Technical Report

FPolicy Solution Guide for Clustered Data ONTAP: Peer Software PeerLink

Brahmanna Chowdary Kodavali, Saurabh Singh, NetApp
Matt Marsala, Peer Software
May 2019 | TR-4449

NetApp®

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Introduction

The NetApp® FPolicy® feature 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 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 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 the following:

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

1.1 Audience

The target audience for this document is customers who want to implement CIFS-based file replication and distributed file locking on clustered Data ONTAP for business file sharing and collaboration.

1.2 Purpose and Scope

The purpose of this document is to provide an understanding of the FPolicy framework and describe the steps needed to deploy a file replication and distributed file locking solution by using PeerLink. 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.

2.1 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.

2.2 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-balancing 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.

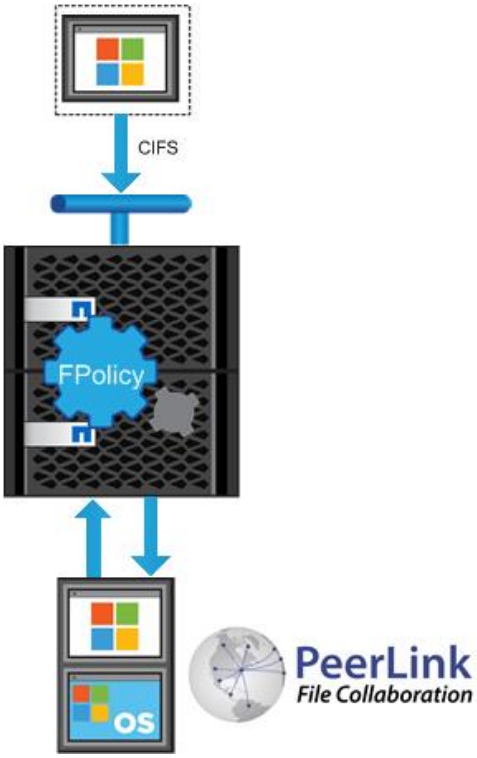
- Ability to bypass any FPolicy checks so that file access over the privileged data path does not generate an FPolicy notification

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 PeerLink File Collaboration. Figure 1 shows the solution architecture.

Figure 1) FPolicy solution architecture.



FPolicy application software is installed on a 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: PeerLink File Collaboration

PeerLink File Collaboration provides distributed teams with a fast and efficient means to collaborate with shared files. PeerLink integrates an enterprise-class, real-time synchronization engine with distributed file locking. The real-time synchronization engine makes sure that the same data exists on all participating servers, regardless of where changes occur. The file-locking component prevents users from accessing files that users at another location currently work on.

The entire system works cross platform between Windows and NetApp clustered Data ONTAP and Data ONTAP operating in 7-Mode.

One or more File Collaboration jobs can be created across the PeerLink environment to work with different groupings of projects, data, servers, and/or sites. Each job consists of two or more participating servers and a folder structure on each participating file server or NetApp system. This folder structure is called the Watch Set and is synchronized in real time across all participating servers. In addition, locks are propagated across all participating servers as users open and modify files at any one location.

Main Features

The main features of the PeerLink File Collaboration are:

- Real-time file synchronization
- Multithreading
- Byte-level replication
- Version conflict prevention
- Cross-platform support (Windows and NetApp clustered Data ONTAP and 7-Mode)
- Sync-on-save support
- Remote conflict resolution
- Easy installation and unobtrusive operation
- No changes required to existing storage hardware or infrastructure
- Centralized management and monitoring
- Unicode compliant
- Full support for distributed file system namespaces
- Administrative log reporting
- E-mail alerts
- Web-based management console
- Intelligent connection checking
- Cross-domain and cross-active-directory collaboration

Components

Following are the components of the PeerLink architecture:

- The PeerLink Hub and Broker are components that handle communication, monitoring, and management.
- The PeerLink Agent is a component installed on all file servers that participate in the File Collaboration. For NetApp environments, the PeerLink Agent is installed on a Windows Server in front of the NetApp device, enabling PeerLink to interact with NetApp through FPolicy.

Figure 2) PeerLink architectural diagram (graphic supplied by Peer Software).

