

Enterprise Container, Serverless, and Kubernetes Security Governance on AWS

Author: Adedayo

Specialization: Cloud Security & Cloud-Native Security

Platform: Amazon Web Services (AWS)

1. Introduction

This document describes the design, implementation, and validation of security controls for containerized, serverless, and Kubernetes workloads in AWS.

I implemented this framework to ensure that container images, Kubernetes workloads, and Lambda functions operate securely, follow least-privilege principles, and prevent vulnerability exploitation and secrets exposure.

The solution integrates vulnerability management, identity governance, secrets management, and runtime security controls.

2. Objectives

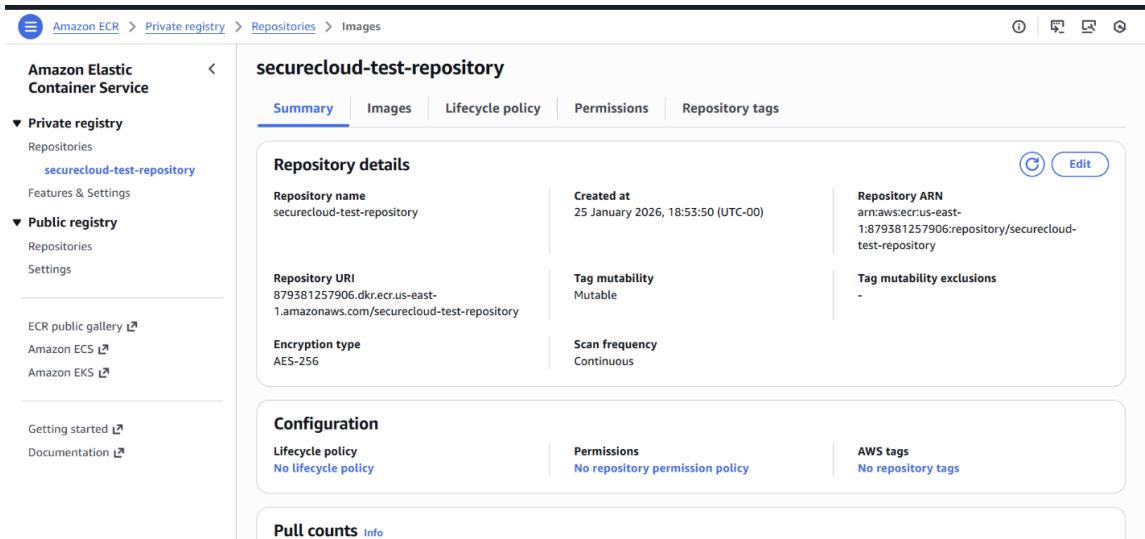
The primary objectives were to:

- Secure container images before deployment
- Detect and remediate vulnerabilities in ECR
- Enforce least privilege for Lambda execution roles
- Prevent secrets leakage
- Enforce Kubernetes workload security standards
- Implement RBAC for container workloads
- Validate security controls through testing

3. Container Image Security (Amazon ECR)

3.1 Vulnerability Scanning

A private Amazon ECR repository was created to store container images.



The screenshot shows the Amazon ECR console's repository details page for 'securecloud-test-repository'. The left sidebar includes links for Amazon Elastic Container Service, Private registry (selected), Public registry, ECR public gallery, Amazon ECS, and Amazon EKS. The main content area has tabs for Summary (selected), Images, Lifecycle policy, Permissions, and Repository tags. Under 'Repository details', it shows the repository name, created at (25 January 2026, 18:53:50 UTC-00), repository URI (879381257906.dkr.ecr.us-east-1.amazonaws.com/securecloud-test-repository), encryption type (AES-256), tag mutability (Mutable), scan frequency (Continuous), and repository ARN (arn:aws:ecr:us-east-1:879381257906:repository/securecloud-test-repository). Under 'Configuration', it shows lifecycle policy (No lifecycle policy), permissions (No repository permission policy), and AWS tags (No repository tags). A 'Pull counts' section is also present.

