

File Access Manager Data Backup

Version: 8.4

Revised: March 27, 2023

This document and the information contained herein is SailPoint Confidential Information

Copyright and Trademark Notices

Copyright © 2023 SailPoint Technologies, Inc. All Rights Reserved.

All logos, text, content, including underlying HTML code, designs, and graphics used and/or depicted on these written materials or in this Internet website are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of SailPoint Technologies, Inc.

"SailPoint," "SailPoint & Design," "SailPoint Technologies & Design," "Identity Cube," "Identity IQ," "IdentityAI," "IdentityNow," "SailPoint Predictive Identity" and "SecurityIQ" are registered trademarks of SailPoint Technologies, Inc. None of the foregoing marks may be used without the prior express written permission of SailPoint Technologies, Inc. All other trademarks shown herein are owned by the respective companies or persons indicated.

SailPoint Technologies, Inc. makes no warranty of any kind with regard to this manual or the information included therein, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. SailPoint Technologies shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Patents Notice. https://www.sailpoint.com/patents

Restricted Rights Legend. All rights are reserved. No part of this document may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of SailPoint Technologies. The information contained in this document is subject to change without notice.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c)(1) and (c)(2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Regulatory/Export Compliance. The export and re-export of this software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Department of Commerce's Entity List in Supplement No. 4 to 15 C.F.R. § 744; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government's Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws and regulations as they relate to software and related documentation.

Contents

Elasticsearch Backup Overview	iv
Continuous Backup Monitoring	5
Elasticsearch Continuous Backup Monitoring Configurations	5
Elasticsearch Backup Installation	7
Backup Elasticsearch Configuration	11
Data Restoration	13
Considerations	13
Restore a Deleted Index	13
Restore an Existing Index	13
Restore an Entire Cluster	15
Retention Backup	19

Elasticsearch Backup Overview

There are two types of Elasticsearch repositories and both are the File System type. For more information, read https://www.elastic.co/guide/en/elasticsearch/reference/current/snapshots-filesystem-repository.html.

The two repositories are:

Continuous_backup

Used for backing up the whole cluster. This repository holds snapshots that are being taken every hour with the following name format "fam-backup-yyyy.MM.dd-hh:mm:ss-UUID." Every snapshot will be saved for 60 days.

This repository can contain up to 1500 snapshots (in case of also creating snapshots manually) and minimum of 100.

Retention_backup

Used for backing up the events indices which are deleted in the activity data retention process. A snapshot of the deleted indices will be created with the following name format: "retention_backup-yyyy.MM.dd-hh:mm:ss." These snapshots will be saved forever.

Continuous Backup Monitoring

The continuous backup repository monitoring is run by the File Access Manager Scheduled Task Handler service. The monitoring starts 3 hours after the service starts and monitors the continuous_backup snapshots once an hour. The results are displayed in the File Access Manager Admin Client Event Viewer. In case of errors, more detailed results can be found in the File Access Manager Scheduled Task Handler log and the Elasticsearch log.

