JM COLLECTION

클라우드
취약점진단 결과보고서

2023. 08. 07.

SK shieldus

Confidentiality Agreements

본 보고서는 시스템 정보와 관련한 비공개 사항이 포함되어 있으므로, 열람권한은 우선적으로 정보보안 책임자로 제한되며, 이외의 열람자격은 정보보안 책임자가 허락한 최소한의 인원으로 제한하여 주시기 바랍니다.

본 보고서는 양사간의 사전 협의 없이 어떠한 목적으로도 외부로 유출되거나 무단 복제, 무단 사용될 수 없으며, 기밀성을 유지한다는 전제하에 사용이 엄격하게 제한됩니다.

본 보고서는 SK쉴더스에서 작성 하였으며, 정보보호 서약에 대한 사항을 준수 합니다.

목 차

그림 목차

표 목차

1. 개요

1.1.진단 목적

본 클라우드 진단은 “JM COMPANY”에서 운영 중인 클라우드서비스에 대해 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제23조 제2항에 따라 정보보호 기준의 준수 여부를 확인을 인증기관에 요청하는 경우 인증기관은 이를 평가·인증하며, 내부 직원이나 내부망에 거점을 확보한 자가 악용할 수 있는 취약성이 존재하는지를 점검하고, 발견된 취약성에 대한 대응책을 수립하여 안전하고 신뢰할 수 있는 정보시스템 구축 및 운영을 위한 기반을 마련 및 보안 수준 향상을 위한 방법을 제시하고자 합니다.

1.2.진단 대상

No	계정	비고
1	sk401-team	리전 –오하이오

[표] 1. 진단 대상

1.3.진단 일정

업무 수행 내역	일정
사전준비 및 대상 관련 자료 수령	2023.07.28 이전
취약점 점검	2023.07.28~ 2023.08.04
결과 분석 및 결과 보고서 작성	2023.08.17
보고서 최종 수정 및 완료	2023.08.31

[표] 2. 진단 일정

1.4.진단 인력

이름	수행업무	연락처	E-Mail
김영준	취약점진단	010-5765-2359	kxc12345@gmail.com
김현정	취약점진단	010-9952-4126	98expins@gmail.com
박지수	취약점진단	010-2660-5047	parkkdk00@gmail.com
복정빈	취약점진단	010-3856-5982	dalparan19@gmail.com
이혜담	취약점진단	010-9156-7088	hdlee0918@gmail.com
전유진	취약점진단	010-4862-1812	ggg00g13g@gmail.com
정현아	취약점진단	010-9157-8299	isabelle0316@gmail.com
한승훈	취약점진단	010-4818-7131	hsh7131@gmail.com

[표] 3. 진단 인력

1.5.진단 항목

클라우드 진단 항목은 “2023 클라우드 보안 가이드 - AWS”을 기반으로 계정 관리(10개 항목), 권한 관리(3개 항목), 가상 리소스 관리(8개 항목), 운영 관리(13개항목)으로 총 4개 영역에서 34개 항목으로 되어 있으며 상세 진단 항목은 다음과 같습니다.

분류	취약점 번호	세부 진단 항목	준수기준
1. 계정 관리	1.1	사용자 계정 관리	상
	1.2	IAM 사용자 계정 단일화 관리	상
	1.3	IAM 사용자 계정 식별 관리	중
	1.4	IAM 그룹 사용자 계정 관리	중
	1.5	Key Pair 접근 관리	상
	1.6	Key Pair 보관 관리	상
	1.7	Admin Console 관리자 정책 관리	중
	1.8	Admin Console 계정 Access Key 활성화 및 사용 주기 관리	상
	1.9	MFA (Multi-Factor Authentication) 설정	중
	1.10	AWS 계정 패스워드 정책 관리	중
2. 권한 관리	2.1	인스턴스 서비스 정책 관리	상
	2.2	네트워크 서비스 정책 관리	상
	2.3	기타 서비스 정책 관리	상
3. 가상 리소스 관리	3.1	보안 그룹 인/아웃바운드 ANY 설정 관리	상
	3.2	보안 그룹 인/아웃바운드 불필요 정책 관리	상
	3.3	네트워크 ACL 인/아웃바운드 트래픽 정책 관리	중
	3.4	라우팅 테이블 정책 관리	중
	3.5	인터넷 게이트웨이 연결 관리	하
	3.6	NAT 게이트웨이 연결 관리	중
	3.7	S3 버킷/객체 접근 관리	중
	3.8	RDS 서브넷 가용 영역 관리	중
4. 운영 관리	4.1	EBS 및 볼륨 암호화 설정	중
	4.2	RDS 암호화 설정	중
	4.3	S3 암호화 설정	중
	4.4	통신구간 암호화 설정	중
	4.5	CloudTrail 암호화 설정	중
	4.6	CloudWatch 암호화 설정	중
	4.7	AWS 사용자 계정 로깅 설정	상