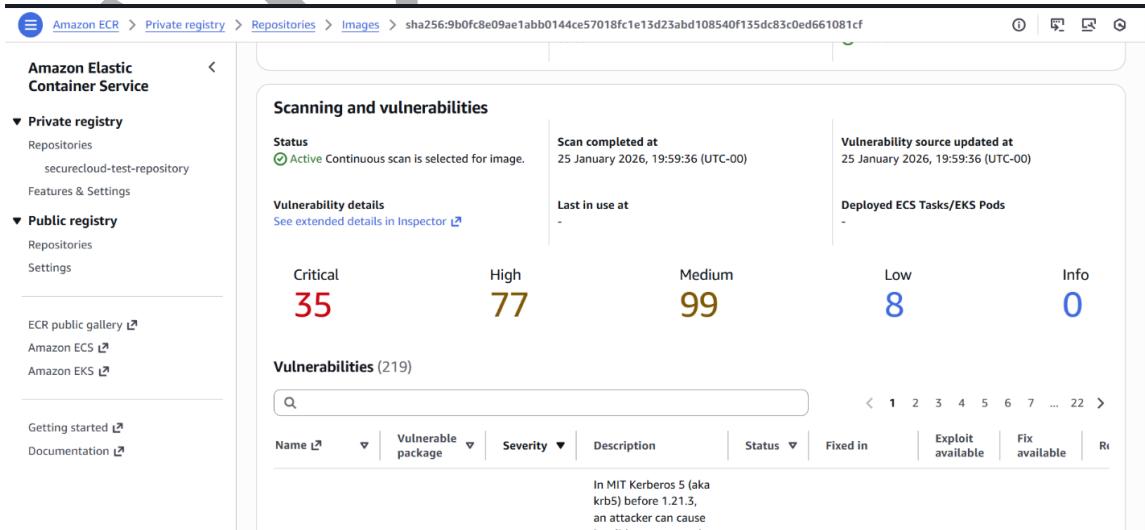
Image scanning on push was enabled and integrated with Amazon Inspector for continuous vulnerability assessments.

Images are automatically scanned for CVEs and categorized by severity.

3.2 Vulnerability Testing

A test image (nginx:1.18) was pushed to ECR and scanned.

Multiple vulnerabilities were detected and documented.



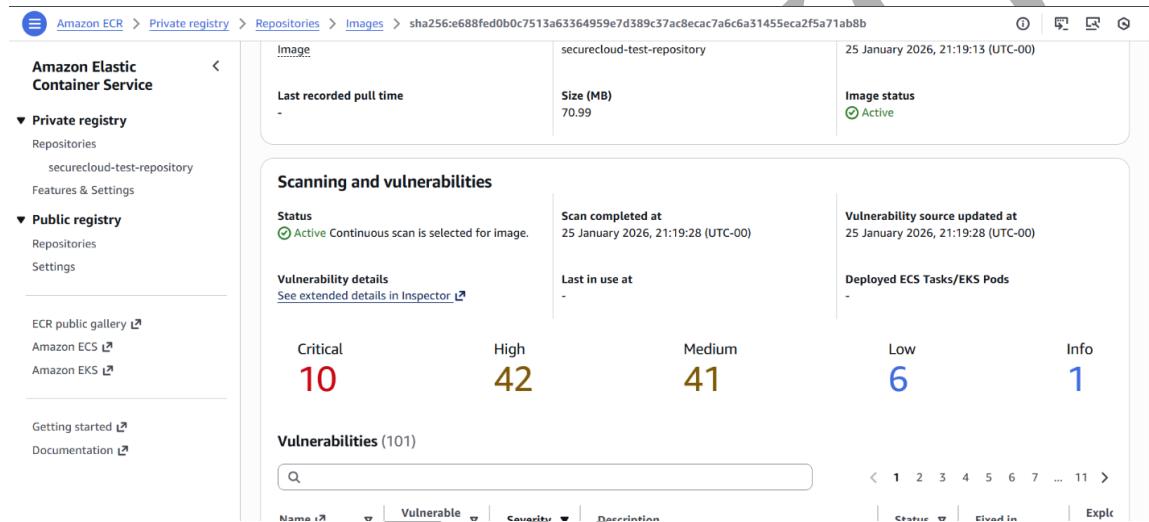
The screenshot shows the 'Scanning and vulnerabilities' page for the 'securecloud-test-repository'. The left sidebar is identical to the previous screenshot. The main content area shows a summary of vulnerabilities: 35 Critical, 77 High, 99 Medium, 8 Low, and 0 Info. Below this is a table titled 'Vulnerabilities (219)' with columns for Name, Vulnerable package, Severity, Description, Status, Fixed in, Exploit available, Fix available, and Re. A single row from the table is visible, detailing a vulnerability in MIT Kerberos 5 (aka krb5) before 1.21.3, where an attacker can cause.