👍 SailPoint 🌙	File Access Manager
< Navigation	Event Viewer
Applications	🖾 Source 28 Selected Start 15/11/2022 🛗 End 22/11/2022 🛗 Level Error 🗸 🗸 Apply
Reports	# Level Date Source Title
Review Processes	1 Error 22/11/2022 16 25 50 File Access Manager Scheduled Task Handler Task: Elasticsearch Continuous Backup verification completed with the following status: Error - No successful snapshots were created in the Last 180 minutes. Check log for details
Access Requests	2 Error 2211/2022 15.25 Fik Access Manager Scheduled Task Handler Task Elaskicsearch Continuous Backup synetication completed with the following status. Error -No successful anaphotis were created in the last 100 minutes. Check tog for details 5 Error 2211/2022 15.25 Fik Access Manager Scheduled Task Handler Task Elaskicsearch Continuous Backup synetication completed with the following status. Error - No successful anaphotis were created in the last 100 minutes. Check tog for details 5 Error 2211/2022 15.25 Fik Access Manager Scheduled Task Handler Task Elaskicsearch Continuous Backup synetication completed with the following status. Error - No successful anaphotis were created in the last 100 minutes. Check tog for details 5 Error 2211/2022 15.25 Fik Access Manager Scheduled Task Handler Task Elaskicsearch Continuous Backup synetication completed with the following status. Error - No successful anaphotis were created in the last 100 minutes. Check tog for details 5 Error 2211/2022 15.25 Fik Access Manager Scheduled Task Handler Task Elaskicsearch Continuous Backup synetication completed with the following status. Error - No successful anaphotis were created in the last 100 minutes. The Access Manager Scheduled Task Handler Task Elaskicsearch Continuous Backup synetication completed with the following status. Error - No successful anaphotis were created in the last 100 minutes. The Access Manager Scheduled Task Handler Task Elaskicsearch Continuous Backup synetication completed with the following status. Error - No successful anaphotis were created in the last 100 minutes. The Access Manager Scheduled Task Handler Task Elaskicsearch Continuous Backup synetication completed with the Scheduled Task Handler Task Elaskicsearch Continuous Backup synetication Completed with the Scheduled Task Handler Task Elaskicsearch Continuous Backup synetication Completed with the Scheduled Task Handler Task Elaskicsearch Continuous Backup synetication Completed with the Scheduled Task Handler Task Handler Task Elaskicsearch Cont
Access Fulfillment	4 Error 22/11/2022 13:25:50 File Access Manager Scheduled Task Handler Task: Elasticsearch Continuous Backup verification completed with the following status: Error - No successful snapshots were created in the last 180 minutes. Check log for details
What-If	5 Errer 2211/2022 12:55 File Access Manager Scheduld Tals Handler Task Etablicsearch Continuous Backup verification completed with the following state. Error - No successful inamphots were created in the last 100 minutes. Check tog for details 6 Errer 2211/2022 12:55 File Access Manager Scheduld Task Handler Task Etablicsearch Continuous Backup verification completed with the following state. Error - No successful inamphots were created in the last 100 minutes. Check tog for details 6 Error 2211/2022 12:55 File Access Manager Scheduld Task Handler Task Etablicsearch Continuous Backup verification completed with the following state. Error - No successful inamphots were created in the last 100 minutes. Check tog for details 6 Error 2211/2022 12:55 File Access Manager Scheduld Task Handler Task Etablicsearch Continuous Backup verification completed with the following state. Error - No successful inamphots were created in the last 100 minutes. Check tog for details 6 Error 2211/2022 12:55 File Access Manager Scheduld Task Handler Task Etablicsearch Continuous Backup verification completed with the following state. Error - No successful inamphots were created in the last 100 minutes. Check tog for details 6 Error 2211/2022 12:55 File Access Manager Scheduld Task Handler Task Etablicsearch Continuous Backup verification completed with the following state. Error - No successful inamphots were created in the last 100 minutes. Check tog for details 6 Error 2211/2022 12:55 File Access Manager Scheduld Task Handler Task Etablicsearch Continuous Backup verification completed with the following state. Error - No successful inamphots were created in the last 100 minutes. Check tog for details 6 Error 2211/2022 12:55 File Access Manager Scheduld Task Handler Task Etablicsearch Continuous Backup verification completed with the following state. Error - No successful inamphots were created in the last 100 minutes. Check tog for details 6 Error 2211/2022 12:55 File Access Manager 2211/2022 12:55 File Access Manager 2211/2022 12:5
Health Center	7 Error 22/11/2022 10.25.50 File Access Manager Scheduled Task Handler Task: Elasticsearch Continuous Backup verification completed with the following status: Error - No successful snapshots were created in the last 180 minutes. Check log for details
Event Viewer	8 Error 22/11/2022 92:550 File Access Manager Scheduled Task Handler Task: Elasticsearch Continuous Backup verification completed with the following status: Error - No successful snapshots were created in the last 180 minutes. Check log for details 22/11/2022 82:550 File Access Manager Scheduled Task Handler Task: Elasticsearch Continuous Backup verification completed with the following status: Error - No successful snapshots were created in the last 180 minutes. Check log for details
Upgrades & Patches	10 Error 22/11/2022 7.25.50 File Access Manager Scheduled Task Handler Task: Elasticsearch Continuous Backup verification completed with the following status: Error - No successful snapshots were created in the last 180 minutes. Check log for details
	11 Error 22/11/2022 625.50 File Access Manager Scheduled Task Handler Task Elasticsearch Continuous Backup verification completed with the following status. Error - No successful snapshots were created in the last 180 minutes. Check log for details
Business December Terr	

There is also an option to generate a report which contains more details in case of failures, including the last successful snapshot name.