분류	취약점 번호	세부 진단 항목	준수기준
	4.8	인스턴스 로깅 설정	중
	4.9	RDS 로깅 설정	중
	4.10	S3 버킷 로깅 설정	중
	4.11	VPC 플로우 로깅 설정	중
	4.12	로그 보관 기간 설정	중
	4.13	백업 사용 여부	중

[표] 4. 주요 진단 항목

※ 취약점심각도
상 : 관리자 계정 및 주요 정보 유출로 인한 치명적인 피해 발생
중 : 노출된 정보를 통해 서비스/시스템 관련 추가 정보 유출 발생 우려
하 : 타 취약점과 연계 가능한 잠재적인 위협 내재

2. 취약점 진단 결과요약

2.1.총평

AWS 'sk401-team'계정에 대한 클라우드 진단 결과, 34개의 진단 항목 중 14개 항목에 대해 **취약**으로 진단되었고, 보안 적용률은 54.8%입니다. 중요도가 높은 취약점이 다수 존재하여 원격 및 로컬 취약점을 이용해 침해가 가능한 수준이라고 판단됩니다.

가상 리소스 관리 부분 등에서 치명적인 취약점이 존재하는 것을 확인하였고 이외에도 다수의 취약점이 확인되었으며, 이에 대한 신속한 조치가 필요합니다. 해당 보고서를 통해 관리자에게 취약점에 대한 정보와 대응 방안을 제공해 안정적으로 AWS 클라우드를 사용할 수 있도록 합니다.

자세한 사항은 아래 취약점 진단 상세 결과를 확인하시고 본 결과 보고서와 함께 제공해 드리는 보안 가이드라인을 참고하시어 적절한 보안 대책을 수립 후 조치하시길 권고 드립니다.

※ 본 진단은 최소한의 취약 포인트만 확인하므로 다수의 취약점 누락 발생 가능성이 존재합니다. 또한, 발견된 취약점의 모든 취약 포인트를 식별하지 않으므로 유사 취약 포인트에 대해 담당자 직접 확인 후 조치가 필요합니다.

2.2.대상 별 취약점 요약

분류	취약점 번호	세부 진단 항목	점검결과
1. 계정 관리	1.1	사용자 계정 관리	양호
	1.2	IAM 사용자 계정 단일화 관리	양호
	1.3	IAM 사용자 계정 식별 관리	취약
	1.4	IAM 그룹 사용자 계정 관리	양호
	1.5	Key Pair 접근 관리	양호
	1.6	Key Pair 보관 관리	양호
	1.7	Admin Console 관리자 정책 관리	양호
	1.8	Admin Console 계정 Access Key 활성화 및 사용 주기 관리	양호
	1.9	MFA (Multi-Factor Authentication) 설정	취약
	1.10	AWS 계정 패스워드 정책 관리	취약
2. 권한 관리	2.1	인스턴스 서비스 정책 관리	양호
	2.2	네트워크 서비스 정책 관리	양호
	2.3	기타 서비스 정책 관리	양호
3. 가상 리소스 관리	3.1	보안 그룹 인/아웃바운드 ANY 설정 관리	취약
	3.2	보안 그룹 인/아웃바운드 불필요 정책 관리	취약
	3.3	네트워크 ACL 인/아웃바운드 트래픽 정책 관리	양호
	3.4	라우팅 테이블 정책 관리	취약
	3.5	인터넷 게이트웨이 연결 관리	양호
	3.6	NAT 게이트웨이 연결 관리	양호
	3.7	S3 버킷/객체 접근 관리	취약
	3.8	RDS 서브넷 가용 영역 관리	양호
4. 운영 관리	4.1	EBS 및 볼륨 암호화 설정	취약
	4.2	RDS 암호화 설정	양호
	4.3	S3 암호화 설정	양호
	4.4	통신구간 암호화 설정	양호
	4.5	CloudTrail 암호화 설정	양호
	4.6	CloudWatch 암호화 설정	*N/A*
	4.7	AWS 사용자 계정 로깅 설정	*N/A*
	4.8	인스턴스 로깅 설정	취약