3.3 Remediation Process

To remediate vulnerabilities:

- Base images were upgraded (nginx:1.25)
- Containers were rebuilt
- Updated images were rescanned

Scan results confirmed reduced risk levels.



3.4 Secure Image Lifecycle

Only compliant images are approved for deployment.

Insecure images are blocked until remediation is completed.

4. Serverless Security (AWS Lambda)

4.1 Execution Role Review

Lambda execution roles were reviewed for:

- Wildcard permissions
- Overly broad managed policies
- Unnecessary service access

4.2 Least Privilege Enforcement

Broad permissions were removed and replaced with scoped policies.

Roles were limited to required services, actions, and resources.

Baseline logging permissions were retained.

4.3 Validation Testing

Functions were tested after permission reduction.

CloudWatch logs confirmed successful execution.

AccessDenied errors were used to validate permission boundaries.

5. Secrets Management and Leakage Prevention

5.1 Secure Secrets Storage

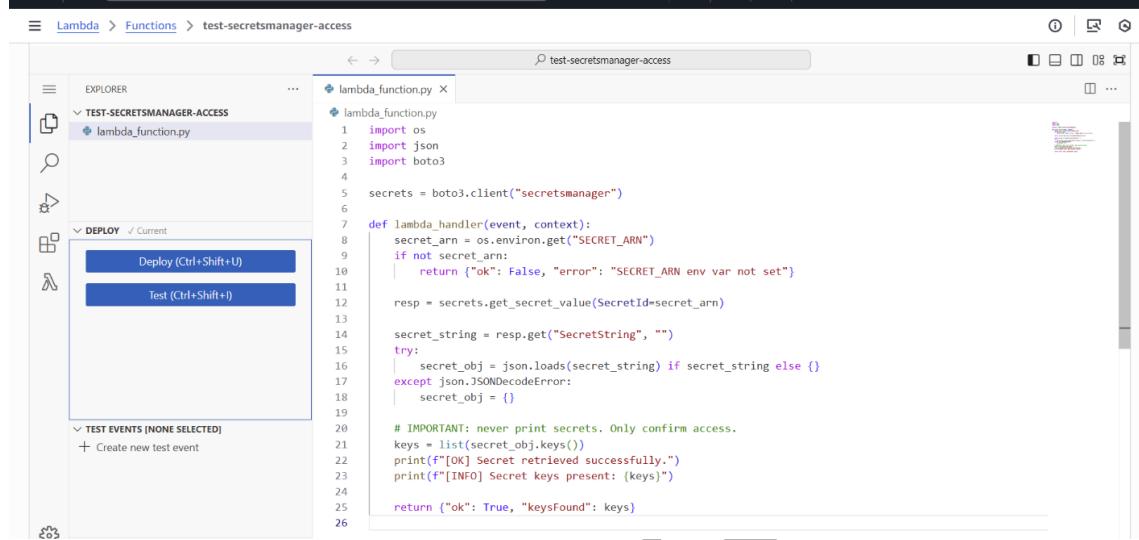
Sensitive credentials were migrated to AWS Secrets Manager.

Secrets were encrypted using KMS.

No plaintext secrets were stored in environment variables.

