

Essential Eight **ML3** on AWS — Reference Diagram

The ASD Essential Eight Maturity Level 3 mitigation strategies mapped to an AWS reference architecture — which services satisfy each of the eight, by layer.

VERSION 1.0 · JUNE 2026 · [AIOPSONE.COM](https://aiopsone.com) · YOUTUBE [@AIOPSONE](https://www.youtube.com/@aiopsone)

How to read this. Each architecture layer (left) runs on a set of AWS services (centre) and contributes to one or more Essential Eight strategies (right, **E1–E8**). Numbers match the legend below.

Governance & Identity who can do what	AWS Organizations IAM Identity Center SCPs IAM (JIT access) Access Analyzer	E5 E7
Compute & Apps what runs	EC2 (CIS AMIs) ECS / EKS Lambda SSM (inventory) ECR scan	E1 E4
Patch & Vuln keep current	SSM Patch Manager Amazon Inspector ECR image scanning	E2 E6
Endpoints managed desktops	WorkSpaces Fleet Manager GPO / MDM	E3 E4
Data & Backup protect & recover	AWS Backup Vault Lock (immutable) S3 / EBS / RDS (KMS) Cross-region copy	E8
Detect & Log supporting controls	CloudTrail GuardDuty Security Hub AWS Config	all

The eight, mapped

#	STRATEGY	AWS SERVICES AT ML3
E1	Application control	Allow-listed AMIs/containers; signed images + ECR scanning + admission control; SSM software inventory vs approved list
E2	Patch applications	Amazon Inspector (vuln findings); ECR image scanning; SSM Patch Manager on SLA
E3	Configure macro settings	N/A for cloud workloads; enforce on managed desktops (WorkSpaces) via GPO/MDM
E4	User application hardening	CIS-benchmarked base images; WorkSpaces hardening; runtime/browser controls
E5	Restrict admin privileges	IAM least-privilege; Identity Center + JIT elevation; SCPs; no standing admin; Access Analyzer
E6	Patch operating systems	SSM Patch Manager (ML3 cadence); immutable infra; ec2-managedinstance-patch-compliance-status-check
E7	Multi-factor authentication	MFA on all human identities; phishing-resistant (FIDO2) for privileged at ML3
E8	Regular backups	AWS Backup + tested restores; Vault Lock immutability; cross-region/cross-account copies

Jayprakash Bilgaye · **AWS Certified Security – Specialty**

Practitioner guidance, not legal or audit advice. The Essential Eight is maintained by the ACSC; validate against the current Maturity Model and your environment.

CPS 234 → **AWS controls + more resources** → aiopsone.com/resources