

Your oldest verified restore is 412 days old — and 10 of 14 resources have never been restored.

PROTECTED RESOURCES
12/14

NEVER RESTORED
10

RESTORE AGE > 180 DAYS
2

OLDEST VERIFIED RESTORE
412d

RESOURCE	TYPE	RETENTION	LAST BACKUP	RESTORE AGE	VERDICT
acme-backup-target	S3	versioning	—	never	NEVER
acme-csv-exports	S3	versioning	—	never	NEVER
acme-logs-archive	S3	versioning	—	never	NEVER
acme-static-site	S3	versioning	—	never	NEVER
acme-user-uploads	S3	versioning	—	never	NEVER
aurora-core	Aurora	7 days	2026-10-27	never	NEVER
aurora-reporting	Aurora	5 days	2026-10-27	never	NEVER
legacy-crm	RDS	—	2026-04-30	never	NEVER
prod-orders	RDS	7 days	2026-10-27	never	NEVER
staging-orders	RDS	1 days	2026-10-26	never	NEVER
analytics-warehouse	RDS	3 days	2026-10-27	247 days	>180 DAYS
prod-identity	RDS	14 days	2026-10-27	412 days	>180 DAYS
acme-invoices	S3	versioning	—	96 days	31-180 DAYS
prod-billing	RDS	7 days	2026-10-27	12 days	OK

Evidence basis: Restore history: readable · AWS Backup plans: readable · Restore testing: readable · Regions: 1 · Coverage of resources with evidence: 29%

What this report is

Facts, not an opinion: for each resource we list the backup configuration and the last restore we could verify. Metadata only — describe/list API calls. No S3 object, database row or backup content was read; no credentials were stored. Restores run outside AWS Backup are not observable, so history is under-reported, never over-reported.

Verdicts

NEVER — no completed restore found in AWS Backup restore history.
>180 DAYS — last verified restore is older than the auditor-relevant 180-day line.
OK / 31-180 DAYS — recent evidence, keep it that way.
UNKNOWN — the role could not read restore history; not reported as a failure.