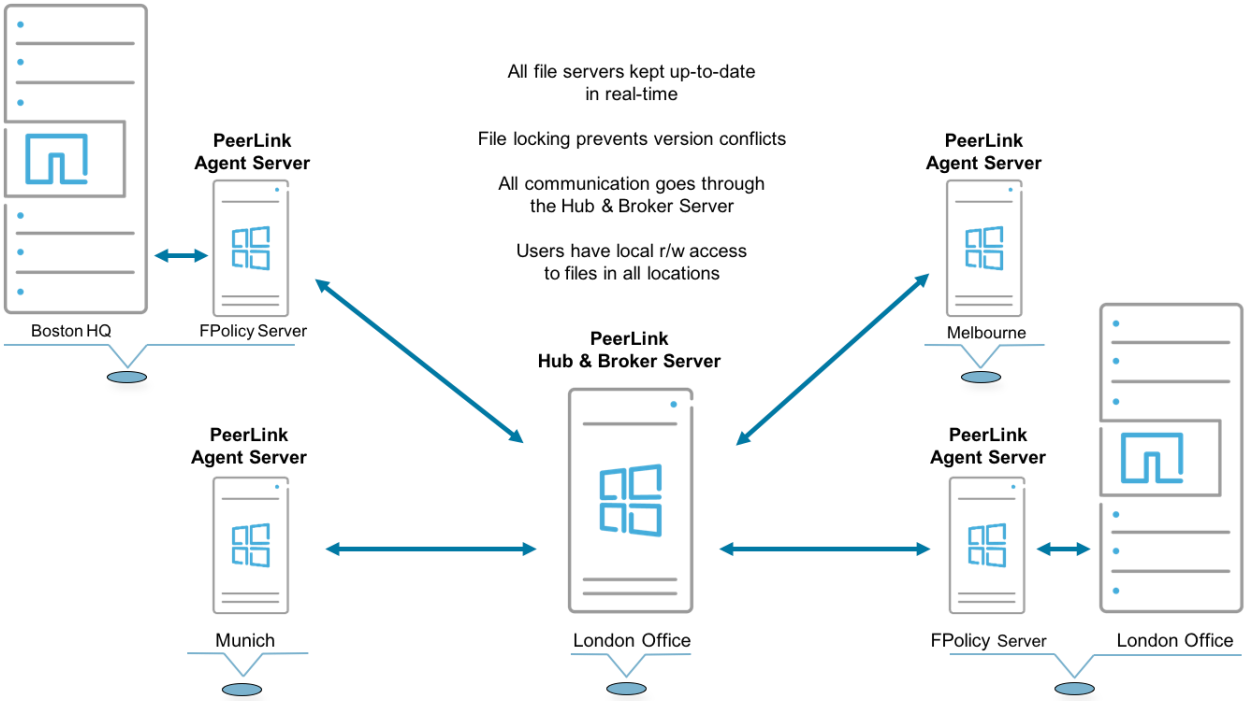


Figure 2 is an example of a typical PeerLink File Collaboration deployment combining Windows File Servers and NetApp systems. There are several important things to note about this diagram:

Note: The PeerLink Hub and Broker are installed on a central server in London.

Note: The PeerLink Agent is installed on Windows File Servers in Munich and Melbourne.

Note: For the NetApp devices in Boston and London, the PeerLink Agent is installed on a Windows Server sitting alongside each NetApp device on the same subnet, network segment, and domain. These Windows Servers are known as FPolicy servers and allow PeerLink to communicate with the NetApp devices.

Note: All communication between sites is handled by the PeerLink Hub and Broker server.

4 Installing and Configuring PeerLink File Collaboration

4.1 Installing PeerLink File Collaboration for NetApp

To install PeerLink File Collaboration for NetApp, review the software requirements and installation procedures using the following references:

- Each component of the PeerLink File Collaboration solution has its own requirements and recommendations. For more information, see the PeerLink Environmental Requirements.
- NetApp clustered Data ONTAP environments require that additional prerequisites be met. For more information, see the NetApp cDOT FPolicy Prerequisites.
- Obtain installers and license keys from Peer Software. For more information, see the PeerLink for NetApp and Windows download site.
- For more information and assistance with the PeerLink installation, contact the Peer Software technical team.

- Installing the PeerLink Hub and Broker and the PeerLink Agent is an easy process. Links to download both are included in a registration e-mail that is sent with every trial or purchase. After downloading both installers, stage each one on the appropriate Windows Server.

  Note: Every PeerLink deployment requires one Hub and Broker server and at least two Agent servers. See Figure 2 for an example of a typical PeerLink deployment.

- After the installers are staged on the appropriate systems, follow the installation steps in the PeerLink Installation and Configuration Guide.
- After installing both the Hub and Broker and the Agent, install the appropriate licenses by following the steps in the PeerLink Licensing Guide.

4.2 Configuring PeerLink File Collaboration for NetApp

Before configuring PeerLink File Collaboration to work with NetApp, it is important to understand how the PeerLink environment interacts with NetApp systems using FPolicy.

Figure 3) How PeerLink works with FPolicy (graphic supplied by Peer Software).