5.2 Secure Access Design

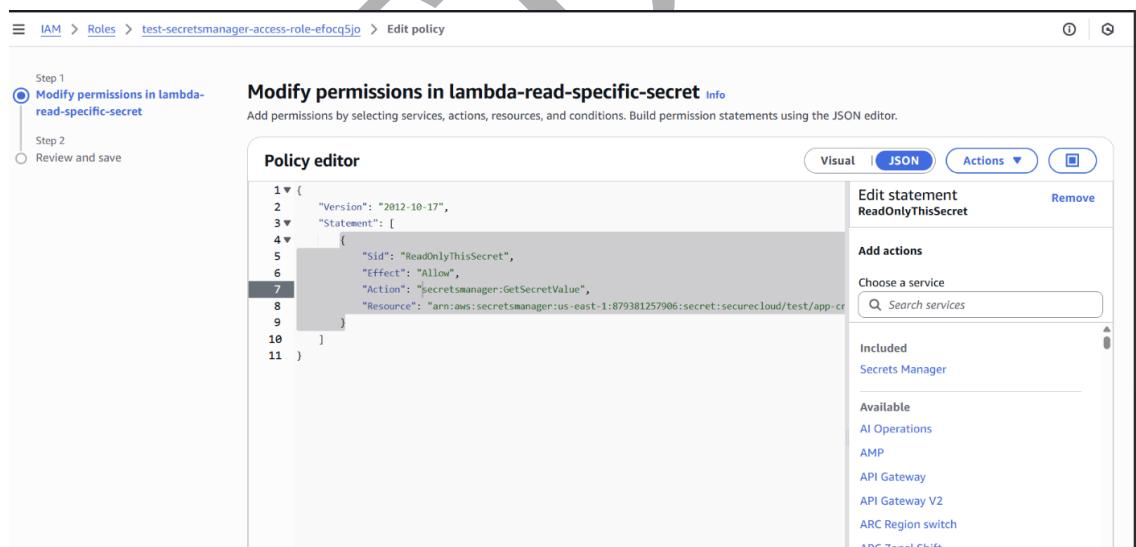
Lambda functions were configured with:



The screenshot shows the AWS Lambda function configuration interface. The left sidebar shows the project structure: EXPLORER, TEST-SECRETSMANAGER-ACCESS (with lambda_function.py selected), and DEPLOY (with Deploy and Test buttons). The right pane shows the code editor for lambda_function.py:

```
lambda_function.py
1 import os
2 import json
3 import boto3
4
5 secrets = boto3.client("secretsmanager")
6
7 def lambda_handler(event, context):
8     secret_arn = os.environ.get("SECRET_ARN")
9     if not secret_arn:
10         return {"ok": False, "error": "SECRET_ARN env var not set"}
11
12     resp = secrets.get_secret_value(SecretId=secret_arn)
13
14     secret_string = resp.get("SecretString", "")
15     try:
16         secret_obj = json.loads(secret_string) if secret_string else {}
17     except json.JSONDecodeError:
18         secret_obj = {}
19
20     # IMPORTANT: never print secrets. Only confirm access.
21     keys = list(secret_obj.keys())
22     print(f"[OK] Secret retrieved successfully.")
23     print(f"[INFO] Secret keys present: {keys}")
24
25
26     return {"ok": True, "keysFound": keys}
```

- secretsmanager:GetSecretValue permission
- Access scoped to specific secret ARNs



The screenshot shows the IAM Role policy editor. The left sidebar indicates Step 1: Modify permissions in lambda-read-specific-secret (selected) and Step 2: Review and save. The main area is titled "Modify permissions in lambda-read-specific-secret" and contains the following JSON policy:

```
1 {
2     "Version": "2012-10-17",
3     "Statement": [
4         {
5             "Sid": "ReadOnlyThisSecret",
6             "Effect": "Allow",
7             "Action": "secretsmanager:GetSecretValue",
8             "Resource": "arn:aws:secretsmanager:us-east-1:879381257906:secret:securecloud/test/app-cr"
9         }
10    ]
11 }
```

The right side of the interface includes tabs for Visual, JSON, Actions, and a search bar for services. A sidebar lists available services: Secrets Manager, AI Operations, AMP, API Gateway, API Gateway V2, and ARC Region switch.

5.3 Validation

Secrets retrieval was tested successfully.

