Technical Report

FPolicy Solution Guide for ONTAP: Varonis DatAdvantage

Brahmanna Chowdary Kodavali, NetApp
September 2018 | TR-4429

TABLE OF CONTENTS

1 Introduction 4

1.1 Audience 4

1.2 Purpose and Scope 4

2 FPolicy Overview 4

2.1 Role of ONTAP Components in FPolicy Configuration 5

2.2 How FPolicy Works with External FPolicy Servers 5

3 FPolicy Solution Architecture for Varonis DatAdvantage 6

3.1 Components of FPolicy on ONTAP 6

3.2 FPolicy Application Software—Varonis DatAdvantage 6

4 Installing and Configuring Varonis DatAdvantage 7

4.1 Varonis DatAdvantage Software Requirements and Installation 7

4.2 Configuring Varonis DatAdvantage for ONTAP 7

4.3 Varonis DatAdvantage Best Practices 13

5 Configuring FPolicy on ONTAP 13

5.1 FPolicy Configuration Workflow 14

5.2 Create an FPolicy Event 14

5.3 Create an FPolicy External Engine 15

5.4 Create an FPolicy Policy 16

5.5 Create an FPolicy Scope 16

5.6 Enable an FPolicy Policy 17

6 Security Login Configuration for FPolicy Server 17

7 Configuring SSL Certificates 18

8 FPolicy Configuration Best Practices on ONTAP 19

8.1 Policy Configuration 19

8.2 Network Configuration 19

8.3 Hardware Configuration 19

8.4 Multiple Policy Configuration 19

8.5 Managing FPolicy Workflow and Dependency on Other Technologies 20

8.6 Sizing Considerations 20

9 Troubleshooting Common Problems 20

9.1 Problem: The FPolicy Server Is Disconnected 20
9.2 Problem: The FPolicy Server Does Not Connect. 20
9.3 Problem: The External Engine Is Not Native for the Policy 21
9.4 Problem: Notifications Are Not Received for the File Operations on Volume, Share, and Export. 21
10 Performance Monitoring 22
10.1 Collect and Display FPolicy Counters 22
10.2 Counters to Monitor 22
11 Conclusion 23
Where to Find Additional Information 23
Version History 23

LIST OF TABLES

Table 1) FPolicy event options. 14
Table 2) FPolicy external engine options. 15
Table 3) FPolicy policy options. 16
Table 4) FPolicy scope options. 16
Table 5) Security login creation options. 17
Table 6) List of FPolicy counters. 22
Table 7) List of `fpolicy_server` counters. 22

LIST OF FIGURES

Figure 1) FPolicy solution architecture. 6
Figure 2) FPolicy configuration workflow. 14

1 Introduction

NetApp® FPolicy® is a file access notification framework that allows an administrator to monitor file access over NFS or CIFS protocol. This feature was introduced in NetApp clustered Data ONTAP® 8.2. The FPolicy framework requires that all the nodes in the cluster run Data ONTAP 8.2 and higher. FPolicy supports all SMB versions such as SMB 1.0 (also known as CIFS), SMB 2.0, SMB 2.1, and SMB 3.0. It also supports major NFS versions such as NFS v3 and NFS v4.0.

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

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

The FPolicy framework natively supports a simple file-blocking use case, which enables administrators to restrict end users from storing unwanted files. For example, an administrator can block audio and video files from being stored in data centers to save storage resources. This feature blocks files based only on extension. For more advanced features, you can consider partner solutions.

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

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

1.1 Audience

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

1.2 Purpose and Scope

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

2 FPolicy Overview

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

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

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

2.1 Role of ONTAP Components in FPolicy Configuration

The following components play a role in FPolicy configuration:

- **Administrative storage virtual machine (administrative SVM, called Vserver in ONTAP CLI and GUI).** The administrative SVM contains the FPolicy management framework and maintains and manages the information about all FPolicy configurations in the cluster.
- **Data SVMs.** FPolicy configuration can be defined at the cluster or at the SVM. The scope defines the resources to be monitored within the context of an SVM and operates only on SVM resources. One SVM configuration cannot monitor and send notifications for the data (shares) belonging to another SVM. However, FPolicy configurations defined on the administrative SVM can be leveraged in all data SVMs.
- **Data logical interfaces (Data LIFs).** Connections to the FPolicy servers are made through data LIFs that belong to the data SVM containing the central FPolicy configuration. The data LIFs used for these connections can fail over in the same manner as data LIFs used for normal client access.

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 a part of connection management, FPolicy controls the:

- Flow of file notifications through the correct LIF to the FPolicy server
- Load balancing of notifications to the FPolicy server when multiple FPolicy servers are associated with a policy
- Reestablishment of broken connections to an FPolicy server
- Sending of notifications to FPolicy servers during an authenticated session
- Establishment of a connection with the data LIFs on all the nodes participating in the SVM

For synchronous use cases, the FPolicy server accesses data on the SVM through a privileged data-access path. To make privileged data-access paths secure, ONTAP uses a combination of specific user credentials and the IP address of the FPolicy server set as a part of the FPolicy configuration. After FPolicy is enabled, the user credentials used in the FPolicy configuration grant the following privileges to the file system:

- Bypassing permissions checks when accessing data, enabling avoiding checks on files and directory access.
- Special locking privileges. ONTAP allows the FPolicy server to read, write, or modify access to any file, regardless of existing locks.

