with a Linux-based Rsync server alongside it.
- The NetApp device in London is fronted by an Rsync daemon relay server.
- As seen in Figure 8, FPolicy framework notifies PeerSync in real time as changes occur. PeerSync offloads all scans and file transfers to the Rsync server and reports back when operations are complete.
- The Rsync daemon provides highly optimized WAN communication between the New York and London NetApp devices to facilitate replication.
- Data ONTAP 7-Mode could be running on the NetApp device in New York and clustered Data ONTAP in London, or vice versa.

For details, see PeerSync for NFS - Prerequisites.

For more information about PeerSync's NFSv3 support, e-mail sales@peersoftware.com.

# 4 Installing and Configuring PeerSync

## 4.1 Software Requirements and Installation

Each component of PeerSync has its own requirements and recommendations:

- For up-to-date details about the PeerSync environmental requirements, see http://www.peersoftware.com/resources/tech-briefs.html?view=document&id=85.
- For up-to-date details about clustered Data ONTAP environments that require that additional prerequisites be met, see http://www.peersoftware.com/resources/tech-briefs.html?view=document&id=85.
- Data ONTAP 7-Mode environments require additional prerequisites. For up-to-date details, see http://www.peersoftware.com/resources/tech-briefs.html?view=document&id=82.
- In order to install PeerSync, installers and license keys must be obtained from Peer software. Trials can be requested by using the form available at http://www.peersoftware.com/trial-software.html.

## 4.2 Configuring PeerSync for NetApp Sources

FPolicy is used if real-time detection is required on a clustered Data ONTAP source. This is regardless of the desired PeerSync solution or configuration. Before configuring PeerSync to work with NetApp sources, it is important to understand how it interacts with NetApp systems using FPolicy.

**Figure 10) How PeerSync works with FPolicy (graphic supplied by Peer Software).**

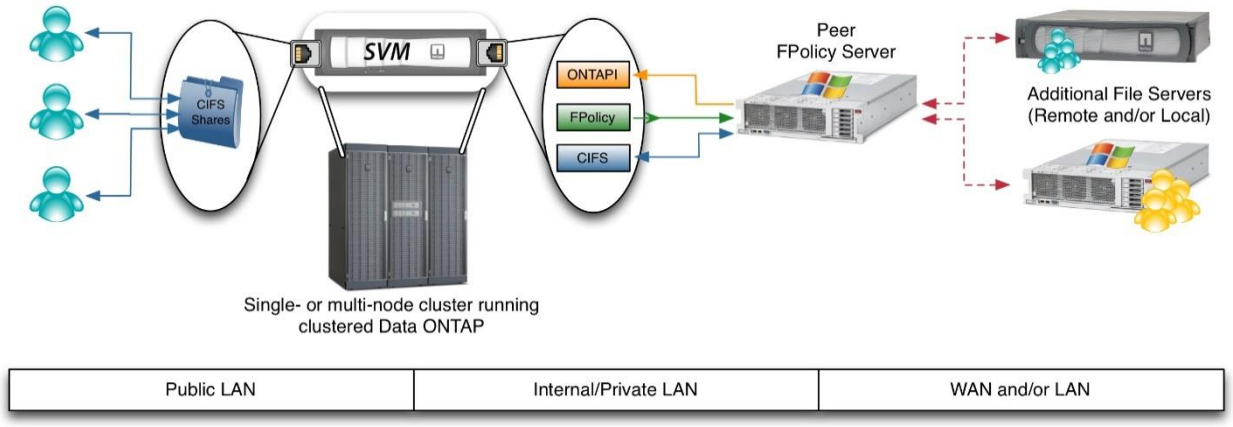



Figure 10 is an illustration of how PeerSync software products interact with clustered Data ONTAP systems. Reading from left to right:

- Users interact with the CIFS/SMB shares or NFS exports on an SVM using a “public” LAN.
- The SVM runs on top of a cluster of one or more nodes, each of which runs clustered Data ONTAP. The physical nodes supply all storage and physical network connections to the SVM.
- Users and PeerSync servers acting as FPolicy servers work with the SVM using logical interfaces (LIFs) configured on the SVM.
- When activity occurs on the SVM through these shares, the PeerSync FPolicy server is notified by the FPolicy framework. The PeerSync FPolicy server then interacts with the same content using CIFS/SMB. In the case of NFSv3, the FPolicy server offloads any replication to be performed to a Linux-based Rsync server.
- Perform the PeerSync FPolicy server’s interaction with the SVM using a private LAN. The PeerSync FPolicy server then coordinates replication to one or more targets.

