# AWS OpenSearch L1 tooling

# In this page you will find some of the tools that all frontline engineers that work with OpenSearch can access

The service team has recently performed a security audit resulting in revoking of some access to commands for all support ops engineers. If you are experiencing any issues in running the below commands and it is blocking troubleshooting/resolution, please raise a ticket to support ops.

## INDEX



**1. INTRODUCTION**

**THERE IS A GREAT DEAL OF TOOLS IN PLACE TO TROUBLESHOOT AND REPAIR ELASTICSEARCH DOMAINS. HOWEVER, NOT ALL THE TOOLING IS AVAILABLE TO EVERYONE, AS SOME TOOLS CAN POTENTIALLY CAUSE HARM WHEN NOT USED CORRECTLY. THE AMOUNT OF ACCESS GRANTED TO FRONTLINE ENGINEERS HAS INCREASED OVER TIME, WHICH ALLOWED RESOLVING CUSTOMER ISSUES FASTER WITHOUT THE NEED OF ESCALATING AS MUCH. HOWEVER, THERE ARE STILL SOME LIMITATIONS WHEN IT COMES TO PERFORMING SIMPLE OPERATIONS WHICH INVOLVE *SOME* AMOUNT OF RISK. IN ORDER TO OVERCOME THIS LIMITATION, WE INTRODUCED 2PR (2 PERSON RULE[1]) REQUESTS, WHICH EMPOWER L1 ENGINEERS TO REQUEST A MORE TENURED ENGINEER (L2 OR L3) TO PERFORM SOME OF SUCH ACTIONS. USING THIS METHOD, YOU WILL BE ABLE TO PERFORM *SUPERVISED EXECUTIONS* WITHOUT THE NEED OF ESCALATING EVERY ISSUE, SOLVING PROBLEMS ON THE SPOT.**

In this wiki page you will find what operations you can execute through 2PR, and how to execute them. You will also be able to find the latest operations that are available for L1 engineers.
But before going any further, what is L1, L2 and L3 access? This acronyms represent the access level to the Elasticsearch

service. L1 access is the default access level for everyone that works in Premium Support with this service. No risky operations can be performed. When an engineer decides to work on becoming an SME, after proving enough skill and understanding, will be granted L2 level (to learn more, contact your local SME). This level enables the engineer to perform low-risk operations, and validate 2PR requests from L1. SMEs get the highest access level in Premium Support: L3.
In order to better understand the tools available on this page, please find the session recording on the OpenSearch L1 tooling walkthrough below:
Broadcast Link

**2. AVAILABLE 2PR OPERATIONS**

**IN ORDER TO EXECUTE 2PR REQUESTS YOU WILL NEED TO CONFIGURE YOUR ACCESS FOR THE AES CLOUD OPS HOST. IF YOU DIDN'T CONFIGURE IT YET, YOU CAN FIND HOW TO DO SO IN THE VIDEO [2][8]. ONCE YOU ARE ABLE TO ACCESS IT, YOU CAN PERFORM 2PR THIS REQUESTS TO YOUR LOCAL ELASTICSEARCH L2S. IF NO L2 IS AVAILABLE, YOU CAN REQUEST IT TO ANY LOCAL SME. YOU CAN FIND A LIST WITH ALL L2S AND SMES FOR THE ELASTICSEARCH SERVICE IN [3].**

Please be mindful before sending the request, and make sure that you understand what you are executing. Ask to yourself "What could be the consequences of running this command on this cluster at the moment?" or "Are there any risks when doing so?". For example, if a DDI failed at the start, and you retry it while the Elasticsearch domain is under a heavy load, you might destabilize it when retrying the failed activity, and you should synchronize with the customer about what time would be the best to trigger this operation (for example, on low-request time frames).
All 2PR commands are the same as any other *aescloudopstools* command, but it includes the flag "—approver-id $L2_peer“

