Overview

This is aimed to assist with troubleshooting the Event Manager and the Elasticsearch service.

> Note: The terms Activities and Events are used interchangeably.

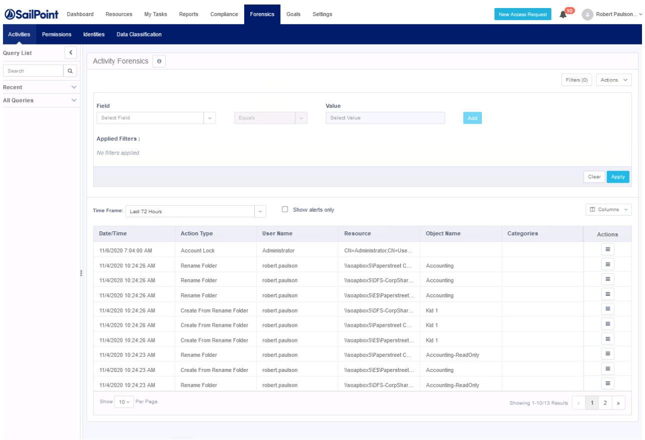
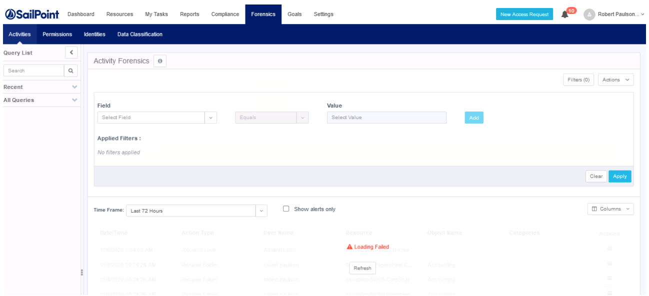
- Activities are collected from the endpoint's Activity Monitor.
- Events are activities that are enriched in the Event Manger (with the support of the Data Enrichment Connector).

Elasticsearch

It is recommended to start with the Elasticsearch. This is because when searching for captured Activities in the WebUI, the WebUI is requesting the events from the Elasticsearch Database, not the SQL database.

Checking the Activties > Forensics page in the WebUI would be the first thing check. If Events appear, this will help narrow down troubleshooting as mentioned in the below steps.

1. Are Activities within the last 72 hours searchable in the WebUI or getting a **Loading Failed**?

Good	Bad
	

Date/Time	Action Type	User Name	Resource	Object Name	Categories	Actions
11/6/2020 7:04:00 AM	Account Lock	Administrator	CN=Administrator,CN=Use...			≡
11/4/2020 10:24:26 AM	Rename Folder	robert.paulson	\\soapbox5\Paperstreet C...	Accounting		≡
11/4/2020 10:24:26 AM	Rename Folder	robert.paulson	\\soapbox5\DFS-CorpShar...	Accounting		≡
11/4/2020 10:24:26 AM	Rename Folder	robert.paulson	\\soapbox5\ES\Paperstreet...	Accounting		≡
11/4/2020 10:24:26 AM	Create From Rename Folder	robert.paulson	\\soapbox5\DFS-CorpShar...	Kid 1		≡
11/4/2020 10:24:26 AM	Create From Rename Folder	robert.paulson	\\soapbox5\Paperstreet C...	Kid 1		≡
11/4/2020 10:24:26 AM	Create From Rename Folder	robert.paulson	\\soapbox5\ES\Paperstreet...	Kid 1		≡
11/4/2020 10:24:23 AM	Rename Folder	robert.paulson	\\soapbox5\Paperstreet C...	Accounting-ReadOnly		≡
11/4/2020 10:24:23 AM	Create From Rename Folder	robert.paulson	\\soapbox5\ES\Paperstreet...	Accounting		≡
11/4/2020 10:24:23 AM	Rename Folder	robert.paulson	\\soapbox5\DFS-CorpShar...	Accounting-ReadOnly		≡