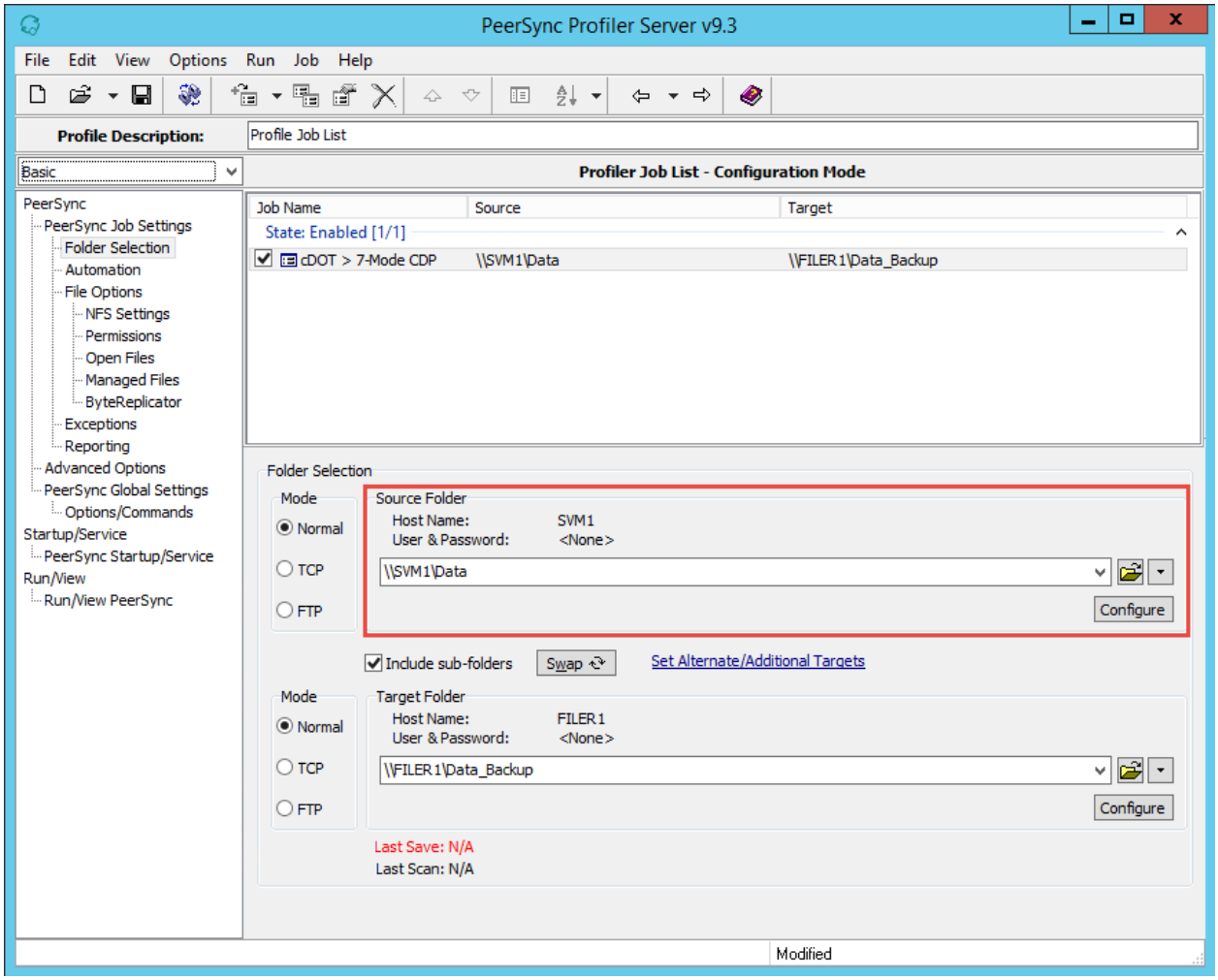
When all elements of the PeerSync system are installed and all prerequisites for NetApp deployments have been met, a replication job can be created from the PeerSync profiler and configured for use with clustered Data ONTAP.

## 4.3 Configuration Steps

| Note |
| --- |
| The following configuration steps are tailored to enable real time with clustered Data ONTAP as a source. Steps 2, 3, and 4 are slightly different when enabling real time with Data ONTAP 7-Mode or Windows as a source. In addition, NFSv3 deployments require some additional steps.<br>For details, e-mail sales@peersoftware.com. |

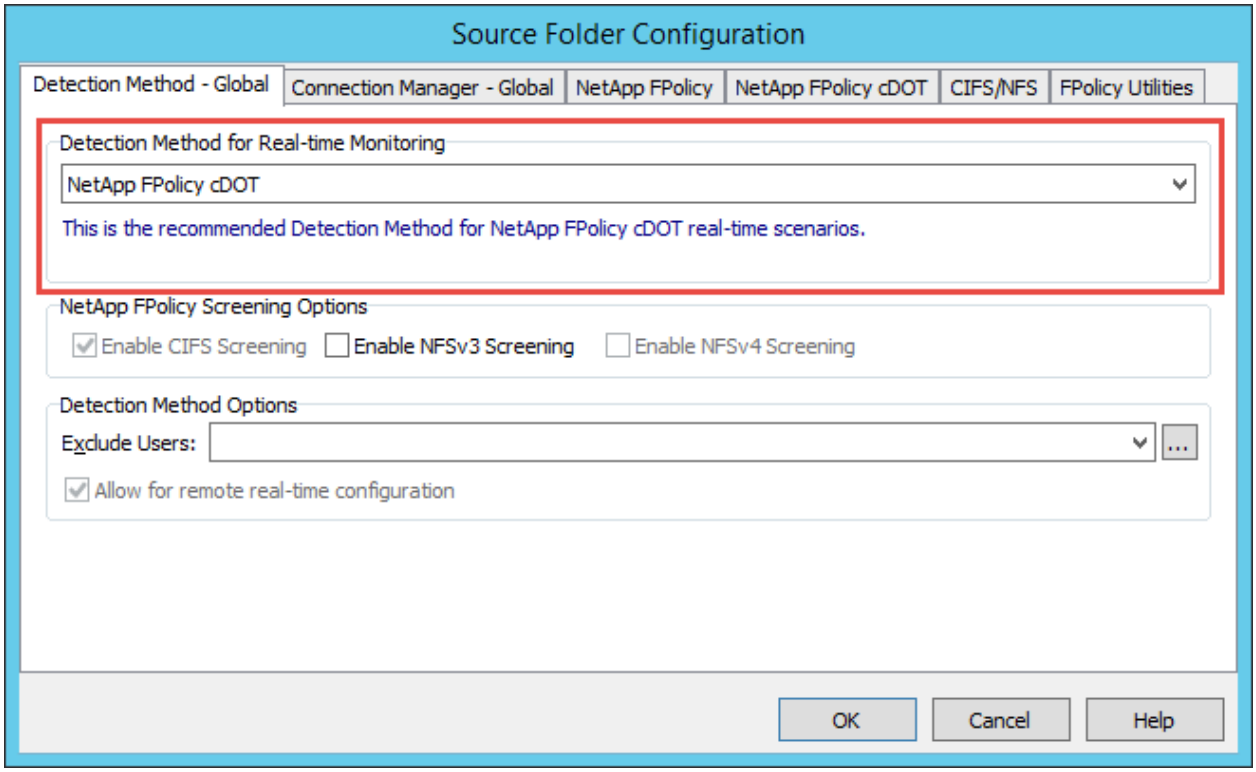
1. Create a new job within the PeerSync profiler. Go to File > New > click Add New Job.
2. In the Folder Selection dialog box, enter a CIFS-based path on the local clustered Data ONTAP SVM to the source folder section. Configure the target folder and mode as required. The source path is `\\SVM1\Data`. The target path is set to `\\FILER1\Data_Backup`, which is a share on Data ONTAP 7-Mode.



