’25년
CSPM(DataDog)
AWS 보안 가이드

SK 쉴더스 | ICT취약점진단팀

목 차

I. 전체목록

1. 체크리스트 항목

진단에 사용될 체크리스트는 국내/외 기술 자료를 바탕으로 작성되었습니다. AWS 보안 가이드라인에서의 영역은 계정 관리(9개 항목), 권한 관리(3개 항목), 가상 리소스 관리(9개 항목), 운영 관리(12개 항목)으로 총 4개 영역에서 33개 항목으로 구성하였습니다.

[표] 1. AWS 보안진단 체크리스트

영역	항목코드	항목명	중요도
계정 관리	1.1	사용자 계정 관리	상
	1.2	IAM 사용자 계정 장기간 비활성화 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	Admin Console 관리자 정책 관리	중
	1.7	Admin Console 계정 Access Key 활성화 및 사용주기 관리	상
	1.8	MFA (Multi-Factor Authentication) 설정	중
	1.9	AWS 계정 패스워드 정책 관리	중
권한 관리	2.1	인스턴스 서비스 정책 관리	상
	2.2	네트워크 서비스 정책 관리	상
	2.3	기타 서비스 정책 관리	상
가상 리소스 관리	3.1	보안 그룹 인/아웃바운드 PORT 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
	3.9	ELB(Elastic Load Balancing) 연결 관리	중
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	AWS 사용자 계정 로깅 설정	상
	4.7	인스턴스 로깅 설정	중
	4.8	RDS 로깅 설정	중
	4.9	S3 버킷 로깅 설정	중

	4.10	VPC 플로우 로깅 설정	중
	4.11	로그 보관 기간 설정	중
	4.12	백업 사용 여부	중

2. AWS 보안 가이드라인/CSPM(DataDog) 탐지규칙 매칭

Cloud 보안가이드의 세부 점검항목을 기준으로 하여, 동일한 통제 목적을 달성 할 수 있는 DataDog CSPM 및 Security Monitoring 규칙을 선별하고 매칭하였습니다. "계정 및 접근통제", "데이터 암호화", "네트워크 관리", "로그 및 모니터링" 등의 핵심 통제 항목을 DataDog의 자동화된 탐지 규칙과 규칙이 존재하지 않는 항목에 대해서는 Custom 규칙을 별도로 생성하여 가이드가 요구하는 보안 수준을 DataDog에서 기술적으로 검증할 수 있도록 구성하였습니다.

[표] 2. AWS 보안 가이드라인과 DataDog 탐지규칙 매칭

영역	항목 코드	항목명	DataDog 탐지규칙 코드
계정 관리	1.1	사용자 계정 관리	**542-ddc-8ba** (공식 문서 Link)
	1.2	IAM 사용자 계정 장기간 비활성화 관리	**7h6-fp7-pc3** (공식 문서 Link)
	1.3	IAM 사용자 계정 식별 관리	**Custom 규칙 (기본 규칙 없음)**
	1.4	IAM 그룹 사용자 계정 관리	**def-000-ysz** (공식 문서 Link) **Custom 규칙 (기본 규칙 없음)**
	1.5	Key Pair 접근 관리	**Custom 규칙 (기본 규칙 없음)**
	1.6	Admin Console 관리자 정책 관리	**v9v-uhp-uk5** (공식 문서 Link)
	1.7	Admin Console 계정 Access Key 활성화 및 사용주기 관리	**ee4-ngx-bwr** (공식 문서 Link) **bcz-prk-dr6** (공식 문서 Link) **r1s-kud-79s** (공식 문서 Link)
	1.8	MFA (Multi-Factor Authentication) 설정	**8yh-cqk-qbn** (공식 문서 Link) **hsh-y5w-hxe** (공식 문서 Link)
	1.9	AWS 계정 패스워드 정책 관리	**2mn-qgc-gka** (공식 문서 Link) **r88-a34-ppx** (공식 문서 Link) **ziw-w2v-e6z** (공식 문서 Link) **z23-f9p-six** (공식 문서 Link) **ayr-n9s-q87** (공식 문서 Link)
권한 관리	2.1	인스턴스 서비스 정책 관리	**Custom 규칙 (기본 규칙 없음)**
	2.2	네트워크 서비스 정책 관리	**Custom 규칙 (기본 규칙 없음)**
	2.3	기타 서비스 정책 관리	**Custom 규칙 (기본 규칙 없음)**
가상 리소스 관리	3.1	보안 그룹 인/아웃바운드 PORT ANY 설정 관리	**Custom 규칙 (기본 규칙 없음)**
	3.2	보안 그룹 인/아웃바운드 불필요 정책 관리	**tch-c9p-gh4** (공식 문서 Link) **def-000-9mn** (공식 문서 Link)
	3.3	네트워크 ACL 인/아웃바운드 트래픽 정책 관리	**rx9-tkr-e6b** (공식 문서 Link)
	3.4	라우팅 테이블 정책 관리	**def-000-j0s** (공식 문서 Link)
	3.5	인터넷 게이트웨이 연결 관리	**def-000-k5x** (공식 문서 Link)
	3.6	NAT 게이트웨이 연결 관리	**def-000-k5x** (공식 문서 Link)

	3.7	S3 버킷/객체 접근 관리	**def-000-hb1** (공식 문서 Link) **def-000-0f1** (공식 문서 Link) **5yq-fi1-8pn** (공식 문서 Link) **hkp-p6b-f7w** (공식 문서 Link)
	3.8	RDS 서브넷 가용 영역 관리	**fu0-rtv-2rb** (공식 문서 Link)
	3.9	ELS(Elastic Load Balancing) 연결 관리	**def-000-khx** (공식 문서 Link) **def-000-v6y** (공식 문서 Link) **def-000-v86** (공식 문서 Link) **ix9-ih4-ucg** (공식 문서 Link)
운영 관리	4.1	EBS 및 볼륨 암호화 설정	**n68-nzh-pl8** (공식 문서 Link) **146-kl4-mas** (공식 문서 Link)
	4.2	RDS 암호화 설정	**625-933-d8d** (공식 문서 Link)
	4.3	S3 암호화 설정	**tcg-c9p-gh4** (공식 문서 Link)
	4.4	통신구간 암호화 설정	**def-000-e19** (공식 문서 Link) **ix9-ih4-ucg** (공식 문서 Link) **def-000-oat** (공식 문서 Link)
	4.5	CloudTrail 암호화 설정	**yg4-3in-tkd** (공식 문서 Link)
	4.6	AWS 사용자 계정 로깅 설정	**def-000-bop** (공식 문서 Link) **6c6-101-b03** (공식 문서 Link)
	4.7	인스턴스 로깅 설정	**Custom 규칙 (기본 규칙 없음)**
	4.8	RDS 로깅 설정	**def-000-3on** (공식 문서 Link) **def-000-u7d** (공식 문서 Link)
	4.9	S3 버킷 로깅 설정	**def-000-o7x** (공식 문서 Link) **def-000-bf9** (공식 문서 Link)
	4.10	VPC 플로우 로깅 설정	**npt-kg2-pv2** (공식 문서 Link)
	4.11	로그 보관 기간 설정	**Custom 규칙 (기본 규칙 없음)**
	4.12	백업 사용 여부	**def-000-5q3** (공식 문서 Link)

3. 위험도 구분

각 취약점으로 인해 발생 가능한 피해에 대하여 위험도 산정을 통해 상, 중, 하 3단계로 분류함.

[표] 3. 위험도 구분

위험도	내 용	조치기간	비고
상	관리자 계정 및 주요정보 유출로 인한 치명적인 피해 발생	단기	
중	노출된 정보를 통해 서비스/시스템 관련 추가 정보 유출 발생 우려	중기	
하	타 취약점과 연계 가능한 잠재적인 위협 내재	장기	

II. 세부항목 설정

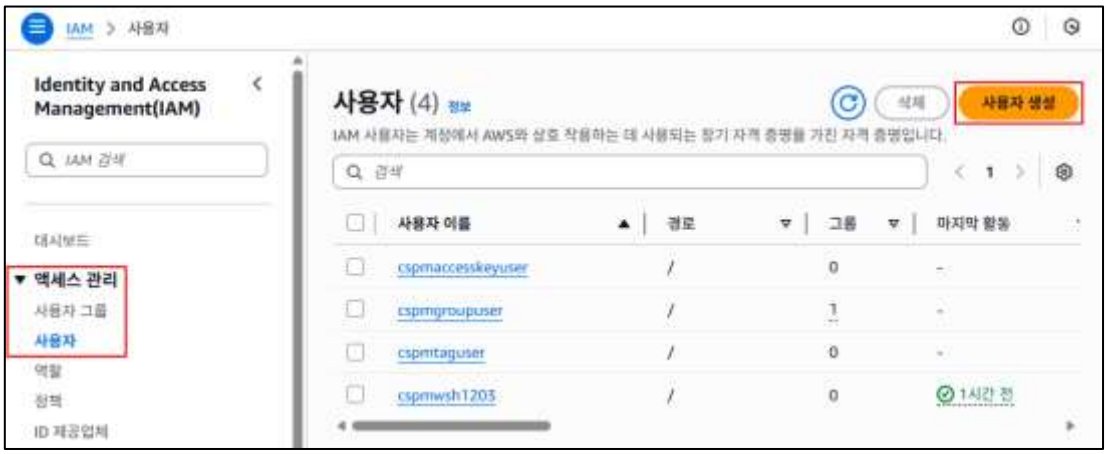
1. 계정 관리

1.1 사용자 계정 관리

<table>
<tr><td>분류</td><td>계정 관리</td><td>중요도</td><td>상</td></tr>
<tr><td>항목명</td><td colspan="3">사용자 계정 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">권한이 있는 IAM 사용자는 “AdministratorAccess IAM” 관리 정책을 통해 모든 AWS 서비스에 액세스하고 리소스를 제어할 수 있습니다. 액세스 권한이 불필요하게 관리자 액세스 권한을 보유하고 있는 사용자가 자신도 모르게 또는 의도적으로 보안 문제나 데이터 유출을 발생시킬 수 있습니다.

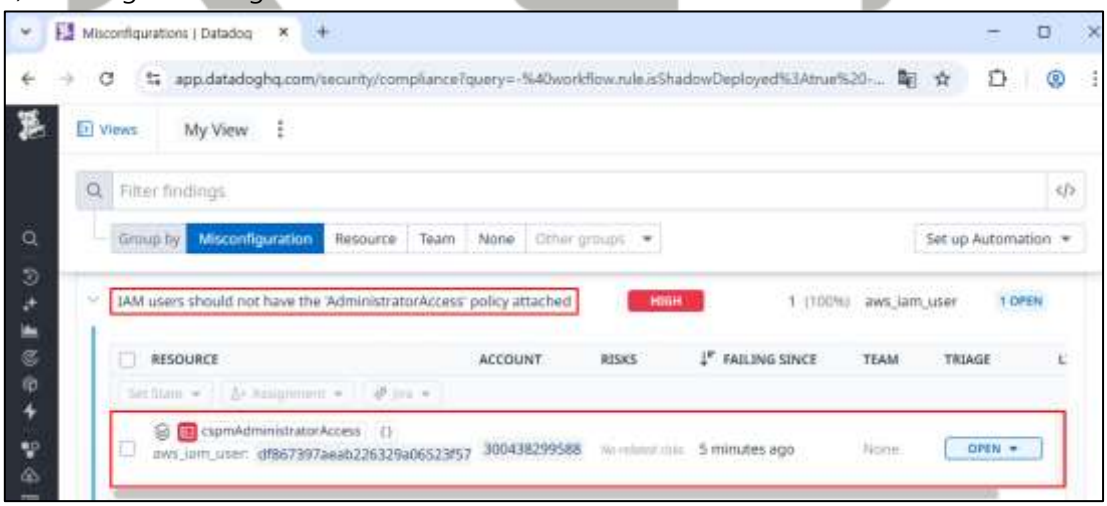
(*) AWS 관리형 정책
서비스 내 FULL ACCESS 등과 같이 중요도가 높은 AWS 관리형 정책은 EC2 서비스 관리/운영자 및 관련 담당자 외에 다른 IAM 계정에 아래와 같은 권한 할당이 되지 않도록 해야합니다. 그중에서도 AWS Admin Console 관리자(AdministratorAccess) 권한은 다수의 IAM 계정에 설정되지 않도록 관리 조치가 필요합니다.