**Retry failed activities**

**In order to assess if retrying failed activities in a domain will bring the Elasticsearch cluster back to a healthy state, you will need to first look into its current state**

```
aescloudopstools $REGION domain cp cs-domain-manager-status --args "-D $DI"
```

After your investigation, if you conclude that this domain requires to restart its failed activities, you can speak with an L2 engineer and discuss whether the failed activities should be restarted, and submit the request to him.
`aescloudopstools $REGION domain cp cs-retry-failed-activities --approver-id $L2_PEER --args "-D $DI“`

*Note: Before running this command, make sure that it will not trigger a blue/green deployment while the domain is under heavy load. Before sending the 2PR request, the domain CPU should be below the 80%, and the JVM stable below a 75%.*

**Delete stuck snapshot**

**If you identify a snapshot is stuck while being created, you can terminate it using the command below**

```
aescloudopstools $REGION domain cp cs-manage-es-snapshots --args "-D $DI -n $SNAPSHOT_ID --action delete --repository-name $REPO_NAME" --approver-id $L2_PEER
```

**Disable hourly snapshots**

**This command will disable hourly snapshots but keep daily snapshots for a set of Elasticsearch domains. However, this command is a bit primitive and fully erases the previous configuration. For this reason, you will need to perform TWO steps when disabling the hourly snapshots for an Elasticsearch domain.**

***Please note: This command requires a 2PR from an L2 engineer. Please add "—approver-id $L2_peer" at the end**

**of the command before running it.**

**1. First step: Retrieving WHAT ELASTICSEARCH DOMAINS ALREADY DO HAVE DISABLED SNAPSHOTS for the region in which the domain you want to configure is located:**

`aescloudopstools $REG domain cp cs-whitelist-client-snapshot --feature es.snapshot.frequent_snapshot_disabled_domains --args "--target-stack swift-$REGION-prod --target-client-id $AWS-ACCOUNT-ID -r prod --region $REGION --action list"`
- Example command:
`aescloudopstools dub domain cp cs-whitelist-client-snapshot --feature es.snapshot.frequent_snapshot_disabled_domains --args "--target-stack swift-eu-west-1-prod --target-client-id 123456789012 -r prod --region eu-west-1 --action list"`
- Example output:

```
INFO Executing (...)
{
    "swift-eu-west-1-prod": {
        "123456789012": {
            "es.snapshot.frequent_snapshot_disabled_domains": "DOMAIN_1,DOMAIN_2",
            "updated_by": "(...)",
            "updated_utc": "(...)"
        }
    }
}SUCCESS
```

*Please note that the command returned a list WITH THE DOMAINS THAT DO NOT HAVE HOURLY SNAPSHOTS ENABLED FOR THAT REGION AND AWS ACCOUNT ID.*
*NOTE:* If you want to re-enable hourly snapshots make sure to swap the "—action" parameter to "disable".
2. Second step: adding **THE FULL LIST OF ELASTICSEARCH DOMAINS THAT SHOULD HAVE NO HOURLY SNAPSHOTS FOR THAT REGION**, using a comma separated list.
`aescloudopstools $REG domain cp cs-whitelist-client-snapshot --feature es.snapshot.frequent_snapshot_disabled_domains --args "--target-stack swift-$REGION-prod --target-client-id $AWS-ACCOUNT-ID -r prod --region $REGION --feature_value $DOMAIN_LIST --action enable"`
- Example command:
`aescloudopstools dub domain cp cs-whitelist-client-snapshot --feature es.snapshot.frequent_snapshot_disabled_domains --args "--target-stack swift-eu-west-1-prod --target-client-id 123456789012 -r prod --region eu-west-1 --feature_value es_domain_1,es_domain_2,es_domain_avocado --action enable"`
Please note how the domains have been added as a list. This change might take a while to kick in, so the next snapshot(s) might be taken after the change was pushed.
To get more info about the different nomenclatures for regions you can visit [4]: https://w.amazon.com/bin/view/AWS/Regions/