Elasticsearch Continuous Backup Monitoring Configurations

The monitoring configurations should not be changed.

In case there is a temporary need to change them, it can be done in the TaskScheduler's App.cofig file:

- elasticBackupHealthMonitoringPoolingIntervalInSeconds the interval to check the "continuous_backup" snapshots (default is 3600 seconds – 1 hour)
- elasticBackupHealthMonitoringDueTimeInSeconds the due time before starting to monitor the "continuous_ backup" snapshots (default is 7200 seconds – 2 hours. Snapshots will start being taken one hour after enabling the backup)
- maxTimeSinceLastSuccessfulSnapshotInMinutes the period since the last successful snapshots before the backup status will be set to Failure (default is 180 minuets – 3 hours)

```
Note: Useful command for manual monitoring is 'GET_slm/policy/fam-backup'
Example of output is:
0 {
   "fam-backup": 🖂 (
      "version":1,
      "modified date millis":1668585570288,
      "policy": 0 {
         "name":"<fam-backup-(now(yyyy.MM.dd-hh:mm:ss))>",
         "schedule":"0 0 * * * ?",
         "repository": "continuous_backup",
         "config": 🕀 (
            "indices":" all"
         1.
         "retention": 3 {
            "expire_after":"60d",
            "min_count":100,
            "max_count":1500
         3
      1,
      "last_success": 0 (
         "snapshot_name":"fam-backup-2022.11.25-12:59:59--aelqogiqmiiz24dgzflvq",
         "start_time":1669381199972,
         "time":1669381203577
      1.
      "last_failure": 🖯 (
         "snapshot_name":"fam-backup-2022.11.27-07:59:59-o3uSetmrtsgrakbvkek9vq",
         "time":1669536000677,
         "details":"{\"type\":\"snapshot_exception\",\"reason\":\"[continuous_backup:fam-backup-2022.11.27-
         07:59:59-o3u5etmrtsgrakbvkek9vq/D6CAvlB9SmmNpqW0GiqAMw) failed to update snapshot in
         repository/", /"csused_by/": {/"type/":/"file_system_exception/", /"reason/":/"//////FAM-
         ANATOLY7////repo///Prod////t14////continuous_backup////snap-D6CAvlB9SmmNpqW0GiqAMw.dat: There is not
         enough space on the disk\",\"suppressed\":
         [{\"type\":\"file_system_exception\", \"reason\":\"\\\\\\FAM-
         ANATOLY7////repo////Prod////tl4///continuous_backup///meta-D6CAvlB9SmmNpqW0GiqAMw.dat: There is not
         enough space on the disk\"}])}"
      1.
      "next_execution_millis":1669539600000,
      "stats": 8 (
         "policy":"fam-backup",
         "snapshots_taken":130,
         "snapshots_failed":119,
         "snapshots_deleted":0,
         "snapshot_deletion_failures":0
```

Elasticsearch Backup Installation

Important: Before you install the Elasticsearch backup, make sure that Elasticsearch has access and proper permissions to the backup folder.

Note: Some setting are applied through a task outside the Server Installer which could result in longer completion time. Verify all changes were applied.

Note: It is recommended not trying to change multiple settings at the same time. Change each setting separately and verify it was completed successfully before continuing with the next change.

To set permissions to the backup folder:

1. Set the folder as share:

Folder Properties > Sharing > Share... > Share.

2. Share the backup base path with all master and data nodes:

Folder Properties > Sharing > Advanced Sharing...

- 3. Check Share this folder.
- 4. Navigate to Permissions > Add... > Object Types....
- 5. Check Computers.
- 6. Select OK.
- 7. Add all the master and data nodes (MACHINE_NAME\$).

Note: It is recommended to have an odd number of nodes. Ideally 3 and above.