분류	취약점 번호	세부 진단 항목	점검결과
	4.9	RDS 로깅 설정	양호
	4.10	S3 버킷 로깅 설정	*N/A*
	4.11	VPC 플로우 로깅 설정	**취약**
	4.12	로그 보관 기간 설정	**취약**
	4.13	백업 사용 여부	**취약**

[표] 5. 대상 별 취약점 요약

3. 취약점진단 상세결과

3.1.계정 관리

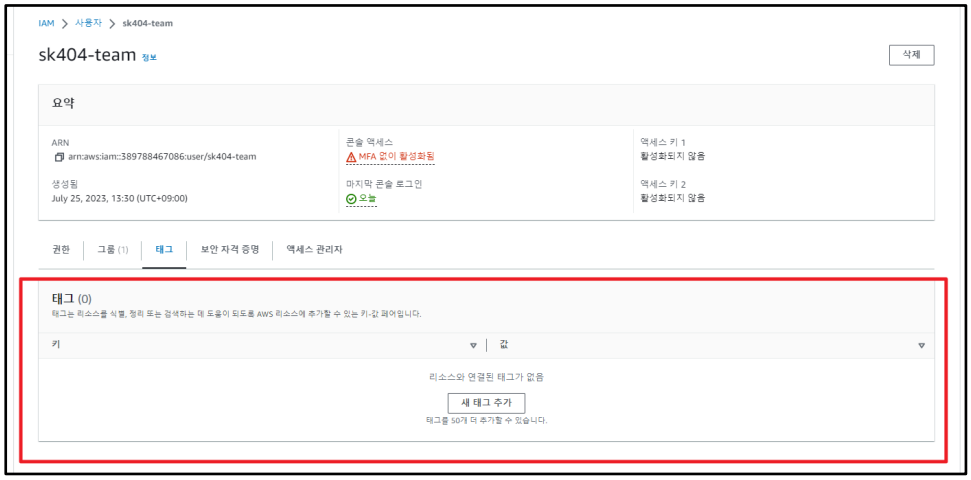
(1) 사용자 계정 관리 (양호)

(2) IAM 사용자 계정 단일화 관리 (양호)

(3) IAM 사용자 계정 식별 관리 (취약)

가. 문제점

IAM 계정에 태그 설정이 되어있지 않아, 사용자 액세스 및 권한 제어가 제한되지 않기 때문에 취약합니다.



[그림] 1. IAM 태그 미 설정

나. 해결방안

IAM 사용자 계정에는 태그를 추가할 수 있으며, 해당 태그 설정은 사용자를 표현하는 정보 및 직책의 내용을 포함할 수 있습니다. 이러한 태그 사용은 IAM 사용자에 대한 액세스를 구성, 추정 또는 제어가 가능합니다.

(4) IAM 그룹 사용자 계정 관리 (양호)

(5) Key Pair 접근 관리 (양호)

(6) Key Pair 보관 관리 (양호)

(7) Admin Console 관리자 정책 관리 (양호)

(8) Admin Console 계정 Access Key 활성화 및 사용주기 관리 (양호)

(9) MFA (Multi-Factor Authentication) 설정 (취약)

가. 문제점

MFA(Multi-Factor Authentication) 설정이 되어있지 않아, AWS 계정 노출에 취약합니다.