The screenshot shows the CloudWatch Log Management interface. The left sidebar is titled "CloudWatch" and includes sections for "Ingestion", "Dashboards", "Alarms", "AI Operations", "GenAI Observability", "Application Signals", "Infrastructure Monitoring", and "Logs". Under "Logs", there are links for "Log Management", "Log Anomalies", and "Live Tail". The main area is titled "Log events" and shows a search bar with placeholder text "Filter events - press enter to search", and buttons for "1m", "1h", "UTC timezone", and "Display". There are also "Actions", "Start tailing", and "Create metric filter" buttons. A large watermark reading "AUDITED" diagonally across the page is present.

Timestamp	Message
2026-01-25T22:26:35.137Z	INIT_START Runtime Version: python:3.12.v101 Runtime Version ARN: arn:aws:lambda:us-east-1::runtime:994aac32248e...
2026-01-25T22:26:35.582Z	START RequestId: 6a33403c-fc84-43a0-b31a-265edd6a613c Version: \$LATEST
2026-01-25T22:26:35.907Z	[OK] Secret retrieved successfully.
2026-01-25T22:26:35.907Z	[INFO] Secret keys present: ['username', 'password']
2026-01-25T22:26:35.919Z	END RequestId: 6a33403c-fc84-43a0-b31a-265edd6a613c
2026-01-25T22:26:35.919Z	REPORT RequestId: 6a33403c-fc84-43a0-b31a-265edd6a613c Duration: 336.32 ms Billed Duration: 778 ms Memory Size: ...

Permission removal resulted in expected failures.

This confirmed strict access control.

6. Kubernetes Workload Security (Amazon EKS)

6.1 Namespace Isolation

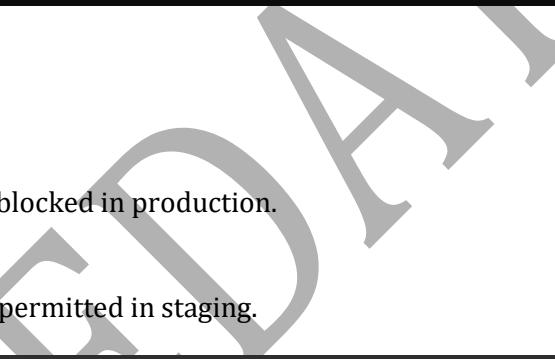
Separate namespaces were created for staging and production environments.

This prevents cross-environment access and supports tiered controls.

6.2 Pod Security Standards Enforcement

Pod Security Standards were enforced using namespace labels:

- Production: Restricted policy
- Staging: Baseline policy



```

Windows PowerShell
45337c89cd57: Pushed
933cc8478577: Pushed
nginx-1.25: digest: sha256:e688fed0b0c7513a63364959e7d389c37ac8ecac7a6c6a31455eca2f5a71ab8b size: 2295
Info + Not all multiplatform-content is present and only the available single-platform image was pushed
sha256:a484819e60211f5299034ac80f6a081b06f89e65866ce91f356ed7c72af059c -> sha256:e688fed0b0c7513a63364959e7d389c37ac8ecac7a6c6a31455eca2f5a71ab8b
PS C:\Users\Green> kubectl version --client
Client Version: v1.32.2
Kustomize Version: v3.5.0
PS C:\Users\Green> aws eks update-kubeconfig --region us-east-1 --name securecloud-eks-cluster
Added new context arn:aws:eks:us-east-1:879381257906:cluster/securecloud-eks-cluster to C:\Users\Green\.kube\config
PS C:\Users\Green> kubectl get nodes
No resources found
PS C:\Users\Green> kubectl get nodes
NAME STATUS ROLES AGE VERSION
i-031f4289605a86bf Ready <none> 15h v1.34.3-eks-3c60543
PS C:\Users\Green> kubectl create namespace staging
namespace/staging created
PS C:\Users\Green> kubectl create namespace production
namespace/production created
PS C:\Users\Green> kubectl label namespace staging pod-security.kubernetes.io/enforce=baseline --overwrite
PS C:\Users\Green> kubectl label namespace production pod-security.kubernetes.io/enforce=restricted --overwrite
namespace/production labeled
PS C:\Users\Green> kubectl get ns staging production --show-labels
NAME STATUS AGE LABELS
staging Active 72s kubernetes.io/metadata.name=staging,pod-security.kubernetes.io/enforce=baseline
production Active 69s kubernetes.io/metadata.name=production,pod-security.kubernetes.io/enforce=restricted
PS C:\Users\Green>