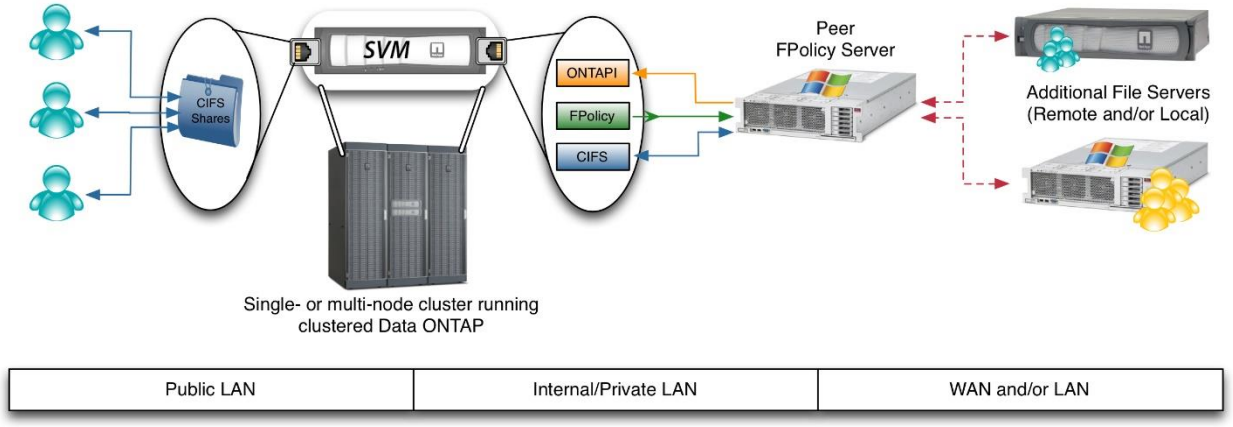
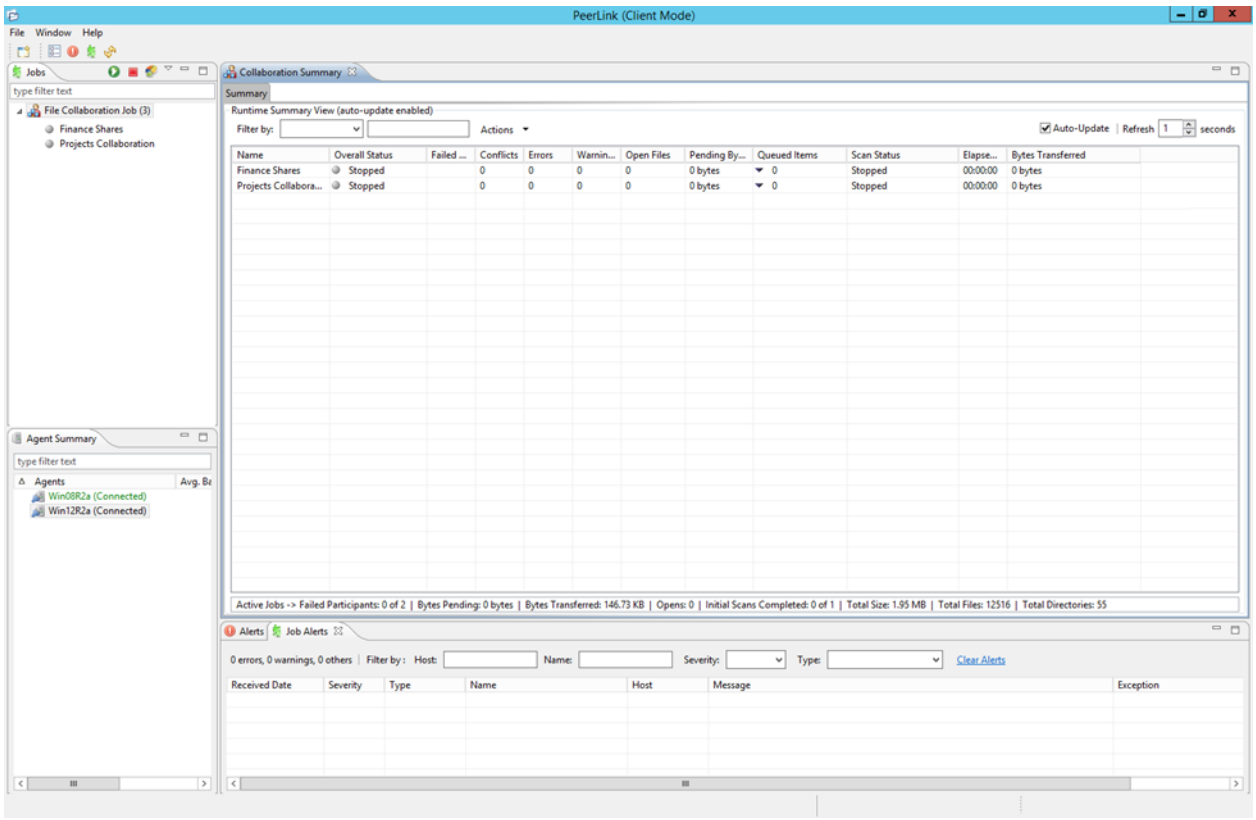


Figure 3 shows how Peer Software products interact with clustered Data ONTAP. Working from left to right, users interact with the CIFS/SMB shares on a NetApp SVM using a public LAN. The SVM runs on top of a cluster of one or more nodes, each running clustered Data ONTAP. The physical nodes supply all storage and physical network connections to the SVM. Users and PeerLink Agents acting as FPolicy servers work with the SVM using LIFs configured on the SVM. When activity occurs on the SVM through these shares, the Agent FPolicy server is notified through the FPolicy framework. The Agent FPolicy server then interacts with the same content through CIFS/SMB. NetApp recommends that the Agent FPolicy server interact with the SVM using a private LAN. The Agent FPolicy server can then facilitate the flow of data to the PeerLink Hub and Broker and on to remote sites.