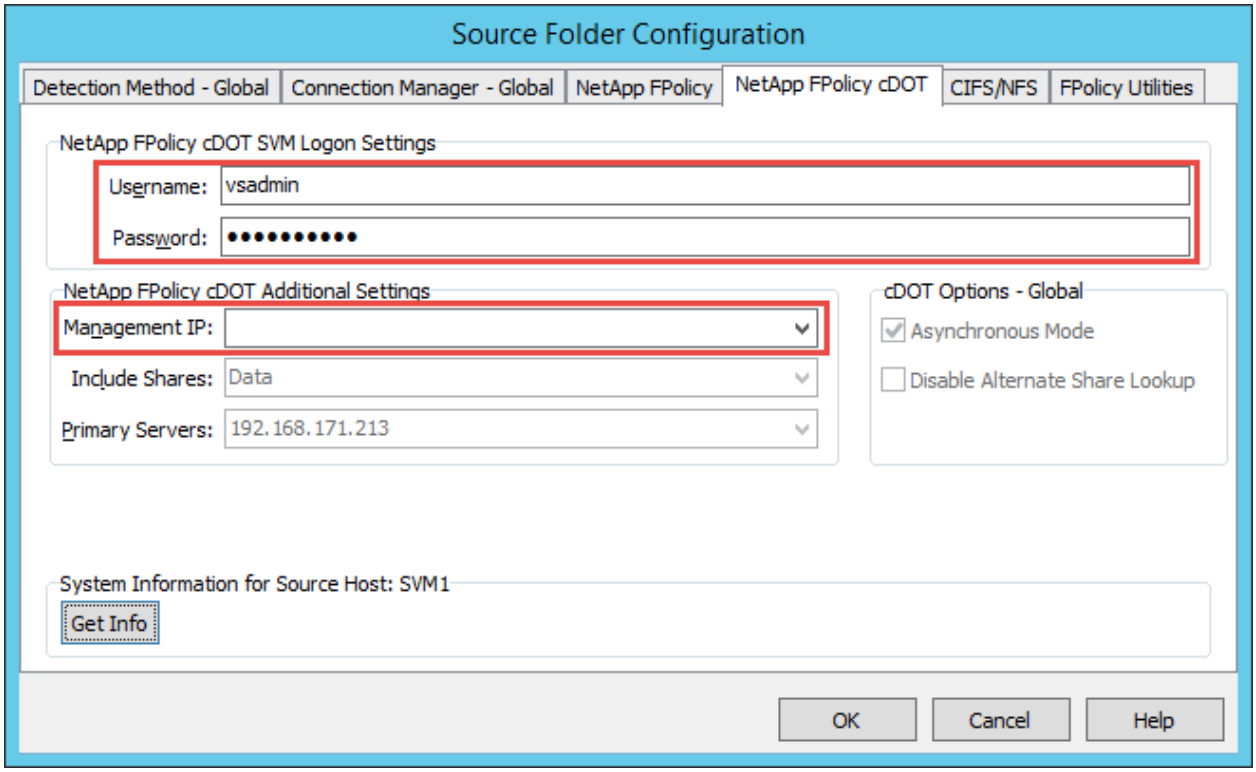

3. Under the Source Folder, click Configure and select NetApp FPolicy cDOT.



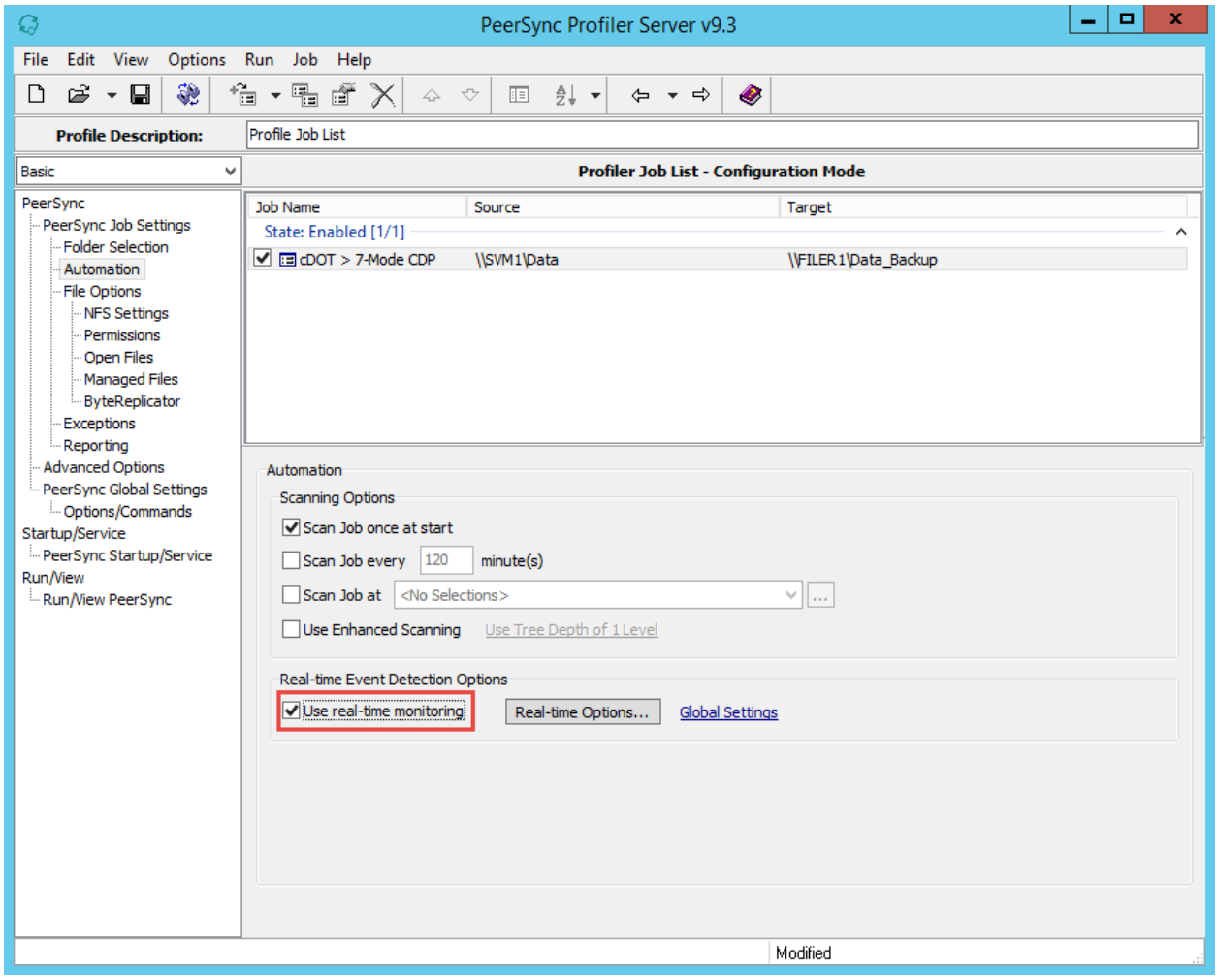

4. Configure the NetApp FPolicy cDOT SVM log-in credentials. The management IP value may also need to be set, depending on the environment. The remaining options should be left at their default settings:
   a. **Username.** The user name of the VSAdmin or similar account on the SVM that has appropriate access to ONTAPI®. In the following screenshot, this value is set to `vsadmin`.
   b. **Password.** The password of the VSAdmin or similar account on the SVM that has appropriate access to ONTAPI.
   c. **Management IP** (optional). If the primary data LIF for the SVM whose IP address is registered in DNS does not support management calls, enter the management IP address of the SVM in the relevant field.




5. Click OK in the previous figure. The automation screen in the main PeerSync profiler window opens. Select the Use real-time monitoring checkbox.




PeerSync is now all set to use FPolicy real-time detection. This configuration can be saved. PeerSync can be started by going to the Run menu and selecting Launch Current Profile.