  Note: If the FPolicy server creates byte-range locks on the file, existing locks on the file are removed immediately.

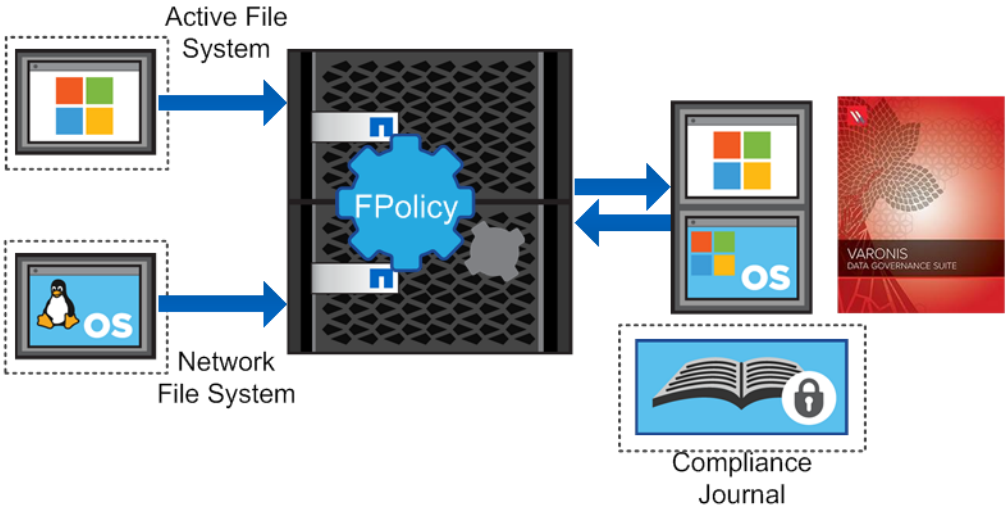
- Bypassing any FPolicy checks. File access over a privileged data path does not generate FPolicy notification.

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

3 FPolicy Solution Architecture for Varonis DatAdvantage

Figure 1 illustrates the FPolicy solution for Varonis DatAdvantage.

Figure 1) FPolicy solution architecture.



FPolicy application software is installed on a Windows server, and the FPolicy framework exists within ONTAP. The FPolicy framework connects to external FPolicy servers and sends notifications to the FPolicy servers for certain file-system events that occur because of client access. The external FPolicy servers process the notifications and return the responses to the node.

3.1 Components of FPolicy on ONTAP

FPolicy on ONTAP consists of the following components:

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

3.2 FPolicy Application Software—Varonis DatAdvantage

Varonis DatAdvantage is an analytical, software-based solution for data-usage management. With DatAdvantage, organizations can view, understand, and manage who is using data to control data access and enforce compliance with data-usage policies. DatAdvantage addresses the growing need for regulating data usage within organizations, enabling full visibility and accountability of data usage for legal, financial, data-security, intellectual-property, and data-privacy purposes.

DatAdvantage consists of three components:

- **DatAdvantage probes and collectors.** Probes and collectors nonintrusively and transparently collect file-server events and thus continuously track data usage, user directory structure, and directory service events to track changes to an organization's user directories.

- **DatAdvantage IDU Analytics.** DatAdvantage IDU Analytics intelligently aggregates and clusters data events and directory-structure information to accurately profile and classify data usage. DatAdvantage automatically maps data to users, and conversely, making sense of data usage patterns and providing an understanding of data access by owners and users while pinpointing potential data-usage risks.
- **DatAdvantage Management UI**. From the DatAdvantage Management UI, you can manage all aspects of data usage across the enterprise, including risk assessment, permission management, auditing, and reporting.

By delivering complete usage visibility, DatAdvantage Management enables simple exploration of data usage through interactive graphical views based on users, data, and their interrelationships.

4 Installing and Configuring Varonis DatAdvantage

4.1 Varonis DatAdvantage Software Requirements and Installation

The FPolicy application featured in this document is Varonis DatAdvantage for NetApp storage systems. For installation of the IDU suite, see the Varonis DatAdvantage Installation Guide, which comes with the software suite. This guide is also available in the Varonis support site.

