EditShare®

EditShare Audit and Monitor User Guide

Version 2021.3

May 2021

Notice:

To the best of our knowledge, the information in this document is accurate; however, EditShare assumes no responsibility or liability for the accuracy or completeness of this information. Mention of trade names or commercial products does not constitute endorsement by EditShare except where explicitly stated.

EditShare
3 Brook Street
Watertown, MA 02472

Tel: 617-782-0479 Fax: 617-782-1071

www.editshare.com

Contents

Chapter 1: Introduction

The EditShare File System (EFS) Audit and Monitor features are optional features that can be enabled.

The EFS Audit feature records user activities such as media space mounts and unmounts, file opens, reads, writes, and deletes. The EFS Monitor feature records a periodic sample of the system state, including the amount of CPU, memory, and disk space being used.

In a post-production facility, for example, each time an editor mounts a Media Space on the EFS storage system via a client workstation, a monitor event records this action. Similarly, each time a file is opened, a timeline is scrubbed, played out and saved or deleted, specific monitor events are generated and time-stamped.

In the same way that footprints, fingerprints and surveillance footage can help a detective understand the who, what, when, where, and how of a crime scene, the content of file monitor logs can help storage system administrators understand who did what, to which files, and when and how they did it.

Depending on how your EFS storage system is configured, monitor events will be recorded in a local directory on your EFS Master's OS drives or on dedicated SSD drives provided specifically for storing monitor data. In the future, EditShare also plans to support forwarding monitor data to third party Security Information and Event Management (SIEM) systems such as SolarWinds LEM, ManageEngine, or similar solutions. Several SIEM system manufacturers have made a commitment to EditShare that they will make their applications understand EFS monitor data as soon as there is a customer who requests this capability and makes a purchase of the SIEM product.

In a busy post production environment, editing workflows can produce large volumes of monitor events which, without efficient and easy-to-use analysis and reporting tools, can be difficult to understand. When configured to support File Audit and System Monitoring, XStream EFS systems also provide an in-situ Analysis Dashboard that makes it easy for system administrators to analyze monitor event logs stored in local directories and generate monitor reports.

The Audit and Monitor features are supported on all EditShare EFS Shared Storage Systems equipped with 7.2.3.0 software and newer.

Chapter 2: Using EFS Audit and Monitor Features

Enabling the Audit and Monitor Role in your EFS System

In order to enable and use EFS Audit and Monitor features, the EFS Audit and Monitor role must be enabled via the EditShare Role Assistant on whatever server is the EFS Master.

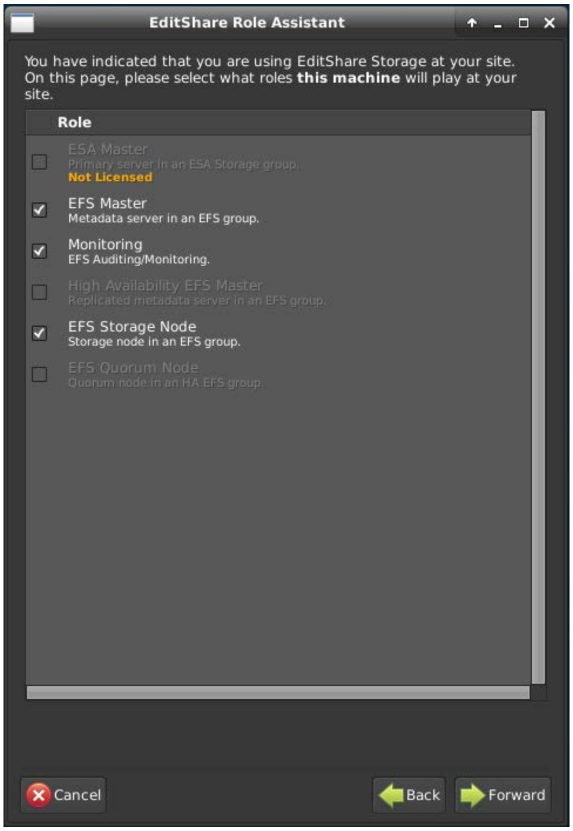
In a High Availability (HA) environment, it is very important that you only enable the EFS Monitor role on one Metadata server. After Auditing and Monitoring is up and running on that Metadata server, it is then necessary to run the Role Assistant on the other Metadata Server without selecting any new roles.

Do not try to enable the Monitor role on both Metadata servers in an HA cluster.

Many other server configuration settings are also established with the ERA. For additional details, see “Configuring EFS Shared Storage Systems” located in the *EditShare Administrator's Guide*.

Configuring the Audit and Monitoring Features

Open the ERA and navigate to the Roles selection panel. Check the EFS Monitor role and save your selections. When you have finished with the ERA, the Audit and Monitor features are active.



EditShare Role Assistant

You have indicated that you are using EditShare Storage at your site. On this page, please select what roles **this machine** will play at your site.

Role

□ ESA Master
Primary server in an ESA Storage group.
Not Licensed

☑ EFS Master
Metadata server in an EFS group.

☑ Monitoring
EFS Auditing/Monitoring.

□ High Availability EFS Master
Replicated metadata server in an EFS group.

☑ EFS Storage Node
Storage node in an EFS group.

□ EFS Quorum Node
Quorum node in an HA EFS group.

Chapter 3: Authentication

NOTE: The authentication (and https) is not used prior to the 2021.1 release.

EditShare's Auditing and Monitoring component has independent authentication from the rest of the storage product. When Auditing and Monitoring is initially installed, it has a default username (editshare) and password (changeme0479) that match the rest of the product.

NOTE: Although this has been previously mentioned, it is worth reiterating the fact that the Auditing and Monitoring password is independent of the standard EditShare password. Changing the standard EditShare password Does Not change the Auditing and Monitoring password.

Updating the Auditing and Monitoring Authentication Password

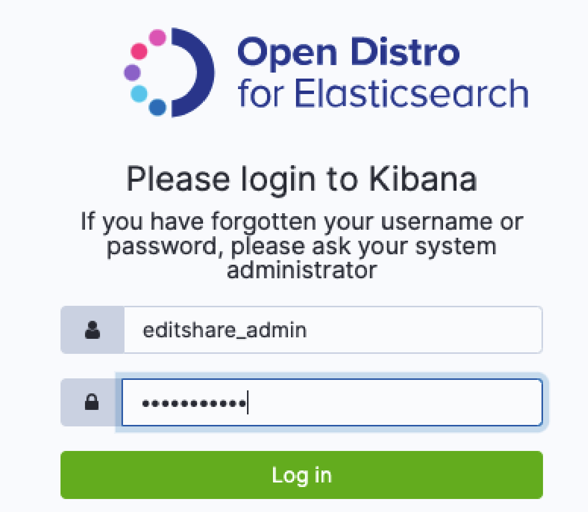
To assign the Auditing and Monitoring Authentication Password:

1. Navigate to the Auditing and Monitoring User Interface. URL is:

   ```
   https://<efsmaster IP_address>:5601/
   ```

2. Login but you can also access the interface from the EditShare Landing page.
3. Kibana is the User Interface for Auditing and Monitoring. Enter the Kibana Administrative username and password.

   NOTE: Out of the box, there are two usernames available in Kibana: the admin one of editshare_admin *and the readonly one of* editshare*. The former has all Kibana privileges; the latter has read only access to Kibana. The default password for* editshare_admin *is* danalex0603. *The default password for* editshare *is* changeme0479. *After entering the username and password, click **Log in**.*



Open Distro for Elasticsearch

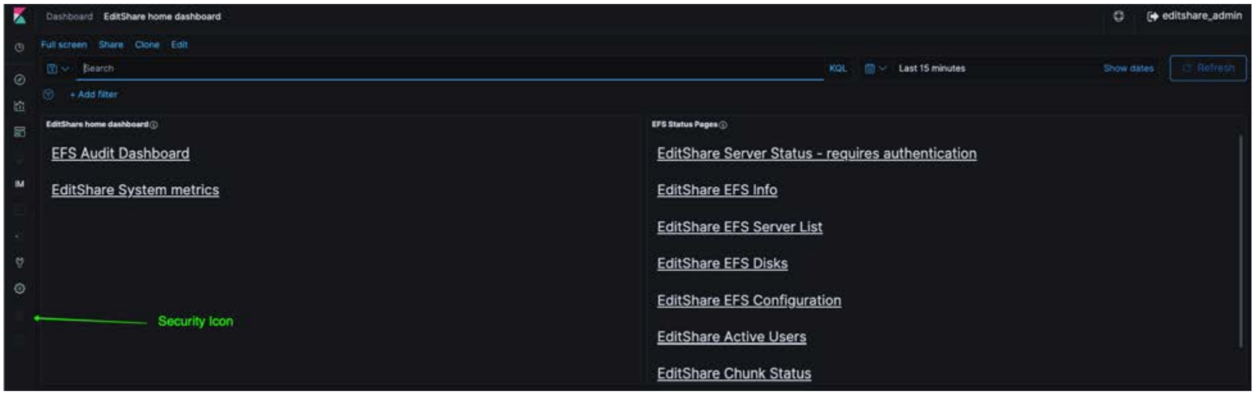
Please login to Kibana

If you have forgotten your username or password, please ask your system administrator

editshare_admin

••••••••••••

4. After Kibana loads, click on the security icon located on the left hand side of the browser. Button is a bit hard to see, but is a “lock icon”. Alternatively, navigate to: https://<master IP_address>:5601/app/security-configuration#



