TEMPLATE

AWS Virtualization Security Hardening Checklist for EC2 and EBS Encryption

A practical template for validating EC2 and EBS encryption hardening before production use, including instance access, key governance, snapshot controls, and evidence capture.

AWS Virtualization Security Hardening Checklist for EC2 and EBS Encryption

Purpose

Use this template to verify that EC2 instance hardening and EBS encryption are both in place before production deployment. This checklist focuses on access control, encryption at rest, key governance, snapshot handling, and evidence collection.

> Use case: Pre-production review, change approval, security baseline validation, or control evidence gathering.

---

1) Workload and data classification

Check	Status	Notes / Evidence
Data classification for the workload is documented	?	

Regulatory, contractual, or internal protection requirements are identified | ? |
Recovery objectives are documented (RTO/RPO) | ? |
All persistent data locations are identified (volumes, snapshots, backups, AMIs, exports) | ? |

Evidence to retain: data classification record, architecture diagram, backup/recovery requirements.

---

2) EC2 instance hardening

Check | Status | Notes / Evidence
Only approved instance profiles/roles are attached | ? |
Administrative access is restricted to named roles or approved break-glass accounts | ? |
SSH/RDP or other admin ports are limited to required sources only | ? |
Security groups follow least privilege and do not expose unnecessary ports | ? |
Instance metadata access is restricted according to policy | ? |
Unused services, listeners, and local accounts are removed or disabled | ? |
Patch baseline and hardened image/AMI are defined | ? |
Logging is enabled for OS and management activity | ? |

Evidence to retain: instance profile list, security group rules, hardening baseline, logging configuration.

---

3) EBS encryption controls

Check	Status	Notes / Evidence
Encryption at rest is mandatory for all new EBS volumes	?	
Default encryption is enabled for the account or provisioning path	?	
All existing persistent volumes are encrypted or formally approved for exception	?	
No unencrypted volumes are attached to production workloads	?	
Encryption settings are consistent across launch templates and automation	?	
Encryption is verified after instance launch or volume modification	?	

Evidence to retain: encryption status report, account or provisioning defaults, launch template settings.

---

4) Key governance and separation of duties

Check	Status	Notes / Evidence
Key ownership model is documented	?	
Only authorized administrators can manage encryption keys	?	
Workload operators do not have unnecessary key administration privileges	?	
Key policy or equivalent access policy is reviewed for least privilege	?	
Key rotation and lifecycle requirements are documented	?	
Emergency access and recovery procedures are defined	?	

Evidence to retain: key ownership record, access policy review, rotation policy, emergency access procedure.

---

5) Snapshot and backup discipline

Check	Status	Notes / Evidence
Snapshots are treated as sensitive artifacts	?	
Snapshot creation and sharing permissions are restricted	?	
Snapshot copying is reviewed and approved where required	?	
Old or unused snapshots are removed according to retention policy	?	
Backup and restore procedures preserve encryption requirements	?	
Restored volumes are verified to remain encrypted	?	

Evidence to retain: snapshot inventory, sharing permissions, retention policy, restore test results.

---

6) Network and workload exposure

Check	Status	Notes / Evidence
Instances are placed in the correct network segment or subnet	?	
Inbound access is limited to required application flows	?	
Outbound access is restricted where feasible	?	
Private access paths are used for administrative and service traffic when possible	?	
Exposure to the public internet is justified and documented	?	

Evidence to retain: network diagram, security group rules, justification for public exposure if any.

---

7) Validation checks before production use

Check	Status	Notes / Evidence
A test instance was launched using the intended production template or automation	?	
Attached volumes are confirmed encrypted	?	
Snapshot creation and restore were tested successfully	?	
Access to the instance and volumes was validated against policy	?	
Key access was reviewed and confirmed to follow least privilege	?	
Monitoring or alerting exists for policy drift or unauthorized changes	?	

Evidence to retain: test output, screenshots, logs, approval record, drift alerts.

---

8) Common failure modes to verify against

- Encryption enabled on new volumes, but older volumes remain unencrypted.
- Launch templates or scripts still create unencrypted storage.
- Snapshots are copied, shared, or retained without the same review as live volumes.
- Key administration is too broad, weakening separation of duties.
- Instance permissions are excessive, allowing unintended access to decrypted data.
- Security group rules are broader than the workload requires.

---

9) Production readiness decision

Ready for production when:

- All required volumes and snapshots are encrypted.
- Key access is restricted and documented.
- Instance access is least privilege.
- Network exposure is justified and limited.
- Restore and validation tests are complete.
- Exceptions, if any, are approved and tracked.

Not ready for production when:

- Any persistent data path is unencrypted without exception.
- Snapshot handling is uncontrolled.
- Key policy or instance access is overly broad.
- Required validation evidence is missing.

---

10) Sign-off record

Field	Value
Workload name	
Environment	
Review date	
Reviewer	

Approver |
Exception(s) approved |
Production decision | ? Approved ? Conditionally approved ? Not approved

Reviewer notes

Quick reference

Goal: Reduce the chance that instance compromise, misconfigured volume access, or exposed snapshots leads to data exposure.

Core principle: EC2 hardening protects the instance; EBS encryption protects persistent data at rest; both are required for a strong control posture.

Minimum evidence set: instance access controls, encryption status, key governance review, snapshot review, and restore validation.