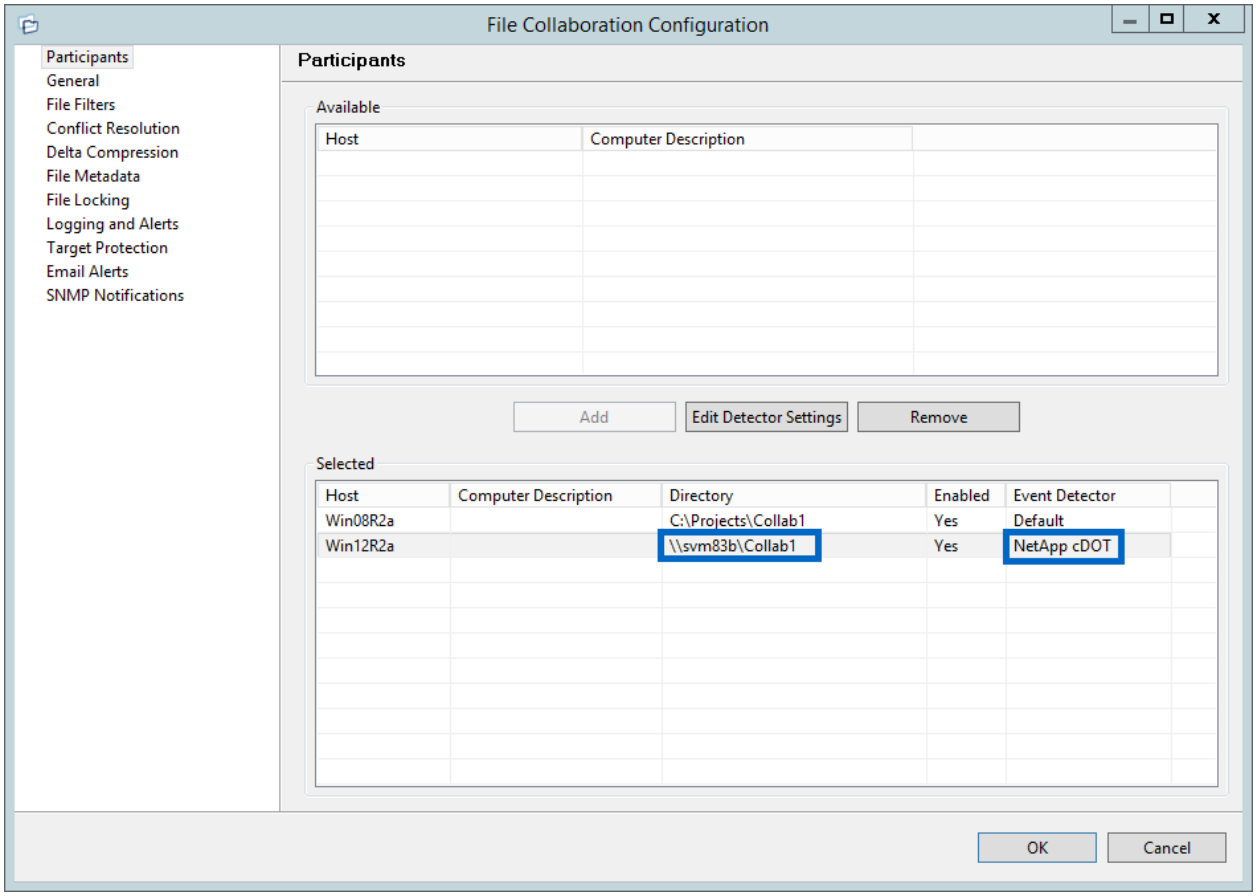
After all PeerLink system elements are installed and all NetApp deployment prerequisites are met, create a File Collaboration job from within the PeerLink Hub Client. Then configure it to use with clustered Data ONTAP.

To configure PeerLink File Collaboration for NetApp, complete the following steps:

1. Within the PeerLink Hub Client, from the Job menu, select New Peerlet, enter a name for the collaboration job, and click OK.



2. On the Participants page, select two or more Agents (either as local Windows File Servers or associated with NetApp devices) to participate in collaboration.
3. Enter a directory on the actual file server or a share on the paired NetApp for each Agent.
4. If an Agent acts as an FPolicy server with clustered Data ONTAP, select NetApp cDOT from the Event Detector list.



In this example, Win08R2a is a Windows-based file server configured to collaborate on the local directory `C:\Projects\Collab1`. Win12R2a is an FPolicy server that works with the share Collab1 on the SVM titled `svm83b`.