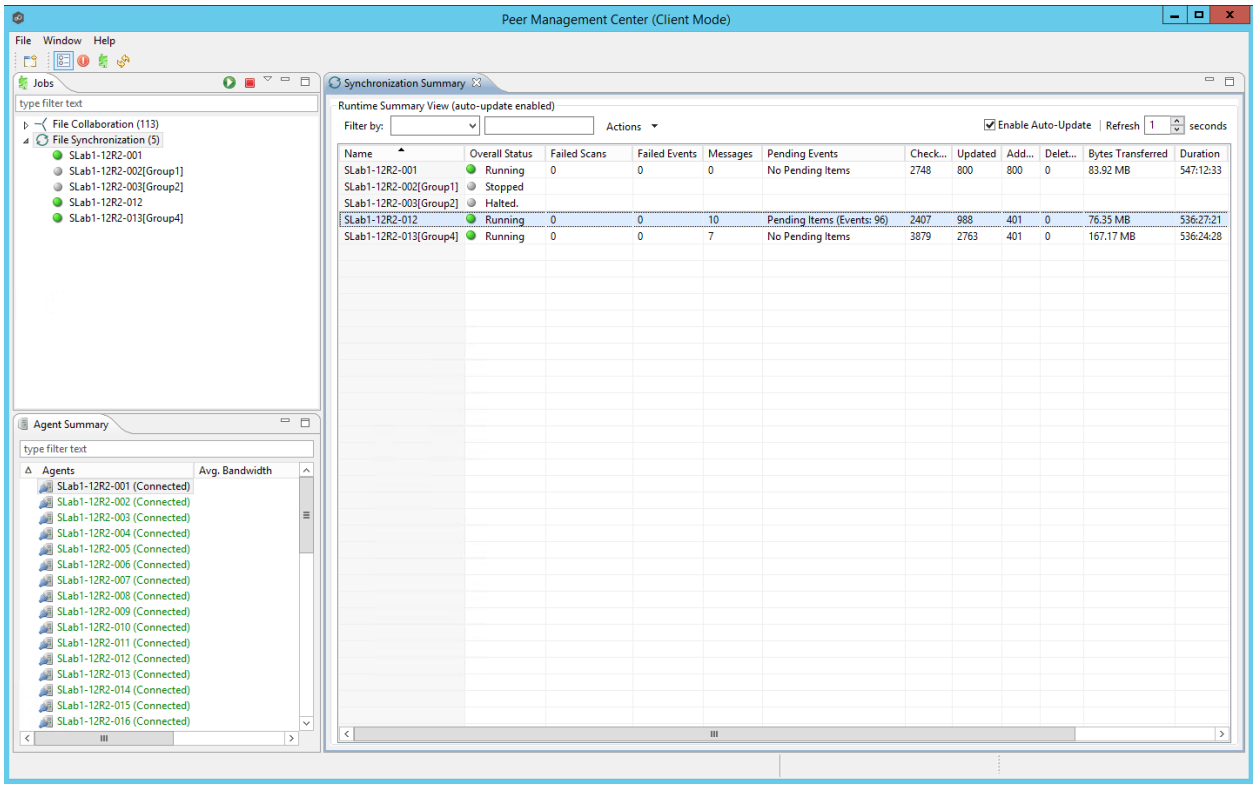
## 4.4 Central Management and Monitoring

PMC is a management and monitoring tool that is available with PeerSync v9.3.1. The PMC works across Peer software's file replication and collaboration solutions, providing users with a single pane for file management. All management is performed using a Windows-based application, as seen in the following figure, or by using a matching web application. For PeerSync solutions, the PMC provides options for deployment, management, and monitoring of PeerSync installations across any number of locations and servers.

For more details about the PMC, contact sales@peersoftware.com.

**Figure 11) Peer management center.**




# 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 instance 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. The scope also allows you to include and exclude all relevant filters.

| Configuration Requirements |
| --- |
| • CIFS/SMB shares must reside on a volume monitored for CIFS events.<br>• NFS exports must reside on a volume monitored for NFSv3 events. |

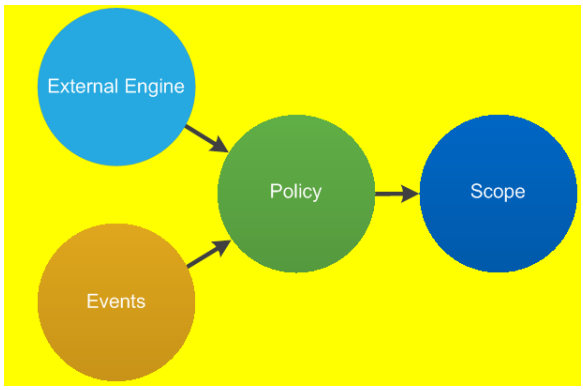
## 5.1 FPolicy Configuration Workflow

Figure 12 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 12) FPolicy configuration workflow.**




| Note |
| --- |
| When configured to work with clustered Data ONTAP, PeerSync automatically configures FPolicy on the SVM.<br>Sections 5.2 through 5.6 explain the commands used by the application in the background to configure the different components. These are strictly for reference only.<br>Manual configurations are not recommended and not supported by PeerSync software. If required, you may use the “show” commands in each section to review PeerSync’s automatic FPolicy configuration. |

## 5.2 Create an FPolicy Event

To enable the application server to connect to a NetApp file server running clustered Data ONTAP, you must configure an FPolicy instance 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 NetApp Data ONTAP management.
2. To create and verify an FPolicy event object, run the following command:

```
fpolicy policy event create -vserver <vserver name>-event-name <event name> -volume-operation
false -protocol cifs -file-operations read,write -filters offline-bit,first-read,first-write
```

The FPolicy event options are described in Table 1.