(*) 계정 종류
<table>
<tr><th>계정 구분</th><th>Description</th><th>확인 필요 사항</th></tr>
<tr><td>Console Admin</td><td>최고 권한을 가지고 있는 단일 계정</td><td>가급적 사용을 지양해야 함</td></tr>
<tr><td>IAM</td><td>AWS IAM 서비스를 통해 생성된 별도 계정</td><td>IAM 역할 및 권한에 대한 현황을 확인해야 함</td></tr>
<tr><td>AD(Active Directory) 연동</td><td>기존 내부에서 사용중인 AD 를 AWS Organizations 서비스에 연동한 계정</td><td>기존 AD 서비스에서 사용중인 각 계정 중 IAM 역할 및 권한이 설정된 현황을 확인해야 함</td></tr>
<tr><td>Access Key</td><td>CLI 환경으로의 접속을 위한 단일 계정 (사용 기간에 대한 기준 명시가 필요함)</td><td>발급일 기준 6 개월을 초과한 Access Key 존재 유무</td></tr>
</table>
(*) 불필요한 계정 예시
1. 비 임직원 계정 (협력사 공통 계정)
2. 테스트 계정 (testuser, test01, test02....)
3. 미사용 계정 (퇴직 및 휴직자)</td></tr>
<tr><td>설정
방법</td><td colspan="3">가. AWS IAM 사용자는 "AdministratorAccess" 정책을 연결하면 안됨 (HIGH)
1) IAM -> 엑세스 관리 -> 사용자 -> 사용자 생성</td></tr>
</table>



2) IAM 사용자 생성 시 "AdministratorAccess" 정책 연결

3) Datadog Misconfiguration 탐지 확인

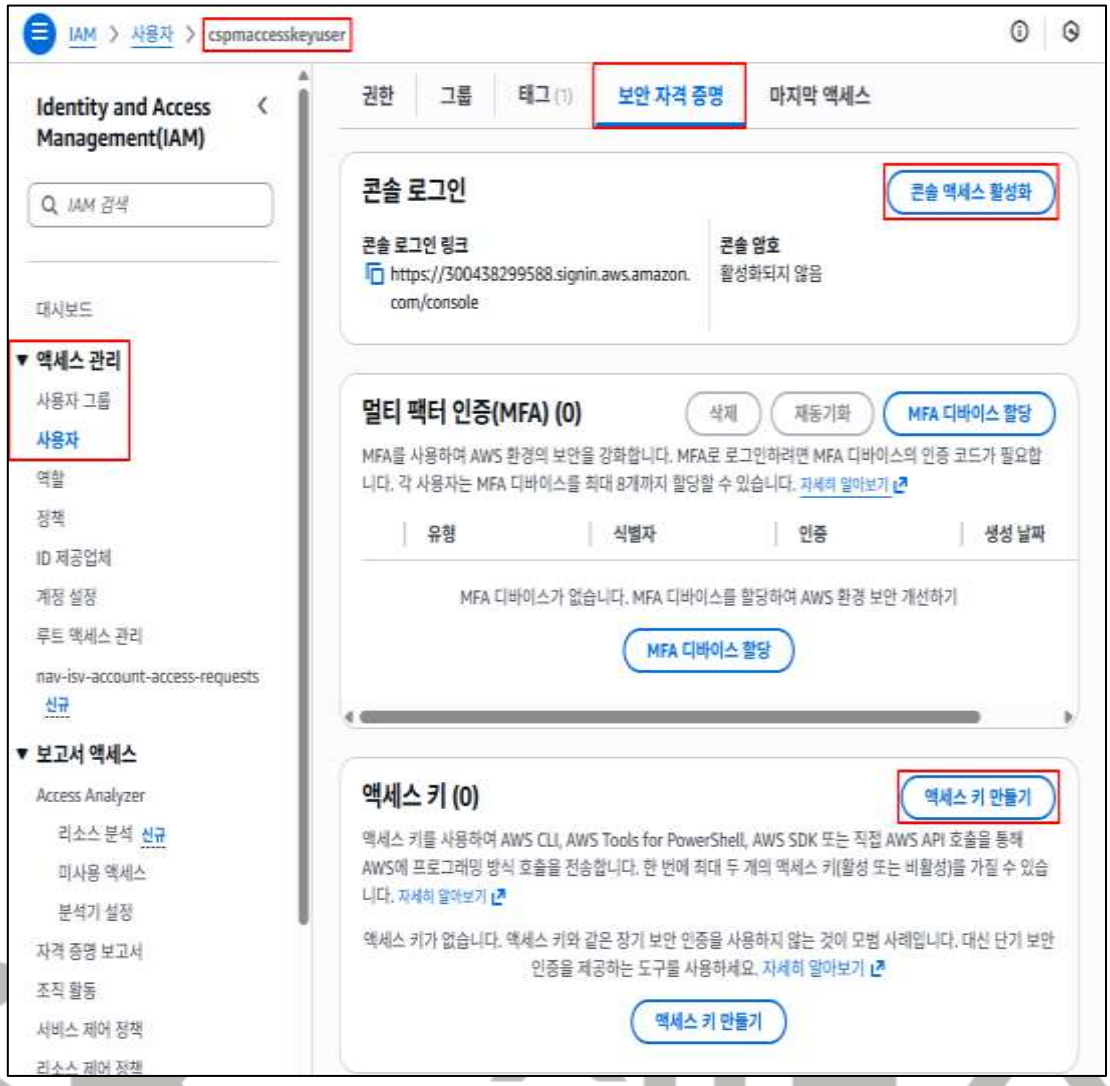


탐지 기준	**542-ddc-8ba** : IAM 사용자가 'AdministratorAccess' 정책이 직접 연결된 경우

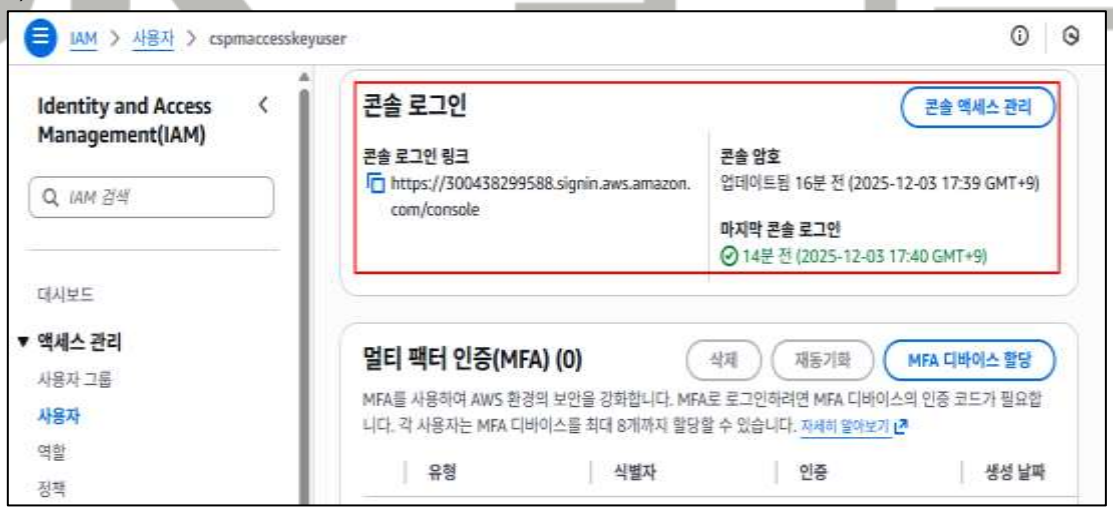
비고	기술 공식 문서 : https://docs.datadoghq.com/ko/security/default_rules/542-ddc-8ba/

1.2 IAM 사용자 계정 장기간 비활성화 관리

분류	계정 관리	중요도	상
항목명	IAM 사용자 계정 장기간 비활성화 관리		
항목 설명	AWS IAM 사용자는 비밀번호, 액세스 키등 다양한 유형의 자격 증명을 사용하여 AWS 리소스에 액세스 할 수 있습니다. Datadog은 보안 강화를 위해 "45일" 이상 사용되지 않는 모든 자격 증명을 비활성화하거나 제거할 것을 권장하며, 불필요한 자격 증명을 비활성화하거나 제거하면 손상되거나 버려진 계정이 악용될 수 있는 보안 위험을 줄일 수 있습니다. **1) 적절한 IAM 계정 사용** - AWS IAM 계정 생성 시 1인 1계정 발급을 원칙으로 하며, 1명의 담당자가 다수의 IAM 계정을 보유하는 것을 지양해야 합니다. Cloud 서비스 리소스 사용이 필요할 경우 내부 정책을 기준으로 목적에 맞게 권한이 부여되어야 합니다. **※ Cloud 서비스 별 IAM 계정 생성 및 관리 금지** **2) 장기간 미사용 계정 관리** - AWS IAM 사용자 계정 생성 후 장기간(45 일) 미사용 계정에 대해 IAM 자격 증명을 관리하고 비활성화 해야 합니다. 다만 사내 규정(정책 및 지침)에 의거하여 미사용 계정에 대한 기준은 별도 관리가 필요합니다.		
설정 방법	**가. 45일 동안 사용하지 않은 경우 자격 증명을 비활성화하거나 제거해야 함 (MEDIUM)** ***※ 자격 증명 검증 기간은 내부 정책 및 보안 수준에 따라 커스텀하여 사용 권고*** 1) IAM -> 엑세스 관리 -> 사용자 -> 사용자 선택 -> 보안 자격 증명 -> 콘솔 엑세스 활성화/엑세스 키 만들기		

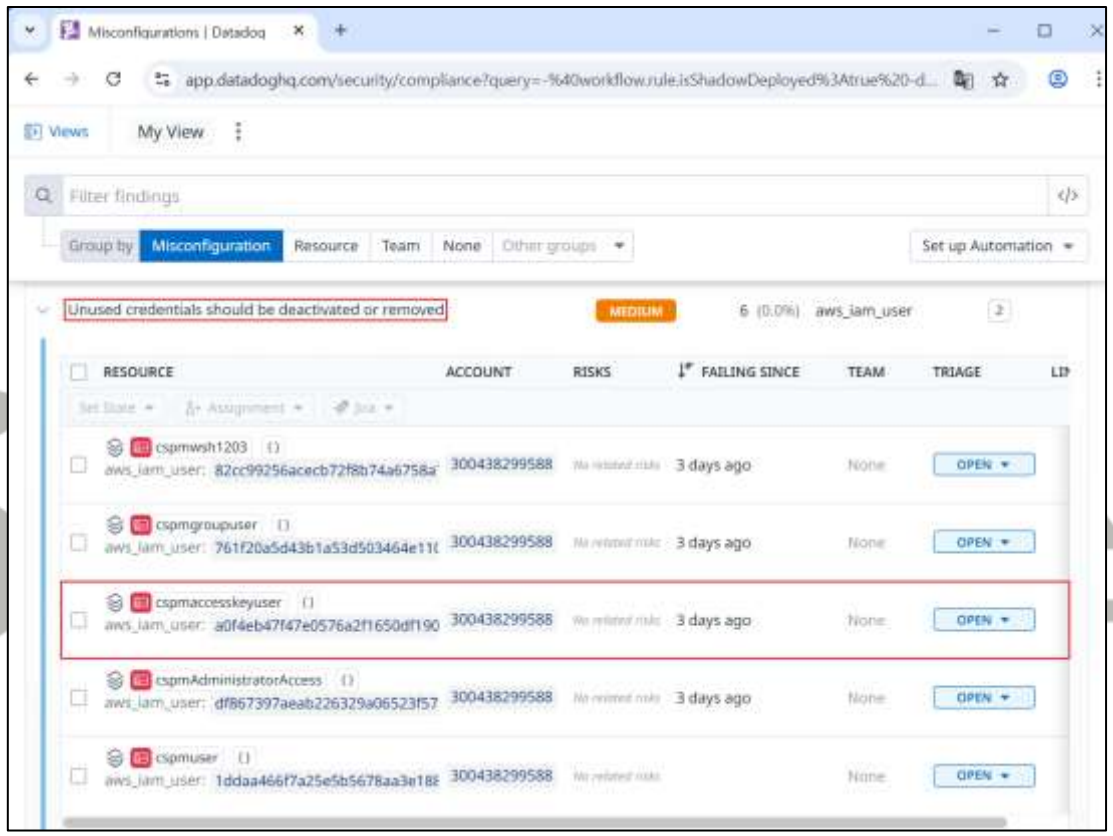


2) 콘솔 로그인 활성화 확인



3) 엑세스 키 생성 확인

<table>
<tr><td></td><td> 

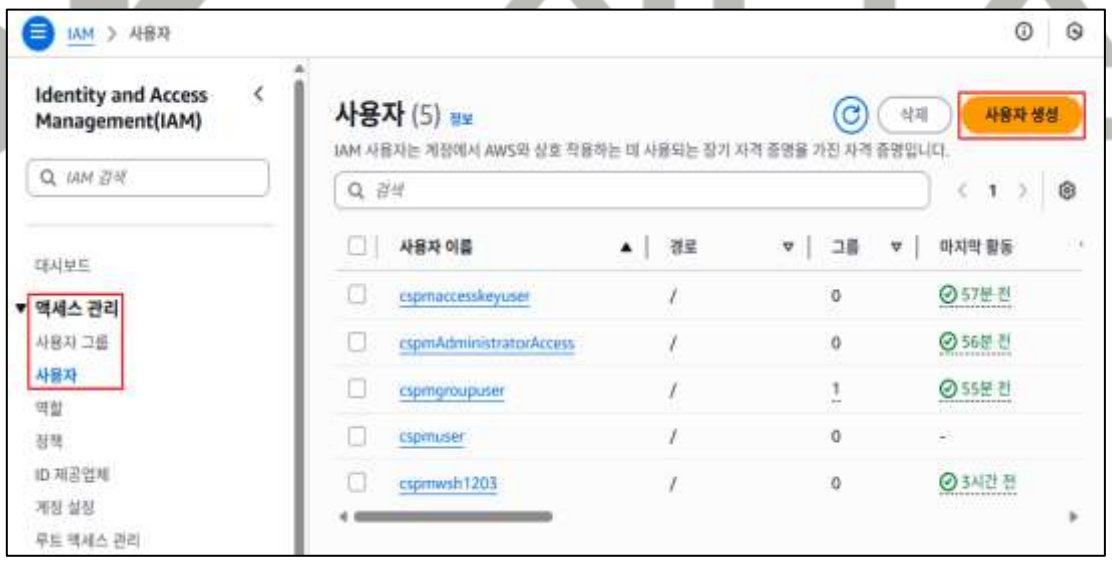
4) Datadog Misconfiguration 탐지 확인
 
</td></tr>
<tr><td>탐지 기준</td><td>7h6-fp7-pc3 : IAM 사용자의 활성화된 비밀번호 또는 Access key 가 45일 이상 사용하지 않은 경우</td></tr>
<tr><td>비고</td><td>기술 공식 문서 :
https://docs.datadoghq.com/ko/security/default_rules/7h6-fp7-pc3/</td></tr>
</table>