EditShare home dashboard

EFS Audit Dashboard

EditShare System metrics

EFS Status Pages

EditShare Server Status - requires authentication

EditShare EFS Info

EditShare EFS Server List

EditShare EFS Disks

EditShare EFS Configuration

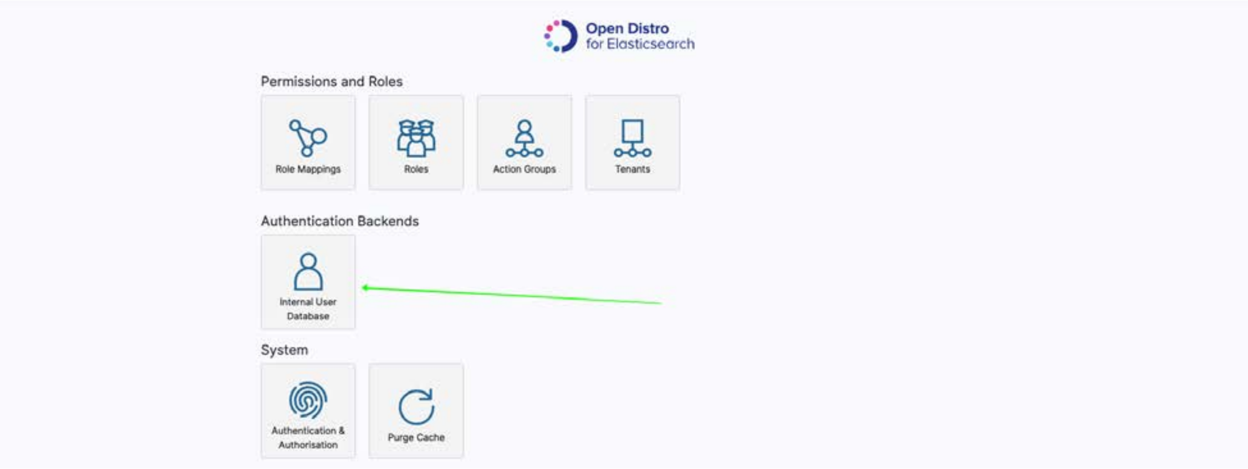
EditShare Active Users

EditShare Chunk Status

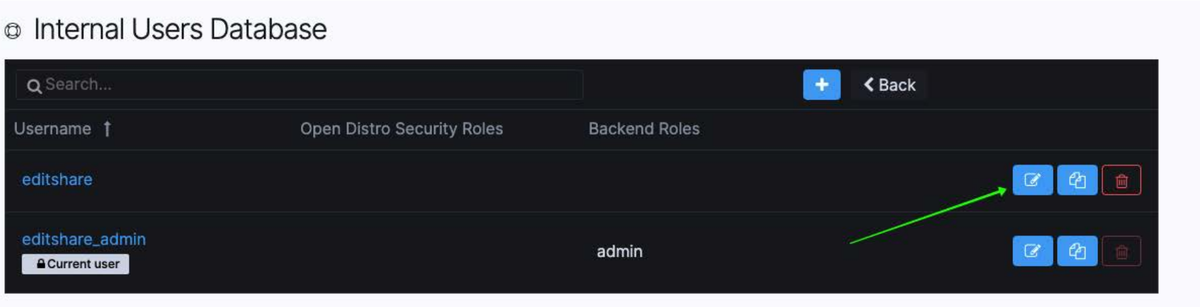
5. From the security page, click on the “Internal User Database” button.

   WARNING: There are two types of users:

   - ***editshare - These users have read only privileges.***
   - ***editshare_admin - Caution must be used, as editshare_admin users can cause damage within this page. Do not manipulate anything beyond what is described.***



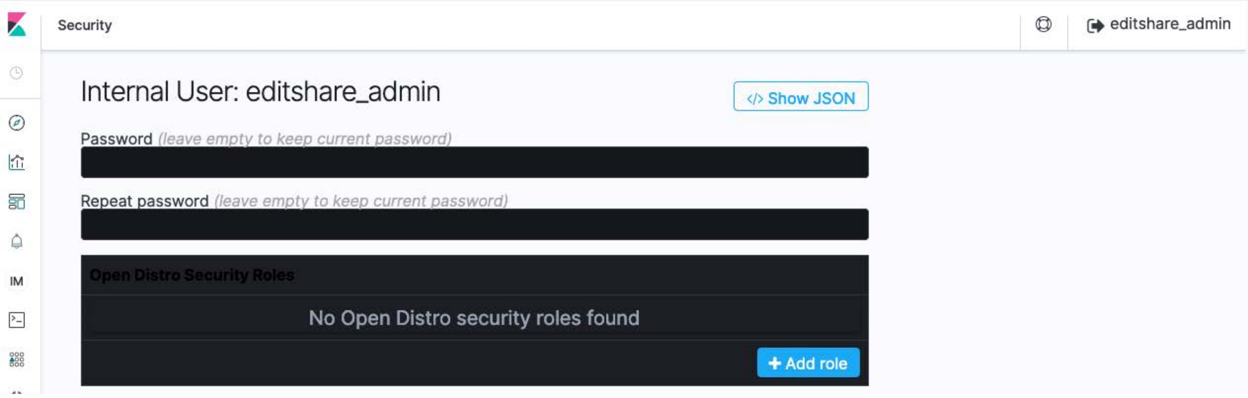
A list of available users (two available users in the following example).



Internal Users Database

Username	Open Distro Security Roles	Backend Roles
editshare		
editshare_admin Current user		admin

6. Click the edit button (✎) next to the desired user.



Internal User: editshare_admin

Password *(leave empty to keep current password)*

Repeat password *(leave empty to keep current password)*

Open Distro Security Roles

No Open Distro security roles found

7. To change the password, Enter the desired password in the first two fields and click **Submit**.
8. Log out of the system by clicking **editshare_admin** in the upper right corner.

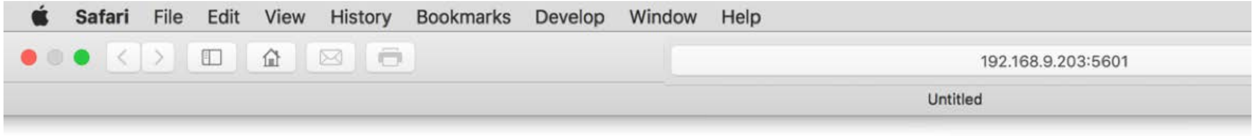
Validating Login Credentials

After you have logged out of the editshare_admin account, you will be brought back to the Kibana login page. Enter **editshare** as the user and the same password you entered previously. You should be logged into Kibana as a read only user.

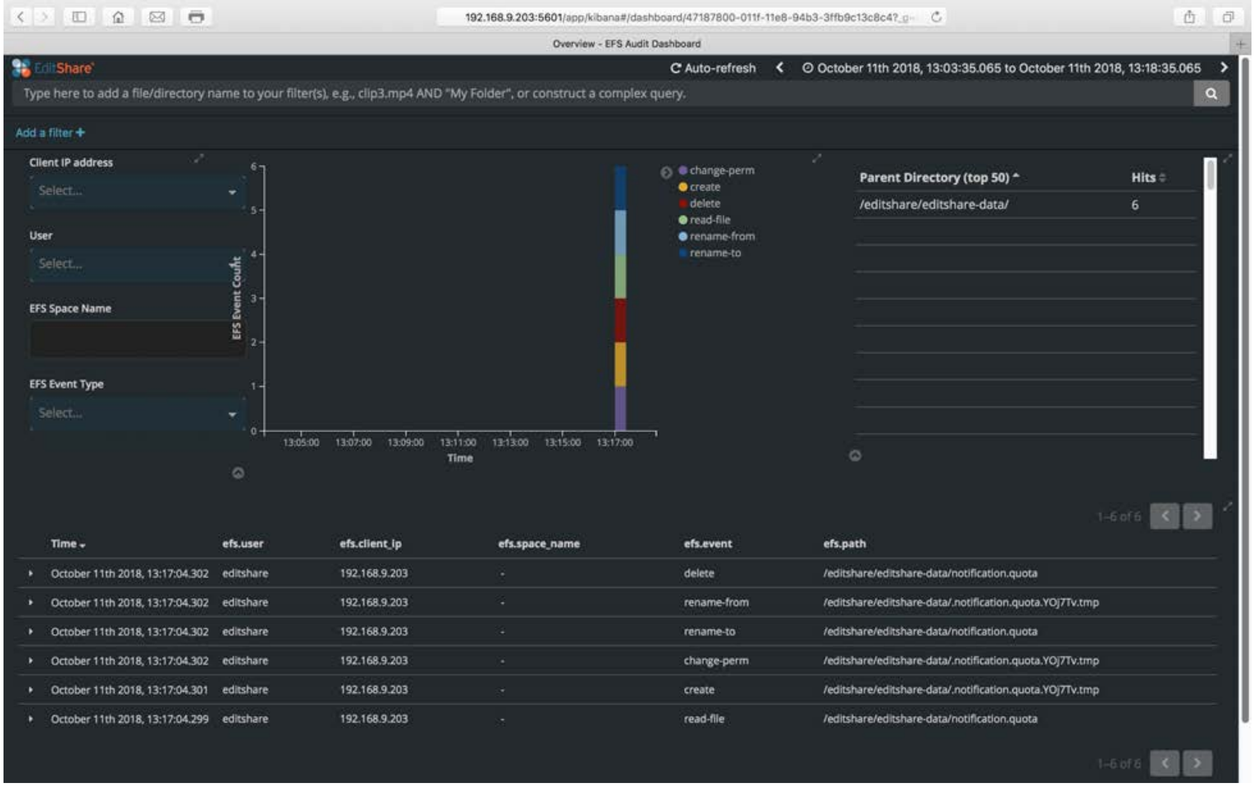
Chapter 4: Configuring the Audit and Monitor Features

Opening the Monitor Dashboard

Using a laptop or workstation and up-to-date browser, enter the IP address of your EFS Master server (https) followed by port 5601 into the URL line as shown below. Or start at the landing page and click on the Audit/Monitor link.



The EFS Monitor Dashboard should now open.