**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.<br>Values: create, create_dir, delete, delete_dir, read, close, write, rename, rename_dir |
| `-protocol` | The name of the protocol for which the event is created.<br>Value: cif |

| Option | Description |
|---|---|
| -filters | Specifies the filters used with a given file operation for the protocol specified in the -protocol parameter. For example: 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 <svm name> -engine-name <engine name> –primary
servers < IP address of FPolicy server> -port 9883 -extern-engine-type asynchronous -ssl-option
no-auth
```

The FPolicy external engine options are described in Table 2.

**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. PeerSync currently supports only asynchronous. |
| -ssl-option | The SSL option for external communication with the FPolicy server. PeerSync currently supports only no-auth. |

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

```
fpolicy policy external-engine show
```

## 5.4 Create FPolicy Policy

Run the following command to create FPolicy policy:

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

The FPolicy policy options are described in Table 3.

**Table 3) FPolicy policy options.**

| Option | Description |
|---|---|
| -vserver | The name of the SVM on which you want to create an FPolicy policy configuration. |
| -policy-name | The name of the FPolicy policy that you want to create. |
| -events | A list of events to monitor for the FPolicy policy created in section 5.2. |
| -engine | The name of the external engine created in section 5.3. |

| Option | Description |
|---|---|
| -is-mandatory | Determines whether the FPolicy connection is mandatory. PeerSync only supports setting this to false. |

To view the policy you created, run `fpolicy policy show`.

### 5.5 Create FPolicy Scope

To create and verify an FPolicy scope, run the following command:

```
fpolicy policy scope create -vserver <svm name> -policy-name <policy name> -volumes-to-include
"*" - export-policies-to-include "*" –shares-to-include <list of shares>
```

The FPolicy scope options are described in Table 4.

**Table 4) FPolicy scope options.**

| Option | Description |
|---|---|
| -vserver | The name of the SVM on which you want to create an FPolicy scope. |
| -policy-name | The name of the FPolicy policy that was created in section 5.4. |
| -volumes-to-include | A comma-separated list of volumes to be monitored. |
| -export-policies-to-include | A comma-separated list of NFS export policies for monitoring file access. Wildcards are supported. |
| -shares-to-include | A comma-separated list of CIFS/SMB shares for monitoring file access. |

To view the FPolicy scope, run the following command:

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

### 5.6 Enable FPolicy Policy

On startup, the application service enables the new FPolicy policy. The following command is for reference only.

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

## 6 Security Login Configuration for FPolicy Server

For PeerSync to successfully register and communicate with clustered Data ONTAP, certain permissions must be configured on the NetApp system. These permissions include access to the FPolicy and Data ONTAP APIs.

PeerSync must be configured with the user name and password of an account that has Data ONTAP API access. It is recommended that this account be locally configured on the SVM and dedicated to PeerSync.

The following Data ONTAP commands can be executed from the cluster context to create a local account <username> with appropriate Data ONTAP API access to the SVM <svm name>:

```
security login create –vserver <svm name> –username <username> –application ontapi -authmethod
password –role vsadmin
```

You are prompted to enter a password. Enter the following command:

```
security login create -vserver <svm name> -username <username> -application ssh -authmethod
password -role vsadmin
```

| Note |
| --- |
| The user name and password of this account must be entered into PeerSync as part of the configuration process described in section 4.2. |

In addition to the preceding security commands related to clustered Data ONTAP, additional commands must be run to grant important permissions and privileges to the service account under which PeerSync runs on the FPolicy server.

To add the PeerSync service account <domain user name> (in the format “DOMAIN\USERNAME”) to the local admin group of SVM <svm name>, run the following command from the cluster context:

```
vserver cifs users-and-groups local-group add-members -vserver <svm name> -group-name
BUILTIN\Administrators -member-names <domain user name>
```

To query and set DACLs, SACLs, and owner and/or group configurations on files and folders, the service account for both PeerSync and the PSListener must be granted special privileges. To grant these privileges to the account <domain user name> (in the format “DOMAIN\USERNAME”) on SVM <svm name>, run the following command from the cluster context:

```
vserver cifs users-and-groups privilege add-privilege -vserver <svm name> -user-or-group-name
<domain user name> -privileges SeBackupPrivilege, SeRestorePrivilege, SeSecurityPrivilege,
SeTakeOwnershipPrivilege, SeTcbPrivilege
```

# 7 Clustered Data ONTAP Best Practices

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

## 7.1 Policy Configuration

### Configuration of an FPolicy External Engine for the SVM

Providing additional security comes with a performance cost. Enabling SSL communication 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, refer to the section “**Error! Reference source not found.**.”

### 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.

## 7.2 Network Configuration

Network connectivity between the FPolicy server and the controller should be of low latency. NetApp recommends separating FPolicy traffic from client traffic by using a private network.

**Note:** For a scenario in which the LIF for FPolicy traffic is configured on a different port than the LIF for client traffic, the FPolicy LIF might fail over to other node because of a port failure. This failover would make the FPolicy server unreachable from the node and cause the FPolicy notifications for 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, make sure to allocate dedicated resources (CPU, network, and memory) to the virtual server.

## 7.4 Multiple Policy Configuration

The FPolicy policy for native blocking has the highest priority, irrespective of the sequence number. Decision-altering policies have a higher priority than others. Policy priority depends on use cases. 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. For example, if you want to add or modify an IP address in the external engine configured for the enabled policy, then first disable the policy.

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

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

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, sends notifications to the external server, and waits for a response, depending on the mode of external engine communication (synchronous or asynchronous). This process affects the performance of CIFS access and CPU resources. To mitigate any issues, NetApp recommends assessing and sizing the environment before enabling FPolicy. Performance is affected by the number of users, by workload characteristics such as operations per user and the data size, and by network latency.

# 8 PeerSync Best Practices

In addition to the FPolicy best practices, Peer Software strongly recommends the best practices listed in this section.

## 8.1 Network Communication

Traffic between the FPolicy server and the NetApp device should flow as quickly as possible. To minimize latency, the following considerations are strongly recommended:

- For best performance, FPolicy traffic should not be routed through a packet scanning firewall or other security device.
- The FPolicy server should be running on a dedicated server or virtual machine with sufficient memory, I/O performance, and resources. A physical service is always preferred. However, if running as a VM, it must be hosted on enterprise-grade hardware and virtualization software.
- The FPolicy server should be kept separate from any Windows Server that is performing virus scanning of content on a NetApp device using the VSCAN API. In addition, no third-party FPolicy applications should be running on the PeerSync FPolicy server.
- FPolicy servers must be kept separate from the management center and PSListener servers. Keeping FPolicy servers separate helps overall performance and greatly reduces the chance of TCP communication issues.

## 8.2 Operating System Requirements

PeerSync servers have a minimum Windows Server version requirement. To support FPolicy, PeerSync must run on a minimum of Windows Server 2008. It is strongly recommended that all PeerSync and PSListener servers be running on Windows Server 2012 R2.

For Rsync and Rsync daemon support, PeerSync has been validated to work with Red Hat Linux v6.5 and above, as well as Ubuntu 14.04 and higher.

For up-to-date details and requirements for PeerSync's NFS support, see http://www.peersoftware.com/doc-lib/peersync-nfs-prerequisites.

## 8.3 New Performance Optimizations

Starting with PeerSync v9.3, a new performance mode is available for use in bidirectional CIFS/SMB deployments with clustered Data ONTAP 8.2.x and later. This mode requires some additional configuration on both the SVM and within PeerSync, but increases PeerSync's replication performance and reduces overhead on the SVM.

Details about how to enable this new performance mode can be found at www.peersoftware.com/doc-lib/peersync-cdot-enhanced-performance-guide.

# 9 Troubleshooting

## 9.1 Problem: 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 why the FPolicy server disconnected using the command `show-engine -instance` and take appropriate action.

For 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 is reachable.