8. Select OK.



9. In the Permissions window, give each node a **Change** permission.

	is PC > Local	Disk (C:) > Share >	Determetical	T		~ (Search Sh	hare	Q
✤ Quick access Desktop	Name Backups		01/08/2022 15:10	File folder	Size				
Downloads *		Backups Properties		×					
Pictures 🖈		General Sharing Security F	Previous Versions Customize Advanced Sharing		×				
network 🎻		Not Shared Network Path: Not Shared Share Advanced Sharing Set custom permissions, cre advanced sharing options.	Share this folder Settings Share name: Backups Add Remov Limit the number of sim Comments:	e ultaneous us	Permissions for Backups Share Permissions Group or user names: Exeryone FAM-AMIR (OFFICE):FAI ISWFAM-AMIR2 (OFFICE)	M-AMIR\$) ENSWFAM-AMIR2\$)	×		
		Advanced Sharing	Permissions	Caching	Pemiasions for ISWFAM-AMI Full Control Change Read	Add	Deny		
item 1 item selected		ОК	Cancel	Apply					REE M

- 10. Select OK > OK > Close.
- Set the shared folder's (e.g., "Backups") NTFS security settings to Modify for all master and data nodes. Do this by navigating to Folder Properties > Security > Advanced > Permissions tab > Add.
- 12. Select a principal.
- 13. Navigate to **Object Types**.
- 14. Select **Computers** and then select **OK**.
- 15. Add one of the nodes (MACHINE_NAME\$) and select **OK**.
- 16. Set Basic permissions to Modify and select **OK**.

Important: Do this for all master and data nodes.

I Image: Share File Home $\leftarrow \rightarrow \checkmark \uparrow$ > Th	View is PC > Local Disk (C:)	> Share			- C × v Ø Search Share P	
+ Ouisk score	Name	^	Date modifie	ed Type	Size	
Desktop #	Backups		01/08/2022	15:10 File fr	Permission Entry for Backups	- 🗆 X
Documents * Documents * Dictures * This PC Network		Backups Propert	ties Security Previous \Share\Backups is;	Versions Custo	Principal FAM-AMIR (OFFICE\FAM-AMIRS) Select a principal Type: Allow Applies to: This folder, subfolders and files	
		Administrato	Advanced Se Name: Owner: Permissions	curity Settings f C:\Share\Bac Administrato Share information do	Basic permissions: Full control Modify Read & execute Clint folder contents Read Write	Show advanced permissions
1 item 1 item selected		Read & execut List folder cont Read Write For special permit click Advanced.	Permission ent Type Allow Allow Allow	tries: Principal ISWFAM-A Administra Administra SYSTEM	Special permissions Only apply these permissions to objects and/or containers within this container Add a condition to limit access. The principal will be granted the specified permissions only if conditions are met. Add a condition	Clear all
			< Add	Remove	Ēdīt	OK Cancel
			Replace all o	child object perm	ission entries with inheritable permission entries from this object	

17. If the Elasticsearch and the backup folder are in different domains, the domains should have trust between them.

Backup Elasticsearch Configuration

1. In the Elasticsearch Configuration window of the Server Installer, select the desired configuration.

File Access Manager Installation	×
Elasticsearch Configuration	
Select services to install, and associate them with servers	
Backup Settings	
✓ Use Elasticsearch Backup (?)	
Repository Path: \\my-machine\ES-BACKUP	
Enable Cluster Backup (2)	

- Select the Use Elasticsearch Backup to enable backup of elastic data. If this option is unchecked, there will be no kind of backup of elastic data. This setting is also applied on the Elasticsearch disaster recovery backup. Without the backup, there will be no disaster recovery.
- 3. If Use Elasticsearch Backup is selected, you must provide the Repository Path. This folder should be configured and have the appropriate permissions according to the above section.

Any change in the repository path will cause a restart of each elastic node.

- 4. Select **Enable Cluster Backup** to run the continuous_backup and take snapshots of the full cluster. This setting is also applied on the Elasticsearch disaster recovery backup.
- 5. If a disaster recovery environment is configured and if Use Elasticsearch Backup was checked, you must provide the Repository Path for the disaster recovery Elasticsearch.

This folder should be configured and have the appropriate permissions according to the above section.