192.168.9.203:5601/app/kibana#/dashboard/47187800-011f-11e8-94b3-3ffb9c13c8c4?_g=

Overview - EFS Audit Dashboard

Parent Directory (top 50)	Hits
/editshare/editshare-data/	6

Time	efs.user	efs.client_ip	efs.space_name	efs.event	efs.path
October 11th 2018, 13:17:04.302	editshare	192.168.9.203	-	delete	/editshare/editshare-data/notification.quota
October 11th 2018, 13:17:04.302	editshare	192.168.9.203	-	rename-from	/editshare/editshare-data/.notification.quota.YOj7Tv.tmp
October 11th 2018, 13:17:04.302	editshare	192.168.9.203	-	rename-to	/editshare/editshare-data/notification.quota
October 11th 2018, 13:17:04.302	editshare	192.168.9.203	-	change-perm	/editshare/editshare-data/.notification.quota.YOj7Tv.tmp
October 11th 2018, 13:17:04.301	editshare	192.168.9.203	-	create	/editshare/editshare-data/.notification.quota.YOj7Tv.tmp
October 11th 2018, 13:17:04.299	editshare	192.168.9.203	-	read-file	/editshare/editshare-data/notification.quota

Configuring Auditing and Monitoring

Setting up the Audit and Monitor roles involves the use of the ERA as well as manual implementation of certain server configuration settings.

Please speak with EditShare Technical Support before attempting to set up Auditing and Monitoring.

Configuring Standard Auditing and Monitoring

Standard Auditing and Monitoring mode requires a system configuration that includes optional redundant fast storage dedicated file monitor event storage. Such a configuration provides 512GB of monitor event storage and can store approximately 3.4 billion events.

Standard Auditing and Monitoring mode is available for use on any variant of EFS Metadata Server or EFS 300 All-in-One server that is equipped with the Auditing and Monitoring Hardware Upgrade Kit. Field upgrade kits are available.

Monitor Event Types

EFS logs the following types of events:

Event	**Action**
mount, unmount	Indicates a successful mounting of a media space by an EFS user. Note: mount/unmount events are only recorded when users connect to EFS storage using the EFS native client. Mount/unmount is not recorded when the connection is over SMB or NFS.
create	Indicates the successful creation of a file or directory by an EFS user.
read-file	Indicates that a file has been opened for reading or has been read by an EFS user.
write-file	Indicates that a file has been opened for writing, has been written or has been truncated by an EFS user.

list-dir	Indicates that the contents of a directory have been listed by an EFS user.
change-perm, rec-change-perm	Indicates that file mode, owner, owning group or access control list have been changed by an EFS user.
rename-from, rename-to	Indicates that a file or directory has been renamed or moved by an EFS user.
delete	Indicates that a file or directory has been deleted by an EFS user.

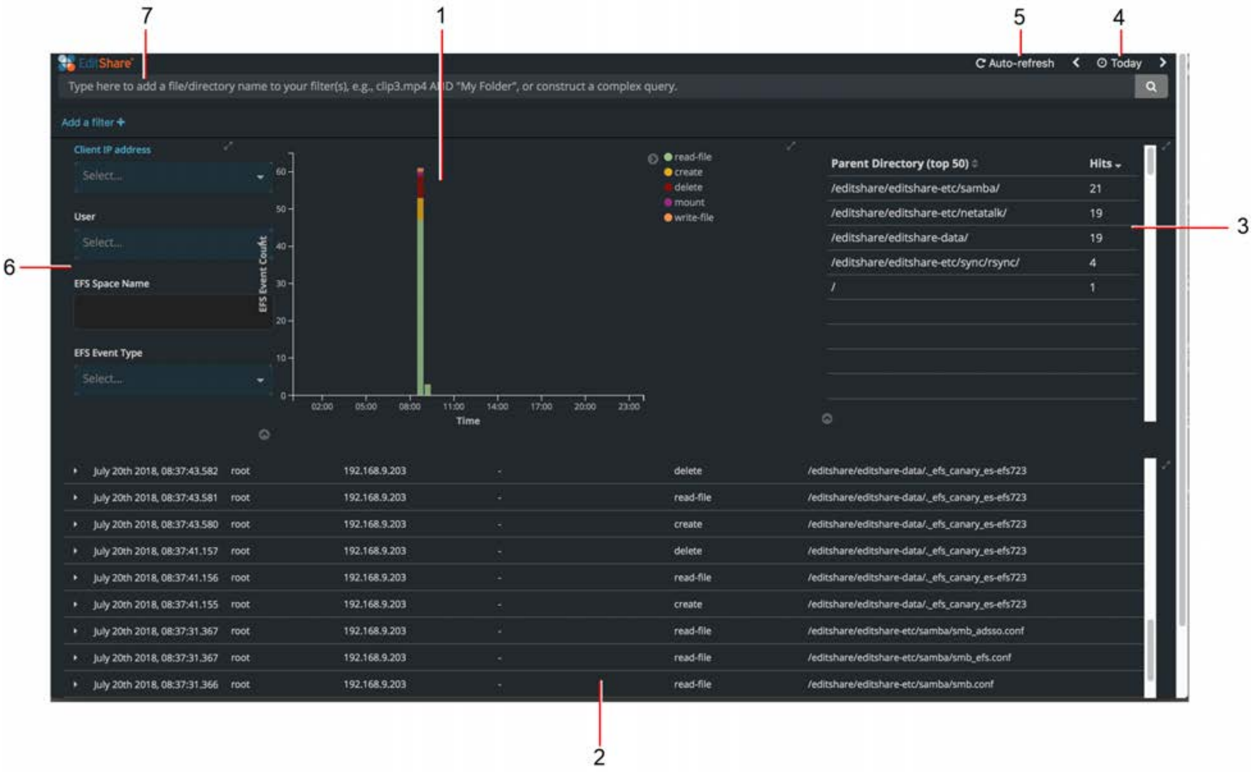
Monitor Event Attributes

In addition to the type of event, every file monitor event is described by the following attributes that play a vital role in EFS monitor event analysis:

Event	**Action**
ts	Unix timestamp of the operation, which is copied and converted to readable content and available in the @timestamp field in Kibana.
uid, username	UID/username of the user who performed the operation.
client_ip	IP address of the machine from which the operation was requested. Note that the IP address is only recorded when EFS storage is accessed by the native EFS client. If it is accessed by SMB or NFS, the IP address of the storage node that was running the Samba or NFS process will be recorded.
path, node	The absolute path to the file or directory subject to the operation and its node number.

Navigating the File Monitor Dashboard

When you open the Monitor Dashboard, the following screen (or similar) is displayed:



Parent Directory (top 50)	Hits
/editshare/editshare-etc/samba/	21
/editshare/editshare-etc/netatalk/	19
/editshare/editshare-data/	19
/editshare/editshare-etc/sync/rsync/	4
/	1

July 20th 2018, 08:37:43.582	root	192.168.9.203	-	delete	/editshare/editshare-data/._efs_canary_es-efs723
July 20th 2018, 08:37:43.581	root	192.168.9.203	-	read-file	/editshare/editshare-data/._efs_canary_es-efs723
July 20th 2018, 08:37:43.580	root	192.168.9.203	-	create	/editshare/editshare-data/._efs_canary_es-efs723
July 20th 2018, 08:37:41.157	root	192.168.9.203	-	delete	/editshare/editshare-data/._efs_canary_es-efs723
July 20th 2018, 08:37:41.156	root	192.168.9.203	-	read-file	/editshare/editshare-data/._efs_canary_es-efs723
July 20th 2018, 08:37:41.155	root	192.168.9.203	-	create	/editshare/editshare-data/._efs_canary_es-efs723
July 20th 2018, 08:37:31.367	root	192.168.9.203	-	read-file	/editshare/editshare-etc/samba/smb_adsso.conf
July 20th 2018, 08:37:31.367	root	192.168.9.203	-	read-file	/editshare/editshare-etc/samba/smb_efs.conf
July 20th 2018, 08:37:31.366	root	192.168.9.203	-	read-file	/editshare/editshare-etc/samba/smb.conf

The following section describes the key features of the Monitor dashboard, and what they are used for:

1 - Analysis Output

The graphical output of the monitor event analysis. Analysis output includes only those events that satisfy the analysis criteria and displays them in bar graph format. The horizontal axis is the timestamp range of interest. Its legend describes monitor event types present. Monitor event analysis output can also be represented in tabular form.

2 - Verbose Analysis Output

A tabular list of all monitor events included in the Analysis Output. Verbose Analysis Output shows each event and the complete set of associated monitor event attributes.

3 - Most Active Directories

A list of the top 50 directories in terms of number of monitor events included in the Analysis Output. At a glance, this section tells you where the largest amount of user activity has occurred.

4 - Timestamp Range

Indicates the range of the monitor event timestamps that are contained in the analysis. Clicking on this indicator opens the Timestamp Range configuration window.

5 - Refresh Rate

Indicates the state of the data refresh mechanism - manual/auto, running/paused. Clicking on this indicator opens the auto Refresh configuration window. From here you can choose a variety of auto refresh options.

6 - Analysis Filters

Analysis filters are an easy way to limit the potentially enormous numbers of file events to a specific range of interest. Drop-down menus make this easy to understand and enables fast analysis.

7 - Search Bar

A powerful, full-text search bar that makes it easy to describe and find monitor events of interest. For example, if you are interested in finding out all events associated with a file called "elephants", simply enter this term in the search bar and your analysis will then include only events associated with that file name.

