**ELK Snapshot and Restore**

**Introduction to Snapshot and Restore**

Snapshot and Restore in Elasticsearch allow users to back up and restore indices, cluster state, and configurations. This is crucial for disaster recovery, migrations, and backups.

**Setting Up a Snapshot Repository**

To create snapshots, you need to set up a snapshot repository. Elasticsearch supports various storage types:

* **File system (fs)**
* **Amazon S3 (s3)**
* **Google Cloud Storage (gcs)**
* **Azure Blob Storage (azure)**

**Example: Registering a File System Repository**

PUT \_snapshot/my\_backup\_repo

{

"type": "fs",

"settings": {

"location": "/mnt/backups/elasticsearch"

}

}

**Creating a Snapshot**

Snapshots capture the state of specified indices at a given time.

**Example: Taking a Snapshot**

PUT \_snapshot/my\_backup\_repo/snapshot\_2025\_04\_03

{

"indices": "logs-\*",

"ignore\_unavailable": true,

"include\_global\_state": false

}

* indices: Specifies the indices to be backed up.
* ignore\_unavailable: Skips missing indices instead of failing.
* include\_global\_state: Decides whether to include cluster settings.

**Restoring a Snapshot**

Restoration allows you to recover indices from a snapshot.

**Example: Restoring a Snapshot**

POST \_snapshot/my\_backup\_repo/snapshot\_2025\_04\_03/\_restore

{

"indices": "logs-\*",

"ignore\_unavailable": true,

"include\_global\_state": false

}

* Use \_restore to recover backed-up indices.
* Ensure no conflicting indices exist before restoration.

**Monitoring and Managing Snapshots**

* **List available snapshots:** GET \_snapshot/my\_backup\_repo/\_all
* **Check snapshot status:** GET \_snapshot/my\_backup\_repo/snapshot\_2025\_04\_03
* **Delete a snapshot:** DELETE \_snapshot/my\_backup\_repo/snapshot\_2025\_04\_03

**Automating Snapshots with SLM (Snapshot Lifecycle Management)**

SLM automates snapshot creation and deletion based on schedules.

**Example: Creating an SLM Policy**

PUT \_slm/policy/daily\_snapshots

{

"schedule": "0 0 2 \* \* ?",

"name": "snapshot-daily-{now/d}",

"repository": "my\_backup\_repo",

"config": {

"indices": "logs-\*",

"ignore\_unavailable": true

},

"retention": {

"expire\_after": "30d",

"min\_count": 5,

"max\_count": 50

}

}

* schedule: Runs the snapshot every day at 2 AM.
* expire\_after: Deletes snapshots older than 30 days.

**Conclusion**

Snapshots ensure data safety in Elasticsearch. Teaching students how to configure, create, restore, and automate snapshots helps them manage ELK clusters effectively.