[그림] 2. MFA 미 설정

나. 해결방안

AWS Multi-Factor Authentication(MFA)은 사용자 이름과 암호 외에 보안을 한층 더 강화할 수 있는 방법으로 MFA를 활성화하면 사용자가 AWS 웹 사이트에 로그인할 때 사용자 이름과 암호뿐만 아니라 AWS MFA 디바이스의 인증 응답을 입력하라는 메시지가 표시됩니다. 이러한 다중 요소를 통해 AWS 계정 설정 및 리소스에 대한 보안을 높일 수 있습니다.

(10) AWS 계정 패스워드 정책 관리 (취약)

가. 문제점

패스워드 복잡성 기준 준수 및 암호 만료/재사용 제한을 하지 않아, 약한 패스워드와 재사용으로 인한 계정 노출 및 해킹 위험이 높아져 취약합니다.

[그림] 3. 암호 정책 미흡

나. 해결방안

AWS Admin Console Account 계정 및 IAM 사용자 계정의 암호 설정 시 일반적으로 유추하기 쉬운 암호를 설정하는 경우 비 인가된 사용자가 해당 계정을 획득하여 접근 가능성이 존재합니다.

3.2.권한 권리

(1) 인스턴스 서비스 정책 관리 (양호)

(2) 네트워크 서비스 정책 관리 (양호)

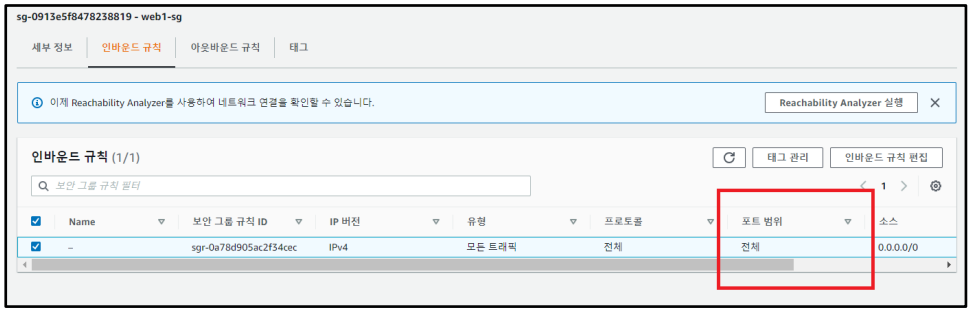
(3) 기타 서비스 정책 관리 (양호)

3.3.가상 리소스 관리

(1) 보안 그룹 인/아웃바운드 ANY 설정 관리 (취약)

가. 문제점

네트워크 ACL에서 모든 트래픽이 허용되어, 네트워크 계층에서의 접근 제어가 없어 악의적인 트래픽이 자유롭게 통과할 수 있어 취약합니다.



[그림] 4. 보안 그룹 포트 범위 설정

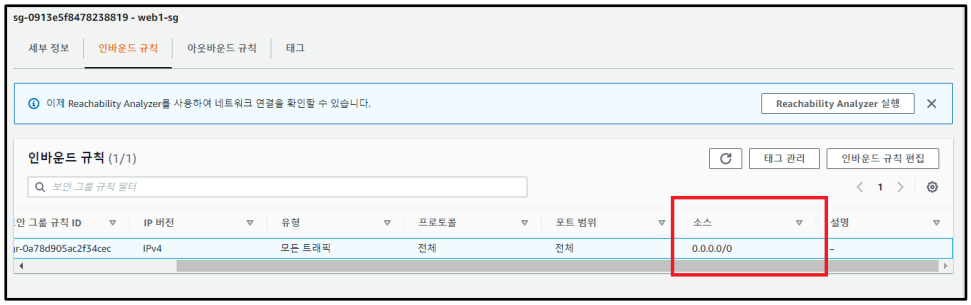
나. 해결방안

VPC에서의 보안 그룹은 EC2 인스턴스에 대한 인/아웃바운드 트래픽을 제어하는 가상 방화벽 역할을 합니다. VPC에서 EC2 인스턴스를 시작할 때 최대 5개의 보안 그룹에 인스턴스를 할당할 수 있습니다. 보안 그룹은 서브넷 수준이 아니라 인스턴스 수준에서 작동하므로 VPC에 있는 서브넷의 각 인스턴스를 서로 다른 보안 그룹 세트에 할당할 수 있습니다.

