

Sample Executive Audit Dossier

Anonymised Australian retail and logistics group, Queensland, Australia. 6 AWS accounts, about \$25,000 AUD per month in ap-southeast-2.

This document is a sample. The organisation, accounts, principals and figures are invented to show the format and depth of an Appware Executive Teardown. It describes no real customer.

Overall Well-Architected score	66 / 100
High-risk issues	20
Medium-risk issues	31
Recoverable spend	\$8,430 AUD per month
Annualised	\$101,160 AUD per year
Share of monthly spend	33.7%
Critical IAM findings	2

Well-Architected scorecard

Operational Excellence

71 / 100



2 high, 5 medium. Runbooks exist for 4 of 11 production services; no tested rollback for 3 stacks.

Security

58 / 100



6 high, 9 medium. 3 cross-account roles trust an external principal without an ExternalId; 5 wildcard policies

Reliability

74 / 100



3 high, 4 medium. Single-AZ RDS in 2 non-production accounts that serve production reporting.

Performance Efficiency

80 / 100



1 high, 3 medium. 212 attached gp2 volumes could move to gp3 with no downtime.

Cost Optimization

49 / 100



7 high, 6 medium. Savings Plan and RI coverage is 18% against a steady-state baseline above 70%.

Sustainability

66 / 100



1 high, 4 medium. Idle non-production fleet runs 24x7; no scheduled stop or scale-to-zero.

FinOps waste breakdown (AUD per month)

ID	Finding	Monthly	Annual
FINOPS-W32	Unattached EBS volumes (9 gp2, 5 io1) Fix: Snapshot, then delete	\$1,420	\$17,040
FINOPS-W41	Unreserved steady-state RDS (On-Demand 24x7 > 90 days) Fix: 1-year Reserved Instances	\$2,310	\$27,720
FINOPS-W44	Unreserved steady-state EC2 (Compute Savings Plan coverage 18%) Fix: Compute Savings Plan to 70% coverage	\$2,870	\$34,440
FINOPS-W57	NAT Gateway hairpin (S3 and DynamoDB traffic via NAT) Fix: Gateway VPC endpoints; one NAT per non-production VPC	\$1,180	\$14,160
FINOPS-W60	gp2 volumes that should be gp3 Fix: In-place modify_volume to gp3	\$360	\$4,320
FINOPS-W71	CloudWatch log groups with no retention Fix: Set 30 to 90 day retention	\$290	\$3,480
Total		\$8,430	\$101,160

IAM wildcard exposure ledger

SEC-IAM-01 CRITICAL

acct-prod-01 role/ci-deploy-legacy
Inline policy allows Action "*" on Resource "*"

SEC-IAM-02 HIGH

acct-prod-01 role/vendor-support-access
Trust policy allows an external account with no ExternalId condition

SEC-IAM-03 HIGH

acct-data-02 role/etl-runner
Action "s3:*" on Resource "arn:aws:s3:::"

SEC-IAM-04 HIGH

acct-shared-01 role/platform-admin-poc
Action "iam:PassRole" on Resource "*" with ec2:RunInstances (privilege escalation path)

SEC-IAM-05 CRITICAL

acct-dev-03 user/build-bot
Long-lived access key, 412 days old, attached AdministratorAccess

SEC-IAM-06 MEDIUM

acct-dev-03 role/lambda-legacy
Action "dynamodb:*" on Resource "*"

Deterministic remediation

Snapshot and remove unattached EBS volumes (FINOPS-W32)

```
import boto3

REGION = "ap-southeast-2"
DRY_RUN = True # review the printed list, then set to False

ec2 = boto3.client("ec2", region_name=REGION)
for page in ec2.get_paginator("describe_volumes").paginate(Filters=[{"Name": "status", "Values":
    for vol in page["Volumes"]:
        vid = vol["VolumeId"]
        print(f"{vid} {vol['VolumeType']} {vol['Size']} GiB unattached")
        if DRY_RUN:
            continue
        snap = ec2.create_snapshot(
            VolumeId=vid,
            Description="pre-delete safety snapshot",
            TagSpecifications=[{"ResourceType": "snapshot", "Tags": [{"Key": "reason", "Value":
```

Move attached gp2 volumes to gp3 in place (FINOPS-W60)

```
import boto3

ec2 = boto3.client("ec2", region_name="ap-southeast-2")
for page in ec2.get_paginator("describe_volumes").paginate(Filters=[{"Name": "volume-type", "Val
    for vol in page["Volumes"]:
        print("modify", vol["VolumeId"], vol["Size"], "GiB")
        ec2.modify_volume(VolumeId=vol["VolumeId"], VolumeType="gp3") # no detach, no downtime
```

Remediation runs in your own account with your own credentials. The Appware audit role is read-only and cannot make these changes. Every script defaults to a dry run.