1.3 IAM 사용자 계정 식별 관리

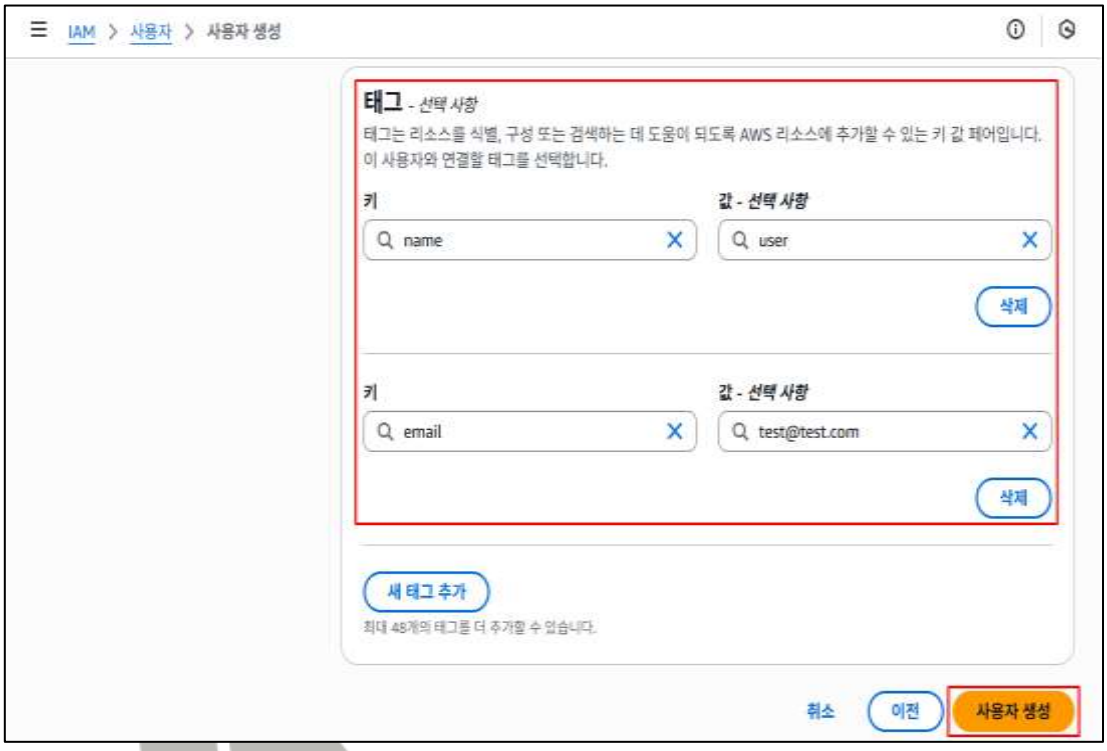
분류	계정 관리	중요도	중

<table>
<tr><td>항목명</td><td>사용자 계정 식별 관리</td></tr>
<tr><td>항목
설명</td><td>
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 액세스 구성, 추정 또는 제어가 가능합니다.

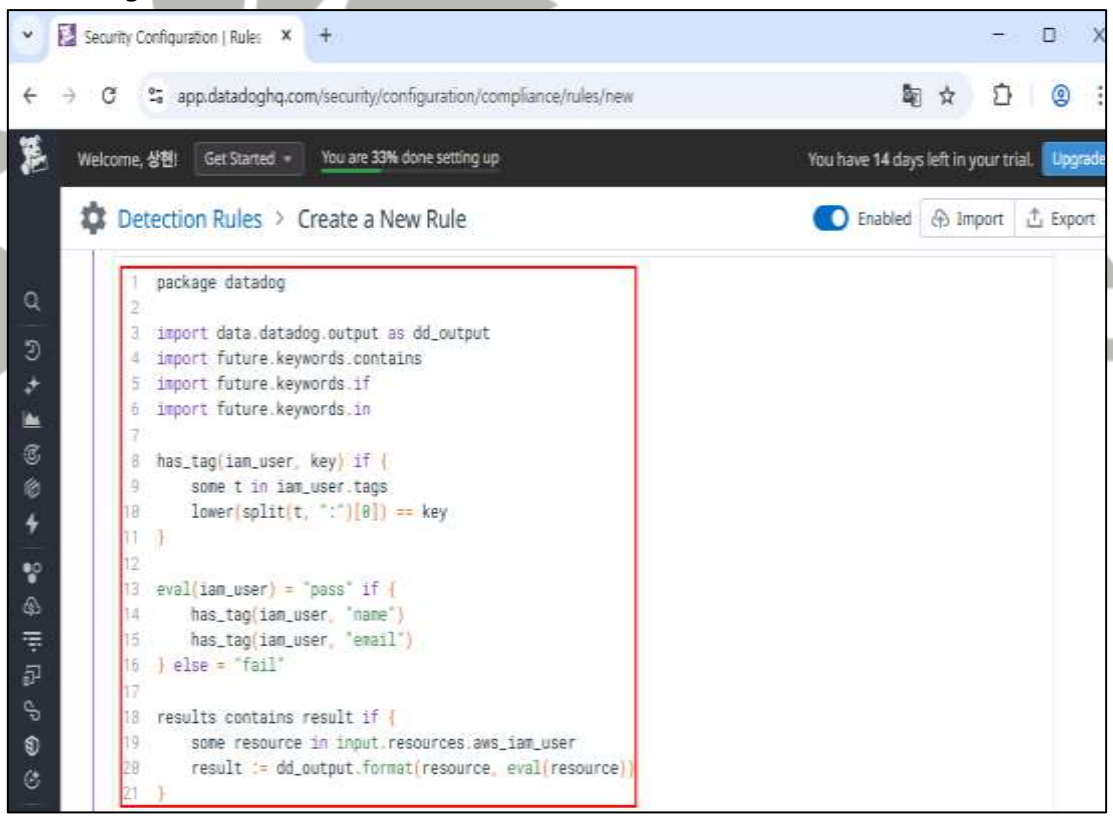
환경 내의 문제를 발견하고 범위를 좁혀 근본적인 원인을 찾을 수 있도록 사용자 계정에 대한 태그를 설정하여 활동여부를 감사하도록 점검해야 합니다.

(*) 계정 종류
<table>
<tr><th>계정 구분</th><th>Description</th><th>확인 필요 사항</th></tr>
<tr><td>Console Admin</td><td>최고 권한을 가지고 있는 단일 계정</td><td>가급적 사용을 지양해야 함</td></tr>
<tr><td>IAM</td><td>AWS IAM 서비스를 통해 생성된 별도 계정</td><td>IAM 역할 및 권한에 대한 현황을 확인해야 함</td></tr>
<tr><td>AD(Active Directory) 연동</td><td>기존 내부에서 사용중인 AD 를 AWS Organizations 서비스에 연동한 계정</td><td>기존 AD 서비스에서 사용중인 각 계정 중 IAM 역할 및 권한이 설정된 현황을 확인해야 함</td></tr>
<tr><td>Access Key</td><td>CLI 환경으로의 접속을 위한 단일 계정 (사용기간에 대한 기준 명시가 필요함)</td><td>발급일 기준 6 개월을 초과한 Access Key 존재 유무</td></tr>
</table>
</td></tr>
<tr><td>설정
방법</td><td>
가. AWS IAM 사용자 태그 지정 정책 준수 (MEDIUM)
1) IAM -> 엑세스 관리 -> 사용자 -> 사용자 생성


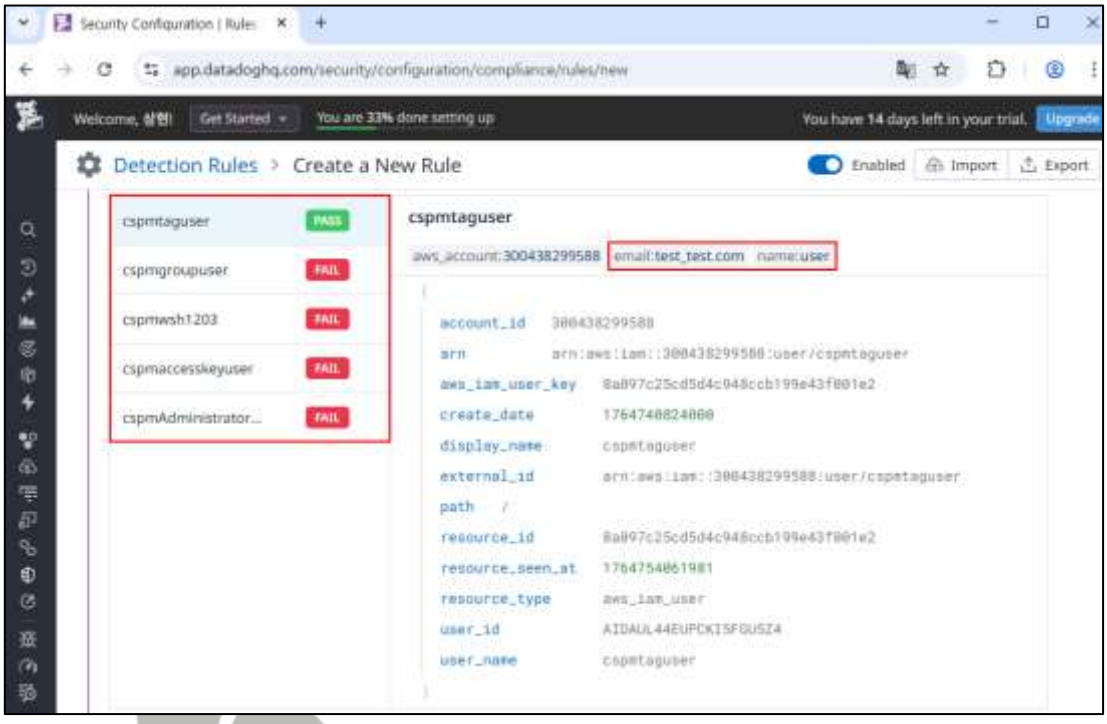
2) IAM 사용자 생성 시 태그 추가
</td></tr>
</table>



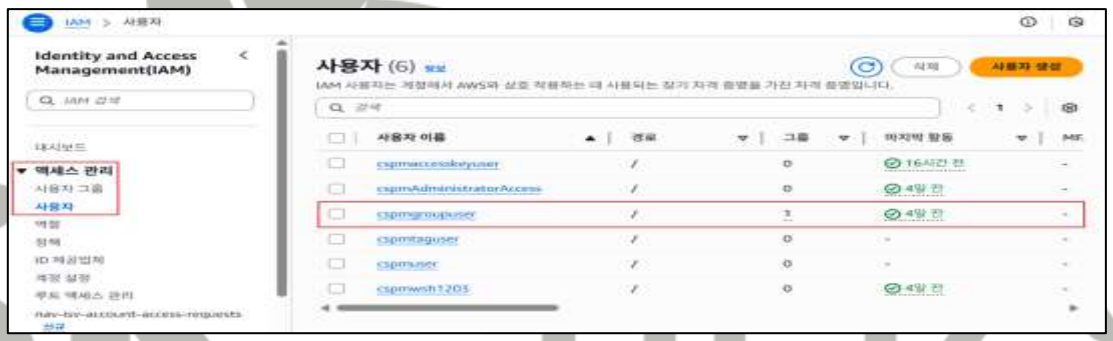
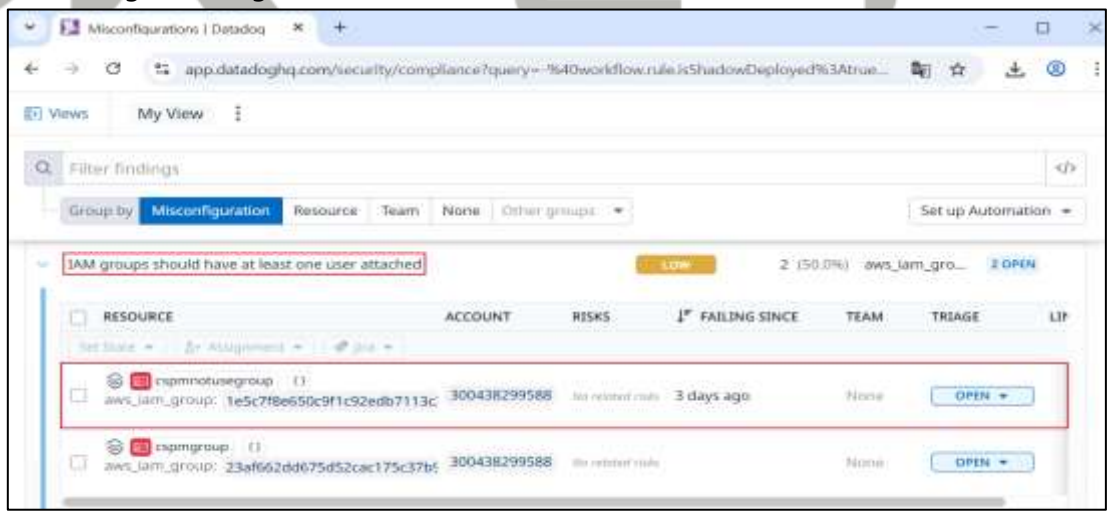
3) Datadog Detection Rule 추가