(2) 보안 그룹 인/아웃바운드 불필요 정책 관리 (취약)

가. 문제점

규칙 대상(0.0.0.0/0)이 모든 IP 주소에서의 접근을 허용하므로, 필요 이상의 네트워크 트래픽이 허용되어 취약합니다.



[그림] 5. 보안 그룹 소스 설정

나. 해결방안

VPC에서의 보안 그룹은 EC2 인스턴스에 대한 인/아웃바운드 트래픽을 제어하는 가상 방화벽 역할을 합니다. VPC에서 EC2 인스턴스를 시작할 때 최대 5개의 보안 그룹에 인스턴스를 할당할 수 있습니다. 보안 그룹은 서브넷 수준이 아니라 인스턴스 수준에서 작동하므로 VPC에 있는 서브넷의 각 인스턴스를 서로 다른 보안 그룹 세트에 할당할 수 있습니다.

(3) 네트워크 ACL 인/아웃바운드 트래픽 정책 관리 (양호)

(4) 라우팅 테이블 정책 관리 (취약)

가. 문제점

라우팅 테이블 내 서비스 타깃 별로 적절한 설정이 이루어지지 않아, 트래픽의 흐름과 목적지를 제어할 수 없게 되어 취약합니다.

[그림] 6. 라우팅 대상 설정

나. 해결방안

VPC를 신규 생성하게 될 경우 기본 라우팅 테이블이 자동으로 생성됩니다. Amazon VPC 콘솔의 [라우팅 테이블] 페이지의 [Main] 열에서 [Yes]를 찾아 VPC에 대한 기본 라우팅 테이블을 볼 수 있습니다. 기본 라우팅 테이블은 다른 라우팅 테이블과 명시적으로 연결되지 않은 모든 서브넷에 대한 라우팅을 제어합니다. 기본 라우팅 테이블에서 라우팅을 추가 및 제거하고 수정할 수 있습니다.

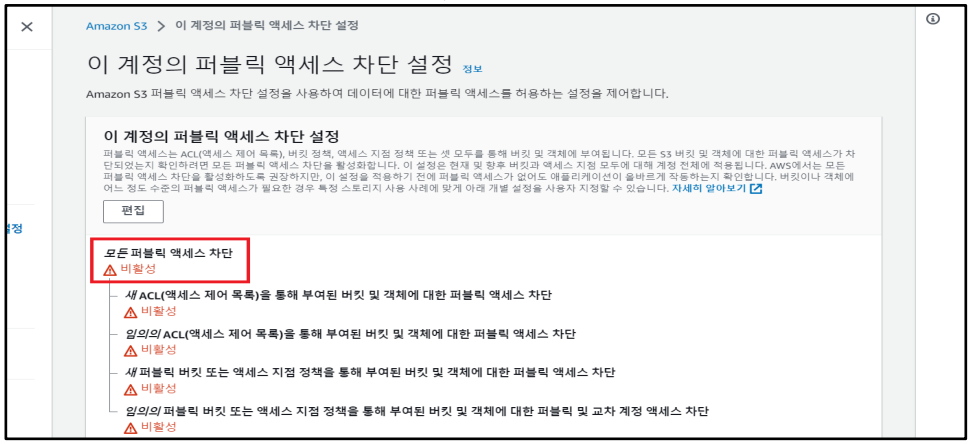
(5) 인터넷 게이트웨이 연결 관리 (양호)

(6) NAT 게이트웨이 연결 관리 (양호)

(7) S3 버킷/객체 접근 관리 (취약)

가. 문제점

모든 퍼블릭 액세스 차단이 활성화되어 있지 않아, 외부로부터 버킷 및 객체가 노출될 수 있어 취약합니다.



