TEMPLATE

EC2 IAM and Encryption Hardening Template

A practical template for validating IAM role scope, EBS encryption, snapshot handling, and evidence collection before production use.

EC2 Hardening Template: IAM and Encryption

Use this template to assess, document, and verify hardening controls for an EC2 workload. It is designed for practical review before production deployment or after significant changes.

---

1) Workload summary

Application name: _____

Environment: ? Dev ? Test ? Staging ? Production

Owner/team: _____

Business purpose: _____

Instance type / ASG / launch template: _____

AWS account / region: _____

Data handled by this workload:

- ? Public
- ? Internal
- ? Confidential
- ? Restricted

Notes: _____

_____

---

2) IAM role scope review

Instance credentials model

- [ ] No long-lived access keys are stored in the AMI, user data, scripts, or configuration files.
- [ ] The instance uses an IAM role attached through an instance profile.
- [ ] The role is dedicated to this workload and not shared with unrelated systems.
- [ ] Temporary credentials are used instead of static credentials.

Least-privilege review

List the exact AWS actions the workload needs:

Service	Required actions	Resource scope	Reason
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Validation questions:

- [ ] The role grants only the actions needed for the workload to function.
- [ ] Resource ARNs are scoped as tightly as possible.
- [ ] Wildcards are justified and documented.

- [ ] The role cannot read unrelated secrets, queues, buckets, or databases.
- [ ] The role cannot create or attach broader access for itself.

Exceptions / approved broad permissions:

_____

_____

---

3) Encryption controls review

EBS volume encryption

- [ ] The root volume is encrypted.
- [ ] Every attached data volume is encrypted.
- [ ] Encryption is enforced by default through the launch process.
- [ ] Unencrypted volumes are not allowed except by documented exception.

Snapshot and copy handling

- [ ] Snapshots of encrypted volumes remain encrypted.
- [ ] Volume copies preserve encryption.
- [ ] Cross-account snapshot sharing is reviewed and approved.
- [ ] Backup destinations follow the same encryption requirements.
- [ ] Restores are tested to confirm access is governed correctly.

Key management

- [ ] The encryption key is owned or governed by the organization?s key management process.

- [ ] Key use is limited to approved principals and services.
- [ ] Key policy changes require review.
- [ ] Access to decrypt, restore, or attach encrypted data is documented.
- [ ] Key rotation and recovery procedures are defined.

Key identifier / alias: _____

Key owner: _____

Recovery and break-glass notes:

_____

_____

---

4) Launch-time guardrails

- [ ] Launch templates or equivalent automation enforce the intended role.
- [ ] Launch templates or equivalent automation enforce encrypted storage.
- [ ] Instance creation is blocked or alerted if the template drifts.
- [ ] Autoscaling, rebuilds, and redeployments preserve the same posture.
- [ ] Manual launches are prevented or monitored.

Guardrail mechanism: _____

Where it is enforced: _____

---

5) Operational verification

Run these checks and record the evidence.

Instance identity

- [ ] Verify the attached IAM role on the running instance.
- [ ] Confirm the application is not using embedded AWS keys.
- [ ] Confirm the role?s effective permissions match the approved scope.

Evidence: _____

Storage encryption

- [ ] Verify the root volume is encrypted.
- [ ] Verify all attached EBS volumes are encrypted.
- [ ] Verify snapshots created from the instance remain encrypted.

Evidence: _____

Access and recovery

- [ ] Verify the workload can perform required actions with the role.
- [ ] Verify unauthorized actions are denied.
- [ ] Verify restore or rebuild procedures work with encrypted volumes.

Evidence: _____

---

6) Risk and trade-off notes

Document any known trade-offs or residual risks.

Area	Risk or trade-off	Mitigation
IAM	_____	_____
Encryption	_____	_____

Snapshots / backups	_____	_____
Operations / recovery	_____	_____

Additional notes: _____

_____

---

7) Approval checklist

Before production use, confirm all of the following:

- [ ] The instance uses least-privilege IAM roles.
- [ ] No long-lived credentials are embedded in the workload.
- [ ] Root and data volumes are encrypted.
- [ ] Snapshots and backups preserve encryption.
- [ ] Key management and recovery ownership are documented.
- [ ] Launch automation preserves the desired posture.
- [ ] Evidence has been collected and reviewed.

Final approval

Reviewed by: _____

Date: _____

Decision: ? Approved ? Approved with exceptions ? Not approved

Exceptions / conditions: _____

_____

---

8) Quick reference: what this template is checking

- IAM roles reduce the blast radius of instance compromise.
- Encryption reduces exposure if disks, snapshots, or backups are copied or stolen.
- Launch automation and monitoring help keep the controls in place over time.
- Evidence matters: if you cannot verify the posture, it is not complete.

9) Suggested evidence to retain

- Launch template or provisioning configuration
- IAM role and policy documents
- Volume encryption settings
- Snapshot and backup configuration
- Key management policy or ownership record
- Screenshots, command output, or audit logs from verification

---

Use this template as an operational record. Adapt the fields to match your organization?s controls, approval process, and audit requirements.