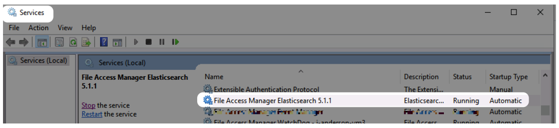
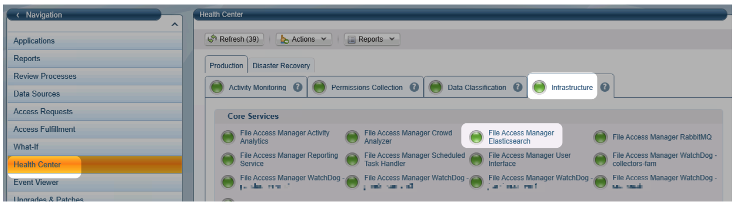
Show 10 Per Page Showing 1-10/13 Results « 1 2 »

Loading Failed

- If events appear, then Elasticsearch is functional and the target to troubleshoot should be the **Event Manager**.
- If events are not viewable for the last 72 hours, test with the **last 30 days** filter. This will broaden the events search even further.
- If events appear at the 30 day range, this may indicate an issue with the Event Manager(s) but proceed troubleshooting Elasticsearch with the steps below.

2. Is the Elasticsearch service "running" on the hosted server (check the Windows Services Panel) and is GREEN in the Health Center of the Admin Client?

Windows Services Panel	Health Center

Windows Services Panel	Health Center
	

Services
File Action View Help
Services (Local)
Services (Local)
File Access Manager Elasticsearch 5.1.1
Stop the service
Restart the service

Name	Description	Status	Startup Type
Extensible Authentication Protocol	The Extensi...		Manual
File Access Manager Elasticsearch 5.1.1	Elasticsearc...	Running	Automatic
[redacted]	[redacted]	[redacted]	Automatic
File Access Manager WatchDog - j-anderson-vm3	File Access...	Running	Automatic

Navigation
Applications
Reports
Review Processes
Data Sources
Access Requests
Access Fulfillment
What-If
Health Center
Event Viewer
Upgrades & Patches
Health Center
Refresh (39)
Actions
Reports
Production
Disaster Recovery
Activity Monitoring
Permissions Collection
Data Classification
Infrastructure
Core Services
File Access Manager Activity Analytics
File Access Manager Crowd Analyzer
File Access Manager Elasticsearch
File Access Manager RabbitMQ
File Access Manager Reporting Service
File Access Manager Scheduled Task Handler
File Access Manager User Interface
File Access Manager WatchDog - collectors-fam
File Access Manager WatchDog - [redacted]
File Access Manager WatchDog - [redacted]
File Access Manager WatchDog - [redacted]
File Access Manager WatchDog - [redacted]

3. Does the Elasticsearch Server itself have disk space remaining and has this Compass article been reviewed?

4. After reviewing this Compass article and confirming the Elasticsearch service is running. Are there any RED Indexes (indices) in the Elasticsearch URL,' https://{servername}/_cat/indices'?

    - If any RED Indexes (indices) are present in the Elasticsearch URL, this indicates that a corrupt event(s) with that given month(s) was collected.

      > This is a very rare occurrence but generally can occur if servers where not shutdown or restarted in the proper sequence. For shutdown and restart sequence please see this Compass Article.

    - The only **Supported** method to delete Activities is by following this Compass Article and it is **highly recommended** to delete events in 48-72 hour or smaller time blocks. This is because the Elasticsearch is trying to delete hundreds to thousands of events at one time which can cause issues as current events are still trying to be recorded to the Elasticsearch Server at the same time. ⚠ **Deleting events from the WebUI will delete event data from both the Elasticsearch Database and the SQL Database.**⚠

Event Manager

> Note: If you have multiple Event Managers in your environnement, please check the respective Event Manager having the issue with the steps below. Additionally, it may benefit to reassign Activity Monitors to a functional Event Manager until the issue is resolved.