4) Datadog Detection Rule 탐지 여부 확인

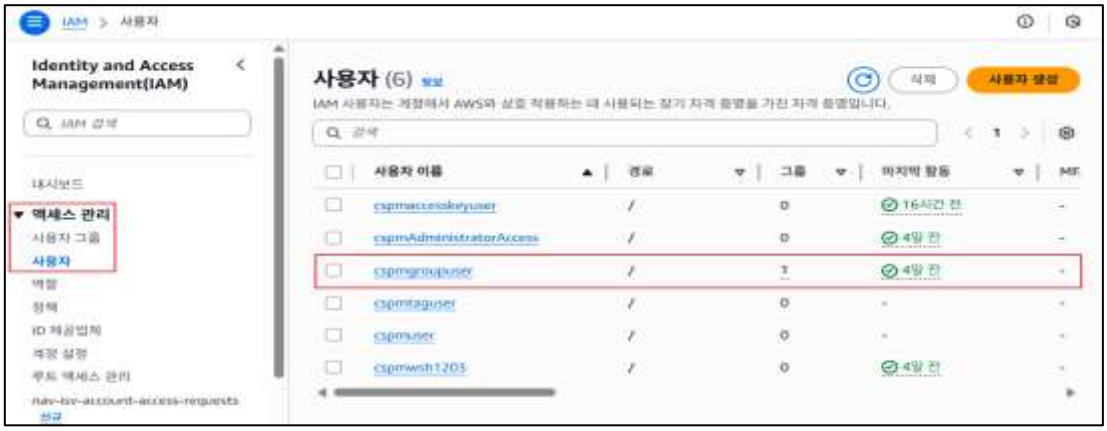
	
탐지 기준	**커스텀** : IAM 사용자의 필수 태그가 정의되어 있지 않은 경우
비고	기술 공식 문서 : 없음

1.4 IAM 그룹 사용자 계정 관리

분류	계정 관리	중요도	중
항목명	IAM 그룹 사용자 계정 관리		
항목 설명	IAM 그룹은 IAM 사용자들의 집합으로 AWS 사용자들에 대한 권한을 쉽게 관리할 수 있습니다. 그룹에 대한 IAM 권한 적용 시 그룹 내 사용자들에게 일괄 적용이 되기 때문에 그룹 별 적절한 권한을 할당하여 사용해야 합니다. 관리 권한이 있는 IAM 그룹은 AWS 계정의 모든 서비스와 리소스에 액세스할 수 있습니다. 액세스 권한이 없는 IAM 사용자가 있는 그룹은 자신도 모르게 또는 의도적으로 보안 문제나 데이터 유출을 유발할 수 있습니다. IAM 그룹은 여러 사용자에게 동시에 적용할 수 있는 정책을 묶어 사용자 권한을 관리하는데 도움이 됩니다. 하지만 더 이상 필요하지 않은 IAM 그룹이 있는 경우 잠재적 보안 위험을 방지하기 위해 제거하는 것이 가장 좋습니다.		
설정 방법	**가. AWS IAM 그룹에는 최소한 한명의 사용자가 연결되어 있어야 함 (LOW)** 1) IAM -> 엑세스 관리 -> 사용자 그룹  2) Datadog Misconfiguration 탐지 확인  **나. IAM 사용자 그룹 감사 (MEDIUM)**		

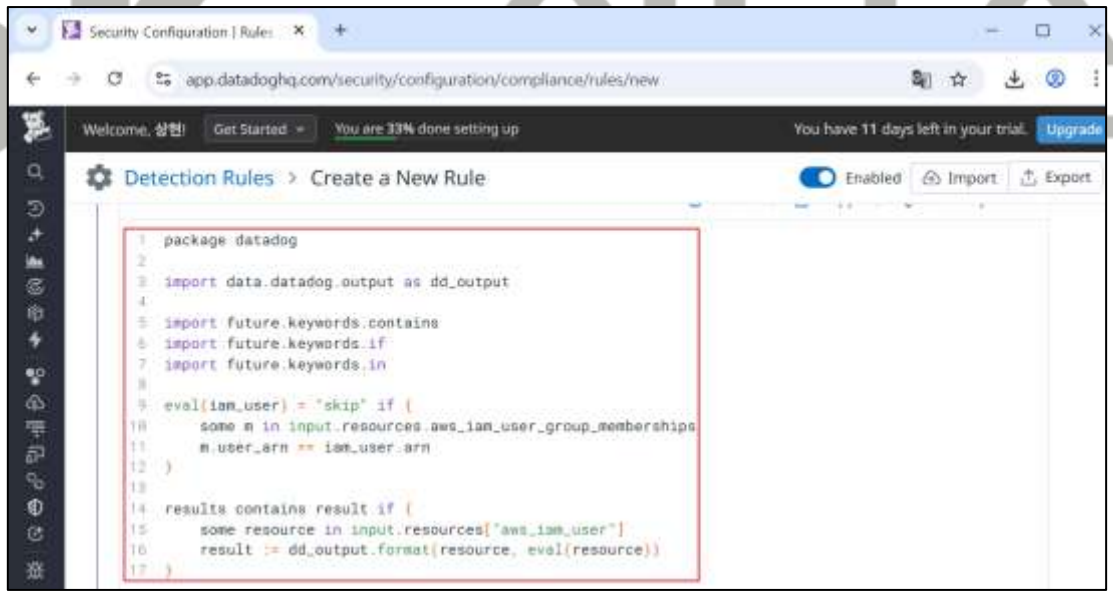
※ IAM 사용자에게 더이상 필요하지 않은 그룹이 사용중인 경우 개별 확인 필요