4.2 Configuring Varonis DatAdvantage for ONTAP

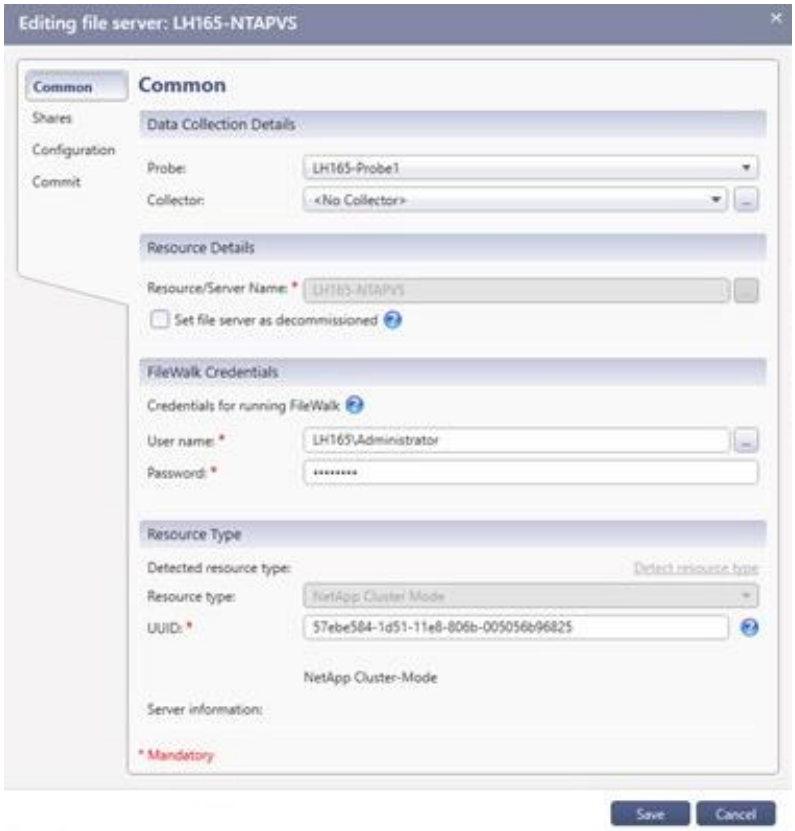
To configure Varonis DatAdvantage for use with ONTAP, complete the steps outlined in this section.

Prerequisites

• Varonis requires the manual configuration of FPolicy in ONTAP before adding the file server to Varonis Management Console. See section 5, “Configuring FPolicy on ONTAP” for the configuration steps.
• The Varonis application sends NetApp ONTAPI™ calls over HTTP to the SVM through the data LIF to manage FPolicy. This requires the IP address of the Varonis application server to be added in to the firewall policy “allow” list.
`system services firewall policy clone -policy data -new-policy-name fp_varonis`
`system services firewall policy create -policy fp_varonis -service http -action allow -ip-list 10.10.160.131/32`
• Use `fp_varonis` firewall policy when configuring the data LIF for SVM.
For details about configuring the Firewall policy, see the Network Management guide for your ONTAP version in the Product Documentation site.

To add a NetApp storage system, complete the following steps in the DatAdvantage File Server wizard:

1. In the Monitored File Server page in the Resources toolbar, click Add. The File Server Wizard opens.
2. Click Common on the left navigation pane.



a. Under Data Collection Details, select the probe to be used with the file server and select the required collector.

Note: After a collector has been configured to interface with a specific probe, that collector must be used with the same probe. This means that if you have already configured a collector to interface with a probe when adding a monitored file server, you must select either the same collector or `<No Collector>`. If no collector is used with the probe server, select `<No Collector>`.

b. Under Resource/File Server Details, enter the resolved name or IP address of the file server to be added, or click Browse to locate it.

c. Under FileWalk Credentials, type the name of the user account to be used for directory crawl (FileWalk), event collection (if set), and user crawl (ADwalk) on local accounts (if set). Then, enter the account password.

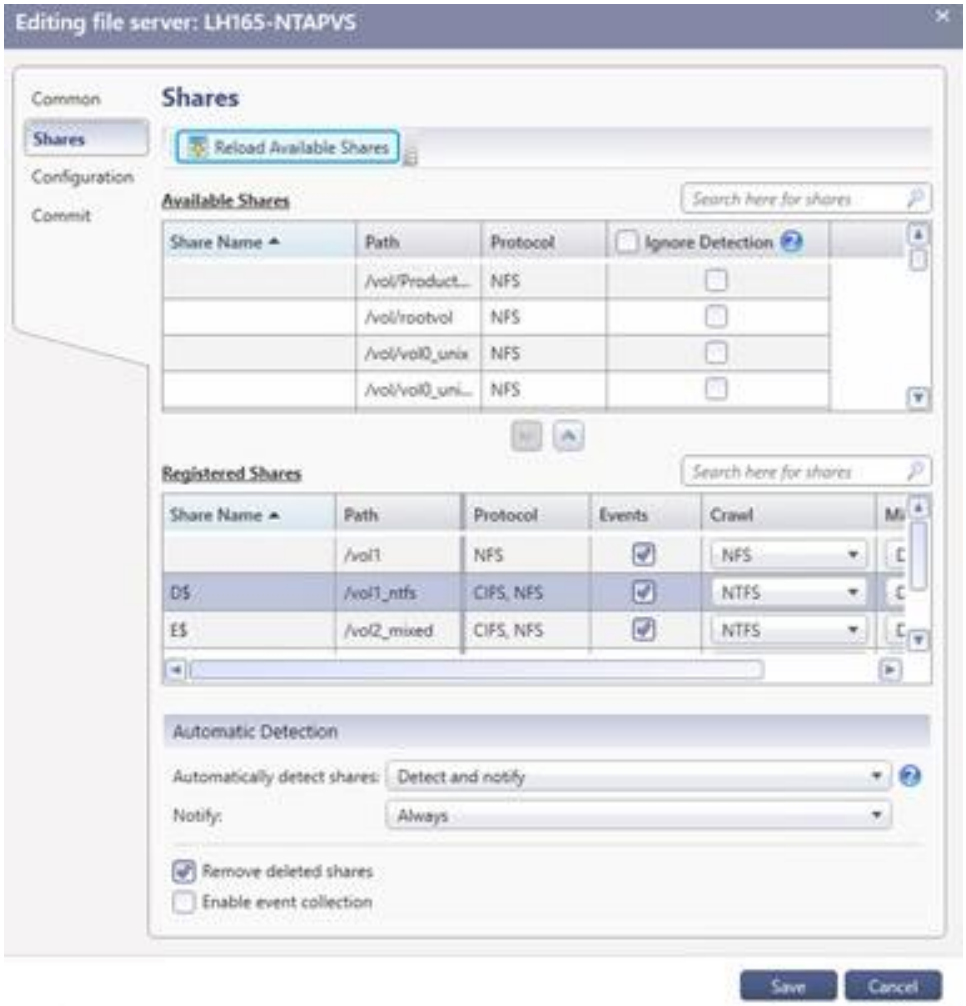
Note: The FileWalk credentials should use the case structure as defined in section 7 “Configuring SSL Certificates.”