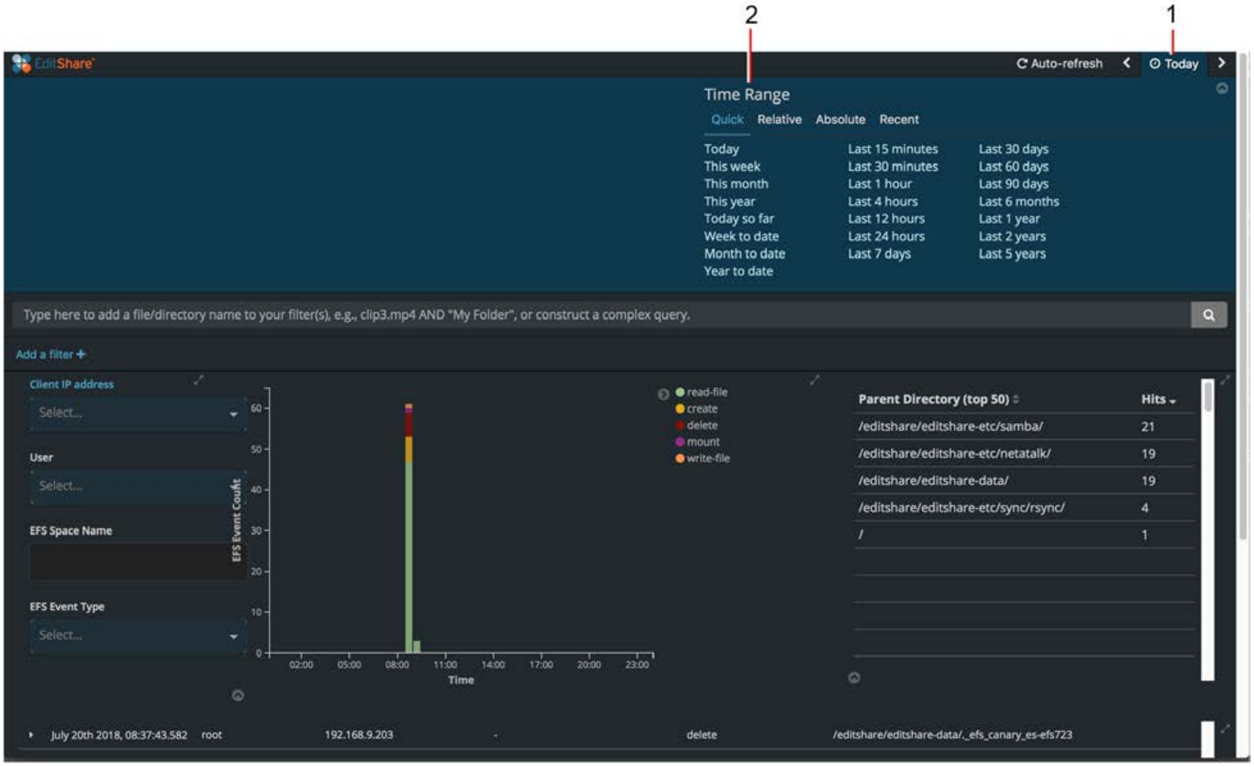
Using the Monitor Analysis Dashboard

There is really no right or wrong place to begin configuring the Monitor Analysis Dashboard. However, when you have a particular objective in mind, certain starting points make more sense than others. For example, if you are investigating the actions of a specific user; it makes sense to begin by limiting the analysis to events associated with that user. Alternatively, if you are investigating events associated with a specific media space, it would make sense to begin by constraining the analysis to events associated with that media space.

Configuring the Timestamp Range

Since the time frame of interest for an investigation is almost always well understood, we will start by explaining the configuration of the timestamp range. This involves opening the configuration panel, choosing the type of timestamp range to apply, and defining the specific range of the events of interest. You can configure the time range panel with 4 different range setting options; Quick, Relative, Absolute, and Recent. By default, the Quick Option is selected.

1. Open the timestamp range window by clicking on the timestamp range indicator.



Parent Directory (top 50)	Hits
/editshare/editshare-etc/samba/	21
/editshare/editshare-etc/netatalk/	19
/editshare/editshare-data/	19
/editshare/editshare-etc/sync/rsync/	4
/	1

```
July 20th 2018, 08:37:43.582   root   192.168.9.203   -   delete   /editshare/editshare-data/._efs_canary_es-efs723
```

2. The Time Range panel displays with four different range setting options:
   - Quick (selected by default)
   - Relative
   - Absolute
   - Recent

Setting the Timestamp Range with the Quick Option

The Quick option provides more than 20 different ways to easily define the time range of interest. In most cases, there will be a Quick option that is suitable for most monitor analysis tasks.

For example, if you want to analyze user events that have occurred in the last 30 minutes, choosing the Last 30 minutes option would be suitable. Similarly, use other "Last x minutes/hours/days/months/years" to specify relevant time frames of interest.

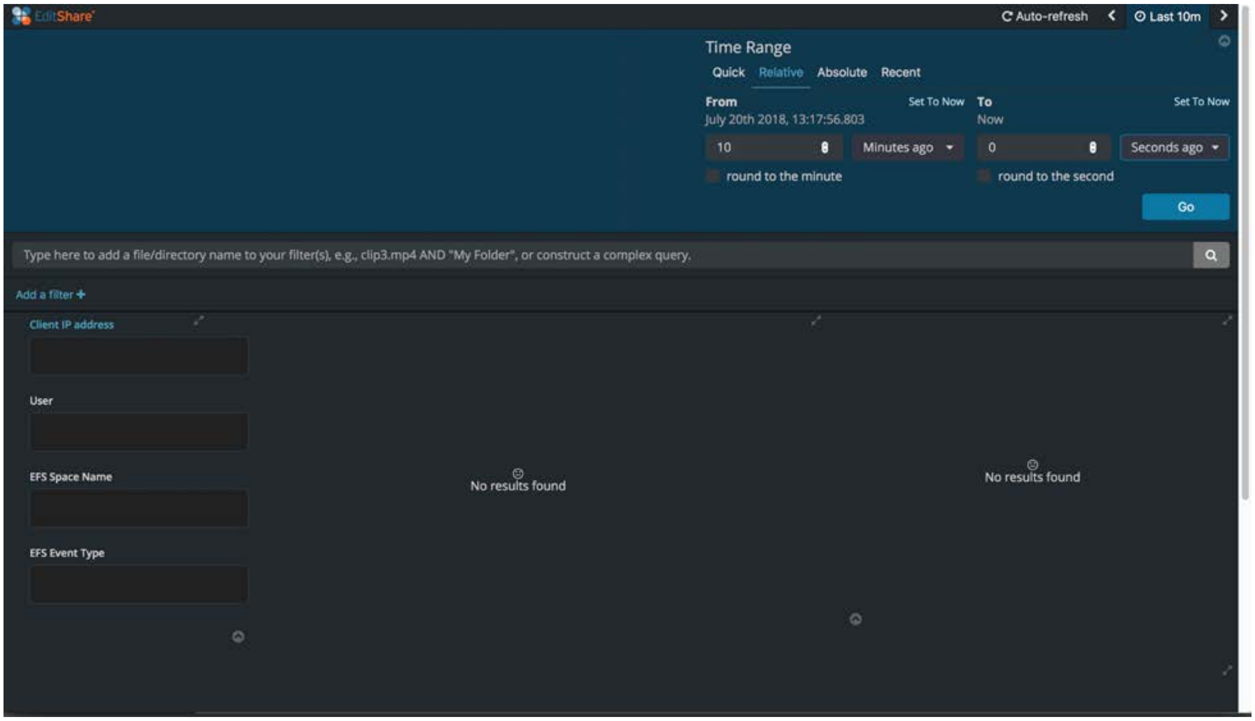
Alternatively, if you want to constrain user events to only those that have occurred today (on this day), you can choose either Today or Today so far. The subtle difference between the two is that the former will always display a 24 hour timeline while the latter will have a timeline only as long as the time that has elapsed so far during the day. This Week and Week to date, This Month and Month to date, and This Year, and Year to date have that same subtle difference.

Note: When Quick options are selected, each time the database is updated by the Auto or Manual refresh mechanism, newer data is appended to, and older data is deleted from the event database. Over time, therefore, refreshing has the potential for changing the results of a monitor analysis.

Setting the Timestamp Range with the Relative Option

You can use the Relative option to specify the time range in terms of a From starting point to a To ending point. When first opened, the default From and To points are both set to Now. Set different Starting and ending points with Seconds ago, Minutes ago, Hours ago, Days ago, Weeks ago, Months ago, Years ago or Seconds from now, Minutes from now, Hours from now, Days from now, Weeks from now, Months from now, Years from now formats.

Note: When Relative options are being employed, each time the database is updated by the Auto or Manual refresh mechanism, newer data is appended to and older data is deleted from the event database. Over time, therefore, refreshing has the potential for changing the results of an monitor analysis whose time range is specified with the Relative option.



Time Range

From
July 20th 2018, 13:17:56.803
10 Minutes ago
□ round to the minute

To
Now
0 Seconds ago
□ round to the second

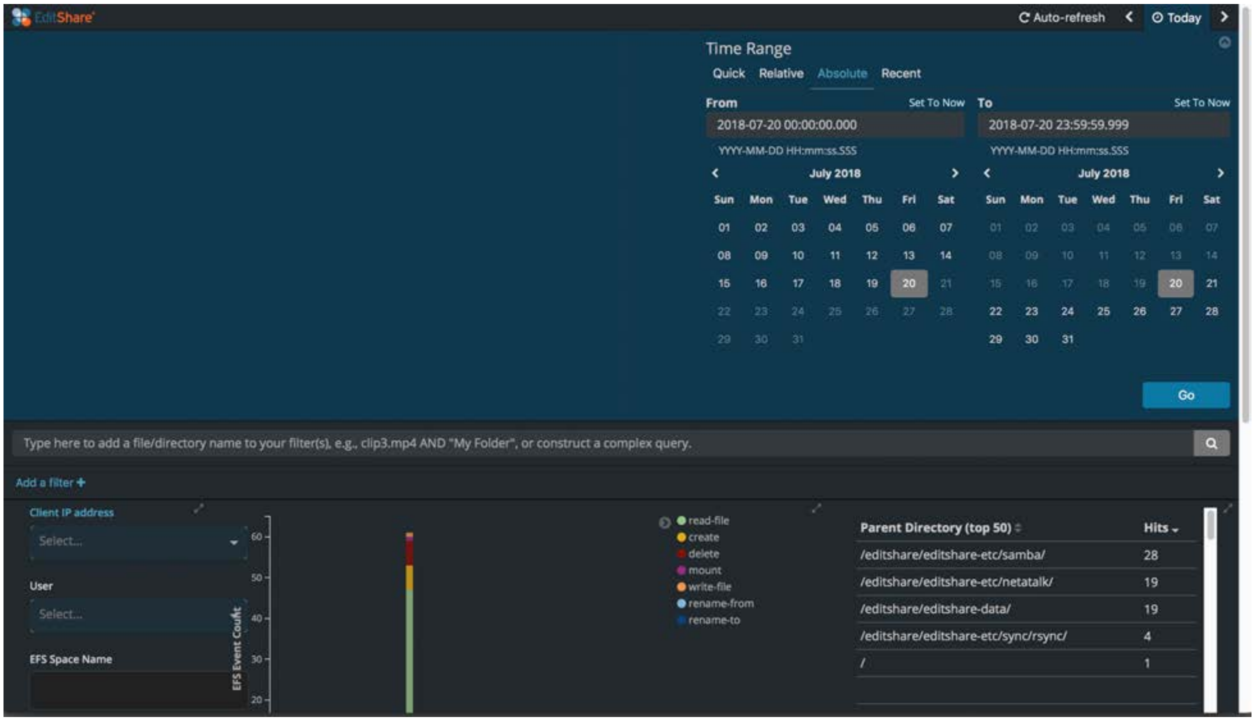
Type here to add a file/directory name to your filter(s), e.g., clip3.mp4 AND "My Folder", or construct a complex query.