When selecting NetApp cDOT from the list of available event detectors, a configuration dialog box is displayed that requires that the following fields be configured:

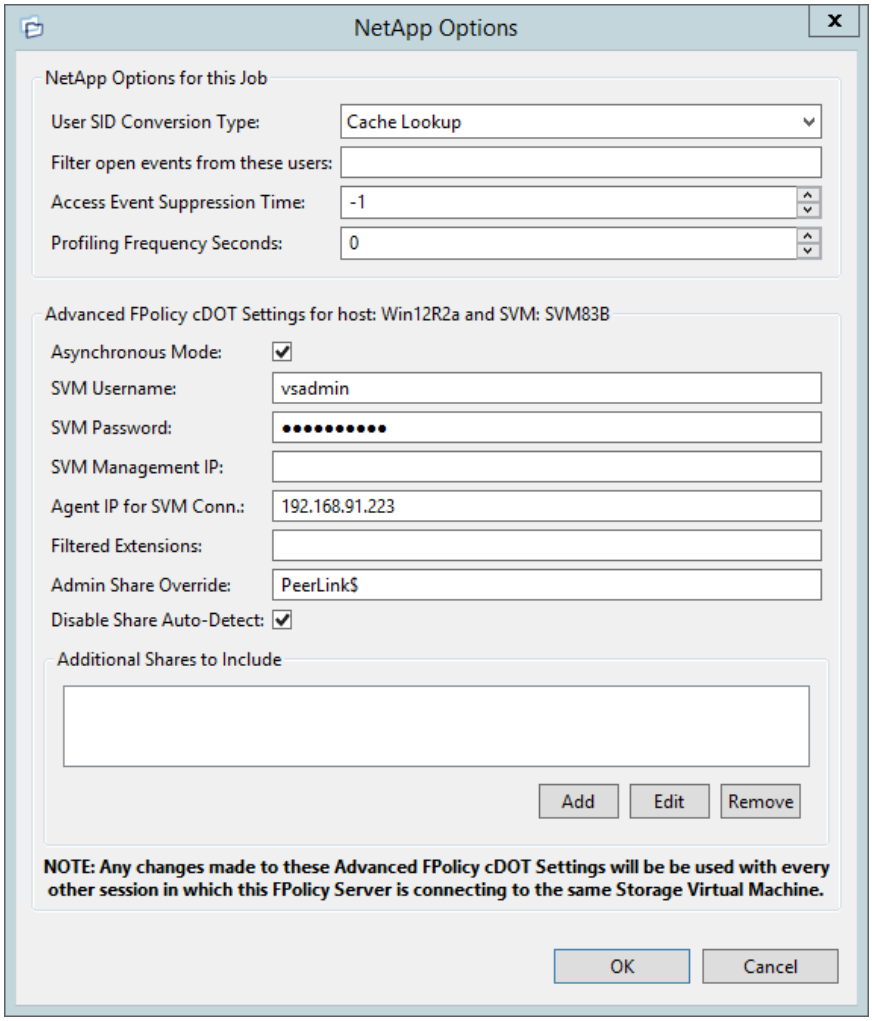
- **SVM Username.** The user name of the VSAdmin or similar account on the SVM that has appropriate access to the NetApp ONTAPI® library.
- **SVM Password.** The password of the VSAdmin or similar account on the SVM that has appropriate access to ONTAPI.
- **SVM Management IP (optional).** If the primary 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 here.
- **Agent IP for SVM Conn.** The IP address over which this Agent will connect to the configured SVM.

  Note: You must enter an IP address.

- **Filtered Extensions (optional).** A list of file extensions (separated by commas) to exclude from FPolicy (without a leading '*.').
- **Admin Share Override (optional).** Available starting with PeerLink v3.5.1, this option is a share name (typically in the format of an administrative share) that is created on clustered Data ONTAP SVMs for use only by PeerLink. When configured properly, this setting and the ones beneath it work together to enable an enhanced performance mode for clustered Data ONTAP environments.

  Note: For detailed steps on configuring this performance mode, see the Improving Clustered Data ONTAP Performance with PeerLink technical brief.

  - Disable Share Auto-Detect (optional): Used only when enabling the enhanced performance mode that is tied to Admin Share Override.
  - Additional Shares to Include (optional): Used only when enabling the enhanced performance mode that is tied to Admin Share Override.
- For all other options, leave the default values.



In this example, FPolicy server Win12R2a is configured to work with SVM83b. The user account with ONTAPI access is `vsadmin` and the IP address over which this Agent talks to the SVM is `192.168.91.223`. This particular clustered Data ONTAP configuration uses the new performance mode within PeerLink v3.5.1 and later, noted by the presence of an Admin Share Override of PeerLink$.

After all participant and clustered Data ONTAP settings are complete, save and close the job configuration. At this point, start the collaboration by right-clicking the newly created collaboration job and select Start.

Note: For more information about available collaboration settings, see the section “Creating a File Collaboration Job” in the PeerLink Help Manual.

