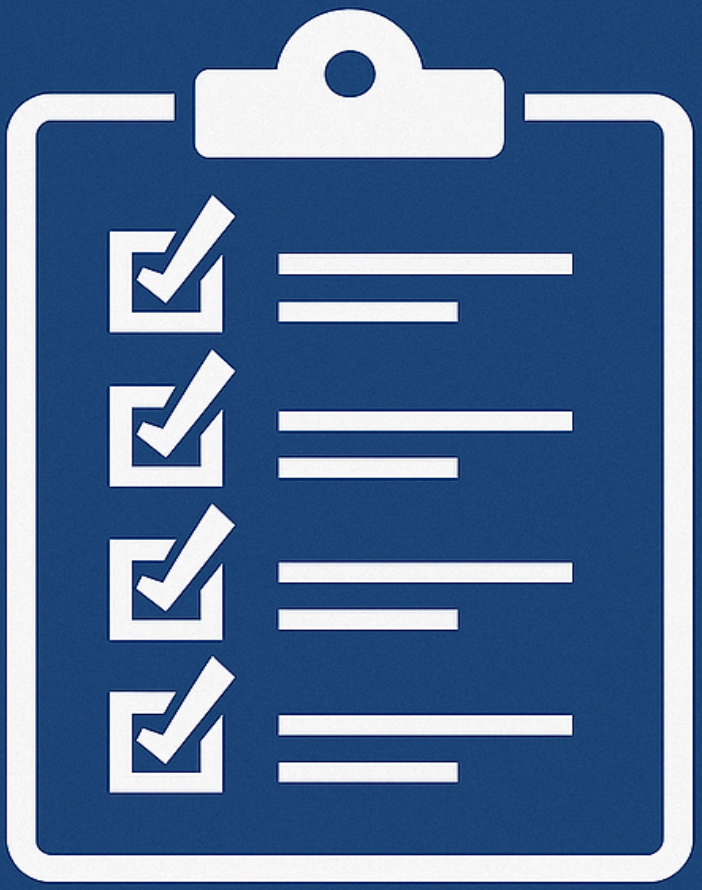
2025 AWS
보안 점검 체크리스트



2025 AWS 보안 점검 체크리스트

2025. 10.

IAM 절대지켜
송지예, 권경탁, 김효주, 이예빈, 이제환, 임예진

NO	항목명	가이드 매핑	O/X	자동 점검 가능
1	EC2 인스턴스 메타데이터 옵션의 IMDSv2를 필수로 선택	1.1 (p.12)		O
2	민감 정보가 안전하게 보관(ex. 환경변수에 민감정보를 평문 저장하지 말고 Secrets Manager에서 보안 암호 형태로 저장)	1.2 (p.13) 3.1 (p.24) 5.1 (p.37)		X
3	EC2 AMI 가용성이 프라이빗으로 설정	1.3 (p.14)		O
4	Organizations SCP 정책 설정에서 사전 허용된 계정 목록의 AMI만 리스트에 등록	1.4 (p.16)		X
5	보안그룹 인바운드 규칙이 원격(SSH, RDP), DB, 관리 포트 소스의 CIDR을 좁은 범위(/16~)로 설정	1.5 (p.17) 4.1 (p.35) 6.2 (p.41)		O
6	EBS 스냅샷의 공유 옵션이 프라이빗으로 설정	1.6 (p.18)		O
7	퍼블릭 용도의 S3 버킷이 아닐 경우, 모든 퍼블릭 액세스 차단 활성화	2.1 (p.20)		O
8	S3 버킷 정책 속 Principal이 특정 ARN으로 제한되어 있고 Resource는 버킷 안 특정 폴더로 지정	2.1 (p.20)		O
9	S3 ACL 설정 속 모든 사람, 인증된 사용자 그룹의 나열, 읽기, 쓰기 권한 체크 해제	2.2 (p.22)		O
10	S3 ACL의 Grantee 목록에 12자리 숫자(외부 AWS 계정 ID)가 있으면 해당 공유를 검증	2.2 (p.22)		X
11	S3 복제 규칙에 사용되는 IAM 역할의 정책 속 Resource에 대상 버킷 ARN 지정	2.3 (p.23)		O
12	시크릿 스캐닝 도구를 통한 자격증명 평문 저장 여부 점검(ex. Trufflehog, Gitleaks 등으로 외부/공개 저장소 속 자격증명 평문 저장 점검)	3.1 (p.24)		X
13	액세스 키가 생성된 후 90일 이내	3.2 (p.25)		O
14	민감 정보의 자동 교체 로직이 존재(ex. Secrets Manager의 보안 암호 자동 교체 구성 활성화)	3.2 (p.25)		X
15	루트 계정의 Active 액세스 키 비활성화	3.3 (p.25)		O
16	루트를 포함한 모든 사용자 계정의 MFA 활성화	3.3 (p.25) 3.9 (p.35)		O
17	신뢰 정책에 사용할 계정/역할/서비스의 ARN으로 Principal 제한 및 Condition 활용	3.4 (p.28)		O
18	iam:PassRole 권한 사용 시, Resource를 특정 ARN으로 제한	3.5 (p.28) 18.1 (p.67) 22.1 (p.72) 27.1 (p.78)		X
19	IdP 연동 시, AssumeRole 정책 속 Principal은 특정 IdP의 ARN으로, Condition은 허용되는 IdP속성 값으로 제한	3.6 (p.29)		X
20	Cross-Account용 IAM 역할의 AssumeRole 정책 속 Principal은 특정 Provider/역할의 ARN으로, Condition은 sts:ExternalId로 제한	3.7 (p.31)		O
21	퇴직자 계정 권한 철회(ex. 콘솔 로그인 프로필, 액세스 키, 연결된 권한 정책, MFA, 인증서, 서비스 자격증명을 모두 삭제/해제)	3.8 (p.32)		X
22	퇴직자 계정 활동 모니터링 및 로그 관리 운영체계 수립(ex. ConsoleLogin, CreateAccessKey 등의 잔여된 의심 활동을 탐지하기 위한 CloudTrail 쿼리 작성)	3.8 (p.32)		X
23	외부 노출이 강력히 제한되어야 하는 내부 네트워크 운영 시, 배스천 호스트 구축	4.2 (p.36)		X