No results found

No results found

Setting the Timestamp Range with the Absolute Option

Like the Relative option, you can use the Absolute option to specify the time range in terms of a From starting point to a To ending point. The difference is that when the Absolute option is used, starting and ending points are specified with absolute YYYY-MM-DD HH:mm:ss:SSS formats (Year-Month-Day Hour:Minute:Seconds:Milliseconds). When specified this way, the contents of the monitor event database do not change as it refreshes.



Time Range

From: 2018-07-20 00:00:00.000 (YYYY-MM-DD HH:mm:ss.SSS)

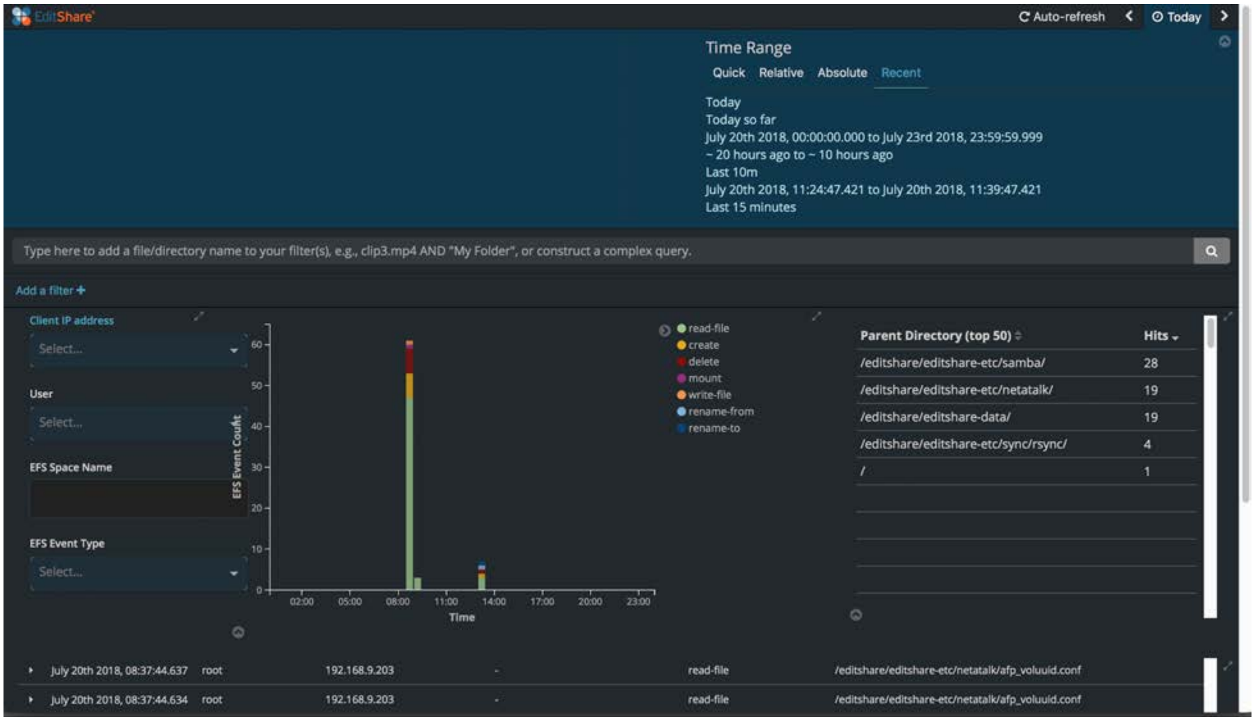
To: 2018-07-20 23:59:59.999 (YYYY-MM-DD HH:mm:ss.SSS)

Type here to add a file/directory name to your filter(s), e.g., clip3.mp4 AND "My Folder", or construct a complex query.

Parent Directory (top 50)	Hits
/editshare/editshare-etc/samba/	28
/editshare/editshare-etc/netatalk/	19
/editshare/editshare-data/	19
/editshare/editshare-etc/sync/rsync/	4
/	1

Setting the Timestamp Range with the Recent Option

The Recent option remembers specific time ranges previously used and provides a simple way to use a time range in a repeated fashion.



Today
Today so far
July 20th 2018, 00:00:00.000 to July 23rd 2018, 23:59:59.999
~ 20 hours ago to ~ 10 hours ago
Last 10m
July 20th 2018, 11:24:47.421 to July 20th 2018, 11:39:47.421
Last 15 minutes

Parent Directory (top 50)	Hits
/editshare/editshare-etc/samba/	28
/editshare/editshare-etc/netatalk/	19
/editshare/editshare-data/	19
/editshare/editshare-etc/sync/rsync/	4
/	1

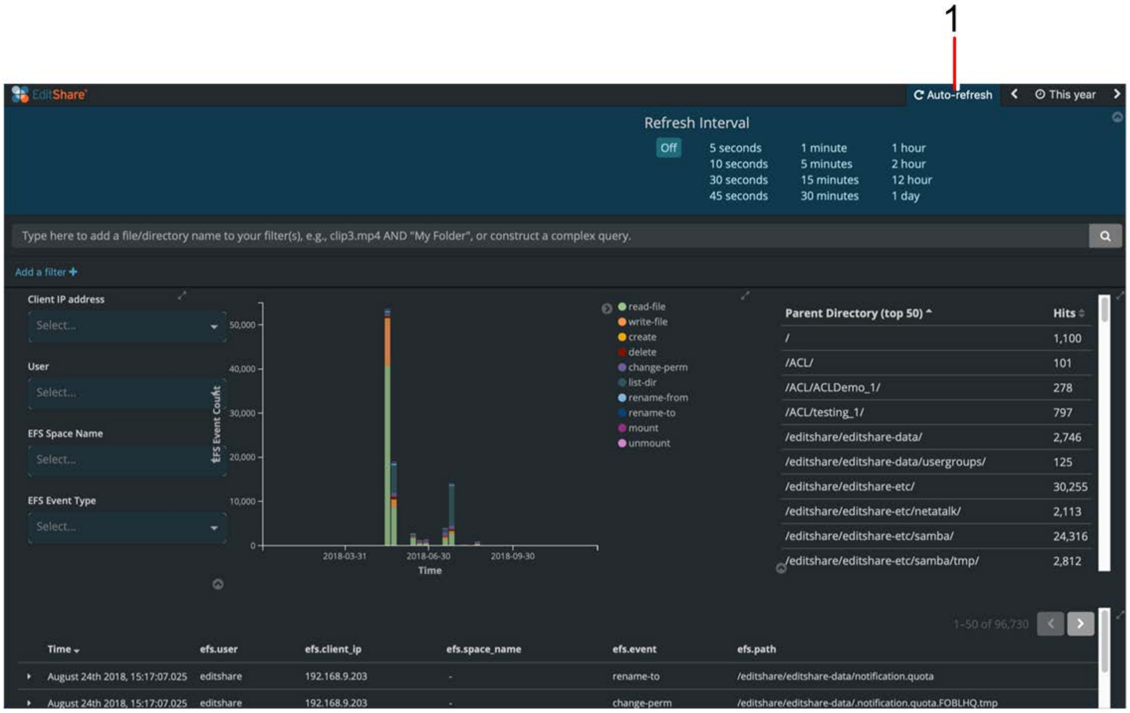
```
July 20th 2018, 08:37:44.637   root   192.168.9.203   -   read-file   /editshare/editshare-etc/netatalk/afp_voluuid.conf
July 20th 2018, 08:37:44.634   root   192.168.9.203   -   read-file   /editshare/editshare-etc/netatalk/afp_voluuid.conf
```

Setting the Timestamp Range Using a Mouse

To set the Timestamp Range, place your mouse pointer on one side of the range of interest and then click and drag it to the other end of the range and release. This allows you to select the time range of interest, based on the range of interest, without knowing the specific time range.

Configuring the Refresh Option

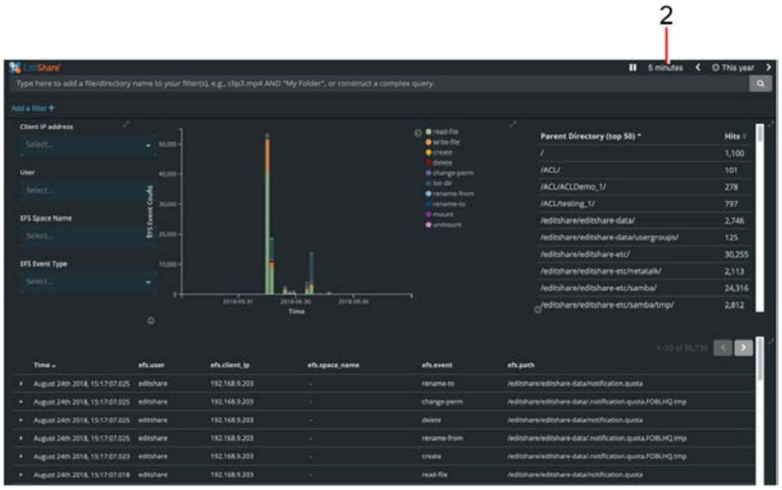
1. When you first open the Analysis Dashboard, click on the Auto-refresh tab to open up the menu.