1) IAM -> 엑세스 관리 -> 사용자 그룹 -> 사용자 선택

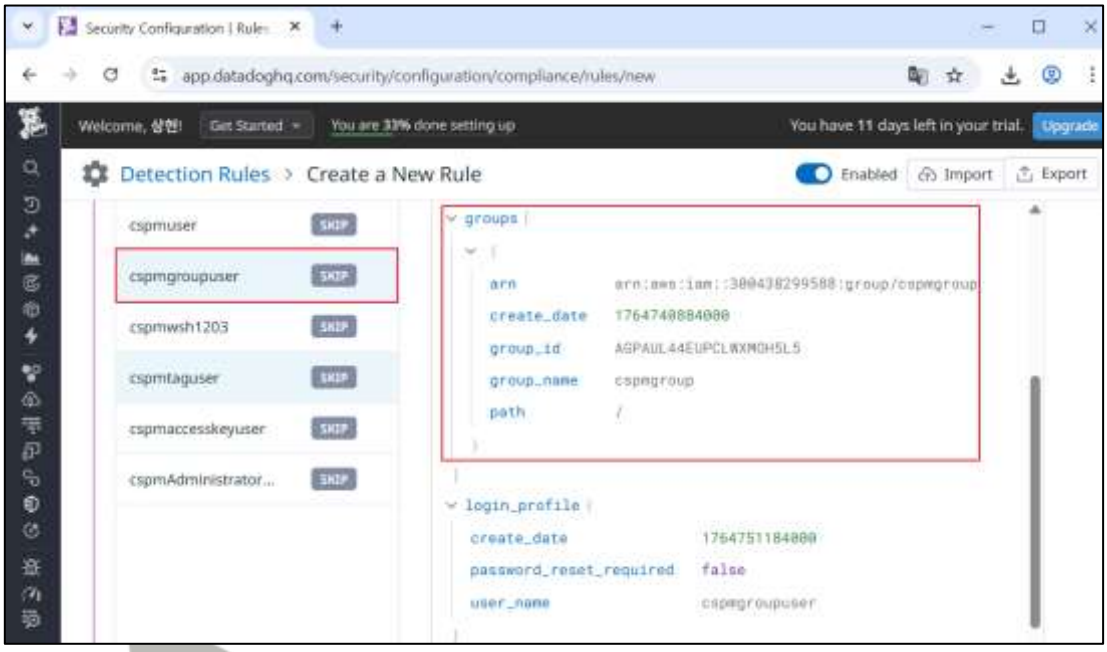


2) 그룹 탭 내 사용중인 그룹 확인

3) Datadog Detection Rule 추가

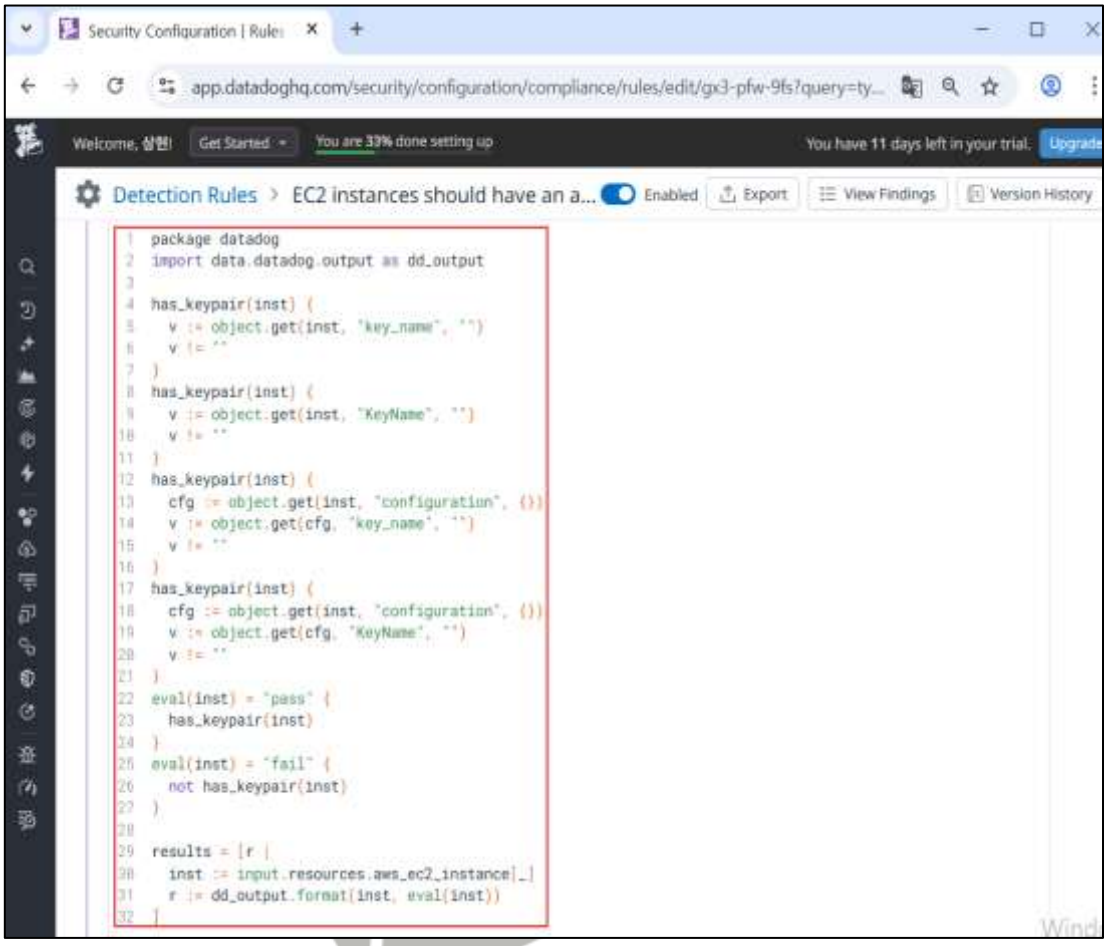


4) Datadog Detection Rule 탐지 결과 확인

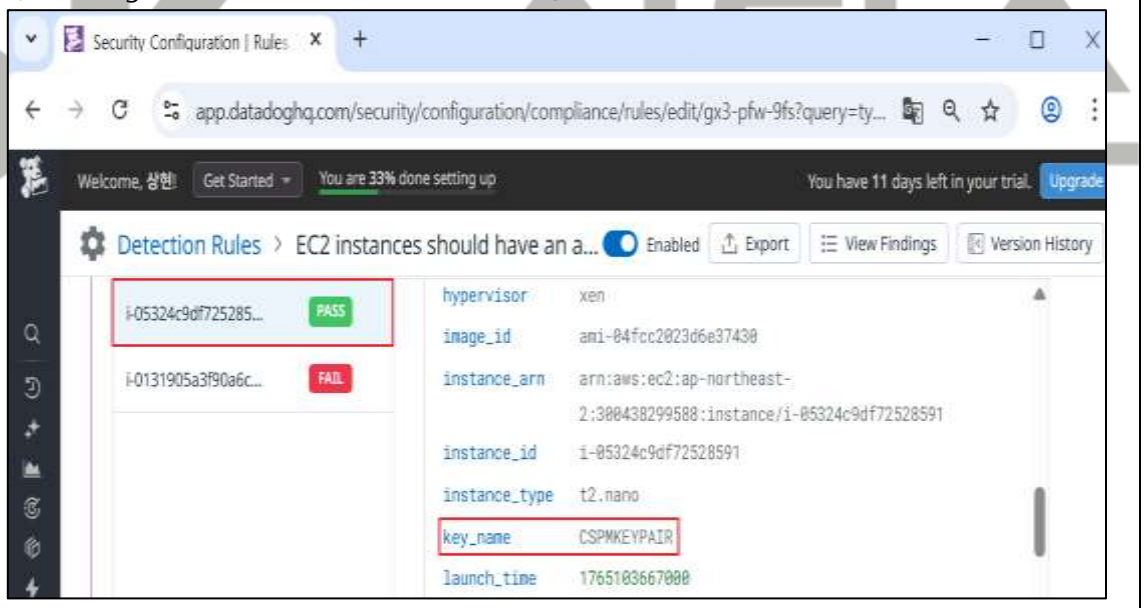
	
탐지 기준	**def-000-ysz** : AWS IAM 그룹에 사용자가 연결되어 있지 않을 경우 **커스텀** : AWS IAM 그룹에 소속된 계정이 존재하는 경우
비고	기술 공식 문서 : https://docs.datadoghq.com/ko/security/default_rules/def-000-ysz/

1.5 Key Pair 접근 관리

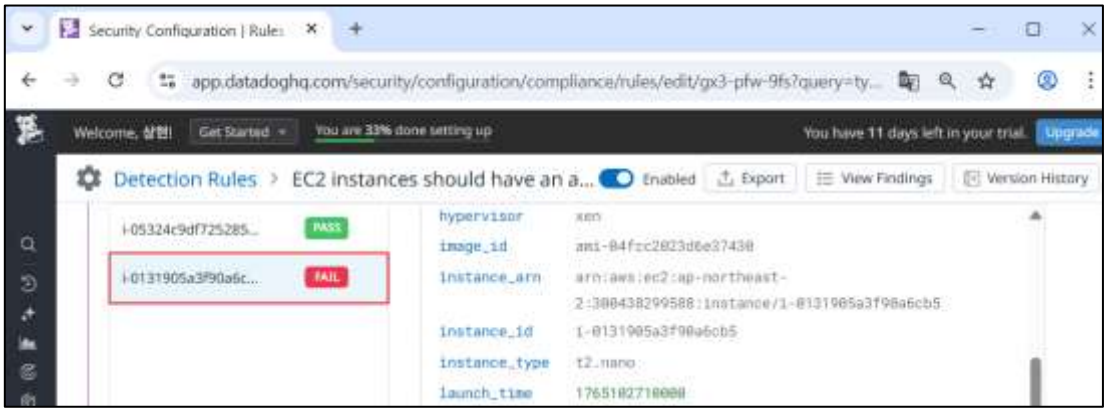
분류	계정 관리	중요도	상
항목명	Key Pair 접근 관리		
항목 설명	EC2는 키(Key)를 이용한 암호화 기법을 제공합니다. 해당 기법은 퍼블릭/프라이빗 키를 통해 각각 데이터의 암호화 및 해독을 하는 방식으로 여기에 사용되는 키를 'Key Pair' 라고 하며, 해당 암호화 기법을 사용할 시 EC2의 보안성을 향상시킬 수 있으므로 EC2 인스턴스 생성 시 Key Pair 등록을 권장합니다. 또한, Amazon EC2에 사용되는 키는 '2048비트 SSH-2 RSA 키'이며, Key Pair는 리전당 최대 5천 개까지 보유할 수 있습니다.		
설정 방법	**가. KeyPair가 없는 EC2 인스턴스 (MEDIUM)** 1) EC2 -> 인스턴스 -> 인스턴스 -> 인스턴스 시작  2) 키 페어 설정 부재 확인  3) Datadog Detection Rule 추가		



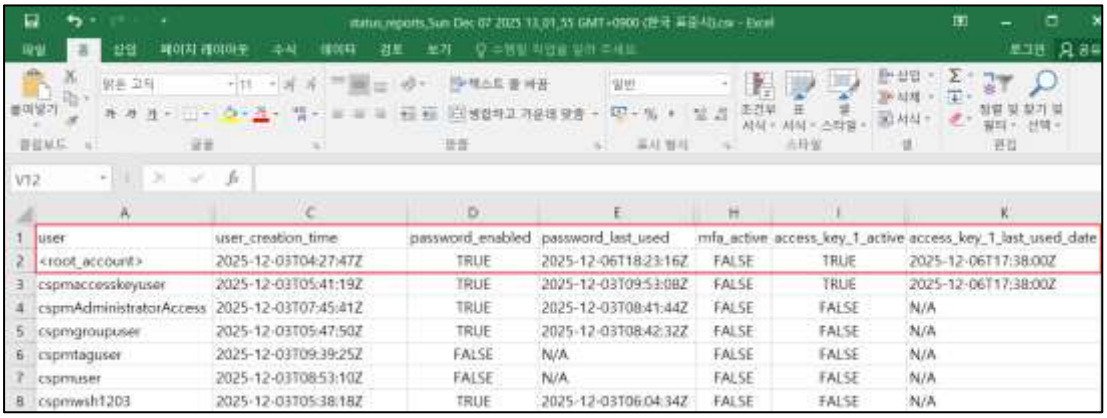
4) Datadog Detection Rule 탐지 결과 확인 ①



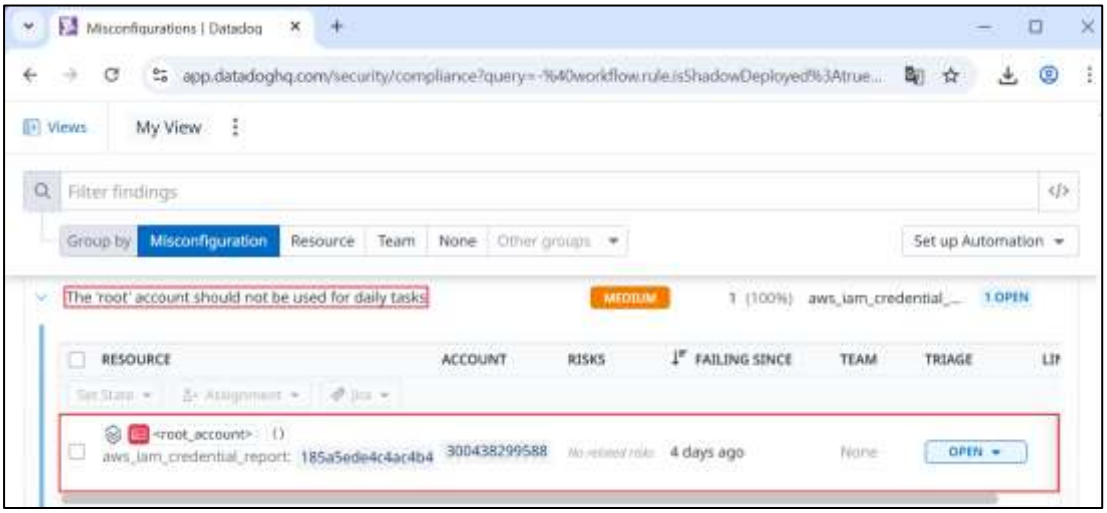
5) Datadog Detection Rule 탐지 결과 확인 ②

	
탐지 기준	**커스텀** : EC2 인스턴스에 할당된 키 페어가 존재하지 않는 경우
비고	기술 공식 문서 : 없음

1.6 Admin Console 관리자 정책 관리

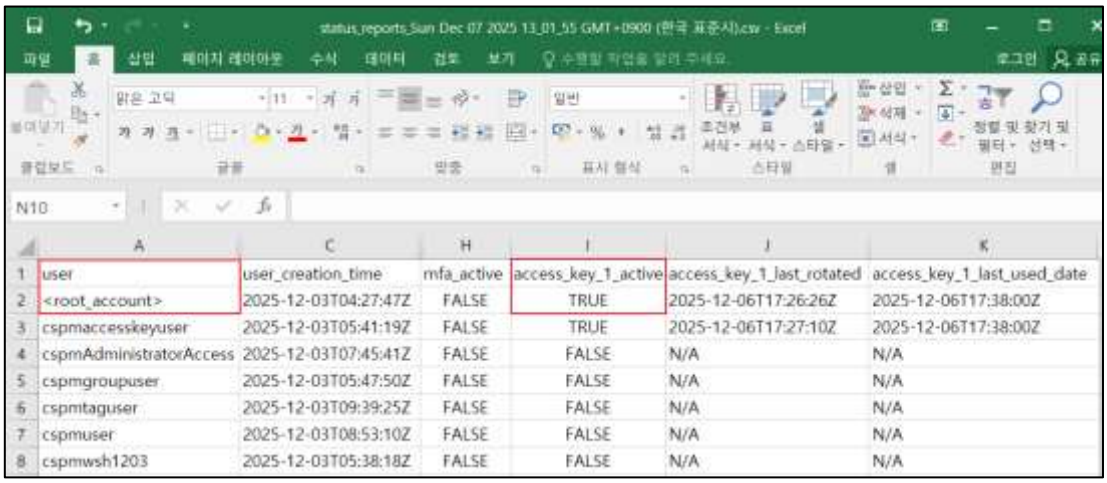
분류	권한 관리	중요도	중
항목명	Admin Console 관리자 정책 관리		
항목 설명	AWS Cloud 사용을 위해 처음 발급한 계정은 IAM 사용자 계정과 달리 모든 서비스에 접근할 수 있는 최고 관리자 계정입니다. Cloud 서비스 특성 상 인터넷 연결이 가능한 망에서 계정정보를 입력하여 WEB Console에 접근하게 됩니다. 이는 최고 권한을 보유하고 있는 관리자 계정이 아닌 권한이 조정된 IAM 사용자 계정을 기본으로 사용해야 보다 안전한 접근이 이뤄질 수 있습니다. AWS 계정을 생성하면 비활성화하거나 삭제할 수 없는 루트 사용자가 설정됩니다. 이 사용자는 계정의 모든 리소스에 대한 무제한 액세스 및 제어 권한을 갖습니다. 루트 사용자의 무제한 접근 권한은 최소 권한 및 업무 분리 원칙에 위배되며, 오류가 계정 침해로 인해 불필요한 피해를 초래할 수 있습니다.		
설정 방법	**가. 루트 계정을 기본 기능으로 사용하지 않아야 함 (MEDIUM)** 1) IAM -> 보고서 엑세스 -> 자격 증명 보고서 -> 보안 인증 보고서 다운로드  2) 루트 사용자 사용 기록 확인  3) Datadog Misconfiguration 탐지 확인		

	A	C	D	E	H	I	K
1	user	user_creation_time	password_enabled	password_last_used	mfa_active	access_key_1_active	access_key_1_last_used_date
2	<root_account>	2025-12-03T04:27:47Z	TRUE	2025-12-06T18:23:16Z	FALSE	TRUE	2025-12-06T17:38:00Z
3	cspmaccesskeyuser	2025-12-03T05:41:19Z	TRUE	2025-12-03T09:53:08Z	FALSE	TRUE	2025-12-06T17:38:00Z
4	cspmAdministratorAccess	2025-12-03T07:45:41Z	TRUE	2025-12-03T08:41:44Z	FALSE	FALSE	N/A
5	cspmgroupuser	2025-12-03T05:47:50Z	TRUE	2025-12-03T08:42:32Z	FALSE	FALSE	N/A
6	cspmtaguser	2025-12-03T09:39:25Z	FALSE	N/A	FALSE	FALSE	N/A
7	cspmuser	2025-12-03T08:53:10Z	FALSE	N/A	FALSE	FALSE	N/A
8	cspmwsh1203	2025-12-03T05:38:18Z	TRUE	2025-12-03T06:04:34Z	FALSE	FALSE	N/A

	
탐지 기준	**v9v-uhp-uk5** : 루트 계정을 비밀번호 또는 Access Key를 통해 30일 이내 사용할 경우
비고	기술 공식 문서 : https://docs.datadoghq.com/security/default_rules/v9v-uhp-uk5/