For example:

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

## Potential Cause 1

There are issues with routing.

**Potential solution:** Check the routing table entries by using the command `routing-groups route show` to check whether a route is available for the SVM. If no route is available, run the `routing-groups route create` command to add a route.

For 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 2

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 listens and modify the external engine configuration to use the same port.

For example:

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

## Potential Cause 3

The security options for the external engine are not the same as for the FPolicy server.

**Potential solution:** Run the command `fpolicy policy external-engine show –instance`.

If the FPolicy server uses 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 does not use SSL. Otherwise, use `mutual-auth/server-auth`, depending upon the level of security needed.

For 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 4

The LIF dedicated for the FPolicy traffic has failed over to a different node.

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

For example:

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

## 9.3 Problem: 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.

For example:

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

## 9.4 Problem: Notifications Are Not Received for the File Operations on Volume, Share, or 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.

For 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 responses are sent back to Data ONTAP. This round trip-process adds additional latency to client access.

Monitoring the performance counters on FPolicy server and Data ONTAP allows you to identify bottlenecks in the solution and 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 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. Use the Data ONTAP FPolicy counters mentioned in Table 5 to monitor the performance of FPolicy subsystems.

| 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 <instance name> -sample-id <id>
statistics start -object fpolicy_server -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 Counter Monitoring

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**

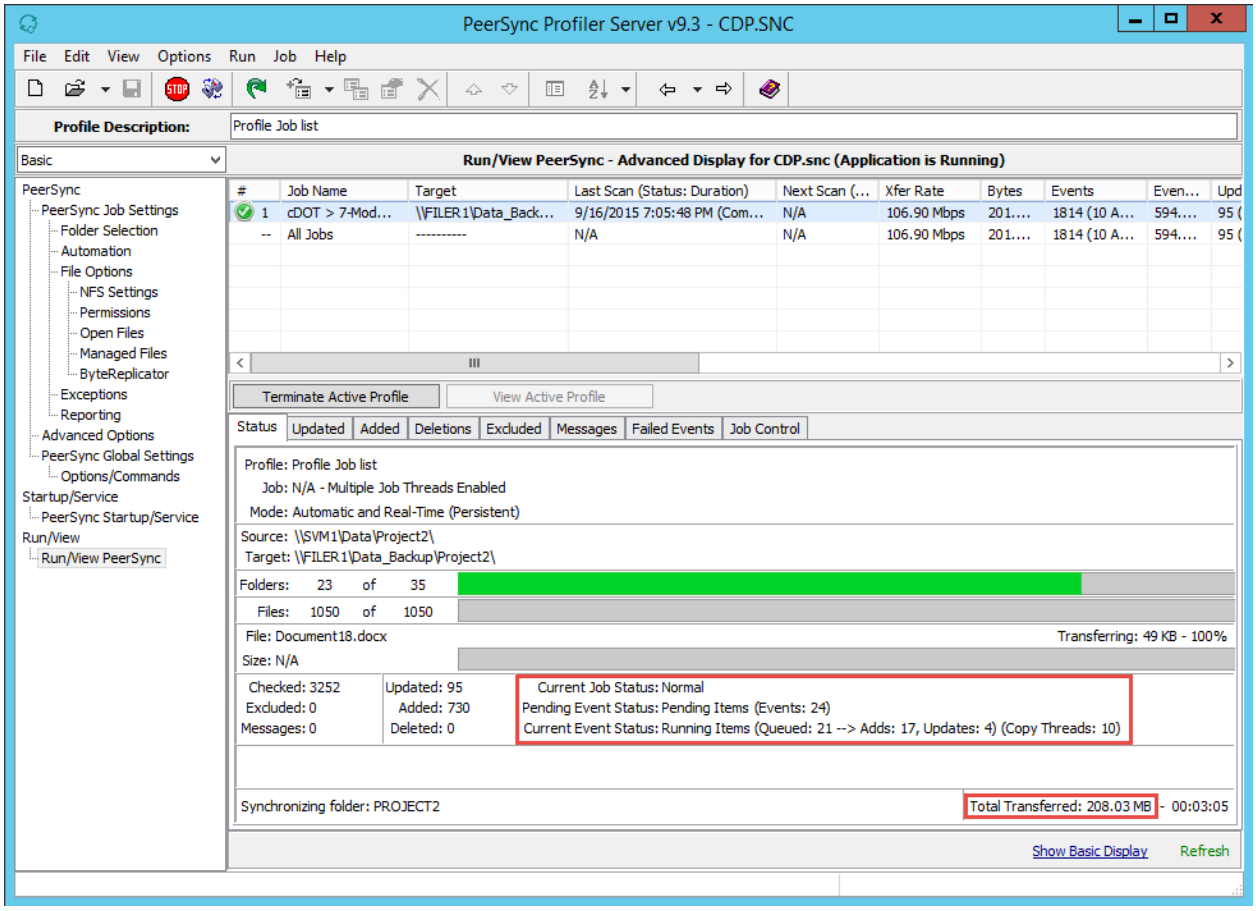
| Counters | Description |
|---|---|
| max_request_latency | Maximum latency for a screen request |
| outstanding_requests | Total number of screen requests waiting for response |
| request_latency | Average latency for screen request |
| request_latency_hist | Histogram of latency for screen requests |
| 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 |

## 10.3 PeerSync-Specific Performance Monitoring

In addition to the performance monitoring steps mentioned earlier in section 10, PeerSync v9.3.1 and later versions have various ways to measure overall collaboration performance as well as FPolicy performance.

### Overall PeerSync Performance Monitoring

The PeerSync profiler contains several counters to help gauge activity and performance during replication.




The following performance counters are seen in the previous screen:

- **Current Job Status.** Shows if there are connectivity or FPolicy issues preventing PeerSync from operating in an optimal state.
- **Pending Event Status.** Represents the current amount of backlog that PeerSync has yet to process, including real-time events and file copy retries. It is normal for numbers in this section to fluctuate. If the number indicated as Events: xx rises above 5,000 and does not decrease, consideration should be given to the performance optimizations recommended in section 8. If the number indicated as Retries: xx rises above 200 and does not decrease, an environmental problem or disconnect could be the issue.
- **Current Event Status.** Gives an overview of what PeerSync is currently doing, including currently running scans, active file copies, and real-time status. These numbers are directly affected by the configuration of PeerSync and should not dramatically increase over time.
- **Total Transferred.** Refers to the total number of bytes transferred during the current run of PeerSync. This number factors in any savings from PeerSync's proprietary byte-level replication technology.

All of these counters are also available within the PMC.

## PeerSync FPolicy Performance Monitoring

The statistical counters in sections 0 and 10.2 are the best way to measure overall FPolicy performance and latency when it comes to communication between the SVM and the FPolicy server. In a healthy environment, there should be very little latency recorded within these counters.

PeerSync performs log-out statistics on items that have been received by the FPolicy server. These are currently contained within a log file at each PeerSync server that is communicating with FPolicy. This file can be found at