Note: For more details about configuring PeerLink to work in NetApp environments, see the section “NetApp Configuration” in the PeerLink Help Manual.

Note: For more details about performance optimizations for PeerLink v3.5.1 and later, see the Improving cDOT Performance with PeerLink technical brief.

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

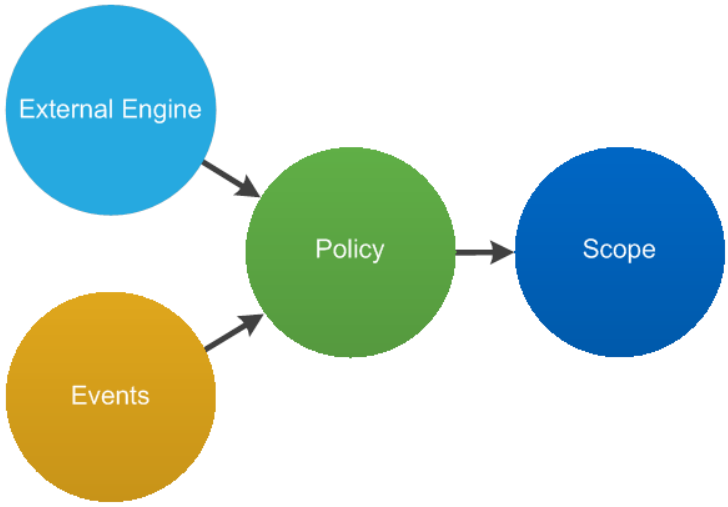
Configuration Requirements
The shares must reside on the volume monitored for CIFS events.

5.1 FPolicy Configuration Workflow

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

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

Figure 4) FPolicy configuration workflow.



Important Note
When configured to work with clustered Data ONTAP, PeerLink automatically configures FPolicy on the SVM. 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 only; Peer Software does not recommend making manual configurations. If necessary, use the `show` commands in each section to review PeerLink's automatic FPolicy configuration.

5.2 Create FPolicy Event

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

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

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

```
fpolicy policy event create -vserver <svm name>
-event-name <event name> -file-operations open, close, create, create_dir, delete, delete_dir,
write, rename, rename_dir, setattr -protocol cifs
```

Table 1 lists the FPolicy event options.

Table 1) FPolicy event options.

Option	Description
`-vserver`	The name of the SVM on which you want to create an FPolicy event configuration.
`-event-name`	The name of the FPolicy event that you want to create.
`-file-operations`	The file operations for the FPolicy event. The values are: `open, close, create, create_dir, delete, delete_dir, write, rename, rename_dir, setattr`.
`-protocol`	The name of the protocol for which the event is created. PeerLink currently supports only CIFS; therefore, NFS events are not monitored.
`-filters`	The filters used with a given file operation for the protocol specified in the `-protocol` parameter. No filters are currently supported by PeerLink.

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
```

Table 2 lists the FPolicy external engine options.

Table 2) FPolicy external engine options.

Option	Description
`-vserver`	The name of the SVM on which you want to create an FPolicy external engine.

Option	Description
-event-name	The name of 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; PeerLink currently supports only asynchronous.
-ssl-option	The SSL option for external communication with the FPolicy server; PeerLink currently supports only no-auth.

To view the external engine, run the following command:

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

5.4 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>
```

Table 3 lists the FPolicy scope options.

Table 3) 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 list of volumes (separated by commas) to be monitored.
-export-policies-to-include	A list of export policies (separated by commas) for monitoring file access; wildcards are supported.
-shares-to-include	A list of shares (separated by commas) for monitoring file access.

To view the FPolicy scope, run the following command:

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

5.5 Enable FPolicy Policy

PeerLink uses the following command to automatically enable the new FPolicy policy at startup:

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

6 Security Login Configuration for FPolicy Server

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

You must configure PeerLink with the user name and password of an account that has Data ONTAP API access. NetApp recommends that this account be locally configured on the SVM and dedicated to PeerLink. To create a local account `<username>` with the appropriate Data ONTAP API access to the SVM `<svm name>`, complete the following steps:

1. Run the following Data ONTAP commands from the cluster context:

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

2. Enter a password:

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

Note: You must specify a user name and password for this account in PeerLink as part of the configuration process discussed in section 4.2.

3. Additional Data ONTAP commands are required to grant important permissions and privileges to the service account under which the PeerLink Agent will run on the FPolicy server.