Parent Directory (top 50)	Hits
/	1,100
/ACL/	101
/ACL/ACLDemo_1/	278
/ACL/testing_1/	797
/editshare/editshare-data/	2,746
/editshare/editshare-data/usergroups/	125
/editshare/editshare-etc/	30,255
/editshare/editshare-etc/netatalk/	2,113
/editshare/editshare-etc/samba/	24,316
/editshare/editshare-etc/samba/tmp/	2,812

Time	efs.user	efs.client_ip	efs.space_name	efs.event	efs.path
August 24th 2018, 15:17:07.025	editshare	192.168.9.203	-	rename-to	/editshare/editshare-data/notification.quota
August 24th 2018, 15:17:07.025	editshare	192.168.9.203	-	change-perm	/editshare/editshare-data/.notification.quota.FOBLHQ.tmp

2. Choose how often you want the monitor information to be updated. In this example, we have elected to have our monitor data updated every 5 minutes. Once selected, the menu closes and the refresh interval is displayed at the top right of the dashboard.

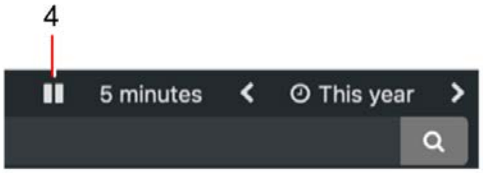


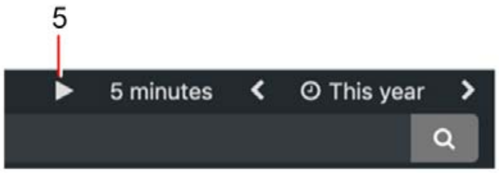
Parent Directory (top 50)	Hits
/	1,100
/ACL/	101
/ACL/ACLDemo_1/	278
/ACL/testing_1/	797
/editshare/editshare-data/	2,746
/editshare/editshare-data/usergroups/	125
/editshare/editshare-etc/	30,255
/editshare/editshare-etc/netatalk/	2,113
/editshare/editshare-etc/samba/	24,316
/editshare/editshare-etc/samba/tmp/	2,812

Time	efs.user	efs.client_ip	efs.space_name	efs.event	efs.path
August 24th 2018, 15:17:07.025	editshare	192.168.9.203	-	rename-to	/editshare/editshare-data/notification.quota
August 24th 2018, 15:17:07.025	editshare	192.168.9.203	-	change-perm	/editshare/editshare-data/.notification.quota.FOBLHQ.tmp
August 24th 2018, 15:17:07.025	editshare	192.168.9.203	-	delete	/editshare/editshare-data/notification.quota
August 24th 2018, 15:17:07.025	editshare	192.168.9.203	-	rename-from	/editshare/editshare-data/.notification.quota.FOBLHQ.tmp
August 24th 2018, 15:17:07.023	editshare	192.168.9.203	-	create	/editshare/editshare-data/.notification.quota.FOBLHQ.tmp
August 24th 2018, 15:17:07.018	editshare	192.168.9.203	-	read-file	/editshare/editshare-data/notification.quota

3. At this point, your data is being updated every 5 minutes. You will see a subtle progress indicator displayed across the top of the Dashboard every 5 minutes.

4. If you want to pause the auto-refresh mechanism, click on the pause icon.



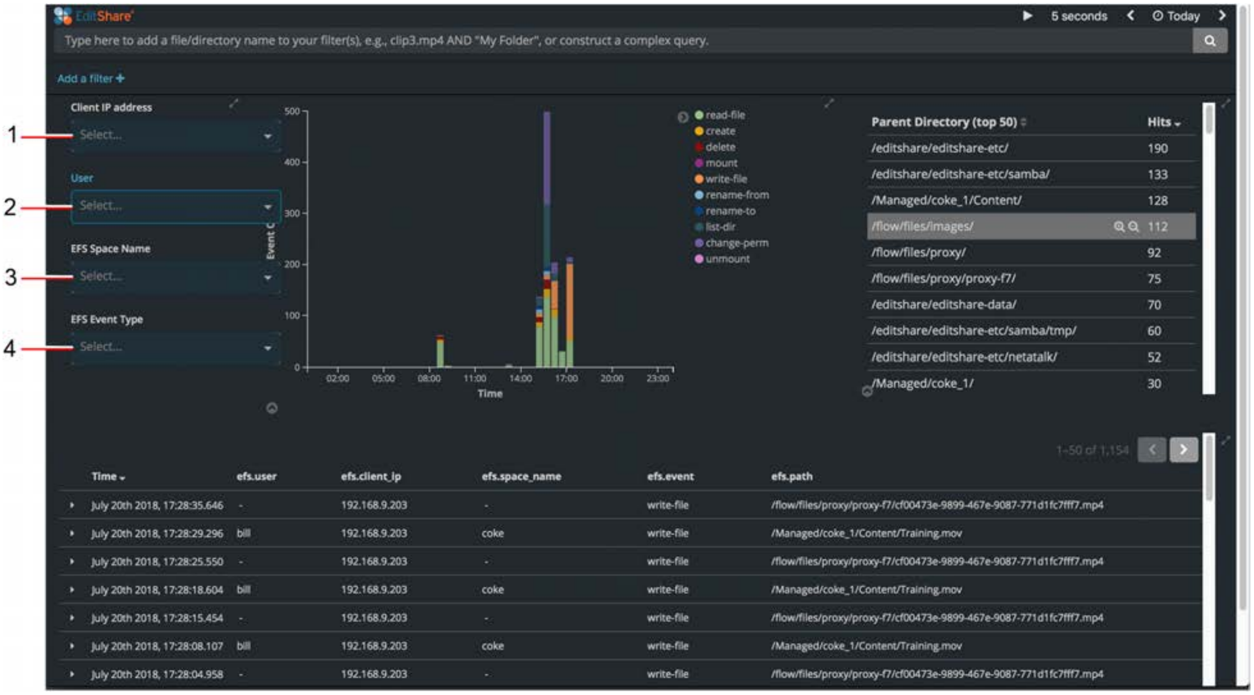


5. You can resume auto-refresh by clicking on the play icon.

Configuring the Analysis Filters

The Analysis Dashboard has four default analysis filters for:

1. Client IP address
2. User
3. EFS Space Name
4. EFS Event Type

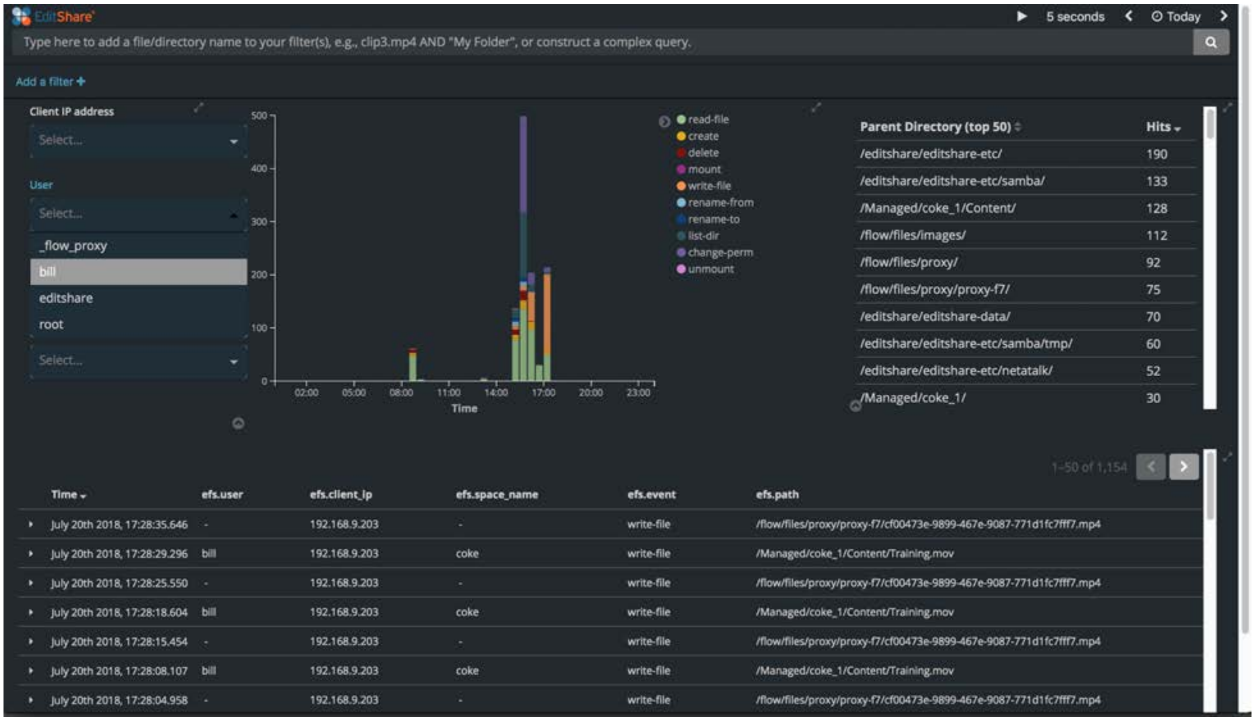


Parent Directory (top 50)	Hits
/editshare/editshare-etc/	190
/editshare/editshare-etc/samba/	133
/Managed/coke_1/Content/	128
/flow/files/images/	112
/flow/files/proxy/	92
/flow/files/proxy/proxy-f7/	75
/editshare/editshare-data/	70
/editshare/editshare-etc/samba/tmp/	60
/editshare/editshare-etc/netatalk/	52
/Managed/coke_1/	30

Time	efs.user	efs.client_ip	efs.space_name	efs.event	efs.path
July 20th 2018, 17:28:35.646	-	192.168.9.203	-	write-file	/flow/files/proxy/proxy-f7/cf00473e-9899-467e-9087-771d1fc7fff7.mp4
July 20th 2018, 17:28:29.296	bill	192.168.9.203	coke	write-file	/Managed/coke_1/Content/Training.mov
July 20th 2018, 17:28:25.550	-	192.168.9.203	-	write-file	/flow/files/proxy/proxy-f7/cf00473e-9899-467e-9087-771d1fc7fff7.mp4
July 20th 2018, 17:28:18.604	bill	192.168.9.203	coke	write-file	/Managed/coke_1/Content/Training.mov
July 20th 2018, 17:28:15.454	-	192.168.9.203	-	write-file	/flow/files/proxy/proxy-f7/cf00473e-9899-467e-9087-771d1fc7fff7.mp4
July 20th 2018, 17:28:08.107	bill	192.168.9.203	coke	write-file	/Managed/coke_1/Content/Training.mov
July 20th 2018, 17:28:04.958	-	192.168.9.203	-	write-file	/flow/files/proxy/proxy-f7/cf00473e-9899-467e-9087-771d1fc7fff7.mp4

In the same way that the timestamp range setting helps you narrow the scope of the monitor events, these filters enable you to further narrow the scope of monitor events. You can apply additional filter types by clicking on Add a filter + and selecting the filter you want.