Note: The disaster recovery repository path must be different then the production repository path.

File Access Manager Installation

Elasticsearch DR Configuration

Configure the following Elasticsearch settings

Backup Settings

Repository Path: \\my-machine_DR\ES-BACKUP

If any change occurs in the backup configuration, it is highly recommended to keep track of the continuous backup monitoring in the File Access Manager Admin client event viewer. Make sure nothing went wrong and that snapshots are being created successfully.

Elasticsearch backup configuration changes are performed in an asynchronous way by a task named Update Elasticsearch Cluster Configuration by the Scheduled Task Handler Service.

🔺 SailPoi	nt File Access Manager 🗙 🔺 SailPoint File Access Manager	× +		v – a
$\leftarrow \rightarrow$	C () localhost/identityiqfam/v2#/settings/task-manageme	ent/tasks		۹ 🖻 🖈 🖬 🛔 🔍
SailPo Message Tenn Taska	int Damboard Resources My Taxis Reports Compriance Kales - Capabilities Account Exclusions - Discard Rules Tack Ma	Task Details Name Losse Exicosen Cuser Contguiston Service Encourse Tax Handler Service Innovatory6		
	Name	Severity	Date	Description
	Event Viewer Messages Report	Information	Nov 22, 2022 3:46:52 PM	Unregistered repository "continuous_backup" on path \\FAM-ANATOLY7.vepo\Prod(s13)continuous_backup in Production cluster (inactive cluster)
	Dashboard Widgets Calculation	Information	Nov 22, 2022 3:46:52 PM	Unregistered repository "retention_backup" on path \\FAM_ANATOLY7yepo\Prod\t13yetention_backup in Production cluster (inactive cluster)
	Database Gean Up	Information	Nov 22, 2022 3:46:51 PM	Task for Elasticsearch Server fam-anatoly6: Completed
	Update Elasticsearch Node Configuration - fam-anatoly6	Information	Nov 22, 2022 3:45:39 PM	Task created for elasticsearch server fam-anatoly6, waiting for task execution
	Update Elasticsearch Node Configuration - fam-anatoly	Information	Nov 22, 2022 3:45:39 PM	Task for Elasticsearch Server fam-anatoly: Completed
0	Update Elasticsearch Node Configuration - fam-anatoly5	Information	Nov 22, 2022 3:44:43 PM	Task created for elasticsearch server fam-anatoly, waiting for task execution
	Update Easticsearch Cluster Configuration	Information	Nov 22, 2022 3:44:43 PM	Task for Easticsearch Server fam-anatolySr Completed
	Update Elasticsearch Node Configuration - fam-anatoly6	Information	Nov 22, 2022 3:43:40 PM	Task created for elasticsearch server fam-anatoly5, waiting for task execution
	Update Elasticsearch Cluster Configuration	Information	Nov 22, 2022 3:43:40 PM	Creating Node Configuration Task for 3 Servers
	Update Elasticsearch Node Configuration - fam-anatoly	Information	Nov 22, 2022 3:43:40 PM	Starting Easticsearch Custer Configuration Update
Rows	per page 100 V 1 - 100 of 198	Information	Nov 22, 2022 3:43:40 PM	Eastloser Custer Configuration Update
		Rows per page 25 1 - 19 of 19		Page 1 of 1 ()

Data Restoration

More information about restoring Elasticsearch data can be found here.

Considerations

Keep the following in mind when restoring data from a snapshot:

- You can only restore an existing index if it's closed and the index in the snapshot has the same number of primary shards
- You cannot restore an existing open index
- The restore operation automatically opens restored indices
- 1. Get a list of available snapshots ordered by descending start time.
 - a. GET_snapshot/continuous_backup/*?order=desc
 - b. GET_snapshot/retention_backup/*?order=desc
- 2. Get a list of available snapshots from a specific date
 - a. GET_snapshot/continuous_backup/fam-backup-2022.08.02-*?verbose=false
 - b. GET_snapshot/retention_backup/retention_backup-2022.08.02-*?verbose=false

Restore a Deleted Index

To restore a deleted index or indices, find the specific snapshots which contain the index you want to restore (you can use the above examples to find the relevant snapshot).

```
POST _snapshot/retention_backup/retention-backup-2022.08.01-00:10:00/_restore
{
    "indices": "events_2022_07_2, events_2022_05_1"
}
```

Restore an Existing Index

If needing to restore an existing index, there are two preferable ways to do it:

1. Delete and Restore

https://www.elastic.co/guide/en/elasticsearch/reference/current/snapshots-restore-snapshot.html#deleterestore

In case you only need to restore a specific index, the simplest way to avoid conflicts is to delete an existing index before restoring it.