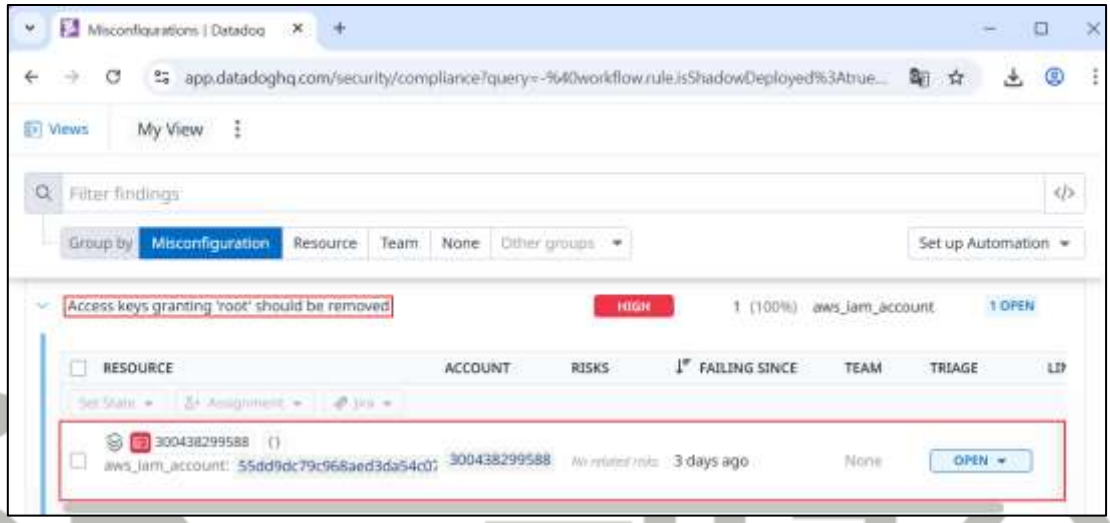
1.7 Admin Console 계정 Access Key 활성화 및 사용주기 관리

분류	계정 관리	중요도	상
항목명	Admin Console 계정 Access Key 활성화 및 사용주기 관리		
항목 설명	Access Key는 AWS의 CLI 도구나 API를 사용할 때 필요한 인증수단으로 생성 사용자에 대한 결제정보를 포함한 모든 AWS 서비스의 전체 리소스에 대한 권한을 갖고있으므로 유출 시 심각한 피해가 발생할 가능성이 높기에 AWS Admin Console Account에 대한 Access Key 삭제를 권장합니다. 루트 계정은 AWS 계정에서 가장 권한이 높은 사용자이며, AWS Access Key는 이 계정에 대한 프로그래밍 방식 액세스를 제공합니다. 보안강화를 위해 루트 계정과 연결된 모든 액세스 키를 제거 할 것을 권장합니다. Access Key는 Access Key ID와 비밀 Access Key로 구성되며, AWS에 대한 프로그래밍 요청에 서명하는데 사용됩니다. AWS 사용자는 AWS CLI, Windows PowerShell 도구, AWS SDK 또는 개별 AWS 서비스용 API를 사용한 직접 HTTP 호출을 사용하여 작업을 수행하려면 자체 Access Key가 필요합니다. 보안을 유지하기 위해서는 모든 Access Key를 정기적으로 교체하는 것이 중요합니다. **※ Access Key 관리 주기** Key 수명(60일 이내), 비밀번호 수명(60일 이내), 마지막 활동(30일 이내)		
설정 방법	**가. 루트 계정 권한을 부여하는 Access Key는 삭제되어야 함 (HIGH)** 1) IAM -> 보고서 엑세스 -> 자격 증명 보고서 -> 보안 인증 보고서 다운로드  2) 루트 사용자 Access Key 활성화 기록 확인		



	A	C	H	I	J	K
1	user	user_creation_time	mfa_active	access_key_1_active	access_key_1_last_rotated	access_key_1_last_used_date
2	<root_account>	2025-12-03T04:27:47Z	FALSE	TRUE	2025-12-06T17:26:26Z	2025-12-06T17:38:00Z
3	cspmaccesskeyuser	2025-12-03T05:41:19Z	FALSE	TRUE	2025-12-06T17:27:10Z	2025-12-06T17:38:00Z
4	cspmAdministratorAccess	2025-12-03T07:45:41Z	FALSE	FALSE	N/A	N/A
5	cspmgroupuser	2025-12-03T05:47:50Z	FALSE	FALSE	N/A	N/A
6	cspmtaguser	2025-12-03T09:39:25Z	FALSE	FALSE	N/A	N/A
7	cspmuser	2025-12-03T08:53:10Z	FALSE	FALSE	N/A	N/A
8	cspmwsh1203	2025-12-03T05:38:18Z	FALSE	FALSE	N/A	N/A

3) Datadog Misconfiguration 탐지 확인

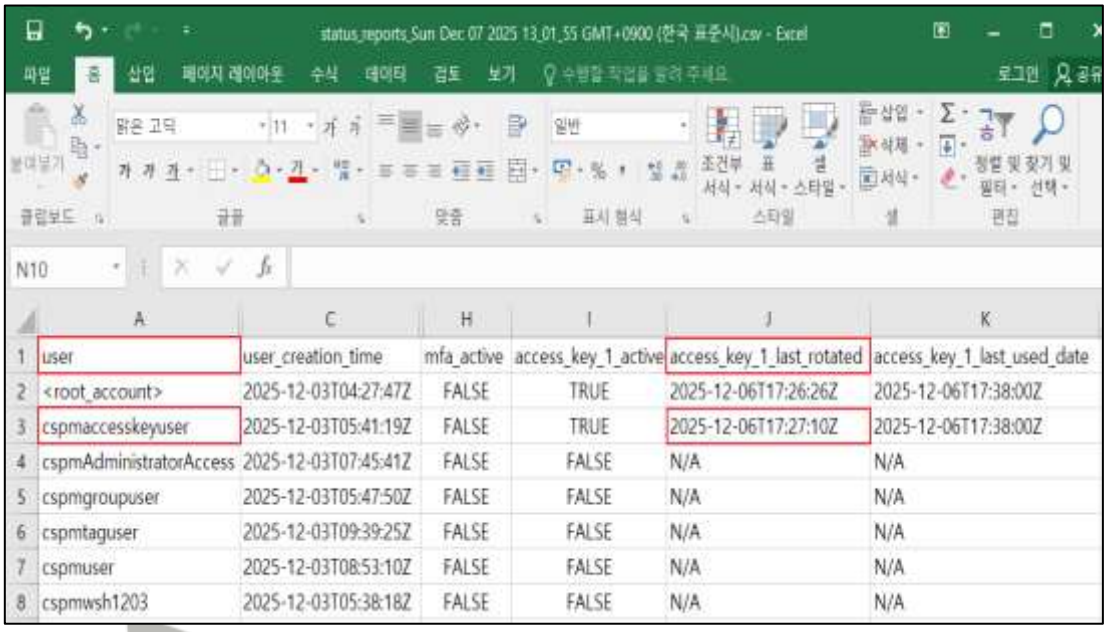


나. Access Key는 90일 이내에 교체되어야 함 (MEDIUM)

※ Access Key는 내부 정책 및 보안 수준에 따라 커스텀 사용 권고

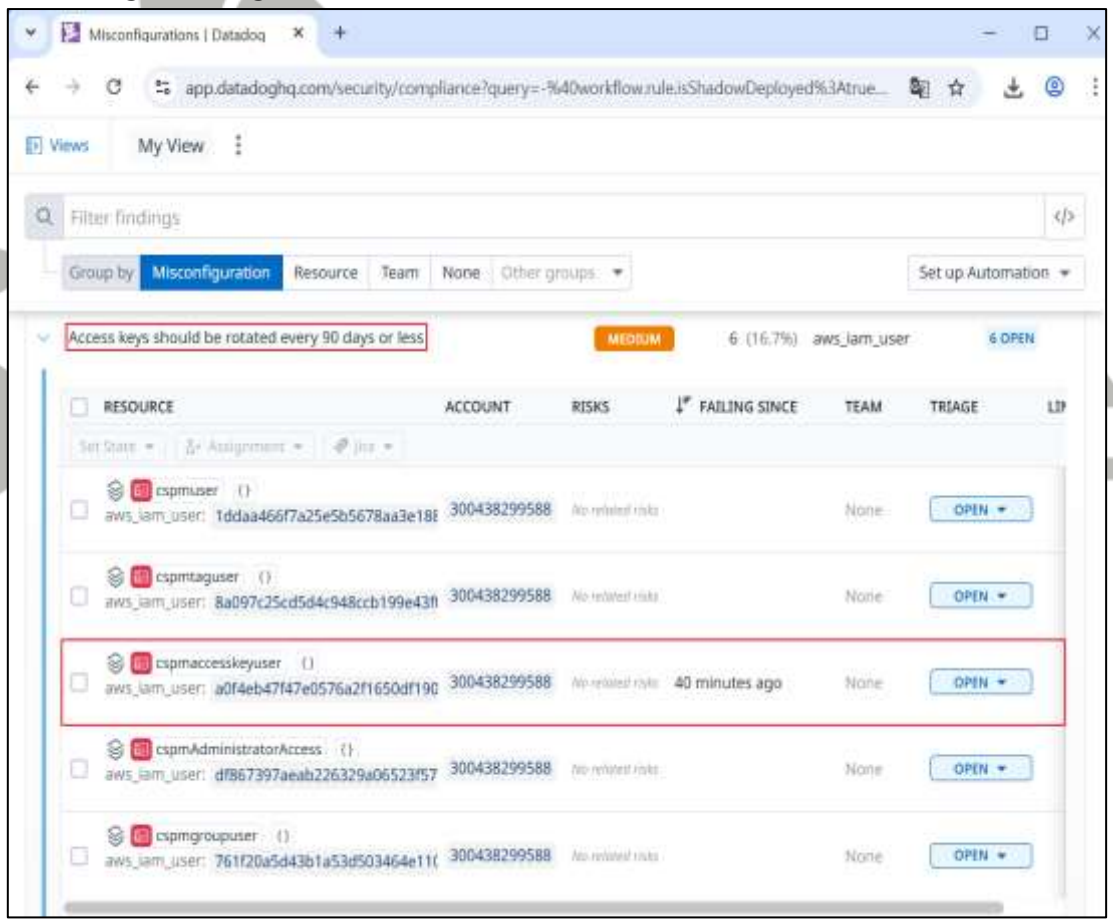
1) IAM -> 보고서 엑세스 -> 자격 증명 보고서 -> 보안 인증 보고서 다운로드

2) IAM 사용자 Access Key 재발급 기록 확인



	A	C	H	I	J	K
1	user	user_creation_time	mfa_active	access_key_1_active	access_key_1_last_rotated	access_key_1_last_used_date
2	<root_account>	2025-12-03T04:27:47Z	FALSE	TRUE	2025-12-06T17:26:26Z	2025-12-06T17:38:00Z
3	cspmaccesskeyuser	2025-12-03T05:41:19Z	FALSE	TRUE	2025-12-06T17:27:10Z	2025-12-06T17:38:00Z
4	cspmAdministratorAccess	2025-12-03T07:45:41Z	FALSE	FALSE	N/A	N/A
5	cspmgroupuser	2025-12-03T05:47:50Z	FALSE	FALSE	N/A	N/A
6	cspmtaguser	2025-12-03T09:39:25Z	FALSE	FALSE	N/A	N/A
7	cspmuser	2025-12-03T08:53:10Z	FALSE	FALSE	N/A	N/A
8	cspmwsh1203	2025-12-03T05:38:18Z	FALSE	FALSE	N/A	N/A

3) Datadog Misconfiguration 탐지 확인

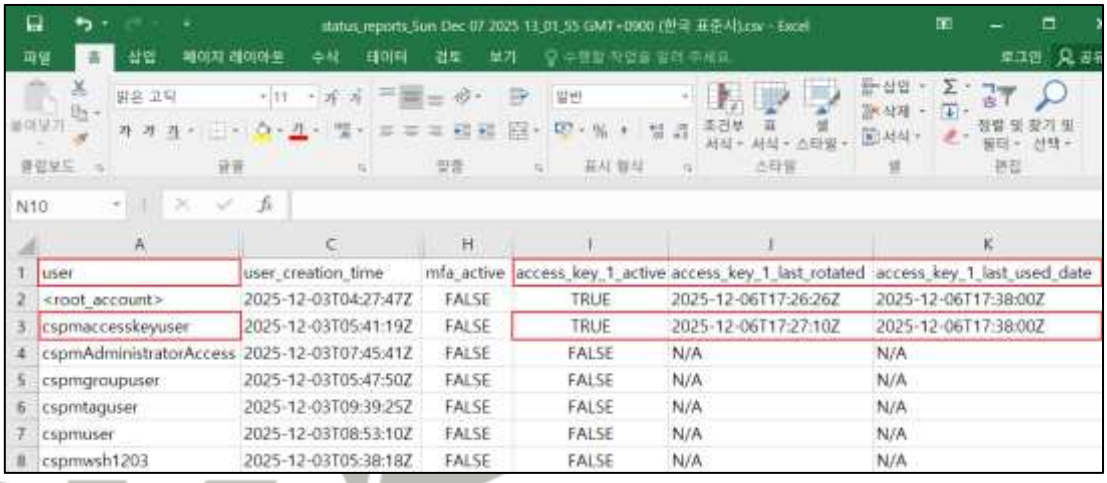


다. 장기 미사용된 Access Key는 365일 이내에 교체되어야 함 (MEDIUM)