d. Under Resource Type, click Detect File Server Type. This action detects the type of the file-server as ONTAP.

The Add This User Account to the Filtered Users List checkbox appears when the file server type is detected. This is the default user account for IDU Suite operations. If you clear this checkbox, several events generated by the IDU Suite are collected.

The UUID field represents the UUID number of the SVM.

3. To select specific shares for the file server, click Shares in the navigation pane The Shares options display.



e. In the Available Shares area, select the required shares and then click . The selected shares are moved to the Registered Shares area.

In Ignore Detection column, select the shares to be ignored (and not be the subject of notifications) by the resource monitor. Note the following:

- Select the shares that are manually moved from registered shares to available shares.
- Clear this option when users manually add shares from available shares to registered shares

f. For each share, review and enter the following information as required:

- **Share Name.** The name of the share.
- **Path.** The path on which the share resides.
- **Protocol.** The protocol defined for the share.

Note: The Varonis FileWalk method uses the SSH protocol to collect this information.

- **Events.** Select the checkbox to collect events for the share.
- **Crawl.** To enable or disable monitoring for the share, click the Crawl column and select the relevant option.
- **Mixed Security.** This indicates the default access control list extraction in mixed NT and UNIX environments.

g. DatAdvantage detects shares that reside at the highest level of the hierarchy that are not already monitored and gives preference to administrative shares over equivalent regular shares.

   In the Automatically Detect Shares field under Automatic Detection, choose from the following options:

- **Never.** Select this to instruct DatAdvantage not to detect shares or mounts automatically.
- **Detect and Notify.** Select this to send users an email that lists all newly detected shares or mounts. Unreachable shares and mounts are removed from DatAdvantage.
- **Detect and Monitor.** Select this to add the newly detected shares or mounts to the Registered Shares or Registered Mounts list in the dialog box, with the Events column checked and the Crawl column set to enable crawling. Unreachable shares and mounts are removed from DatAdvantage.
- **Detect, Monitor, and Notify.** Select this to add the newly detected shares or mounts as described previously and send users an email listing them. Unreachable shares and mounts are removed from DatAdvantage.

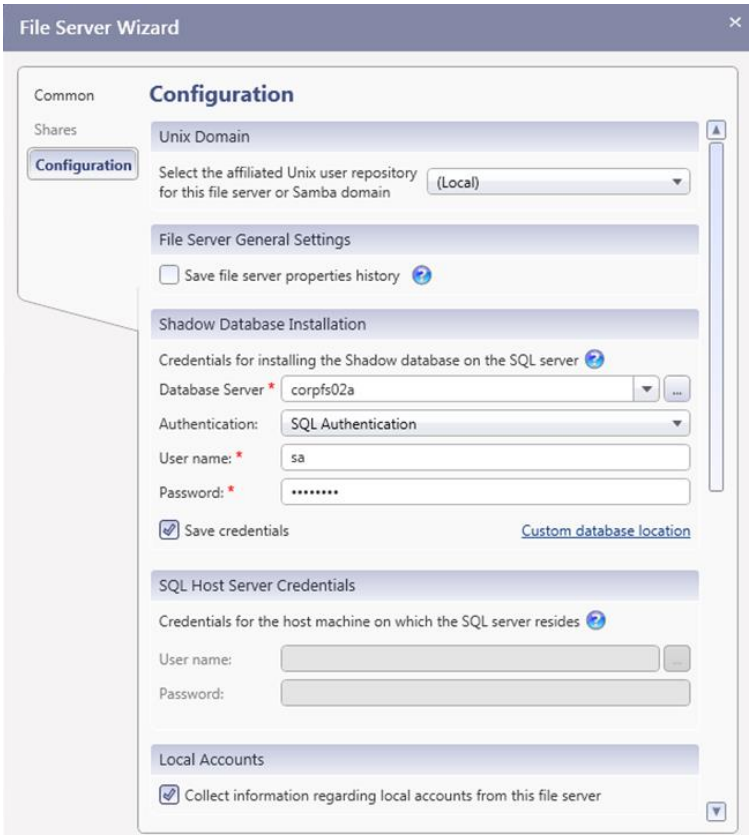
h. In the Notify field under Automatic Detection, select the frequency at which notification of new shares or mounts are sent:

- **Always.** Send a cumulative list of all changes made (for example, detection or deletion) to all shares and mounts.
- **Once.** Send a notification of a change (for example, detection or deletion) to a share or mount only when that change occurs.

i. Select the Remove Deleted Shares checkbox, if required. Shares that were deleted (and deselected) from the file server will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the file server is unavailable, the shares will not be removed.

j. Select the Enable Event Collection checkbox, if required. This setting enables collecting events from all shares added from this volume or file server.

4. To set configuration options, click Configuration in the navigation pane. The configuration options display.



a. Under UNIX Domain, select the affiliated UNIX user repository for this file server or Samba domain. Use the drop-down list to select a predefined UNIX domain.

Note: You must define these domains before you define the file server. By default, the domain is set to Local.

b. Under File Server General Settings, select Save File Server Properties History if you want DatAdvantage to monitor changes in folder properties such as size, number of nested folders, number of files, and number of nested files.

Note: This data might occupy substantial storage space on the database over a long period.

c. Under Shadow Database Installation, enter the credentials needed for installing the Shadow database on the SQL Server. The user must have the sysadmin role on the selected SQL Server.

- This area is displayed only when the file server is initially installed. It is not displayed during subsequent editing.
- **Database Server.** Enter or browse for the machine on which the Shadow database server resides.
- **Authentication.** Select the required type of authentication, either SQL or Windows authentication.
- **User Name.** Enter the account user name.
- **Password.** Enter the account password.
- **Save Credentials.** Select this option to save the database credentials.
- **Custom Database Location.** Click this to set the location of data files.

d. Under SQL Host Server Credentials, enter the installation credentials for the machine on which the Shadow server resides. This account must be a member of the local administrators' group on

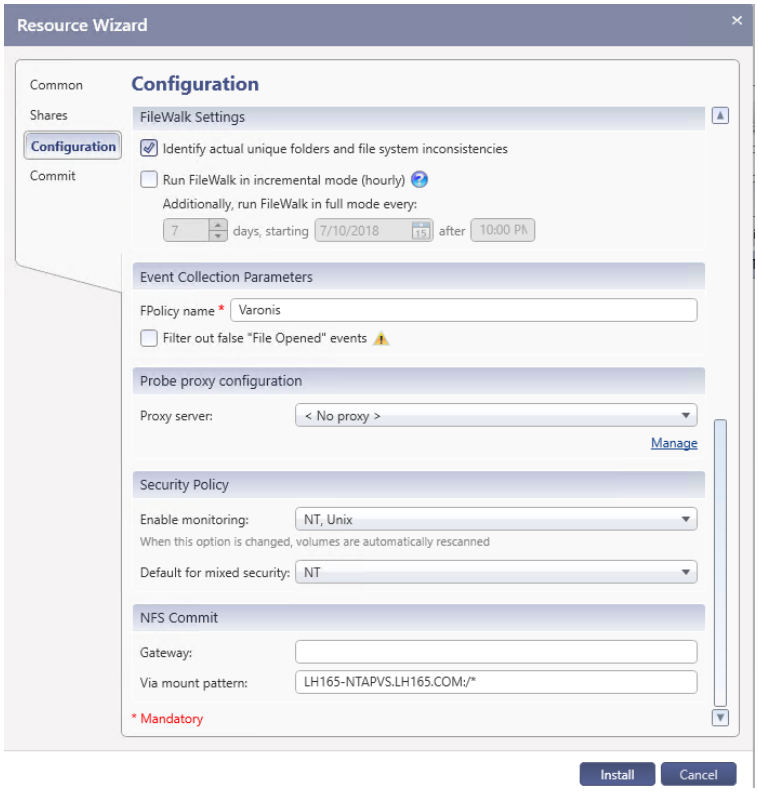
the machine during installation. The credentials are required only when the Shadow server does not reside on the IDU machine.

Note: This area is displayed only when the file server is initially installed. It is not displayed during subsequent editing.