```

6.3 Policy Validation

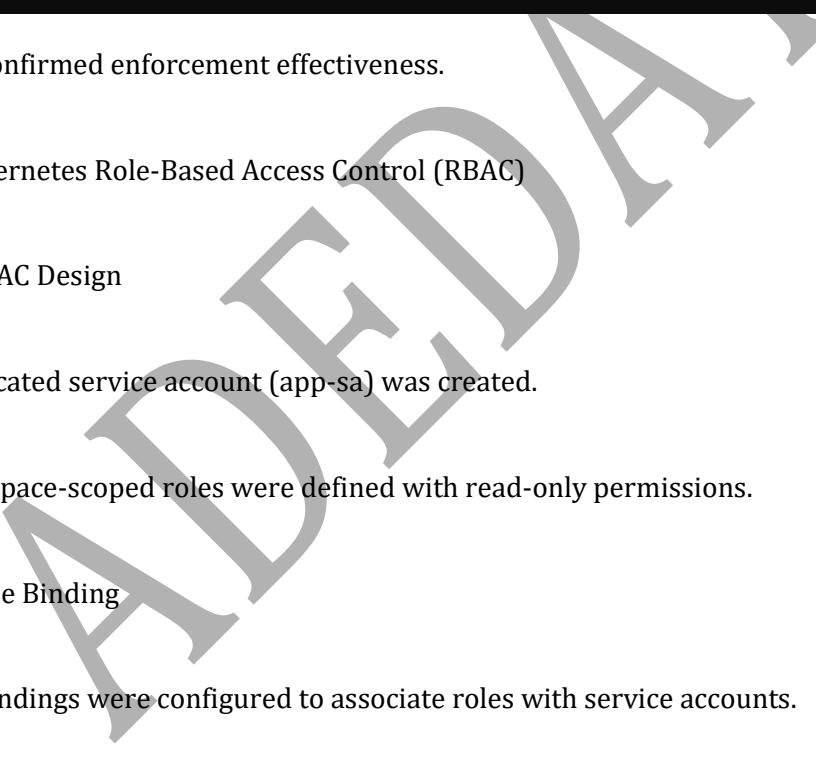
Privileged containers were blocked in production.

Compliant workloads were permitted in staging.


```

Windows PowerShell
45337c89cd57: Pushed
933cc8478577: Pushed
nginx-1.25: digest: sha256:e688fed0b0c7513a63364959e7d389c37ac8ecac7a6c6a31455eca2f5a71ab8b size: 2295
Info + Not all multiplatform-content is present and only the available single-platform image was pushed
sha256:a484819e60211f5299034ac80f6a081b06f89e65866ce91f356ed7c72af059c -> sha256:e688fed0b0c7513a63364959e7d389c37ac8ecac7a6c6a31455eca2f5a71ab8b
PS C:\Users\Green> kubectl version --client
Client Version: v1.32.2
Kustomize Version: v3.5.0
PS C:\Users\Green> aws eks update-kubeconfig --region us-east-1 --name securecloud-eks-cluster
Added new context arn:aws:eks:us-east-1:879381257906:cluster/securecloud-eks-cluster to C:\Users\Green\.kube\config
PS C:\Users\Green> kubectl get nodes
No resources found
PS C:\Users\Green> kubectl get nodes
NAME STATUS ROLES AGE VERSION
i-031f4289605a86bf Ready <none> 15h v1.34.3-eks-3c60543
PS C:\Users\Green> kubectl create namespace staging
namespace/staging created
PS C:\Users\Green> kubectl create namespace production
namespace/production created
PS C:\Users\Green> kubectl label namespace staging pod-security.kubernetes.io/enforce=baseline --overwrite
PS C:\Users\Green> kubectl label namespace production pod-security.kubernetes.io/enforce=restricted --overwrite
namespace/production labeled
PS C:\Users\Green> kubectl get ns staging production --show-labels
NAME STATUS AGE LABELS
staging Active 72s kubernetes.io/metadata.name=staging,pod-security.kubernetes.io/enforce=baseline
production Active 69s kubernetes.io/metadata.name=production,pod-security.kubernetes.io/enforce=restricted
PS C:\Users\Green> kubectl apply -f bad-pod.yaml
error: the path "bad-pod.yaml" does not exist
PS C:\Users\Green> kubectl apply -f bad-pod.yaml
Error from server (Forbidden): error when creating "bad-pod.yaml": pods "bad-pod" is forbidden: violates PodSecurity "restricted:latest": privileged (container "nginx" must not set securityContext.privileged=true), allowPrivilegeEscalation != false (container "nginx" must set securityContext.allowPrivilegeEscalation=false), unrestricted capabilities (container "nginx" must set securityContext.capabilities.drop=["ALL"]), runAsNonRoot != true (pod or container "nginx" must set securityContext.runAsNonRoot=true), seccompProfile (pod or container "nginx" must set securityContext.seccompProfile.type to "RuntimeDefault" or "localhost")
PS C:\Users\Green>