※ Access Key는 내부 정책 및 보안 수준에 따라 커스텀 사용 권고

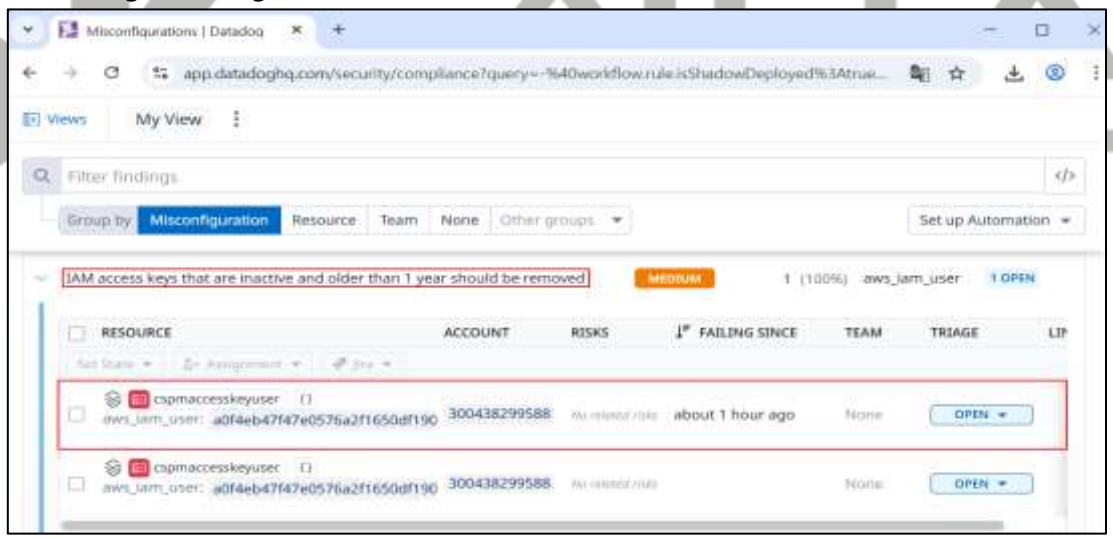
1) IAM -> 보고서 엑세스 -> 자격 증명 보고서 -> 보안 인증 보고서 다운로드

2) IAM 사용자 Access Key 재발급 기록 확인



user	user_creation_time	mfa_active	access_key_1_active	access_key_1_last_rotated	access_key_1_last_used_date
<root_account>	2025-12-03T04:27:47Z	FALSE	TRUE	2025-12-06T17:26:26Z	2025-12-06T17:38:00Z
cspmaccesskeyuser	2025-12-03T05:41:19Z	FALSE	TRUE	2025-12-06T17:27:10Z	2025-12-06T17:38:00Z
cspmAdministratorAccess	2025-12-03T07:45:41Z	FALSE	FALSE	N/A	N/A
cspmgroupuser	2025-12-03T05:47:50Z	FALSE	FALSE	N/A	N/A
cspmtaguser	2025-12-03T09:39:25Z	FALSE	FALSE	N/A	N/A
cspmuser	2025-12-03T08:53:10Z	FALSE	FALSE	N/A	N/A
cspmwsh1203	2025-12-03T05:38:18Z	FALSE	FALSE	N/A	N/A

3) Datadog Misconfiguration 탐지 확인



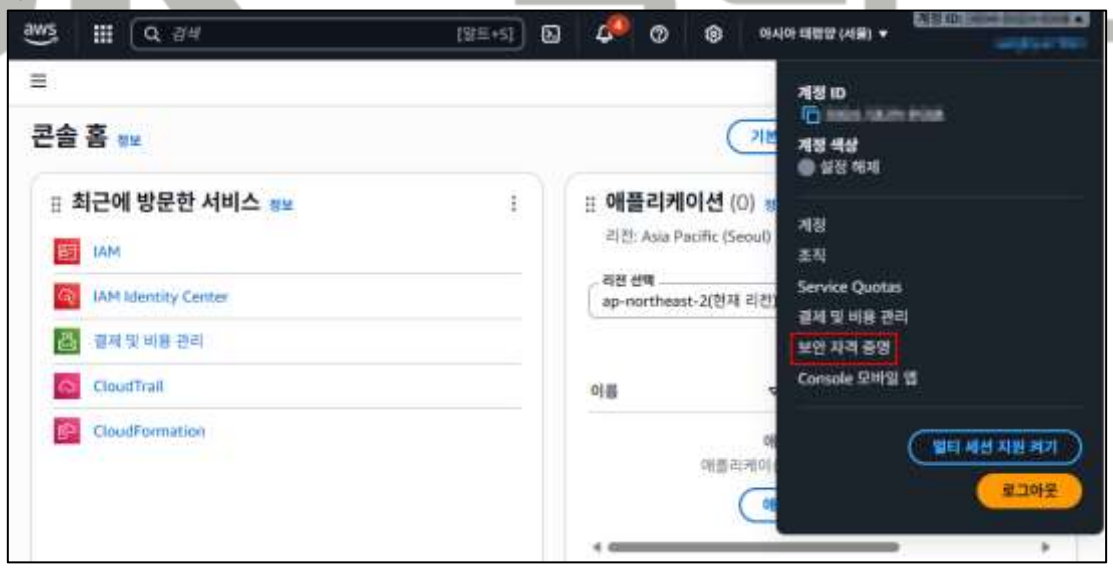
탐지 기준	**ee4-ngx-bwr** : 루트 계정에 Access Key가 활성화되어 있을 경우 **bcz-prk-dr6** : 발급된 Access Key가 90일을 초과하고 있을 경우 **r1s-kud-79s** : 30일 이내 Access Key가 사용되지 않고, 재발급 시점이 365일이 경과한 경우
비고	기술 공식 문서 :

	https://docs.datadoghq.com/security/default_rules/ee4-ngx-bwr/ https://docs.datadoghq.com/security/default_rules/bcz-prk-dr6/ https://docs.datadoghq.com/security/default_rules/r1s-kud-79s/

1.8 MFA (Multi-Factor Authentication) 설정

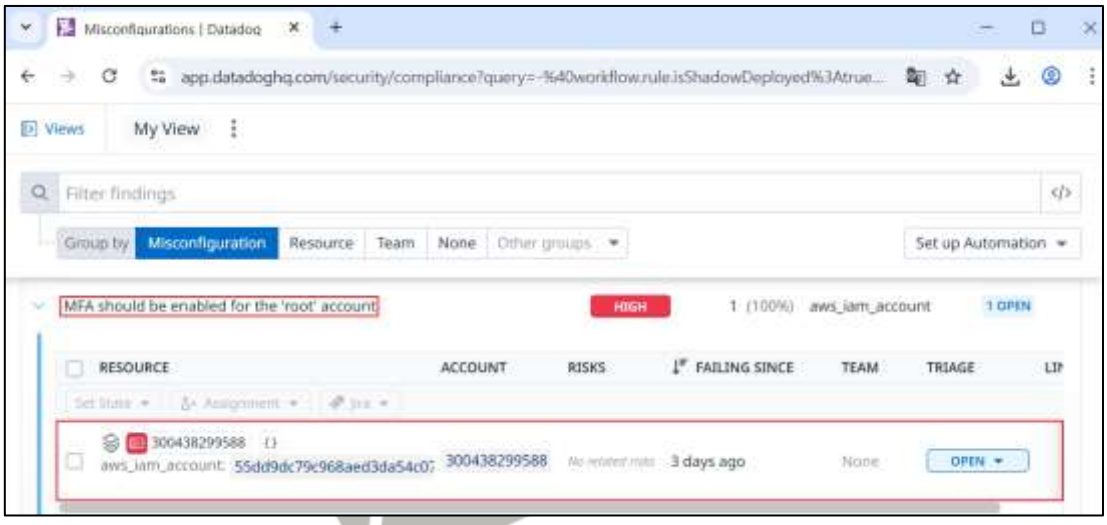
<table>
<tr><td>분류</td><td>계정 관리</td><td>중요도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">MFA (Multi-Factor Authentication) 설정</td></tr>
<tr><td>항목
설명</td><td colspan="3">AWS Multi-Factor Authentication(MFA)은 사용자 이름과 암호 외에 보안을 한층 더 강화할 수 있는 방법으로 MFA를 활성화하면 사용자가 AWS 웹 사이트에 로그인할 때 사용자 이름과 암호뿐만 아니라 AWS MFA 디바이스의 인증 응답을 입력하라는 메시지가 표시됩니다. 이러한 다중 요소를 통해 AWS 계정 설정 및 리소스에 대한 보안을 높일 수 있습니다.

루트 계정은 AWS 계정에서 가장 권한이 높은 사용자입니다. MFA는 사용자 이름과 비밀번호 외에 추가적인 보안 계층을 제공합니다. MFA를 활성화하면 인증 주체가 시간 제한 키를 생성하는 디바이스를 소유하고 자격 증명을 알고 있어야 하므로 콘솔 액세스 보안이 강화됩니다. 또한 AWS에서 중앙 집중식 루트 관리가 활성화된 경우 루트 사용자에 대한 MFA가 적용되지 않습니다.

(*) 계정 종류
<table>
<tr><th>계정 구분</th><th>Description</th><th>확인 필요 사항</th></tr>
<tr><td>Console Admin</td><td>최고 권한을 가지고 있는 단일 계정</td><td>가급적 사용을 지양해야 함</td></tr>
<tr><td>IAM</td><td>AWS IAM 서비스를 통해 생성된 별도 계정</td><td>IAM 역할 및 권한에 대한 현황을 확인해야 함</td></tr>
</table>
※ 기존 내부 AD(Active Directory) 서버를 AWS Organizations 서비스와 연동해서 SSO(Single Sign On)을 활성화하여 사용할 경우 양호로 처리될 수 있음</td></tr>
<tr><td>설정
방법</td><td colspan="3">가. '루트' 계정에 MFA를 활성화해야 함 (HIGH)
1) 보안 자격 증명
 

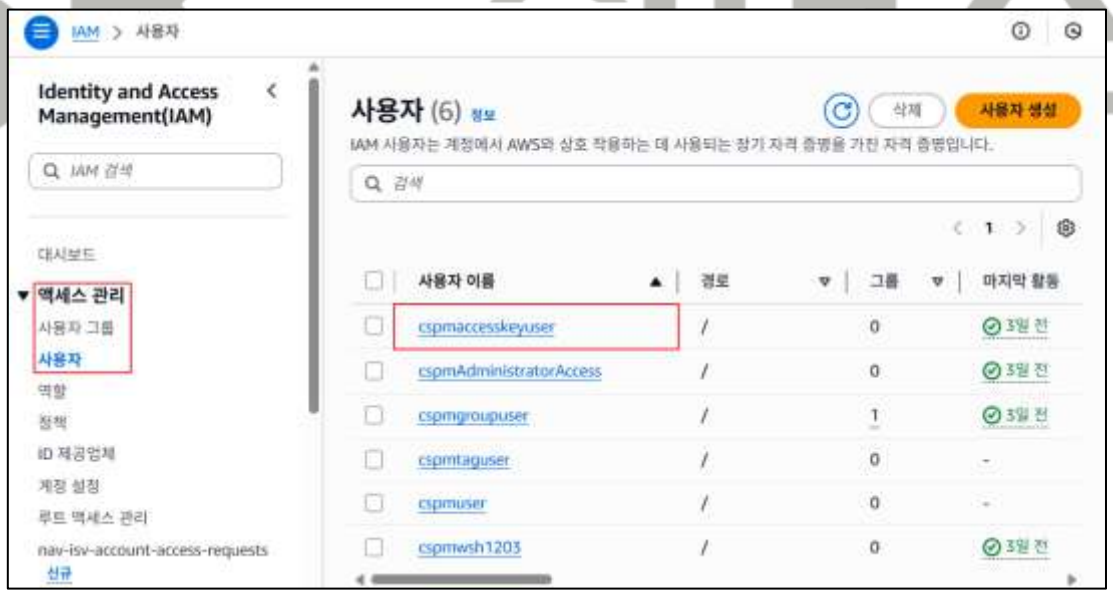
2) 멀티 팩터 인증 비활성화 확인</td></tr>
</table>

3) Datadog Misconfiguration 탐지 확인

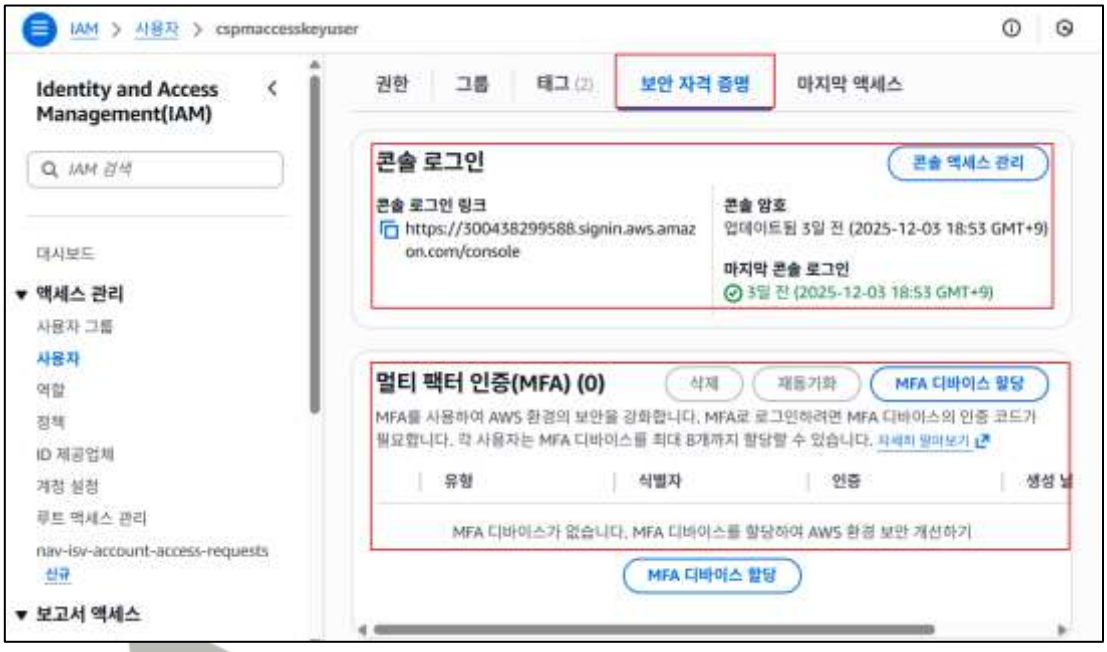


나. 콘솔 액세스 권한이 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 함 (HIGH)