NO	항목명	가이드 매핑	O/X	자동 점검 가능
24	Lambda 함수 실행 시, 환경 변수를 KMS의 고객 마스터 키로 사용	5.1 (p.37)		X
25	Lambda 함수에 결함이 존재하는 코드 스캔(ex. Inspector 연동 및 사용 후 결과에서 심각도 HIGH, CRITICAL 미포함)	5.2 (p.38)		X
26	RDS의 DB 스냅샷 가시성이 프라이빗으로 설정	6.1 (p.40)		O
27	RDS의 퍼블릭 액세스 항목이 아니오로 설정	6.2 (p.41)		O
28	RDS의 DB 서브넷 그룹에 포함된 모든 서브넷을 프라이빗으로 설정	6.2 (p.41)		O
29	CloudTrail 추적에서 Organization 계층을 포함한 추적 로깅 활성화	7.1 (p.43)		O
30	CloudTrail 추적의 API 활동(읽기/쓰기) 모두 활성화	7.2 (p.44)		O
31	비정상적인 API 호출 모니터링 및 로그 관리 운영체계 수립(ex. 대량 호출 RunInstances를 탐지 가능한 CloudTrail 쿼리 작성)	7.2 (p.44)		X
32	EKS 서비스 계정에 연결된 IAM 역할 정책 속 Action은 필요 권한으로, Resource는 특정 ARN으로 제한	8.1 (p.46)		O
33	EKS 사용 시, 쿠버네티스의 서비스 계정별로 IAM 역할 할당	8.1 (p.46)		X
34	KMS에서 외부 고객 관리형 키 Import 시, 만료 기간 설정	9.1 (p.47)		O
35	KMS에서 외부 고객 관리형 키 Reimport/삭제 시, 키 정책 속 Action은 특정 권한으로 제한되어 있고, Resource는 해당 고객 관리형 키의 ARN으로 제한하고, MFA를 강제	9.1 (p.47)		X
36	KMS에서 외부 고객 관리형 키의 키 정책 속 Principal의 KMS 관련 고위험 권한(ex. kms:ImportKeyMaterial, kms:decrypt)을 특정 고객 관리형 키의 역할 ARN으로 제한	9.1 (p.47)		X
37	SNS 주제 액세스 정책에서 sns:Publish, sns:Subscribe을 포함한 SNS 관련 권한이 Principal은 특정 ARN으로, Resource는 해당 주제의 ARN으로 제한	10.1 (p.48)		O
38	SQS 큐 정책 속 Principal이 특정 계정/역할/서비스의 ARN으로 제한	11.1 (p.50)		O
39	Route 53 레코드에 실제 소유/운영 중인 리소스만 존재	12.1 (p.51)		X
40	Organizations의 신뢰할 수 있는 액세스가 업무상 필요한 서비스에만 활성화	13.1 (p.52)		X
41	Organizations SCP 정책 속 불필요한 API(ex. ModifyReservedInstances, aws-marketplace:Subscribe)에 대해 Deny로 설정	13.2 (p.53)		X
42	ECR 리포지토리 정책 속 Principal을 리소스에 접근할 역할 ARN으로 제한	14.1 (p.54)		X
43	ECR의 이미지 스캔과 태그 불변성 활성화	14.1 (p.54)		X
44	ssm:SendCommand 권한 사용 시, 실행 대상의 리소스 ARN으로 제한	15.1 (p.56)		X
45	SSM 문서를 프라이빗으로 설정	15.2 (p.58)		X
46	GuardDuty에서 모든 멤버 계정과 모든 사용 리전에 일괄 활성화 적용 및 신규 계정 자동 가입 설정	16.1 (p.59)		O
47	Cognito Identity Pool에 연결된 IAM 역할 정책 속 Action은 필요 권한으로, Resource는 해당 역할이 접근 가능한 리소스의 ARN으로, Condition은 비인증(Unauthenticated) 역할에 대한 민감 리소스 접근 권한을 제한	17.1 (p.60)		X
48	Cognito를 통한 사용자 관리 시, 내부 서비스거나 관리자 계정만 발급해야 하는 경우 Self Sign Up 비활성화	17.2 (p.62)		X
49	Cognito에서 토큰 만료 시간을 애플리케이션 운영에 필요한 최소 시간으로 설정(ex. 액세스/ID 토큰은 15분~60분, 갱신 토큰은 7일~30일, 기준은 조직 정책에 따라 정의)	17.3 (p.63)		O