```
<PeerSync Install Directory>\workspace\Logs\FPServiceC.log.
```

Open this file and look for the following text:

```
******* Current global queue: 0 Total callbacks: 4059171 Total filtered by
IP: 0
```

It should appear every 10 minutes while PeerSync is communicating with FPolicy.

- **Current global queue.** Refers to the total number of notifications received from FPolicy that are waiting to be passed on to PeerSync. In a well-performing environment, this number should always be less than 100. If not, consideration should be given to the performance optimizations recommended in section 8.
- **Total callbacks.** Refers to the total number of notifications received after the FPolicy connection was started. This number is the cumulative total across all clustered Data ONTAP replication jobs that are running on the selected PeerSync server. It is normal for this number to climb in active and healthy environments. It never comes back down.
- **Total filtered by IP.** Refers to the total number of notifications received from FPolicy that were automatically ignored by the FPolicy server, due to an excluded IP address. If this number grows with each 10-minute stats cycle, consideration should be given to the performance optimizations recommended in section 8. This number is also a cumulative total across all clustered Data ONTAP replication jobs that are running on the selected PeerSync server.

## Where to Find Additional Information

To learn more about the information that is described in this document, review the following documents and/or websites

- PeerSync for NFS - Prerequisites
  http://www.peersoftware.com/resources/tech-briefs.html?view=document&id=112
- PeerSync Environmental Requirements
  http://www.peersoftware.com/resources/tech-briefs.html?view=document&id=85
- NetApp 7-Mode Prerequisites
  http://www.peersoftware.com/resources/tech-briefs.html?view=document&id=82
- Peer Trial Software
  http://www.peersoftware.com/trial-software.html
- Improving cDOT Performance with PeerSync
  http://www.peersoftware.com/resources/tech-briefs.html?view=document&id=110

## Version History

| Version | Date | Document Version History |
|---|---|---|
| 1.1 | May 2019 | Refreshed the date on the cover page, footers, and back page. Reformatted the cover page tio align with the current template. |
| 1.0 | February 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.



TR-4472-0519