**Change daily snapshot time**

*For L1 engineers, this command need 2PR from L2/L3 engineers.
In order for us to access this command, we would need to follow a contingent security mechanism which is implemented by creating a ticket to the below mentioned CTI:
C: AWS
T: OpenSearch Tool Usage
I: Customer Issue
To ease this activity of creating a ticket and following the specified format, we have created a ticket template which can be found below:

https://t.corp.amazon.com/create/templates/76128b53-02ee-42b2-9e23-ed39e55af773
The Command usage have been described below:
`aescloudopstools run <REGION> domain cp cs-override-es-domain-config-snapshot-hour --args "-D <DI> --ticket-id <Ticket-Id>" --snapshot-hour <Value>`
***Please note**: The `—ticket-id` in above command is for the new TT you just created and while you are running the command, you need to make sure the TT is in Open status.

**3. CLOUDWATCH AGENT RESTART**

The AWS Elasticsearch managed service has some mechanisms to upkeep the cloudwatch agent health. However, there are some edge cases where the agent needs to be restarted manually. In order to do so, you will need to use the tumbler CLI in the Ops Host that you configured in the introduction. You can find more info on tumbler in [5]. There are two ways to restart the Cloudwatch agent: the automated and the manual
When Cloudwatch isn't reporting metrics for a node, use the automated approach. It will first check if the Cloudwatch agent is running, and it will start it only if the Cloudwatch agent is not generating any logs. As explained in the CWAgentUnhealthy SOP[6], there are three steps to perform this operation:

- **Step 1:** `tumbler <region> aes domain cw restart -D <domain-id>` command will check count of cw.agent.log* files in `/apollo/env/swift-*-LogPusherAMI-ES2/var/output/logs` across all the nodes from a domain. **If count is greater than 0**, it will return status of that **CloudWatch agent for that node** as healthy else unhealthy.
- **Step 2:** To Restart CloudWatch agent (kill CloudWatch process id) operator need to pass `--submit` flag to above command. `tumbler <region> aes domain cw restart -D <domain-id> --submit` will kill CloudWatch agent processes across domain if CloudWatch agent is unhealthy.
- **Step 3:** To verify if CloudWatch restarted successfully wait for a minute and then check status by running command (`tumbler <region> aes domain cw restart -D <domain-id>`) mentioned in Step 1.

In some edge cases, it might be required to restart the Cloudwatch agent manually. For example, https://issues.amazon.com/BeagleRock-965. In such cases, **please synchronize with the customers so they do not get surprised/alarmed if some specific nodes stops sending metrics**.

- **Step 1:** Stop the Cloudwatch agent in the problematic node tumbler `tumbler <region> aes domain cw stop -D <domain-id> -i <instance_id>`. You can find instance IDs in Domain Resources.
- **Step 2:** This command takes a while to run. Please wait until it finishes and confirm from the output that the execution was successful.
- **Step 3:** Make sure that the agent is active for that very same instance id. `tumbler <region> aes domain cw start -D <domain-id> -i <instance_id>`. The supervisor process should bring up the Cloudwatch agent as soon as it stops working, but always double check by running the command specified in this step.

**4. PERFORMING SETTING CHANGES**

Currently all frontline engineers can change the following settings when the customer requests for it. The max buckets and scroll setting will require a 2PR:

- Max Buckets
- Max Shard per Node Limit
- Max Open Scroll Context Limit
- Remove Write Block

Before you apply the new setting, make sure that the customer understands the implications of such change.
You can get the current settings using the command below:
`tumbler run $REGION aes domain dp node es curl cluster get-settings --domain-identifier=$DOMAINIDENTIFIER`

