AWS WELL ARCHITECTED.

It's a tool to review architectures on AWS. It's based on a set of "pillars".

- Operational Excellence
- Security
- Reliability
- Performance
- Cost
- Sustainability

SCORPS

helps remember pillars.

Benefits

✓ move faster through automation

✓ reduce risks

✓ informed decision

Design principles

- Estimate, measure, capacity. No guessing
- Test at production scale; traffic, data, ...

  ! Thanks to serverless services we can setup a production environment and only pay when we use it.

- Automate to enable easy + parallel experimentation

Intent of WA

- Not an audit -> work together.
- Best advice is proven designs.

=> Use well architected Tool !

① Operational Excellence

- Run workload efficiently
- gain insights into the run.
- continuous improve processes

How ?

- use IAC (infrastr. as code) and make small, frequent changes.
- Continuous process refinement. setup game days to review and share procedures.
- Anticipate failure
  - auto scaling
  - fail over
  - have a post mortem procedure

=> Look at AWS Incident Manager after incident check this service for advice (alarms / playbook

② Reliability

Recover from disruptions

- Automated using thresholds for example
- Stateless service for automatic recovery

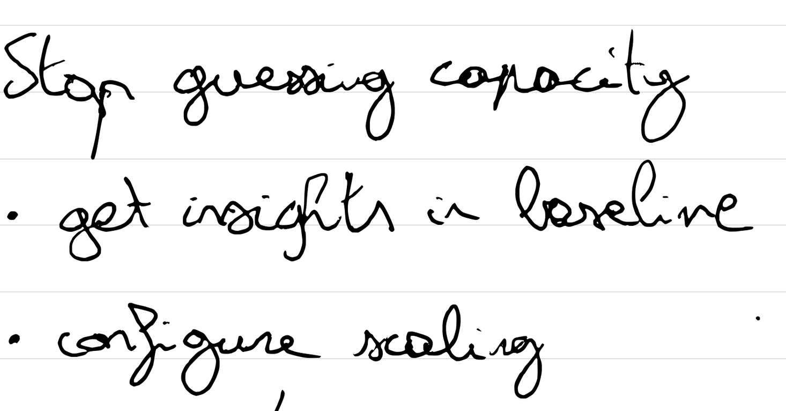
  run -> EC-2

  state -> Elasticache ← EC2, EC2', EC2"

=> AWS Fault Injection Simulator.

- Find perf. bottlenecks.
- Roll back to a pre-experiment state.
- Define tests via templates

- Vertical vs. Horizontal scaling



! more smaller is more reliable than fewer bigger

- Stop guessing capacity
  - get insights in baseline
  - configure scaling
    - -> with λ out of the box.
    - -> use thresholds for trigger with EC-2

=> AWS SSM Change Manager

what did change ? for audit and reporting.

Looks like only used for EC-2, RDS, S3, ALB, ... no serverless services like lambda

③ Security

- Identity

  RBAC (role based access control)

  Multi account setup -> isolation

- Traceability

  Monitor + remediate

=> Amazon inspector

Checks for software vulnerabilities and network exposure. + automatic remediation.

=> AWS Config

audit service configuration and relationships.

- Automate security

  Security via IAC

  => Inspector - Automate

  => Macie - Sensitive data on S3

  => Trusted Advisor - Best practices

  => Config

  => Guard Duty

- Data in transit / rest

  -> Macie - Sensitive data on S3

  => KMS / Cloud HSM / SSE

  => Certificate manager

- Keep people away from data
- Prepare for security events

④ Performance

- Democratise advanced tech.

  -> By leveraging API's to abstract away complexity.

- Go global in minutes
- Use serverless architecture
  - no physical servers
  - scale-to-zero
  - auto scale-out
  - experiment more often.
- Mechanical Sympathy
  - get the car to the end of the race, adapt your driving style
    - -> Analogy of F1 racing