- **User Name.** Type the installation account user name.
- **Password.** Type the installation account's password.

e. Under Local Accounts, select Collect Information Regarding Local Accounts from This Server to collect Windows local groups, local accounts, and relations.

f. Under FileWalk Settings, select Identify Actual Unique Folders and File System Inconsistencies to detect broken inheritance in NTFS file systems.



g. Under, Incremental FileWalk Settings, configure the following settings:

- **Use Incremental FileWalk.** Select this option to run scheduled FileWalk processes on folders in which events have occurred. You can modify scheduled FileWalk settings under the File Servers Jobs tab. This option is supported only for file servers on which all monitored shares use the CIFS protocol.
- **Probe Proxy Configuration.** For performance reasons, you can define a probe proxy that is located near the NetApp file server. The probe proxy can be installed on any Windows machine in the same LAN as the NetApp file server being monitored. A single proxy can be used to monitor more than one file server.
- **Proxy Server.** Select the probe proxy used to monitor the file server.
- **Manage.** Click this to add, edit, or remove proxy servers.

h. Under Event Collection Parameters, enter the FPolicy name created on the SVM. Select Filter Out False File Opened Events if you would like to filter out false reads. See the section “Create an FPolicy Event” for more details.

i. Under Security Policy, configure mixed NT and UNIX environments as follows:

- **Enable Monitoring.** Select the type of file system to be monitored in the mixed environment. When this option is changed, volumes are automatically rescanned.
- **Default for Mixed Security.** Select the default for extraction of the access control list.

5. The definitions in the NFS Commit section enable the commit process on NFS for UNIX, EMC Celerra, NetApp, and HP-NAS operating systems. To maintain security, the commit process must be activated through a gateway, which can be any UNIX machine that has access to the NFS exports on the file server and that is accessible through SSH. The gateway need only be defined for file servers on which NFS commit is available. To enable NFS commit, configure the following settings:
   - **Gateway.** Enter the IP address of the UNIX machine that acts as the gateway.
   - **Via Mount Pattern.** Enter the required pattern. This can be a host-name pattern (for example, `NETAPP10:/*`) or an IP address pattern (for example, `10.10.10.160:/*`). The asterisk (*) indicates multiple mounts on the same machine with different exports.

4.3 Varonis DatAdvantage Best Practices

To avoid performance issues, deactivate FPolicy during the following scenarios:

- When performing large data migrations from one NetApp storage system to another (large write or modification of files)
- When upgrading your release of ONTAP to a newer version
- When performing a Varonis upgrade (both IDU and probes or collectors)

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

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

5 Configuring FPolicy on ONTAP

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

The FPolicy structure is defined as follows:

- **Event.** Defines which operations and protocol types FPolicy audits.
- **External engine.** Defines the endpoint (the Varonis probe server) to which the FPolicy sends notification information.
- **Policy.** The aggregation of events policy, external engine, and scope.
- **Scope.** Defines the volumes, shares, export policies, and file extensions to which the FPolicy policy applies. You can also include and exclude all relevant filters.

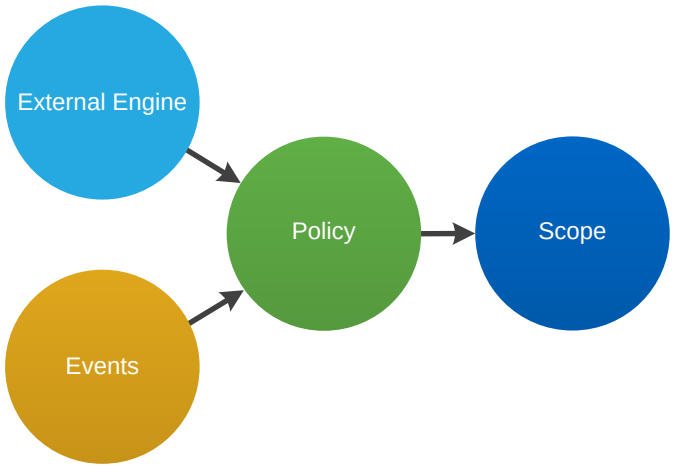
Configuration Requirements
• The shares must reside on the volume monitored for CIFS events. • The export policy must be created on and applied to the volume monitored for NFS events.

5.1 FPolicy Configuration Workflow

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

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

Figure 2) FPolicy configuration workflow.



5.2 Create an FPolicy Event

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

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

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

```
fpolicy policy event create -vserver <Vserver Name> -event-name fp_event_varonis_cifs -file-operations create, create_dir, open, delete, delete_dir, read, write, rename, rename_dir, setattr -protocol cifs -filters first-read, first-write, open-with-delete-intent
```

3. To create and verify an FPolicy event object for NFS protocol, run the following commands:

```
fpolicy policy event create -vserver <Vserver Name> -event-name fp_event_varonis_nfs -file-operations create, create_dir, delete, delete_dir, read, write, rename, rename_dir, setattr -protocol nfsv3,nfsv4 -filters first-read, first-write
```

Table 1) FPolicy event options.

Option	Description
`-vserver`	The name of the SVM on which you want to create an FPolicy external engine.
`-event-name`	The name of the FPolicy event that you want to create.
`-file-operations`	The file operations for the FPolicy event. Available values are: `create`, `create_dir`, `open`, `delete`, `delete_dir`, `read`, `write`, `rename`, `rename_dir`, and `setattr`.

Option	Description
-protocol	The name of the protocol for which the event is created. Available values are: cifs, nfsv3, and nfsv4.
-filters	The filters used with a given file operation for the protocol specified in the -protocol parameter (for example, first-read, first-write).