NO	항목명	가이드 매핑	O/X	자동 점검 가능
50	CloudFormation을 위한 IAM 역할 정책 속 두개의 권한(CloudFormation:CreateStack, iam:PassRole)을 동시 부여 제한	18.1 (p.65)		O
51	OpenSearch 도메인의 네트워크가 VPC 액세스 전용으로 설정	19.1 (p.66)		O
52	OpenSearch 도메인의 액세스 정책이 IP 또는 특정 IAM 역할/사용자로 제한	19.1 (p.66)		O
53	Elastic Beanstalk 환경 속성 속 소스가 Secrets Manager 혹은 SSM Parameter Store로 지정	20.1 (p.67)		X
54	Redshift 클러스터 암호화	21.1 (p.68)		O
55	Glue를 위한 IAM 역할 정책 속 두개의 권한(glue:CreateDevEndpoint, iam:PassRole)의 동시 부여 제한	22.1 (p.69)		O
56	조직 내 Service Catalog 포트폴리오 공유가 필요한 경우, 조직 전체에 AcceptPortfolioShare 차단하는 SCP 정책 작성 및 조직 구조 내의 공유 방법 선택	23.1 (p.71)		X
57	Service Catalog 제약 조건 생성 시 할당하는 IAM 역할에 Principal은 Service Catalog 서비스 지정, Action은 고위험 권한(ex. iam:CreatePolicy, iam:AttachRolePolicy) Deny, Condition은 호출 출처 제한	23.1 (p.71)		X
58	DocumentDB 스냅샷의 공유 속성이 프라이빗 설정	24.1 (p.73)		O
59	DocumentDB 스냅샷 생성할 클러스터의 KMS 암호화	24.1 (p.73)		O
60	Bedrock 모델 활성화/호출 계열 권한(ex. bedrock:InvokeModel)을 특정 모델 ARN으로, Condition을 호출 리전/주체로 제한	25.1 (p.75)		O
61	SES 고위험 권한(ex. SendEmail, PutAccountDetails)을 승인된 관리자 또는 서비스 전용 IAM 역할에만 허용	26.1 (p.76)		X
62	SES를 위한 IAM 역할 정책 속 Resource를 구체적인 ARN, 도메인, 아이덴티티로 제한	26.1 (p.76)		O
63	AppStream의 Fleet/이미지 빌더에 연결된 IAM 역할 정책 속 Resource를 특정 IAM 역할의 ARN으로 제한	27.1 (p.78)		X

2025 AWS 보안 점검 체크리스트

발행일 : 2025. 10.
발행처 : IAM 절대지켜