- Example command:
`tumbler run dub aes domain dp node es curl cluster get-settings --domain-identifier=123456789012:my-beloved-domain`
You can update any of the below four settings using the next tumbler command:
`tumbler run iad aes domain dp node es curl cluster update-settings --domain-identifier=$DOMAINIDENTIFIER --approver-id=<alias> [--bucket-limit=INT] [--scroll-limit=INT] [--shard-limit=INT] [--is-cluster-read-only-block-enabled=INT]`
The setting `--is-cluster-read-only-block-enabled=INT`will convey whether the cluster is in a read-only (write block) mode or not. The setting takes the value as 0 to remove the write block (set read only to false) and a value of 1 to set the write block (set read only to true).
Example: To remove the cluster write block / (to remove the cluster from read only mode) you would trigger the below command:
`tumbler run iad aes domain dp node es curl cluster update-settings --domain-identifier=$DOMAINIDENTIFIER --approver-id=<alias> --is-cluster-read-only-block-enabled=0`
Again, please be mindful about performing such configuration changes, as they can severely impact the cluster performance in some circumstances.
For max buckets, max scroll contexts and max shards per nodes, tthe command does not restrict to any upper bound limit anymore. If customers request higher values you could explain the disadvantages with regards to cluster instability and also review it from the 2PR.

**5. RETRYING FAILED SHARD ALLOCATIONS**

**ONE OF THE REASONS CLUSTER'S CAN END UP IN A RED/YELLOW STATE IS DUE TO A FAILED SHARD ALLOCATION. BY DEFAULT, ELASTICSEARCH WILL RETRY UP TO 5 TIMES TO ALLOCATE THE SHARD.**

**IT IS POSSIBLE FOR US TO PERFORM THE BELOW API ON A GIVEN DOMAIN WHICH WILL ATTEMPT A SINGLE RETRY ROUND FOR THESE SHARDS [7].**
**`POST _CLUSTER/REROUTE?RETRY_FAILED=TRUE`**

**FIRSTLY YOU WILL WANT TO VERIFY THAT THIS WILL SOLVE THE ISSUE USING THE BELOW API CALL:**
**`GET _CLUSTER/ALLOCATION/EXPLAIN`**

**IF YOU SEE A SIMILAR OUTPUT AS BELOW WHERE FAILED_ALLOCATION_ATTEMPTS HAS REACHED IT'S MAX:**

```
{
    "index": "index-name",
    "shard": 3,
    "primary": true,
    "current_state": "unassigned",
    "unassigned_info": {
        "reason": "ALLOCATION_FAILED",
        "at": "2022-01-06T13:09:28.055Z",
        "failed_allocation_attempts": 5,
...
```

It is likely that the allocation can be retried given that all other issues have been resolved.
You can execute this command on a given domain with the following:
`tumbler run $REGION aes domain dp node es curl cluster reroute-retry-failed -D $DOMAINIDENTIFIER --submit`
- Example command:
`tumbler run dub aes domain dp node es curl cluster reroute-retry-failed -D 123456789012:my-beloved-domain --submit`

**6. CLUSTERS STUCK IN DELETION**

**IN SOME SITUATIONS, DOMAIN DELETIONS MIGHT GET STUCK. THIS ISSUE CAN BE ADDRESSED MOST OF THE TIMES BY TRIGGERING A "RECOVER" OPERATION OVER THE STUCK DOMAIN. HOWEVER, TRIGGERING A RECOVER DOMAIN ACTIVITY THIS IS A RESTRICTED OPERATION AS IT KILLS THE DOMAIN MANAGER FOR THE DOMAIN. FOR THIS REASON, THE SERVICE TEAM HAS PROVIDED A COMMAND THAT WILL TRIGGER A "RECOVER" OPERATION ONLY IF THE DOMAIN HAS RECEIVED A DELETION OPERATION.**

**TO KNOW IF A DOMAIN IS STUCK ON DELETION, YOU CAN USE K2 CR/TUMBLER, AND EXECUTING "CS-DOMAIN-MANAGER-STATUS" AS EXPLAINED IN THE POINT 2. PLEASE CHECK BOTH TOOLS TO MAKE SURE THAT THE DOMAIN IS INDEED STUCK IN DELETION.**