   To add the PeerLink Agent service account `<domain user name>` (in the format `DOMAIN\USERNAME`) to the Local Admin Group of SVM `<svm name>`, run the following Data ONTAP 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>
```

4. To properly query and set discretionary access control lists, system access control lists, and owner and/or group configurations on files and folders, the service account for the PeerLink Agent 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 Data ONTAP 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 following FPolicy best practices for server hardware, operating systems, patches, and so on.

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.

Note: PeerLink does not currently support secure sockets layer (SSL) communication.

Configuration of FPolicy Events for 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 types 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 “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 across the entire SVM. NetApp recommends checking directory extensions. If parameter `is-file-extension-check-on-directories-enabled` is set to true, directory objects are subjected to the same extension checks as regular files.

Network Configuration

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

Note: 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.

7.2 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. Virtual FPolicy servers must run on enterprise-grade hypervisors and host servers. For environments with high-file activity loads, NetApp strongly recommends a physical server as the FPolicy server.

7.3 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.

7.4 Managing FPolicy Workflow and Dependency on Other Technologies

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

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 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. Because a slow AV scanner can affect overall performance, AV solutions must be sized properly.

7.5 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 PeerLink Best Practices

In addition to the FPolicy best practices, Peer Software strongly recommends considering the following.

8.1 Network Communication

Traffic between the FPolicy server and the NetApp device should flow as quickly as possible. To minimize latency, NetApp recommends considering the following:

- For best performance, do not route FPolicy traffic through a packet-scanning firewall or other security device.
- Run the FPolicy server on a dedicated server or virtual machine with sufficient memory, I/O performance, and resources. A physical service is always preferred; however, if it runs as a VM, it must be hosted on enterprise-grade hardware and virtualization software.
- Keep the FPolicy server separate from any Windows Server that scans content for viruses on a NetApp device through the VSCAN API. In addition, do not run third-party FPolicy applications on the PeerLink Agent FPolicy server.
- Keep FPolicy servers separate from the PeerLink Hub and Broker server. Keeping FPolicy servers separate helps overall performance and greatly reduces the chance of TCP communication issues.

8.2 Operating System Requirements

PeerLink Agent FPolicy servers require a minimum Windows Server version. To support FPolicy, the Agent must run on a minimum of Windows Server 2008. NetApp strongly recommends that all Agents run on Windows Server 2012 R2.

New Performance Optimizations

Starting in PeerLink v3.5.1, a new performance mode is available with clustered Data ONTAP 8.2.x and later. This mode requires additional configuration on both the SVM and within PeerLink, but it increases PeerLink's replication performance as well as reduces overhead on the SVM.

For more information about how to enable this new performance mode, see the Improving cDOT Performance with PeerLink technical brief.

9 Troubleshooting

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 reason the FPolicy server disconnected, and take appropriate action.

For example:

```
1. fpolicy show-engine
```



```
2. fpolicy engine-connect –node <node name> -vserver <svm 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.

For example:

```
network interface show
network ping -lif <svm_data_lif> -destination <fpolicy server IP address>
```

Potential Cause #1

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.

