# **Centralized CloudTrail Logging & Retention (AWS Control Tower)**

## **Objective**

* Centralize **CloudTrail logs** in the **Log Archive account (mwt-log)**.
* Apply **3-year retention on S3**.
* Apply **1-year retention on CloudWatch Logs**.
* Review **AWS Config retention** and extend if possible.

We use **AWS Control Tower**, which already creates and manages an **Organization CloudTrail**.  
Our work focuses on **verifying configuration, applying retention, and tuning lifecycle rules**.

## **Implementation Steps (via AWS Console)**

### **Step 1 – Verify Organization Trail (Control Tower)**

1. Go to **CloudTrail Console → Trails**.
2. Confirm that an **organization trail** exists — created by Control Tower.
3. Check it writes logs to the **Log Archive account (mwt-log)** S3 bucket.

Docs: [Logging AWS Control Tower actions with CloudTrail](https://docs.aws.amazon.com/controltower/latest/userguide/logging-using-cloudtrail.html?utm_source=chatgpt.com)

### **Step 2 – Locate CloudTrail Logs in S3**

1. In the **Log Archive (mwt-log) account**, open **S3 Console → Buckets**.
2. Find the Control Tower bucket:  
    aws-controltower-logs-<account-id>-<region>
3. Confirm CloudTrail logs appear under AWSLogs/.

Docs: [Logging and monitoring in AWS Control Tower](https://docs.aws.amazon.com/controltower/latest/userguide/logging-and-monitoring.html?utm_source=chatgpt.com)

### **Step 3 – Add S3 Lifecycle Rule (3-Year Retention)**

1. In the bucket → **Management tab → Lifecycle rules → Create rule**.
2. Name: cloudtrail-3year-retention.
3. Scope: apply to prefix AWSLogs/.
4. Expiration: delete objects after **1095 days (~3 years)**.
5. (Optional) Transition to **S3 Intelligent-Tiering or Glacier** after 90 days to optimize cost.

Docs: <https://docs.aws.amazon.com/controltower/latest/userguide/logging-and-monitoring.html#log-retention>

Ensures CloudTrail logs don’t grow infinitely but remain available for compliance.

### **Step 4 – Configure CloudWatch Log Group Retention (1 Year)**

1. In **CloudTrail Console → Organization Trail → Edit**.  
   * Check which CloudWatch **Log Group** is used (e.g., /aws/controltower/CloudTrailLogs).
2. In **CloudWatch Console → Log groups**, select the group.
3. Actions → **Edit retention** → set to **1 year (365 days)**.

Docs: <https://docs.aws.amazon.com/awscloudtrail/latest/userguide/send-cloudtrail-events-to-cloudwatch-logs.html>

### **Step 5 – Review AWS Config Retention**

1. Go to **AWS Config Console → Settings**.  
   * Confirm Config is enabled across the organization (Control Tower enables it by default).
2. Config delivers history to an S3 bucket in the log archive.
3. To extend retention:  
   * Go to Config S3 bucket → **Lifecycle rules**.
   * Set expiration >3 years (or unlimited, based on compliance).

Docs: [AWS Control Tower governance with Config](https://docs.aws.amazon.com/controltower/latest/userguide/what-is-control-tower.html#governance)

## **End State (Acceptance Criteria)**

* CloudTrail logs centralized in **mwt-log S3 bucket**
* **S3 lifecycle rule = 3 years retention** (optional tiering for cost savings)
* **CloudWatch Logs retention = 1 year**
* **AWS Config history extended** (if needed for compliance)

## **Notes**

* Our role is to **tune retention and lifecycle**, not duplicate resources.
* Terraform can optionally enforce lifecycle rules & retention for repeatability.