**YOU CAN FIND THE COMMAND TO RECOVER A DOMAIN STUCK IN DELETION BELOW:**

```
AESCLOUDOPSTOOLS <REGION> DOMAIN CP CS-RECOVER-DELETED-DOMAIN --ARGS " -D <DOMAIN-IDENTIFIER>"
```

**EXAMPLE COMMAND:**

```
AESCLOUDOPSTOOLS PDX DOMAIN CP CS-RECOVER-DELETED-DOMAIN ARGS "-D 795XXXXX822:DEMO-LOGGING"
```

**7. RESTARTING OPENSEARCH SERVICE ON NON-PRODUCTION CLUSTERS**

**FOR SITUATIONS THAT REQUIRE ENGINEERS TO RESTART/BOUNCE ES/OPENSEARCH PROCESS ON THE NODES, *(SITUATIONS FOR EXAMPLE WHEN THE NODE IS MARKED UNHEALTHY BY THE ELB, MANAGING STUCK SNAPSHOTS, ETC)*. BOUNCING/RESTARTING ES/OS PROCESS ON A NODE IS NOW POSSIBLE USING THE BELOW COMMAND `SAFE-REBOOT-TTYPE-INSTANCE.`**

**HOWEVER THIS COMMAND IS ONLY LIMITED TO NON-PRODUCTION CLUSTERS. CLUSTERS WHERE**
**1) DOMAIN HAS NO MASTER NODES**
**2) DOMAIN HAS LESS THAN 3 DATA NODES**
**3) DOMAIN HAS DATA NODE TYPE WHICH STARTS WITH T (T2 OR T3)**

**THE COMMAND WOULD NOT WORK IF DOMAIN HAS MASTER NODES OR DOMAIN HAS MORE THAN THREE NODES OR THE DOMAIN HAS INSTANCE TYPES OTHER THAN THE <T> FAMILY ONES.**

```
TUMBLER RUN <REGION> AES DOMAIN DP NODE SAFE-REBOOT-TTYPE-INSTANCE –DOMAIN-IDENTIFIER=<DOMAIN-IDENTIFIER> --INSTANCE-ID=<EC2-INSTANCE-ID> --APPROVER-ID=<ALIAS>
```

**EXAMPLE COMMAND:**

```
TUMBLER RUN PDX AES DOMAIN DP NODE SAFE-REBOOT-TTYPE-INSTANCE --DOMAIN-IDENTIFIER=XXXX:TEST-DOMAIN-SNAPSHOT-2 --INSTANCE-ID=I-0F56166XXXXD16F --APPROVER-ID=CXF
```

**8. DOWNLOADING HISTORICAL LOGS VIA TUMBLER**

**WHEN PERFORMING A ROOT CAUSE ANALYSIS, YOU MIGHT BE REQUIRED TO LOOK AT THE `ELASTICSEARCH.LOG` OR OTHER LOG FILES TO UNDERSTAND WHY SOMETHING HAPPENED.**

**BELOW IS A SHORT VIDEO THAT DEMONSTRATES HOW TO REQUEST LOGS, ASSUME THE SERVICE TEAM OPS-DATALAKE ROLE, DOWNLOAD THE LOGS, UNZIP THE LOGS AND A FEW BASIC COMMANDS FOR BROWSING THEM ON THE COMMAND LINE.**

Broadcast Link

**9. RESTART OPENSEARCH DASHBOARDS/KIBANA**

**AMAZON OPENSEARCH CUSTOMERS REACH OUT TO AWS SUPPORT ENGINEERING WHEN THEY SEE OPENSEARCH DASHBOARDS/KIBANA UNHEALTHY FROM THEIR END. DURING SUCH SITUATIONS, L1 ENGINEERS NEED TO VERIFY THE CLUSTER RESOURCES AND ESPECIALLY THE METRIC OPENSEARCHDASHBOARDSHEALTHYNODES (KIBANAHEALTHYNODES FOR VERSION <= 7.10). THE SUM STATISTIC FOR THIS METRIC SHOULD BE EQUIVALENT**