```



```

Windows PowerShell
4537c09cd57: Pushed
933cc878d577: Pushed
nginx-1.25: digest: sha256:e688fed0b0c7513a63364959e7d389c37ac8ecac7a6c6a31455eca2f5a71ab8b size: 2295
Info : Not all multiplatform-content is present and only the available single-platform image was pushed
sha256:0480819eb60211f5299034ac80f6xa81b06f89e65866ce91f356ed7c72af059c -> sha256:e688fed0b0c7513a63364959e7d389c37ac8ecac7a6c6a31455eca2f5a71ab8b
PS C:\Users\Green> kubectl version --client
Client Version: v1.32.2
Helm Version: v3.5.0
PS C:\Users\Green> aws eks update-kubeconfig --region us-east-1 --name securecloud-eks-cluster
Added new context: arm:aws:eks:us-east-1:879381257906:cluster/securecloud-eks-cluster to C:\Users\Green\.kube\config
PS C:\Users\Green> kubectl get nodes
No resources found
PS C:\Users\Green> kubectl get nodes
NAME STATUS ROLES AGE VERSION
i-031f4289605a86bfdf Ready <none> 15h v1.34.3-eks-3c60543
PS C:\Users\Green> kubectl create namespace staging
namespace/staging created
PS C:\Users\Green> kubectl create namespace production
namespace/production created
PS C:\Users\Green> kubectl label namespace staging pod-security.kubernetes.io/enforce=baseline --overwrite
namespace/staging labeled
PS C:\Users\Green> kubectl label namespace production pod-security.kubernetes.io/enforce=restricted --overwrite
namespace/production labeled
PS C:\Users\Green> kubectl get ns staging production --show-labels
NAME STATUS AGE LABELS
staging Active 72s kubernetes.io/metadata.name=staging,pod-security.kubernetes.io/enforce=baseline
production Active 69s kubernetes.io/metadata.name=production,pod-security.kubernetes.io/enforce=restricted
PS C:\Users\Green> kubectl apply -f bad-pod.yaml
error: the path "bad-pod.yaml" does not exist
PS C:\Users\Green> kubectl apply -f bad-pod.yaml
Error from server (Forbidden): error when creating "bad-pod.yaml": pods "bad-pod" is forbidden: violates PodSecurity "restricted:latest": privileged (container "nginx" must not set securityContext.privileged=true), allowPrivilegeEscalation != false (container "nginx" must set securityContext.allowPrivilegeEscalation=false), unrestricted capabilities (container "nginx" must set securityContext.capabilities.drop=["ALL"]), runAsNonRoot != true (pod or container "nginx" must set securityContext.runAsNonRoot=true), seccompProfile (pod or container "nginx" must set securityContext.seccompProfile.type to "RuntimeDefault" or "Localhost")
PS C:\Users\Green> kubectl apply -f good-pod.yaml
pod/good-pod created
PS C:\Users\Green> kubectl get pods -n staging
NAME READY STATUS RESTARTS AGE
good-pod 0/1 ContainerCreating 0 29s
PS C:\Users\Green>

```

This confirmed enforcement effectiveness.