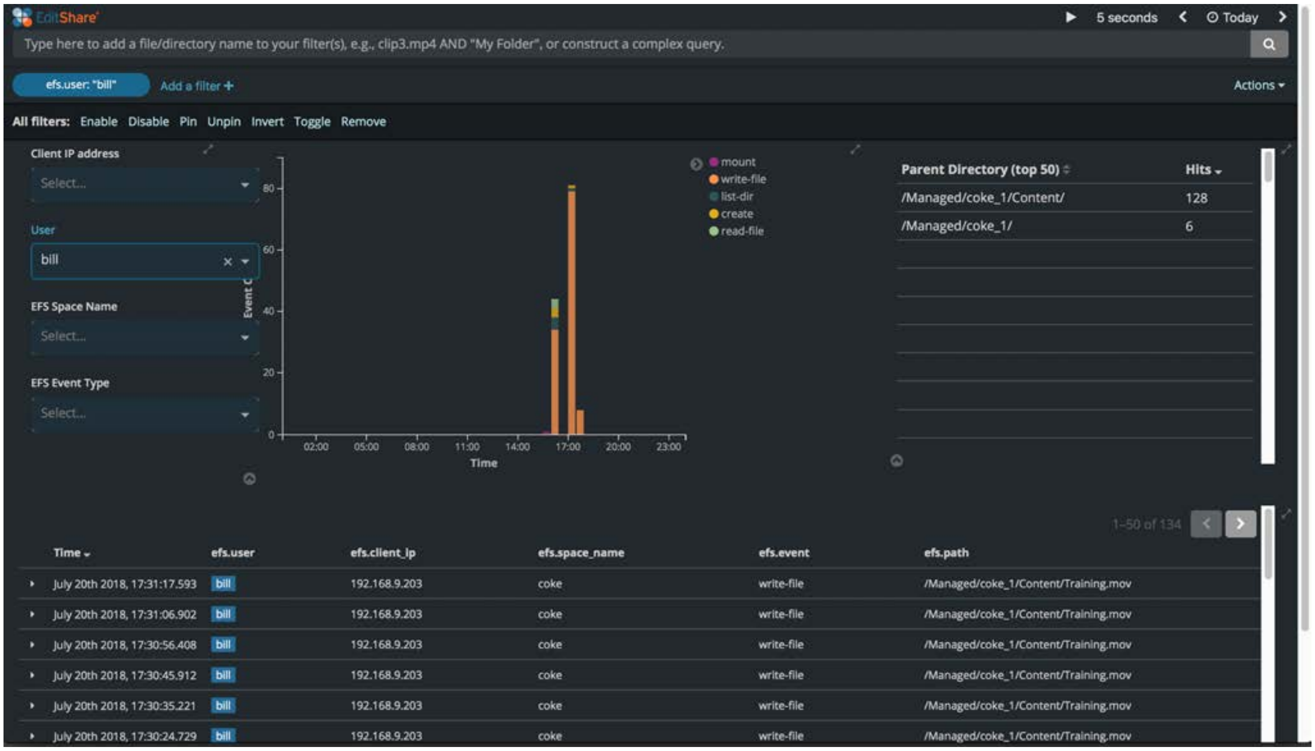
In the example above we have specified the timestamp range "Today". The resulting analysis yields 1154 separate monitor events. But suppose we are interested in understanding only Today's events associated with the user bill.



Parent Directory (top 50)	Hits
/editshare/editshare-etc/	190
/editshare/editshare-etc/samba/	133
/Managed/coke_1/Content/	128
/flow/files/images/	112
/flow/files/proxy/	92
/flow/files/proxy/proxy-f7/	75
/editshare/editshare-data/	70
/editshare/editshare-etc/samba/tmp/	60
/editshare/editshare-etc/netatalk/	52
/Managed/coke_1/	30

Time	efs.user	efs.client_ip	efs.space_name	efs.event	efs.path
July 20th 2018, 17:28:35.646	-	192.168.9.203	-	write-file	/flow/files/proxy/proxy-f7/cf00473e-9899-467e-9087-771d1fc7fff7.mp4
July 20th 2018, 17:28:29.296	bill	192.168.9.203	coke	write-file	/Managed/coke_1/Content/Training.mov
July 20th 2018, 17:28:25.550	-	192.168.9.203	-	write-file	/flow/files/proxy/proxy-f7/cf00473e-9899-467e-9087-771d1fc7fff7.mp4
July 20th 2018, 17:28:18.604	bill	192.168.9.203	coke	write-file	/Managed/coke_1/Content/Training.mov
July 20th 2018, 17:28:15.454	-	192.168.9.203	-	write-file	/flow/files/proxy/proxy-f7/cf00473e-9899-467e-9087-771d1fc7fff7.mp4
July 20th 2018, 17:28:08.107	bill	192.168.9.203	coke	write-file	/Managed/coke_1/Content/Training.mov
July 20th 2018, 17:28:04.958	-	192.168.9.203	-	write-file	/flow/files/proxy/proxy-f7/cf00473e-9899-467e-9087-771d1fc7fff7.mp4

By clicking on the User filter and selecting bill from the drop-down menu, we further narrow the range of monitor events to only those occurring Today and associated with the user bill. Instead of 1154 monitor events, we now have just 134 to evaluate. By examining the bar graph representation of the analysis output, we see that the lion's share of bill's activity has been write-file activity. Furthermore, by examining the tabular output in the Verbose Analysis Output, it is easy to see that Bill has written the file "Training.mov" into a Manage Media Space called coke_1.


EditShare
▶ 5 seconds
‹ Today ›
Type here to add a file/directory name to your filter(s), e.g., clip3.mp4 AND "My Folder", or construct a complex query.
Add a filter +
Actions
All filters: Enable Disable Pin Unpin Invert Toggle Remove
Select...
● mount
● write-file
● list-dir
● create
● read-file
Event C
80
60
40
20
0
02:00
05:00
08:00
11:00
14:00
17:00
20:00
23:00
Time
1–50 of 134

efs.user: "bill"

Client IP address: Select...

User: bill

EFS Space Name: Select...

EFS Event Type: Select...

Parent Directory (top 50)	Hits
/Managed/coke_1/Content/	128
/Managed/coke_1/	6

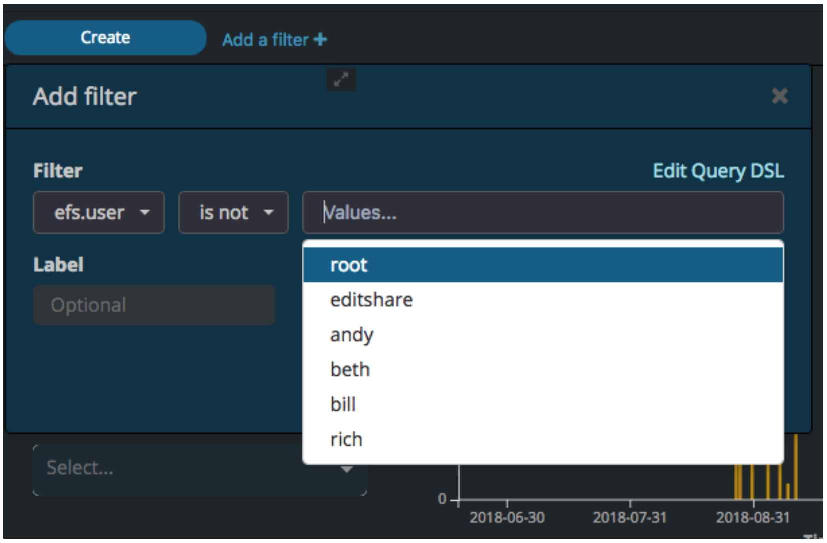
Time	efs.user	efs.client_ip	efs.space_name	efs.event	efs.path
July 20th 2018, 17:31:17.593	bill	192.168.9.203	coke	write-file	/Managed/coke_1/Content/Training.mov
July 20th 2018, 17:31:06.902	bill	192.168.9.203	coke	write-file	/Managed/coke_1/Content/Training.mov
July 20th 2018, 17:30:56.408	bill	192.168.9.203	coke	write-file	/Managed/coke_1/Content/Training.mov
July 20th 2018, 17:30:45.912	bill	192.168.9.203	coke	write-file	/Managed/coke_1/Content/Training.mov
July 20th 2018, 17:30:35.221	bill	192.168.9.203	coke	write-file	/Managed/coke_1/Content/Training.mov
July 20th 2018, 17:30:24.729	bill	192.168.9.203	coke	write-file	/Managed/coke_1/Content/Training.mov

We can further narrow the scope of the analysis by multiple filters. Had we, for example, selected the value coke-1 in the EFS Space Name filter, we would only see monitor events satisfying Today and bill and coke_1. It is obvious that the analysis output is composed of events that are the boolean AND of any of the filters (including the timestamp range.)

