



AWS Well-Architected Tool

AWS Well-Architected Tool My Workload - Sample Lens Report

AWS Account ID:



AWS Well-Architected Tool Report

Copyright © 2023 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

All information, guidance and materials (collectively, "Information") provided to you in connection with the Program are for informational purposes only. You are solely responsible for making your own independent assessment of the Information and your use of AWS's products or services. Neither this document nor any other Information provided to you creates any warranties (express or implied), representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. Neither this document nor any other information provided to you are part of, nor do they modify, any agreements between you and AWS. All information in this document will be shared with only the Customer and the AWS Team.

Table of contents

Workload properties	4
Lens overview	6
Improvement plan	7
High risk	7
Medium risk	8
Lens details	10
Operational Excellence	10
Security	13
Reliability	15
Performance Efficiency	17
Cost Optimization	19

Workload properties

Workload name

My Workload

ARN

arn:aws:wellarchitected:us-east-1:[REDACTED]:workload/493d54d6513dcdb8aeef80a67ddef91d

Description

My Workload Description

Review owner

your_review_owner_email@example.com

Industry type

-

Industry

-

Environment

Production

AWS Regions

US East (N. Virginia)

Non-AWS regions

-

Account IDs

-

Architectural design

-

Application

-

Lens overview

Questions answered

6/6

Version

Sample Lens, 1.0

Pillar	Questions answered
Operational Excellence	2/2
Security	1/1
Reliability	1/1
Performance Efficiency	1/1
Cost Optimization	1/1

Lens notes

-

Improvement plan

Improvement item summary

High risk: 1

Medium risk: 4

Pillar	High risk	Medium risk
Operational Excellence	0	2
Security	0	1
Reliability	0	1
Performance Efficiency	0	0
Cost Optimization	1	0

High risk

Operational Excellence
No improvements identified

Security
No improvements identified

Reliability
No improvements identified

Performance Efficiency
No improvements identified

Cost Optimization
<ul style="list-style-type: none"> • 5.1.Cost Management

Medium risk

Operational Excellence
<ul style="list-style-type: none"> • 1.1.Monitoring • 1.2.Incident Management

Security
<ul style="list-style-type: none"> • 2.1.Data Protection

Reliability
<ul style="list-style-type: none"> • 3.1.Fault Tolerance

Performance Efficiency
No improvements identified

Cost Optimization
No improvements identified






Lens details

Operational Excellence

Questions answered

2/2

Question status

-  High risk: 0
-  Medium risk: 2
-  No improvements identified: 0
-  Not Applicable: 0
-  Unanswered: 0

Pillar notes

-

1. Monitoring

 Medium risk

Selected choice(s)

- Use Amazon CloudWatch
- Implement Centralized Logging

Not selected choice(s)

- Use AWS X-Ray for Tracing
- Implement Health Checks

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

These links were provided by the lens owner and have not been validated by AWS.

- Implement AWS X-Ray to trace requests as they travel through your application. This helps in identifying bottlenecks and understanding application performance.
- Set up health checks for your resources to monitor their availability and performance. Use Route 53 or ELB health checks to automate failover and ensure high availability.

2. Incident Management

 Medium risk

Selected choice(s)

- Automated Incident Detection
- Runbooks and Playbooks

Not selected choice(s)

- Incident Response Drills
- Post-Incident Analysis

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

These links were provided by the lens owner and have not been validated by AWS.






- Conduct regular incident response drills to ensure your team is prepared to handle incidents effectively. Review and update procedures based on drill outcomes.
- Perform post-incident analysis to identify the root cause of incidents and implement corrective actions to prevent recurrence.

Security

Questions answered

1/1

Question status

-  High risk: 0
-  Medium risk: 1
-  No improvements identified: 0
-  Not Applicable: 0
-  Unanswered: 0

Pillar notes

-

1. Data Protection

 Medium risk

Selected choice(s)

- Encrypt Data in Transit
- Implement IAM Policies
- Regular Security Audits

Not selected choice(s)

- Encrypt Data at Rest

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

These links were provided by the lens owner and have not been validated by AWS.






- Implement AWS Key Management Service (KMS) to encrypt your data at rest. Configure policies to enforce encryption across all storage services.

Reliability

Questions answered

1/1

Question status

-  High risk: 0
-  Medium risk: 1
-  No improvements identified: 0
-  Not Applicable: 0
-  Unanswered: 0

Pillar notes

-

1. Fault Tolerance

 Medium risk

Selected choice(s)

- Implement Auto Scaling
- Backup and Restore Procedures

Not selected choice(s)

- Implement Multi-AZ Architecture
- Use Load Balancers

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

These links were provided by the lens owner and have not been validated by AWS.






- Design your workload to use a multi-AZ architecture to ensure high availability. Use services like Amazon RDS with Multi-AZ deployments.
- Implement load balancers such as Elastic Load Balancer (ELB) to distribute traffic across multiple instances, enhancing fault tolerance.

Performance Efficiency

Questions answered

1/1

Question status

-  High risk: 0
-  Medium risk: 0
-  No improvements identified: 1
-  Not Applicable: 0
-  Unanswered: 0

Pillar notes

-

1. Scalability

✔ No improvements identified

Selected choice(s)

- Use Elastic Load Balancing
- Use Auto Scaling
- Use Caching
- Optimize Database Performance

Not selected choice(s)

-

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan






No risk detected for this question. No action needed.

Cost Optimization

Questions answered

1/1

Question status

-  High risk: 1
-  Medium risk: 0
-  No improvements identified: 0
-  Not Applicable: 0
-  Unanswered: 0

Pillar notes

-

1. Cost Management

⊗ High risk

Selected choice(s)

- Use Reserved Instances
- Implement Right-Sizing

Not selected choice(s)

- Implement Cost Monitoring
- Optimize Storage Costs

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

These links were provided by the lens owner and have not been validated by AWS.

- Use AWS Cost Explorer and AWS Budgets to monitor and analyze your spending. Set up alerts for unexpected cost increases.
- Review your storage usage and implement lifecycle policies to move data to lower-cost storage tiers. Use Amazon S3 Intelligent-Tiering to automatically optimize storage costs.