

CHG0030110 — [TITAN] Medium — logging on rds-telco-ocs

Severity	Medium	Priority	3 - Moderate
Cloud	AWS	State	Assigned
Resource	rds-telco-ocs	Group	observability_engineering
Resource type	AWS::RDS::DBInstance	Change type	Normal
Opened	2026-04-22 19:19:25	Closed	2026-04-22 19:19:25
CAB required	No	Close code	—

Security Finding

Online Charging System DB has CloudTrail data-events disabled – prepaid balance manipulation cannot be audited. Fraud-risk control gap for prepaid MVNO operations.

Justification

Medium: Online Charging System DB has CloudTrail data-events disabled – prepaid balance manipulation cannot be audited. Fraud-risk control gap for prepaid MVNO operations.

Implementation Plan

1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:

```
aws cloudtrail put-event-selectors --trail-name telco-audit --event-selectors '[{"ReadWriteType": "All", "IncludeManagementEvents": true, "DataResources": [{"Type": "AWS::RDS::DBInstance", "Values": [{"arn": "aws:rds:*:*:db:rds-telco-ocs"}]}]'
```
3. TITAN FORGE verifies the fix was applied.
4. Post-change rescan by TITAN SCOUT – finding must no longer appear.
5. Close ticket with Successful close_code.

Risk & Impact Analysis

Risk level: MEDIUM risk – weaker control, should be hardened.
 Business impact if unremediated: Control weakness that compounds with other gaps.
 Scope: single resource (rds-telco-ocs).
 Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available if rescan fails.
 Finding detail: Online Charging System DB has CloudTrail data-events disabled – prepaid balance manipulation cannot be audited. Fraud-risk control gap for prepaid MVNO operations.

Backout / Rollback Plan

1. TITAN auto-captured snapshot of rds-telco-ocs before change (baseline: titan-telecom-demo-20260422T201925Z).
2. If post-change rescan still shows the finding OR a new issue appears within 15 min:
 - a. TITAN FORGE fires rollback automatically using stored snapshot.
 - b. Incident reopens and escalates to on-call.
3. Manual rollback command path (human override) is documented in close notes.

Test Plan

1. TITAN SCOUT rescans rds-telco-ocs immediately after FORGE applies the change.
2. PASS criteria: the specific finding no longer appears in SCOUT results.

3. PASS criteria: no new CRITICAL or HIGH findings introduced by the change.
4. Automated compliance check: HIPAA/PCI/SOC2 controls re-evaluated.
5. If any check fails, backout plan fires automatically.

Recommended Fix Command

```
aws cloudtrail put-event-selectors --trail-name telco-audit --event-selectors '[{"ReadWriteType": "All", "IncludeManagementEvents": true, "DataResources": [{"Type": "AWS::RDS::DBInstance", "Values": [{"arn:aws:rds:*:*:db:rds-telco-ocs"}]}]']
```

Compliance Mapping

SOC 2 CC7.1, HIPAA §164.312(b)

AI Close Notes

TITAN CONDUIT opened this medium logging change request and assigned it to the regulatory_affairs group for review. STATE: ASSIGNED – awaiting human action. Per TITAN AI policy (and Kazmi rule, 2026-04-22), configuration changes are NEVER auto-applied and change tickets are NEVER auto-closed by TITAN. The assigned group reviews the recommended fix, schedules a CAB-approved change window, applies the fix manually, validates via SCOUT rescan, and closes this ticket themselves. TITAN documents and routes – the human owns the change from here.