7. Kubernetes Role-Based Access Control (RBAC)

7.1 RBAC Design

A dedicated service account (app-sa) was created.

Namespace-scoped roles were defined with read-only permissions.

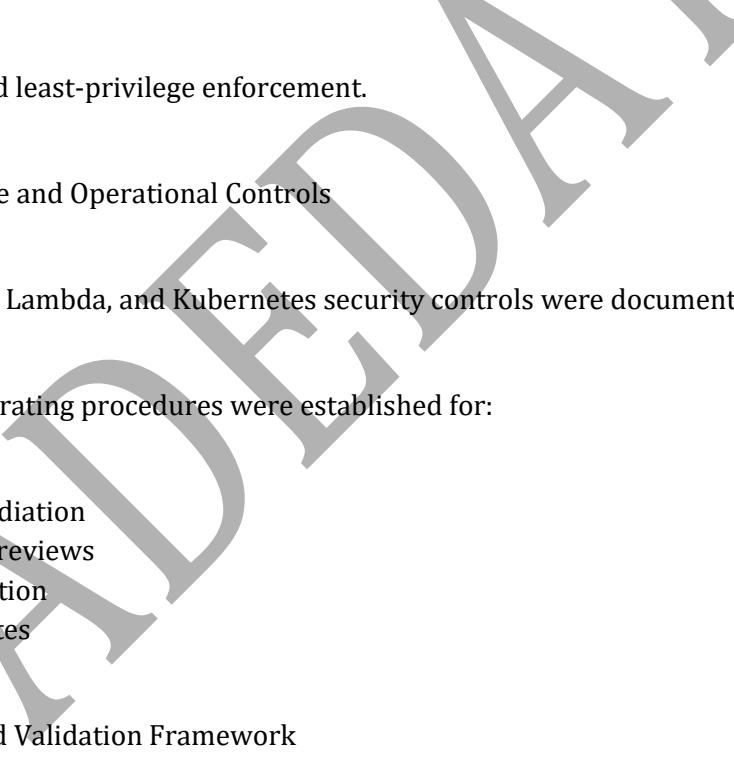
7.2 Role Binding

RoleBindings were configured to associate roles with service accounts.

7.3 Authorization Testing

The service account could list pods.

Access to delete pods and secrets was denied.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Green> kubectl create serviceaccount app-sa -n staging
serviceaccount/app-sa created
PS C:\Users\Green> kubectl apply -f pod-reader-role.yaml
role.rbac.authorization.k8s.io/pod-reader created
PS C:\Users\Green> kubectl apply -f pod-reader-binding.yaml
rolebinding.rbac.authorization.k8s.io/pod-reader-binding created
PS C:\Users\Green> kubectl run rbac-test --image=nginx:1.25 -n staging
pod/rbac-test created
PS C:\Users\Green> kubectl get pods -n staging
NAME          READY   STATUS    RESTARTS   AGE
rbac-test     0/1     ContainerCreating   0          25s
PS C:\Users\Green> kubectl auth can-i list pods -n staging --as=system:serviceaccount:staging:app-sa
yes
PS C:\Users\Green> kubectl auth can-i delete pods -n staging --as=system:serviceaccount:staging:app-sa
no
PS C:\Users\Green> |
```

This validated least-privilege enforcement.

8. Governance and Operational Controls

All container, Lambda, and Kubernetes security controls were documented.

Standard operating procedures were established for:

- Image remediation
- Permission reviews
- Secrets rotation
- Policy updates

9. Testing and Validation Framework

Security controls were validated through:

- ECR vulnerability remediation testing
- Pod Security enforcement testing
- RBAC authorization testing
- Lambda permission testing

- Secrets access validation

All controls operated as intended.

10. Outcomes and Impact

This implementation delivered:

- Reduced container vulnerability exposure
- Secure serverless execution roles
- Protected secrets management
- Enforced Kubernetes security standards
- Strong workload isolation
- Improved cloud-native security posture

11. Conclusion

I designed and implemented an enterprise-grade security governance framework for containerized, serverless, and Kubernetes workloads on AWS.

Through integrated vulnerability management, identity controls, secrets protection, and runtime enforcement, this solution ensures secure and resilient cloud-native operations.