Example: DELETE pii-1, pii-8

In the restore request, explicitly specify the repository name, snapshot name, and any indices to restore.

```
POST _snapshot/continuous_backup/fam-backup-2022.08.03-09:00:00-
fv59i0lpqjipxdtcwirs8a/_restore
{
    "indices": "pii-1", "pii-8"
  }
```

2. Rename and Restore

https://www.elastic.co/guide/en/elasticsearch/reference/current/snapshots-restore-snapshot.html#rename-on-restore

If you want to avoid deleting existing data, you can instead rename the indices you restore. You typically use this method to compare existing data to historical data from a snapshot. For example, you can use this method to review documents after an accidental update or deletion.

```
POST _snapshot/my_repository/my_snapshot_2099.05.06/_restore
{
    "indices": "my-index,logs-my_app-default",
    "rename_pattern": "(.+)",
    "rename_replacement": "restored-$1"
  }
```

When the restore operation is complete, you can compare the original and restored data. If you no longer need an original index, you can delete it and use a reindex to rename the restored one.

a. To delete the original index: DELETE my-index

b. To reindex the restored index and rename it: POST_reindex

```
{
    "source": {
        "index": "restored-my-index"
    },
    "dest": {
        "index": "my-index"
     }
}
```

Restore an Entire Cluster

Caution: This should only be used in case of a failure.

Note: File Access Manager recommends reading the Elasticsearch guide first which can be accessed here.

1. Temporarily stop indexing and turn off the following features:

GeoIP database downloader

```
PUT _cluster/settings
{
    "persistent": {
        "ingest.geoip.downloader.enabled": false
    }
}
```

ILM

POST _ilm/stop

Monitoring

```
PUT _cluster/settings
{
    "persistent": {
    "xpack.monitoring.collection.enabled": false
    }
}
```

Machine Learning

POST _ml/set_upgrade_mode?enabled=true

Watcher

POST _watcher/_stop

2. Use the cluster update settings API to set **action.destructive_requires_name to false**. This allows you delete data streams and indices using wildcards.

```
PUT _cluster/settings
{
    "persistent": {
        "action.destructive_requires_name": false
    }
}
```

3. Delete all existing data streams on the cluster.

DELETE _data_stream/*?expand_wildcards=all

4. Delete all existing indices on the cluster.

DELETE *?expand_wildcards=all

5. Restore the entire snapshot, including the cluster state. By default, restoring the cluster state also restores any feature states in the snapshot.

```
POST _snapshot/my_repository/my_snapshot_2099.05.06/_restore
{
    "indices": "*",
    "include_global_state": true
}
```

Note: Restore request return immediately. The restore happens in the background and the user needs to wait while it completes.

The GET_cluster/health request can be used to monitor Cluster Health and restore progress. See below for the Health request example of response. Green status indicates that the cluster is fine and the restore is complete.

6. When the restore operation is complete, resume indexing and restart any features you stopped.

GeoIP database downloader

```
PUT _cluster/settings
{
    "persistent": {
    "ingest.geoip.downloader.enabled": true
    }
}
```

ILM

POST _ilm/start

Machine Learning

POST _ml/set_upgrade_mode?enabled=false

Monitoring

```
PUT _cluster/settings
{
    "persistent": {
        "xpack.monitoring.collection.enabled": true
    }
}
```

Watcher

POST _watcher/_start

7. Reset the action.destructive_requires_name cluster setting.

```
PUT _cluster/settings
{
    "persistent": {
        "action.destructive_requires_name": null
    }
}
```

Retention Backup

In case backup was enabled in the system level (see Backup Elasticsearch Configuration), snapshots of activities indices will be taken for any of application which have Activity Data Retention configured.