**TO THE NUMBER OF DATA-NODES IN THE CLUSTER. IF YES, THIS CONFIRMS THE OPENSEARCH DASHBOARDS SERVICE/KIBANA SERVICE IS RUNNING ON ALL DATA-NODES AND IS HEALTHY. IF THE SUM STATISTIC IS LESS THAN THE COUNT OF DATA-NODES IN THE CLUSTER THIS TELLS US THAT THE OPENSEARCH DASHBOARDS/KIBANA SERVICE IS NOT RUNNING AT LEAST ON ONE DATA-NODE AND THIS NEEDS TO BE FIXED. ALTERNATIVELY, L1 ENGINEERS CAN RE-CONFIRM USING THE MINIMUM STATISTIC FOR THE OPENSEARCHDASHBOARDSHEALTHYNODES (KIBANAHEALTHYNODES) METRIC WHICH WILL BE 0 IF OPENSEARCH DASHBOARDS/KIBANA SERVICE IS NOT RUNNING AT LEAST ON ONE DATA-NODE. AFTER VERIFYING THE METRIC IS INDEED UNHEALTHY WE RECOMMEND YOU TO PERFORM THE FOLLOWING STEPS:**

---

**Step 1: Run the Dashboards/Kibana diagnostic tool**

The below command will tell you exactly on which data-node dashboards/kibana service is unhealthy

```
tumbler <region> aes domain dp node kibana diagnostic -D <domain-identifier>
```

Example:

```
tumbler pdx aes domain dp node kibana diagnostic -D 12345678910:prod
```

The output to the above will display the data-node on which we need to restart the dashboards/kibana service. (As of today the output displays the deactivate and activate command separately however L1 engineers will run the restart command as below on those data-nodes since the restart command internally calls the de-activate and activate explicitly) . The output alternatively will also provide the command to restart kibana on the entire cluster (all data-nodes at once) and if dashboards/Kibana service is unhealthy on majority of the data-nodes you can restart kibana on the cluster level (which would restart the kibana process on all data-nodes together). Please take a look at the example diagnostic command in this ticket under the overview section: https://t.corp.amazon.com/V720034164/overview

**Step 2: Restart Dashboards/Kibana**

This step is important here and needs attention. The above diagnostic command will output the action to be taken when kibana is unhealthy. In most cases the fix/action item is just a quick deactivate and activate kibana (which we also term as 'bounce') and only in such cases you will proceed with the below. However in few cases, the diagnostic tool will output the fix as re-index the kibana index or make the kibana alias point to the new kibana index and so on. L1 engineers still do not have access to help with re-index and alias actions so if the tool recommends the same you will escalate to support-operations. If the tool recommends a deactivate and activate only, then you proceed with the below.

***Restart Kibana on a data-node***

---

```
tumbler run <region> aes domain dp node kibana restart --domain-
identifier=DOMAINIDENTIFIER --approver-id=<alias> --instance-id=<id>
```

Example:

```
tumbler run <region> aes domain dp node kibana restart --domain-
identifier=12345678910:prod --approver-id=cxf --instance-id=i-02b5xxxx1923a9f30
```

The diagnostic command will provide you with the instance-id you need to restart kibana on.