[그림] 7. S3 버킷 퍼블릭 액세스 설정

나. 해결방안

S3 버킷의 경우 리소스(버킷)를 생성한 소유자에 대해 리소스 액세스가 가능하며 액세스 정책을 별도(버킷, 객체) 설정하여 다른 사람에게 액세스 권한을 부여할 수 있습니다. 또한, 퍼블릭 액세스 차단 설정이 되지 않을 경우 외부로부터 버킷 및 객체가 노출되므로 안전한 버킷/객체 접근을 위해 목적에 맞는 접근 설정을 해야 합니다.

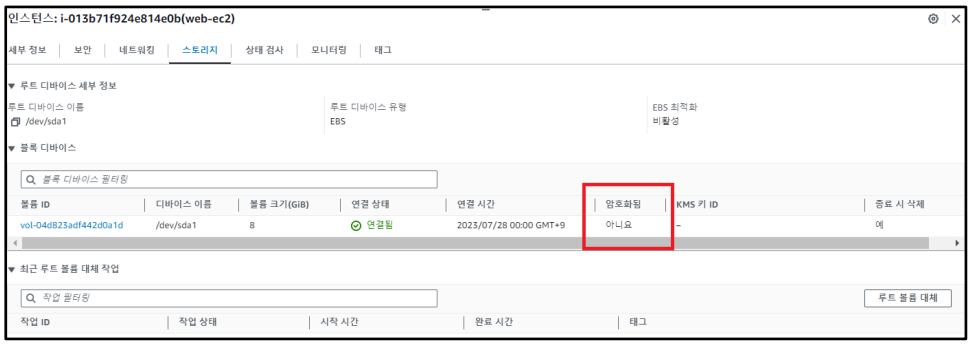
(8) RDS 서브넷 가용 영역 관리 (양호)

3.4.운영 관리

(1) EBS 및 볼륨 암호화 설정 (취약)

가. 문제점

암호화가 비활성화되어, 데이터 저장이 안전하게 이루어지지 않아 취약합니다.



[그림] 8. EBS 암호화 활성화 여부

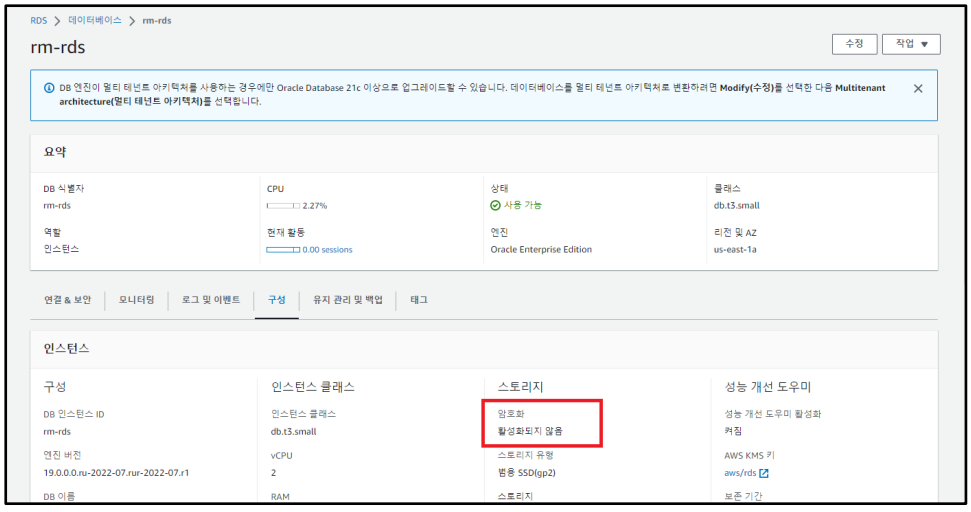
나. 해결방안

EBS는 EC2 인스턴스 생성 및 이용 시 사용되는 블록 형태의 스토리지 볼륨이며 파일시스템 생성 및 블록 디바이스 사용 등을 할 수 있습니다. 또한 EBS는 AES-256 알고리즘을 사용하여 볼륨 암호화를 지원하며 데이터 및 애플리케이션에 대한 다양한 정보를 안전하게 저장할 수 있게 해줍니다.

(2) RDS 암호화 설정 (취약)

문제점

RDS 데이터베이스 암호화가 비활성화되어 있어, DB 인스턴스의 모든 로그, 백업 및 스냅샷이 암호화되지 않아 취약합니다.