For example:

```
route create -vserver <svm 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 does not listen 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 <svm 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 `fpolicy policy external-engine show –instance` command. If the FPolicy server uses SSL, the SSL Option for External Communication field 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.

For example:

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

Potential Cause #4

The LIF dedicated for 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 new node to process FPolicy requests for file operations performed on that node.

For example:

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

9.3 Problem: External Engine Is Not Native for Policy

Potential solution: Run the `fpolicy policy show` command to verify that the Engine field is set to Native. 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 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 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.

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 for generating a response 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 4 to monitor the performance of FPolicy subsystems.

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_server -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 Counter Monitoring

Table 4 and Table 5 contain lists of FPolicy counters that can be monitored.

Table 4) 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 5) 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

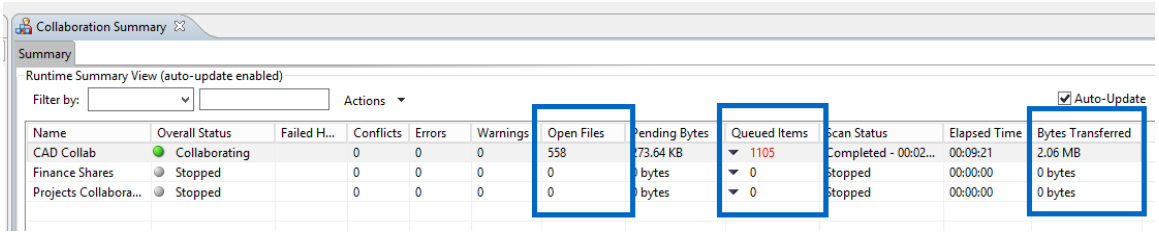
10.3 PeerLink-Specific Performance Monitoring

In addition to the FPolicy performance monitoring steps above, PeerLink v3.5.1 and later have various ways to measure overall collaboration performance as well as FPolicy performance.

Overall PeerLink Performance Monitoring

Starting with v3.5.1, PeerLink includes statistical counters for all collaboration activity from within the PeerLink Hub Client.

Figure 5) PeerLink statistical counters.

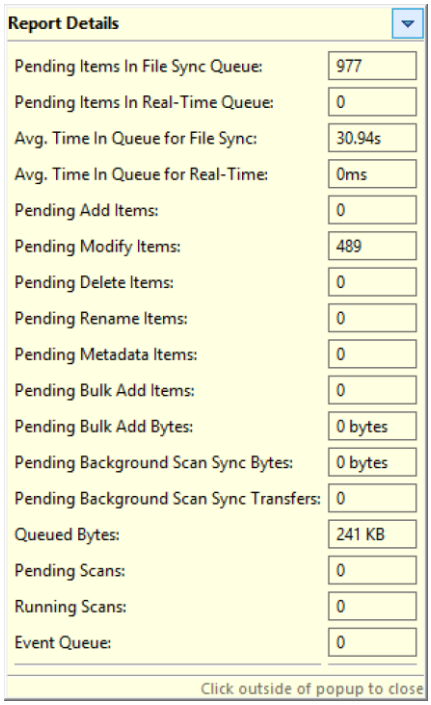


The following performance counters are highlighted in Figure 5:

- **Open files.** The number of files that are currently opened with corresponding locks across all file servers in the selected collaboration job.
- **Queued items.** The total number of backlogged events across all file servers in the selected collaboration job. Numbers above 5,000 are normal for active environments and should come down over the course of a business day. If this number goes above 10,000 for one or more jobs and does not come down over time, consider the performance optimizations recommended in section 7.
- **Bytes transferred.** The total number of bytes transferred during the current run of the selected collaboration job. This number factors in any savings from PeerLink's proprietary byte-level replication technology.

Click a cell in the Queued Items column to display the statistical counters.

Figure 6) PeerLink job-level statistical counters.



The counters in Figure 6 are static when the screen is first displayed. To refresh them, click outside the screen and then reclick the appropriate cell in the Queued Items column. The most important counters are:

- **Pending Items in File Sync Queue.** This counter represents the total number of items that are queued to be replicated between any file servers in a collaboration job. The number of items shown in this queue depends heavily on the network performance between each PeerLink Agent and the PeerLink Hub and Broker. It also depends on the rate of file change activity.
- **Pending Items in Real-Time Queue.** This counter represents the total number of opens and closes that are queued to be mirrored across any file servers in a collaboration job. The number of items shown in this queue depends more on the rate of file-access activity than on network performance between each PeerLink Agent and the PeerLink Hub and Broker. In most environments, this number should be lower than the number of Pending Items in File Sync Queue.
- **Avg. Time in Queue for File Sync.** This counter represents the average amount of time that a single item waits in the File Sync Queue before being processed. This average depends on the network

performance between each PeerLink Agent and the PeerLink Hub and Broker, as well as on the rate of file change activity.

- **Avg. Time in Queue for Real-Time.** This counter represents the average amount of time that a single item waits in the Real-Time Queue before it is processed. This average depends more on the rate of file access activity than on network performance between each PeerLink Agent and the PeerLink Hub and Broker. In most environments, this number should be lower than the number in Avg. Time in Queue for File Sync.
- **Pending Bulk Add Items.** This counter represents the number of added files and folders that were detected in the same folder in a short period of time. If this counter goes above 100 at any given time, then users are likely copying a large number of folders within a collaboration job's watch set. This happens in most environments from time to time, but it has an impact on normal replication performance.

If either average time counter increases to hours (especially for the Real-Time Queue) and does not decrease over time, review the performance optimizations recommended in "Clustered Data ONTAP Best Practices."

PeerLink FPolicy Performance Monitoring

For communication between the SVM and the FPolicy server, the statistical counters documented in "Collect and Display FPolicy Counters" and "Counter Monitoring" are best to measure overall FPolicy performance and latency. In a healthy environment, very little latency is recorded within these counters.

The PeerLink Agent does log out statistics on items that are received by the FPolicy server. They are contained within a log file at each PeerLink Agent that communicates with FPolicy. This file is located at <PeerLink Agent Install Directory>\workspace\Logs\FPServiceC.log.

Within the file, look for a text similar to the following example. It should appear every 10 minutes while the Agent communicates with FPolicy:

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

Where:

- **Current global queue** is the total number of notifications from FPolicy waiting to be passed to the PeerLink Agent. In a healthy environment, this number is always less than 100. If it is not, consider the performance optimizations recommended in "PeerLink Best Practices."
- **Total callbacks** is the total number of notifications received since the FPolicy connection started. This number is a total across all clustered Data ONTAP collaboration jobs that run on the selected Agent. It is normal for this number to increase in active and healthy environments; however, it will never decrease.
- **Total filtered** by IP is the total number of notifications received from FPolicy that were automatically ignored by the FPolicy server because of an excluded IP address. If this number increases with each 10-minute stats cycle, consider the performance optimizations recommended in "PeerLink Best Practices." This number is also a cumulative total across all clustered Data ONTAP collaboration jobs that run on the selected Agent.

Where to Find Additional Information

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

- NetApp Product Documentation
  https://docs.netapp.com

Version History

Version	Date	Document Version History
Version 1.0	May 2019	Refreshed date on the cover page, footers, and back page. Reformatted the cover page to align with the current template. .
Version 1.0	August 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-4449-0519