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

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

4. View the event object.

```
fpolicy policy event show fp_event_varonis_cifs -instance
```

5.3 Create an FPolicy External Engine

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

```
fpolicy policy external-engine create -vserver<Vserver Name> -engine-name fp_ex_eng
-primaryservers <Varonis Probe server IP> -port 2002 -extern-engine-type asynchronous
-ssl-option no-auth
```

Table 2) FPolicy external engine options.

Option	Description
-vserver	The name of the SVM on which you want to create an FPolicy external engine
-engine-name	The name of the external engine that you want to create
-primary-servers	The IP addresses for the primary FPolicy servers
-port	The port number for the FPolicy service
-extern-engine-type	The type of external engine. Only asynchronous is supported.
-ssl-option	The SSL option is for external communication with the FPolicy server. Available values include: server-auth – Provides probe authentication mutual-auth – Provides both probe and NetApp authentication When set to mutual-auth, change the SSLMutualAuth parameter to 1 in the VrnsProbeSvc.exe.user.config file. In the <ntap_cm> section of the VrnsProbeSvc.exe.user.config file, add or modify the following parameters: <ntap_cm> <add key="FilePolicyTCPPort" value="2002"/> <add key="FilePolicySSLPort" value="2003"/> <add key="SSLCACertPath" value="C:\ca.cert"/> <add key="SSLProbeCertPath" value="C:\Sample5-Server.cert"/>

Option	Description
	<add key="SSLProbeKeyPath" value="C:\Sample5-Server.key"/> <add key="SSLMutualAuth" value="0"/> </ntap_cm>

Note: By default, Varonis DatAdvantage uses TCP/2002 as the port number. You can change this number by configuring another port in the `VrnsProbeSvc.exe.user.config` file.

View the external engine or engines that you created.

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

5.4 Create an FPolicy Policy

To configure FPolicy policy, run the following commands:

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

Table 3) FPolicy policy options.

Option	Description
`-vserver`	The name of the SVM on which you want to create an FPolicy external engine.
`-policy-name`	The name of the FPolicy policy that you want to create. The default policy name, as registered in the management console, is Varonis.
`-events`	A list of events to monitor for the FPolicy policy.
`-engine`	The name of the external engine that you want to create.
`-is-mandatory`	Determines whether the FPolicy object is mandatory.

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

```
fpolicy policy show
```

5.5 Create an FPolicy Scope

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

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

Table 4) FPolicy scope options.

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

Option	Description
`-export-policies-to-include`	A comma-separated list of export policies for monitoring file access. Wildcards are supported.

2. View the FPolicy scope you created.

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

5.6 Enable an FPolicy Policy

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

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

6 Security Login Configuration for FPolicy Server

You must create a login method to work with ONTAP. Certain permissions are required to perform the following activities:

- Starting the FPolicy engine after the probe starts.
- Acquiring the volume information.
- Acquiring the `close_on_modification` settings.
- Acquiring user information.

The predefined `vsadmin` role is sufficient. To create a login method, complete the following steps:

1. Connect to the ONTAP management console.
2. Run the following command:

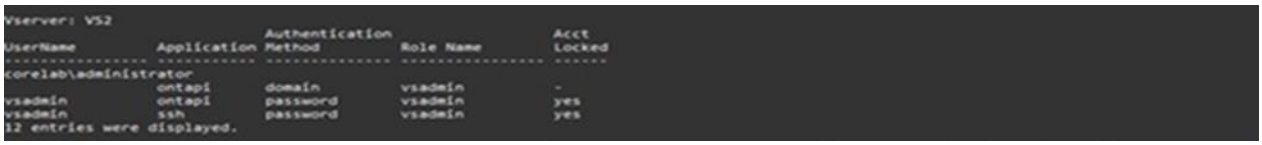
```
security login create -username <domain\username> -application ontapi -authmethod domain -role
vsadmin -vserver <Vserver Name>
```

Table 5) Security login creation options.

Option	Description
`-username`	The user name configured to send ONTAPI calls.
`-application`	The application of the login method.
`-authmethod`	The Microsoft Active Directory authentication method for the login method.
`-role`	The access-control role name for the login method.
`-vserver`	The SVM name of the login method.

Prerequisites
• Both the domain and the user name are case-sensitive and must be identical to those defined in the Management Console. • The name of the Varonis service account is limited to 15 characters.

3. After you run the previous command, run the `security login show` command to view information about user login methods on the file server.



4. If you cannot use the vsadmin role, the following permissions are sufficient.

```
security login role create –role vrnsrole –cmddirname “vserver fpolicy” –vserver CIFSVS1
security login role create –role vrnsrole –cmddirname “volume” –vserver CIFSVS1 –access readonly
security login role create –role vrnsrole –cmddirname “vserver” – vserver CIFSVS1 –access
readonly
security login role create -role vrnsrole -cmddirname "version" – vserver CIFSVS1 -access
readonly
```

The role appears as follows:

```
L65SONTAPCM::> security login role show -vserver CIFSVS1 -role vrnsrole
                    Command/
Vserver Name   Role                 Directory                              Access Query Level
-------------- -------------------- -------------------------------------- ------------------
CIFSVS1        vrnsrole             DEFAULT                                none
CIFSVS1        vrnsrole             version                                readonly
CIFSVS1        vrnsrole             volume                                 readonly
CIFSVS1        vrnsrole             vserver                                readonly
CIFSVS1        vrnsrole             vserver fpolicy                        all
```

Note: Some roles have the `-access` parameter set to `all` and not to `readonly` so that FPolicy can be enabled or disabled as needed.