[그림] 9. RDS 암호화 활성화 여부

가. 해결방안

RDS는 데이터 보호를 위해 DB 인스턴스에서 암호화 옵션 기능을 제공하며 암호화 시 AES-256 암호화 알고리즘을 이용하여 인스턴스의 모든 로그, 백업 및 스냅샷 암호화가 가능합니다.

(3) S3 암호화 설정 (양호)

(4) 통신구간 암호화 설정 (양호)

(5) CloudTrail 암호화 설정 (양호)

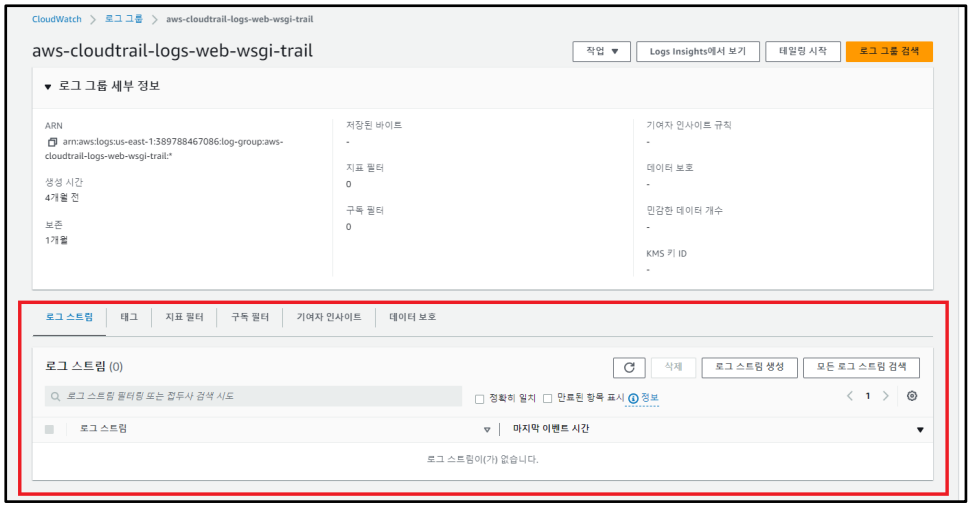
(6) CloudWatch 암호화 설정 (N/A)

(7) AWS 사용자 계정 로깅 설정 (N/A)

(8) 인스턴스 로깅 설정 (취약)

가. **문제점**

CloudWatch 로그 스트림으로 보관하지 않아, 관련된 로그기록이 없어져 문제 진단, 보안 감사 및 문제 해결에 필요한 중요한 정보를 잃게 될 수 있어 취약합니다.



[그림] 10. 인스턴스 로깅 설정 여부

나. **해결방안**

Amazon CloudWatch Logs는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스, AWS CloudTrail, Route 53 및 기타 소스에서 로그 파일을 모니터링, 저장 및 액세스할 수 있습니다. 또한, 가상 인스턴스에 에이전트를 설치하여 로그 그룹에 등록된 로그 스트림을 통해 관련 로그를 확인할 수 있습니다.

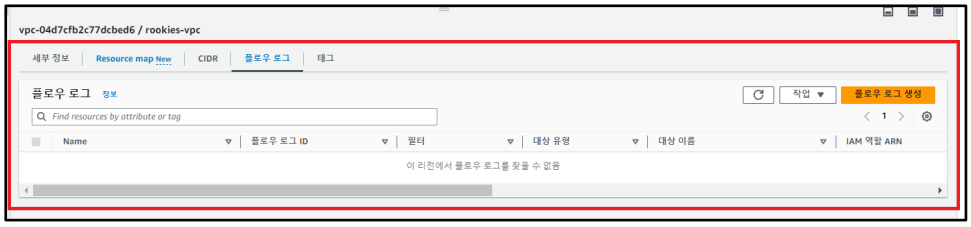
(9) RDS 로깅 설정 (양호)

(10) S3 버킷 로깅 설정 (N/A)

(11) VPC 플로우 로깅 설정 (취약)

가. **문제점**

VPC 플로우 로그를 설정하지 않아, 송수신되는 IP 트래픽에 대한 정보를 수집하지 못하여 모니터링이 제한되므로 취약합니다.