The snapshot will contain all the indices that should be deleted and will be created before the retention deletion process takes place. The snapshot repository and format is in Elasticsearch Backup Overview.

To enable retention backup, the following steps should be performed:

1. In the Server Installer, select the Use Elasticsearch Backup option.

ackup Settings	Far Chi Settings
🛛 Use Elasticsearch Backup 👔	
Repository Path: \\FAM-ANATC	Elasticsearch activity retention backup feature on/off.
Enable Continuous Cluster Backup (2)	
radaptiala Cattinga	
Use Manual Credentials	
Jsername: famuser	Password:
uster Nodes Settings	
Elasticsearch Node fam-anatoly5	Database Path: c:\temp +

2. When setting up an application, on the Activity Configurations and DECs screen, enable **Clear Activity Data** and Backup **Events Before Clearing**.

Provide the time frame for keeping the backup data.

	Resources My Tasks	Reports	Compliance	Forensics	Goals	Settings	Admin						
is Data Sources Perr	missions Management 🗸	Identity Col	llectors										
	Activit	y Configu	rations &	k DECs									
	Change th attributes.	e default values	of the activit	y monitoring		Activi	ty Monito	ring					
						Polling	Interval (s	ec) *					
		°				60							\$
						Report	Interval (s	ec) *					
		-	I			60							\$
			×			Local E	uffer Size	(MB) *					
						This cycl	ic buffer is u	ed to store activitie	s on the Application	Monitor's m	nachine i	in case of network error	's that prevent
						200	tiles nom be	ing seria					\$
					Activity	/ Data Ret o data will be r	ention Period etained for the spec	ified period. Followi	ng that time	period,	activities will be cleared	i.	
							Clear Activ	ity Data					
					/	How	long do y	ou want to keep	activity data? *				
						12				;	:	Month(s)	~
					~	Check	this option	to backup activity da	ata before it is clear	ed.			
							Backup Ev	ents Before Cleari	ng				
	APPLICATION	_								(Car	ncel Previo	ous 🖉
	Step 6 of	'											

3. Within the Tasks screen, initiate the Activity Data Retention Cleanup task.

Running this task will:

- Mark indices for deletion for each configured application
- Back indices to the "retention_backup" folder

• Delete the backup indices

lessage Te Tas	mplates ∨ Capabilities Account	Exclusions 🗸	Name: Activity Data Retention Cleanup Service: Scheduled Task Handler Server: fam-anatoly5			
C	Name	Status	Severity	Date	Description	
C	Activity Data Retention Cleanup		information	1/30/25 8/56/11 PM	Successfully Deleted 72/72 indices	
C	Scheduled Events Deletion		Information	1/30/23 8:56:06 PM	Starting deletion of total 72 indices	
ſ	Scheduled Events Deletion		Information	1/30/23 8:56:06 PM	Finished 72 indices backup	
	Scheduled Events Deletion		Information	1/30/23 8:54:39 PM	Started backup of 72 indices	
	fam-anatolu5 - Crawler Scheduler		Information	1/30/23 8:54:39 PM	Marked 24 indices for deletion for application id: 3	
	Crawl feet anatoly 5 Ten Lavel Dece		Information	1/30/23 8:54:39 PM	Preparing indices older than 1/1/2022 for application id: 3	
	Craw ran-anatorys top Level Kesu.		Information	1/30/23 8:54:39 PM	Marked 24 indices for deletion for application id: 2	
	Synchronize identity Collector	_	Information	1/30/23 8:54:39 PM	Preparing indices older than 1/1/2022 for application id: 2	
	Password encryption	_	Information	1/30/23 8:54:39 PM	Marked 24 indices for deletion for application id: 1	
			Information	1/30/23 8:54:39 PM	Preparing indices older than 1/1/2022 for application id: 1	
			Information	1/30/23 8:54:37 PM	Cleaning activities data for applications: 1,2,3	
Ro	ws per page 25 🗸 1 - 8 of 8		Information	1/30/23 8:54:37 PM	Activity Data Retention Cleanup	
			Rows per page 25 ¥ 1 - 13 of 13		•	Page 1 of 1
			1-130113			

Activate Windows