7 Configuring SSL Certificates

The following procedure describes how to install a public certificate of certificate authority (CA) that is used to sign the FPolicy server certificate.

To install a public certificate of CA, complete the following steps:

1. Connect to the ONTAP management console by using PuTTY.
2. To install a public certificate and a private key:

   Note: Installing a public certificate and a private key for an FPolicy server certificate is required for mutual authentication.

   a. Run the following command:

```
security certificate install -type server –vserver <Vserver Name>
```

   Where `–type` is the certificate type and `–vserver` is the name of the SVM that contains the certificate.

   b. When prompted, enter the certificate by copying the contents of the certificate file, and enter the private key by copying the contents of the key file in the ONTAP CLI window.

   Note: From the Windows, Linux, or UNIX machine on which the certificate and key were created, you can run the `cat` command on the certificate and key files, copy the command to the clipboard, and paste the content in the ONTAP CLI window.

3. Install the public certificate of CA.

```
security certificate install -type client-ca – vserver <Vserver Name>
```

Where `–type` is the public key certificate and `–vserver` is the name of the SVM that contains the certificate.

Note: The FPolicy server certificate and the public certificate are signed by the same CA. Installing a public certificate of CA is required for FPolicy server authentication.

4. To view the public certificate of CA, run the `security certificate show` command.

   Note: When the certificates have been installed, you can use this command to view the serial number, the common name, and the certificate's CA name.

8 FPolicy Configuration Best Practices on ONTAP

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

8.1 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, see the section "Create an FPolicy Event."

Configuration of an FPolicy Scope for the SVM

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

8.2 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: In a scenario where the LIF for FPolicy traffic is configured on port different from the LIF for client traffic, the FPolicy LIF may fail over to other node because of a port failure. This renders the FPolicy server unreachable from the node and the FPolicy notifications for file operations on the node fail.

Make sure that the FPolicy server is reachable through at least one LIF on the node, to process FPolicy requests for the file operations performed on that node.

8.3 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.

8.4 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. To determine the appropriate priority, NetApp recommends working with partners.

8.5 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, first disable the policy.

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

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

8.6 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 issues, NetApp recommends assessing and sizing the environment before enabling FPolicy. Performance is affected by the number of users; workload characteristics, such as operations per user and the data size; and network latency.

9 Troubleshooting Common Problems

9.1 Problem: The FPolicy Server Is Disconnected

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

Command example:

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

9.2 Problem: The FPolicy Server Does Not Connect.

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

Command example:

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

Potential cause number 1: There are issues with routing.

Potential solution: Check the routing table entries by using the command `routing-groups route show` to check whether a route is available for the SVM. If not, add a route with the `routing-groups route create` command.

Command example:

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

Potential cause number 2: The FPolicy server is not listening on the port specified.

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

Command example:

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

Potential cause number 3: The security options for the external engine are not the same as for the FPolicy server.

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

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

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

Command example:

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

Potential cause number 4: The LIF dedicated for the FPolicy traffic has failed over to a different node.

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

Command example:

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

9.3 Problem: The External Engine Is Not Native for the Policy

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

Command example:

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

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

Potential cause: The FPolicy policy scope is not set properly.

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

Command example:

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

10 Performance Monitoring

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

Monitoring the performance counters on FPolicy server and ONTAP identifies bottlenecks in the solution and allows you to tune the parameters necessary for an optimal solution. For example, an increase in FPolicy latency has a cascading effect on CIFS latency. Therefore, you should monitor both workload (CIFS) and FPolicy latency. Also, you can use quality-of-service policies in ONTAP to set up a workload for each volume or SVM that is enabled for FPolicy.

NetApp recommends displaying workload statistics by using the `statistics show –object workload` command. NetApp also recommends that you monitor the average, read, and write latencies; the total number of operations; and the read and write counters. You can also use the following ONTAP FPolicy counters to monitor the performance of FPolicy subsystems.

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

10.1 Collect and Display FPolicy Counters

To collect FPolicy counters, run the following commands:

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

To display FPolicy counters, run the following commands:

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

10.2 Counters to Monitor

Table 6 and Table 7 contain lists of FPolicy counters that can be monitored.

Table 6) 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 7) 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

Counters	Description
response_received_rate	Number of screen responses received from FPolicy server per second

11 Conclusion

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

Where to Find Additional Information

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

Version History

Version	Date	Document Version History	Author
Version 2.0	September 2018	Partner content and FlexGroup update	Brahmanna Chowdary Kodavali
Version 1.1	June 2016	ONTAP updates	Brahmanna Chowdary Kodavali, Saurabh Singh
Version 1.0	June 2015	First version of the document	Brahmanna Chowdary Kodavali, Saurabh Singh

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

Copyright Information

Trademark Information