[그림] 11. VPC 로깅 설정 여부

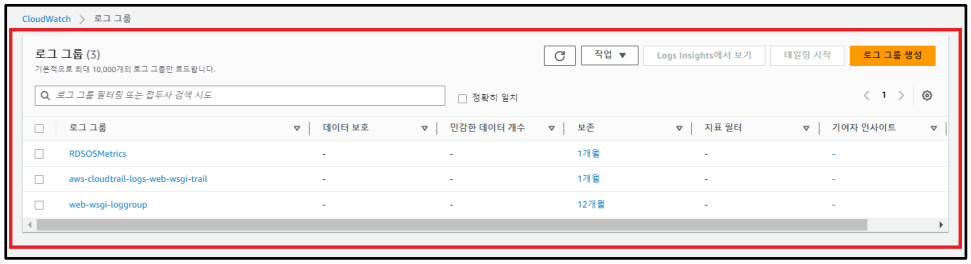
나. **해결방안**

VPC 플로우 로그는 VPC의 네트워크 인터페이스에서 송·수신되는 IP 트래픽에 대한 정보를 수집할 수 있는 기능으로 VPC, 서브넷 또는 네트워크 인터페이스에 생성할 수 있습니다. 플로우 로그는 AWS Management 콘솔의 [VPC] - [플로우 로그] 항목에서 설정 가능하며, 수집된 로그 데이터는 CloudWatch Logs 또는 S3로 저장할 수 있습니다.

(12) 로그 보관 기간 설정 (취약)

가. **문제점**

AWS 서비스 로그를 1년 이상 보관하고 있지 않으면, 보안 사고 분석 및 감사 트레일 추적이 어려워져 취약합니다.



[그림] 12. 로그 보관 기간 설정 여부

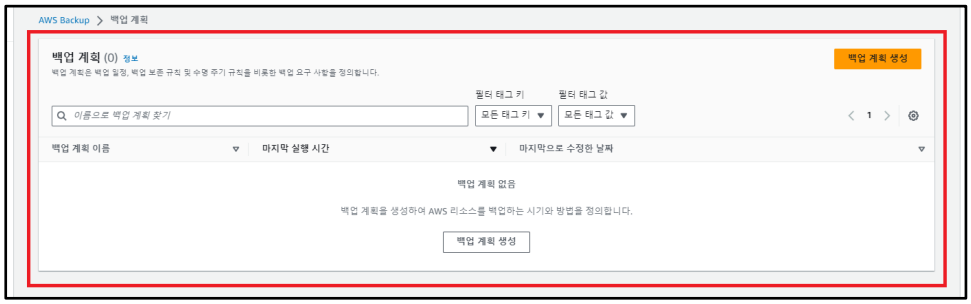
나. 해결방안

CloudWatch Logs에 저장되는 로그 데이터는 기본적으로 무기한 저장되므로, 기업 내부 정책 및 컴플라이언스 준수 등에 부합하도록 로그 데이터 저장 기간을 설정해 주어야 하며, AWS Management 콘솔의 CloudWatch 로그 그룹에서 저장 기간 설정이 가능합니다.

(13) 백업 사용 여부 (취약)

가. 문제점

클라우드 리소스 백업 정책이 없으면, 장애 발생과 인적 재해를 포함한 모든 상황에 대비할 수 없어 데이터 손실 및 시스템 복구에 어려움을 겪게 되어 취약합니다.



[그림] 13. 백업 사용 여부

나. 해결방안

운영 중인 클라우드 리소스에 대한 시스템 충돌, 장애 발생, 인적 재해 등 기업의 사업 연속성을 해치는 모든 상황에 대비하기 위해 백업 서비스를 구성해야 데이터를 안전하게 보관할 수 있습니다. 이에 보안 담당자 및 관리자는 클라우드 리소스에 대한 백업을 설정하여 데이터 손실을 방지할 수 있도록 정책을 수립하고 관리하여야 합니다.