Filter Builder

The Analysis Dashboard includes a graphical "Filter Builder" that allows you to build custom filter items. To use this feature:

1. Click on the "Add a filter+" link to open up the "Add Filter" dialog.



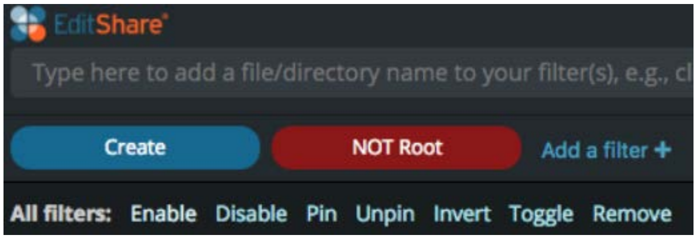
Filter: efs.user | is not | Values...

Label: Optional

2. In the Filter drop down box, select the attribute you want to filter on. For instance, in the example to the right, efs.user is selected.
3. Select the "operator" from a choice of: is, is not, is one of, is not one of, exists, does not exist.

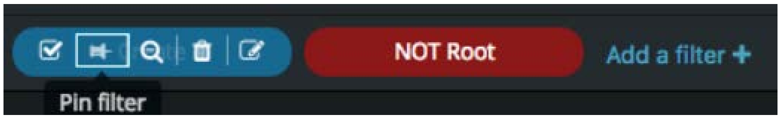
   Note: The choices give you more flexibility than the choices in the main Monitoring Dashboard, where the only choice is really "is".

4. In the Values box, type in or select the value you want to include or exclude. If you want to search for a particular file name extension (*.mov, *.mp4, *.pdf, *.exe, *.tmp, etc), simply type the characters. Values that you have previously searched for may already appear as options you can select. When you want to build filters based on specific user names or Media Spaces, the names of all current user accounts and Media Spaces will appear for you to select.
5. When you have finished configuring your filter, give it a label (optional).
6. Click SAVE. The new filter you just created will appear under the Query bar. Negative filters that exclude something are shown in red.



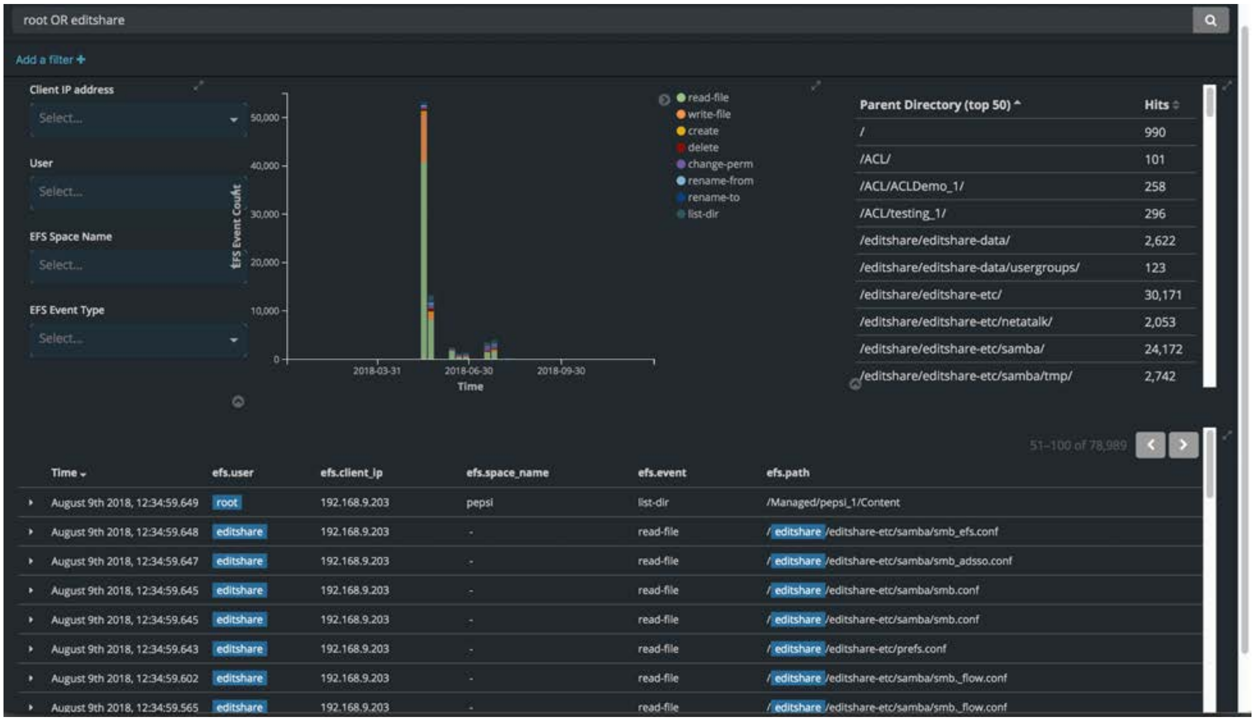
Type here to add a file/directory name to your filter(s), e.g., cl

7. Repeat to add additional filters.



8. Click on the "push-pin" icon inside the filter to make that filter permanent (until you unpin it).
9. Click again on the "push-pin" icon to unpin the filter.
10. Click on the trash icon to delete the filter.
11. Click on the pencil and paper icon to edit the filter.
12. Click on the check box to temporarily enable or disable the filter.

Configuring Filtering via the Search Bar


root OR editshare

Parent Directory (top 50)	Hits
/	990
/ACL/	101
/ACL/ACLDemo_1/	258
/ACL/testing_1/	296
/editshare/editshare-data/	2,622
/editshare/editshare-data/usergroups/	123
/editshare/editshare-etc/	30,171
/editshare/editshare-etc/netatalk/	2,053
/editshare/editshare-etc/samba/	24,172
/editshare/editshare-etc/samba/tmp/	2,742

Time	efs.user	efs.client_ip	efs.space_name	efs.event	efs.path
August 9th 2018, 12:34:59.649	root	192.168.9.203	pepsi	list-dir	/Managed/pepsi_1/Content
August 9th 2018, 12:34:59.648	editshare	192.168.9.203	-	read-file	/editshare/editshare-etc/samba/smb_efs.conf
August 9th 2018, 12:34:59.647	editshare	192.168.9.203	-	read-file	/editshare/editshare-etc/samba/smb_adsso.conf
August 9th 2018, 12:34:59.645	editshare	192.168.9.203	-	read-file	/editshare/editshare-etc/samba/smb.conf
August 9th 2018, 12:34:59.645	editshare	192.168.9.203	-	read-file	/editshare/editshare-etc/samba/smb.conf
August 9th 2018, 12:34:59.643	editshare	192.168.9.203	-	read-file	/editshare/editshare-etc/prefs.conf
August 9th 2018, 12:34:59.602	editshare	192.168.9.203	-	read-file	/editshare/editshare-etc/samba/smb._flow.conf
August 9th 2018, 12:34:59.565	editshare	192.168.9.203	-	read-file	/editshare/editshare-etc/samba/smb._flow.conf

The Analysis Dashboard Search Bar is a free-form text search tool that can provide a similar capability to the Filter Builder, but has even more flexibility and power. The Search Bar can be used to quickly search for particular information by typing in the exact value of a field. For example, a query like `efs.user:john` or `efs.cliend_ip:192.168.11.63` searches for all entries related to user `john` and a query like `192.168.11.63` finds entries related to that IP address. However, such queries can also be performed using other controls of the Monitor Dashboard. The most important use case for the Search Bar is to look for Monitor Events related to the particular file or path. See the following examples:

1. The query can be the exact value of a path component (file name with extension or name of any directory in its path) optionally enclosed in double quotes. Examples:
   - Seasons
   - The final episode.mov
   - "Season 02 Episode 03.mov"
2. The query can include multiple path components separated with forward slashes, but in that case it always has to be enclosed in double quotes. Examples:
   - "Season 02/Episode 03.mov"
   - "MediaSpace_1/Content/Seasons"
3. To match files using only a part of their name, the query can include wildcards (* and ?) Examples:
   - Season02*.*
   - Season0?.mp4
4. Double quotes cannot be used together with wildcards. When a query with wildcards has to include spaces as well, instead of double quotes, you have to escape the spaces by preceding them with backslash. Examples:
   - Season\ 02\ Episode\ *.mov
5. In order to look for all the files with the given extension, search the efs.file_type field by typing just the extension because path queries beginning with * are slow. For Example:
   - mov
   - mp4

More advanced queries can be constructed by joining the queries described above using `AND`, `OR`, and `( )` operators. For example:

- `(john OR ann) AND "Season 02/Episode 03.mov"`
- `efs.user:john` AND `efs.client_ip:192.168.11.63`

The Search Bar uses Lucene Query syntax . The user can also enable Kibana Query Language) KQL and use KQL .

Learn more about this feature at:

http://www.lucenetutorial.com/basic-concepts.html

http://www.lucenetutorial.com/lucene-query-syntax.html

https://www.elastic.co/guide/en/kibana/6.8/kuery-query.html

Modes of Operation

Depending upon how your EFS Shared Storage is configured, as many as three different Auditing and Monitoring modes of operation are available for your use. These differ by the location and amount of storage allotted for file monitor information.

Audit and Monitor Mode

When Auditing and Monitoring mode is activated, file monitor event logs are stored on the OS drives of the associated EFS Master node. Because OS drives are critical to the performance of the EFS storage systems, it is important to preserve adequate storage space on these drives for storage-related data. Therefore, when an EFS Master node is configured for Auditing and Monitoring, approximately 30% of the capacity of the OS drive (150GB) is made available to file monitor event storage. At 150 bytes/event, there will be capacity to store approximately 1 billion events.

When the allocated capacity is filled, the EFS will automatically begin removing the oldest data. It will stop deleting data when it gets to the current day, even if the remaining data from the current day occupies more than 30% of the OS drive.

File Monitor Forwarding

Instead of storing file events locally, it is theoretically possible to configure your EFS server to forward file event information to a central log collection server or Security Information and Event Management server. Analysis of file event information would be done with the third party tools that accompany these servers.

Currently, file event forwarding must be configured manually by EditShare technical support personnel and there aren't yet any SIEM manufacturers who have updated their products to be able to understand and analyze EFS monitor data. EditShare will keep customers updated about SIEM options as they develop in the future.