---

***Restart Kibana on domain level (all data-nodes at once)***

This is only to be done when most or all of the data-nodes need a kibana restart

```
tumbler run <region> aes domain dp restart-kibana --domain-identifier=DOMAINIDENTIFIER --approver-id=<alias>
```

Example:

```
tumbler run <region> aes domain dp restart-kibana --domain-identifier=12345678910:prod --approver-id=cxf
```

---

**Step 3: Verify**

As the restart command runs keep an eye on the output. If the output of the kibana restart command displays a SUCCESS for that data-node (or all nodes for domain level) then wait for a couple minutes and verify from cloudwatch metrics if the OpenSearchDashboardsHealthyNodes (KibanaHealthyNodes) metric is now showing the expected value. If the restart command does display a FAILED message or any error, then this indicates the problem for kibana could not be fixed by just a restart and that more deep dive would be needed. In such a case, reach out to a L3 engineer (support-ops) or escalate to service team. You will only escalate to service team if the issue needs urgent attention.
**Note**:
For L1 engineers, while doing this for the first few times, please perform these commands in the shadow of the L2/L3 peer who is the approver. If any questions, please reach out to the available L2/L3 engineers. Please remember running these commands impact the customer production clusters directly.

**10. RESTORE ACCIDENTALLY DELETED DOMAIN (WITH 2PR) IF THE DOMAIN WAS NOT FGAC ENABLED (THIS IS ONLY FOR L3 NOW)**

**FOR L1 SUPOPS ENGINEERS, NOW YOU ARE ABLE TO HELP CUSTOMER TO RESTORE ACCIDENTALLY DELETED DOMAIN (WITH 2PR) IF THE DOMAIN WAS NOT FGAC ENABLED.**

**FIRST PLEASE RUN BELOW COMMAND TO CHECK IF THE DELETED DOMAIN STILL HAVE AVAILABLE SNAPSHOT:**

```
AESCLOUDOPSTOOLS $REGION DOMAIN CP ES-TOMBSTONE-RESTORE-SNAPSHOT --ARGS "--DELETED-DOMAIN-IDENT
<ACCOUNT ID:DOMAIN NAME> --VALIDATE-DELETED-DOMAIN"
```

**IF THE OUTPUT SHOWS THAT THERE IS STILL SNAPSHOT AVAILABLE FOR THE DOMAIN, ASK CUSTOMER TO CREATE A NEW DOMAIN AND MAKE SURE THAT THE CONFIGURATION OF THIS NEW DOMAIN IS EXACTLY THE SAME AS THE OLD DOMAIN. ONCE NEW DOMAIN IS AVAILABLE, PLEASE RUN BELOW COMMAND (WITH 2PR) TO RESTORE THE DOMAIN:**

```
AESCLOUDOPSTOOLS $REGION DOMAIN CP ES-TOMBSTONE-RESTORE-SNAPSHOT --ARGS "--DELETED-DOMAIN-IDENT
<ACCOUNT ID:DOMAIN NAME> --NEW-DOMAIN-IDENT <ACCOUNT ID:DOMAIN NAME> --RESTORE"
```

**IF THE ACCIDENTALLY DELETED DOMAIN WAS FGAC ENABLED, PLEASE CREATE TT TO SUPOPS OR SERVICE TEAM.**

**References**

**[1] 2 Person Rule/2PR**

**https://w.amazon.com/bin/view/Quadiir/2PersonRule**

[2] DevDesktop + Tumbler CLI & CloudOpsTools Setup for L1s
https://broadcast.amazon.com/videos/415727
[3] AWS Elasticsearch Ops Members
https://w.amazon.com/bin/view/AmazonWebServices/SalesSupport/DeveloperSupport/Internal/AmazonElasticsearch/SupportOperations/OpsMembers
[4] Region Codes
https://w.amazon.com/bin/view/AWS/Regions
[5] Tumbler Wiki
https://w.amazon.com/bin/view/AWS/SearchServices/OpsTumbler/UserGuide
[6] CwAgentUnhealthy SOP
https://w.amazon.com/bin/view/Search/A9/Swift/Ops/Procedures/CwAgentUnhealthy
[7] Elasticsearch - _cluster/reroute API
https://www.elastic.co/guide/en/elasticsearch/reference/current/cluster-reroute.html#cluster-reroute

Tags: inclusive_tech_exceptionX
[+]