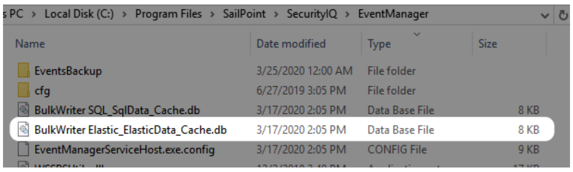
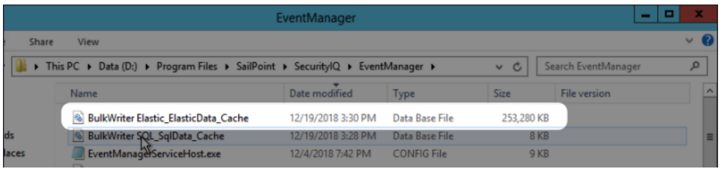
1. Is the Event Manager service running on the hosted server (check the Windows Services Panel) and is GREEN in the Health Center of the Admin Client?
2. Does the server hosting the Event Manager itself have disk space remaining?
    - If there is little to no disk space remaining, ensure the Event Manager service is **stopped** and more disk space (~40GB) will need to be allocated to allow for "working room".

      > This generally occurs when servers were improperly rebooted or the Elasticsearch Server runs out of disk space. For shutdown and restart sequence please see this Compass Article.

3. Is there a large **BulkWriter Elastic_Elastic_Cache.db** file?

- The main cause of disk space being taken is normally due to the **BulkWriter Elastic_Elastic_Cache.db** file becoming expanded. This cache file holds collected events in the scenario where the Event Manager cannot communicate with the Elasticsearch Server.

> This can be located at the default directory on the server hosting the Event Manager. C:\Program Files\SailPoint\File Access Manager\EventManager
> ⚠️ For 6.1 Versions or upgrades from 6.1 the path name will differ: C:\Program Files\SailPoint\SecurityIQ\EventManager\ ⚠️

Normal (~8-20KB)	Abnormal
	

s PC › Local Disk (C:) › Program Files › SailPoint › SecurityIQ › EventManager

Name	Date modified	Type	Size
EventsBackup	3/25/2020 12:00 AM	File folder	
cfg	6/27/2019 3:05 PM	File folder	
BulkWriter SQL_SqlData_Cache.db	3/17/2020 2:05 PM	Data Base File	8 KB
BulkWriter Elastic_ElasticData_Cache.db	3/17/2020 2:05 PM	Data Base File	8 KB
EventManagerServiceHost.exe.config	3/17/2020 2:05 PM	CONFIG File	9 KB

EventManager

This PC ▸ Data (D:) ▸ Program Files ▸ SailPoint ▸ SecurityIQ ▸ EventManager ▸

Name	Date modified	Type	Size	File version
BulkWriter Elastic_ElasticData_Cache	12/19/2018 3:30 PM	Data Base File	253,280 KB	
BulkWriter SQL_SqlData_Cache	12/19/2018 3:28 PM	Data Base File	8 KB	
EventManagerServiceHost.exe	12/4/2018 7:42 PM	CONFIG File	9 KB	

- If a abnormal Elastic_Cache file is present. Most times the RESOLUTION is to **stop** (do not just 'restart' the service) make sure to stop and then start the Event Manager service then start the service once more.

  > Note: The Event Manger service may throw an Windows error stating the service could not be stopped. If this occurs, please stop the service via the **Windows Task Manager**.

- You should then see the Elastic Cache file decrease in size by several thousand to several hundred thousand KBs. **It may take multiple stop and starts of the Event Manager** to get this file down and size and your hard drive disk space back in normal use limits.

4. Is the Elasticsearch Cache file in Normal limits again?
   - Check the WebUI Activity > Forensics page once again and events should be present.

Please be sure to reassign any Activity Monitors that were reconfigured during troubleshooting back to their designated Event Manager.