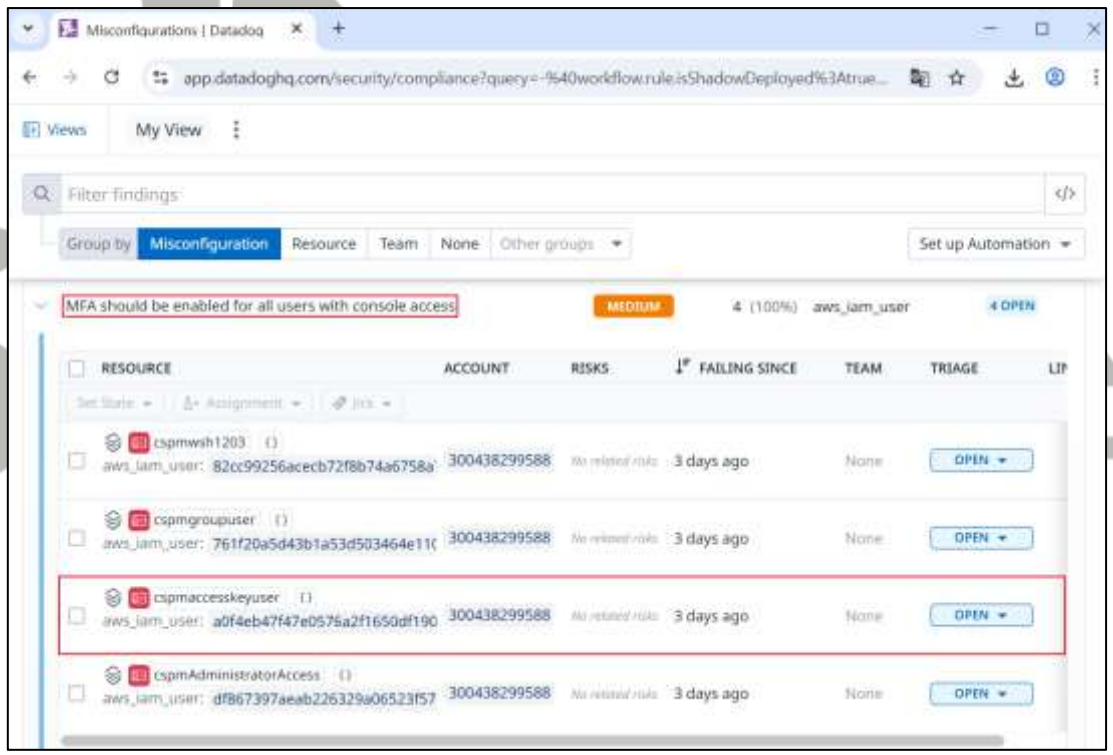
1) IAM -> 엑세스 관리 -> 사용자 -> 사용자 선택



2) 보안 자격 증명 내 콘솔 로그인 활성화 및 멀티 팩터 인증 비활성화 확인



3) Datadog Misconfiguration 탐지 확인



탐지 기준	**8yh-cqk-qbn** : 루트 계정에 MFA가 비활성화되어 있을 경우 **hsh-y5w-hxe** : 콘솔 로그인이 활성화된 IAM 계정에 MFA가 비활성화되어 있을 경우
비고	기술 공식 문서 : https://docs.datadoghq.com/security/default_rules/8yh-cqk-qbn/ https://docs.datadoghq.com/security/default_rules/hsh-y5w-hxe/

1.9 AWS 계정 패스워드 정책 관리

분류	계정 관리	중요도	중
항목명	AWS 계정 패스워드 정책 관리		

항목 설명

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.

<패스워드 설정 기준>

1) 패스워드는 아래의 4가지 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성
 * 영문 대문자(26개), 영문 소문자(26개), 숫자(10개), 특수문자(32개)

<패스워드는 비인가자에 의한 추측이 어렵도록 다음의 사항을 반영하여 설계해야 함>

1) Null 패스워드 사용 금지
2) 문자 또는 숫자만으로 구성 금지
3) 사용자 ID와 동일한 패스워드 금지
4) 연속적인 문자 및 숫자 사용 금지
5) 주기성 패스워드 사용 금지
6) 전화번호, 생일, 계정명, hostname과 같이 추측하기 쉬운 패스워드 사용 금지

1) 패스워드 최소길이
패스워드 추측공격을 피하기 위하여 패스워드 최소길이가 설정되어 있는지 점검함
패스워드 최소길이가 설정되어 있지 않거나 짧게 설정되어 있을 경우 취약한 패스워드를 사용함으로 인해 악의적인 사용자가 패스워드를 쉽게 유추 할 수 있음

2) 패스워드 최대 사용기간
패스워드가 임의의 경로를 통해 유출되었을 때, 임의로 접속한 사용자가 언제든 다시 접속할 수 있는 환경을 방지하기 위해 패스워드 날짜 제한을 점검함

3) 패스워드 최소 사용기간
패스워드가 임의의 경로를 통해 유출되었을 때, 임의로 접속한 사용자가 언제든 다시 접속할 수 있는 환경을 방지하기 위해 패스워드 날짜 제한을 점검함

4) 이전 패스워드 기억
이전에 사용하였던 패스워드를 기억하여 패스워드 변경 시 기존에 사용하였던 패스워드 재사용 금지
- 패스워드 길이는 8자 이상 설정하는 것을 권고
- 패스워드 최대 사용 기간을 60일 이하로 설정할 것을 권고
- 패스워드 최소 사용 기간을 1일 이상으로 설정할 것을 권고

5) 암호 만료 활성화 및 재사용 제한
- 암호 만료 활성화, 암호 만료일은 90일 이하여야 함
- 암호 재사용 제한 최소 1개 이상이어야 함

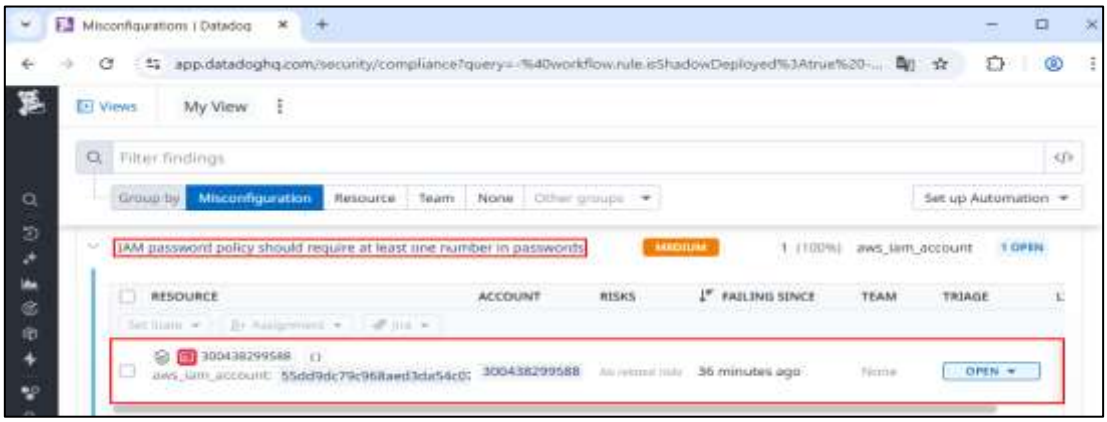
설정 방법

가. IAM 비밀번호 정책은 숫자를 하나 이상 요구해야 함 (MEDIUM)

1) IAM -> 엑세스 관리 -> 계정 설정-> 암호 정책 -> 편집

2) 암호 강도 설정 확인

3) Datadog Misconfiguration 탐지 확인

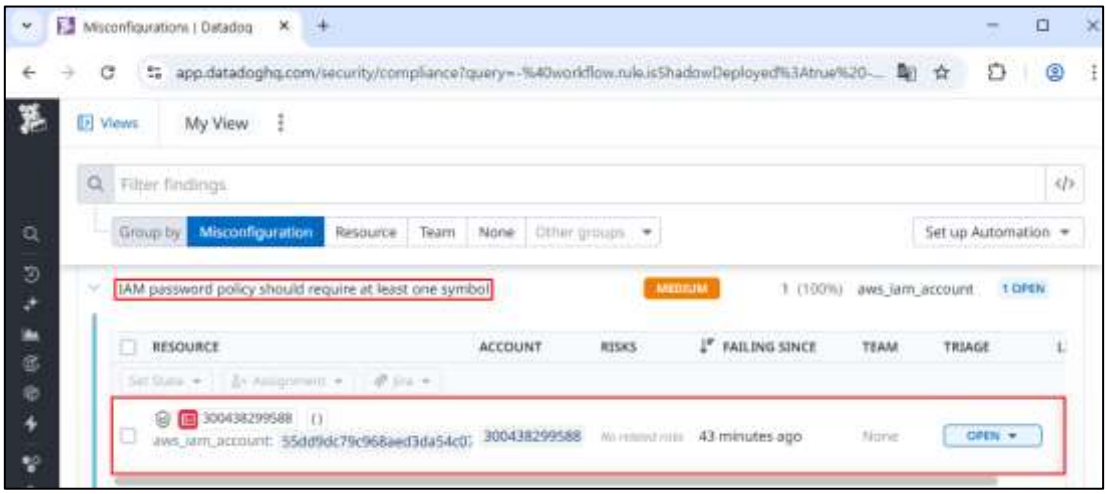


나. IAM 비밀번호 정책은 기호를 하나 이상 요구해야 함 (MEDIUM)

1) IAM -> 엑세스 관리 -> 계정 설정-> 암호 정책 -> 편집

2) 암호 강도 설정 확인

3) Datadog Misconfiguration 탐지 확인

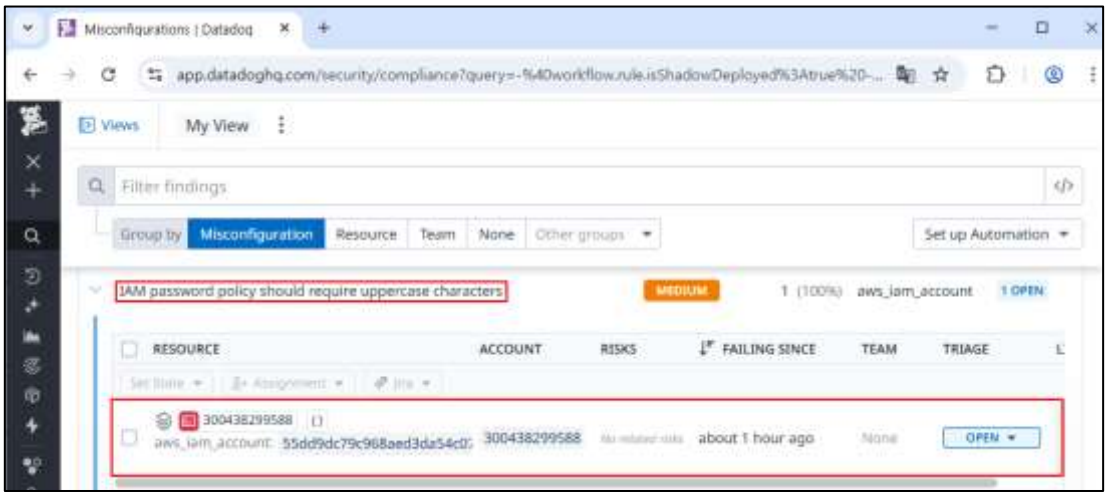


다. IAM 비밀번호 정책은 대문자가 필요함 (MEDIUM)

1) IAM -> 엑세스 관리 -> 계정 설정-> 암호 정책 -> 편집

2) 암호 강도 설정 확인

3) Datadog Misconfiguration 탐지 확인



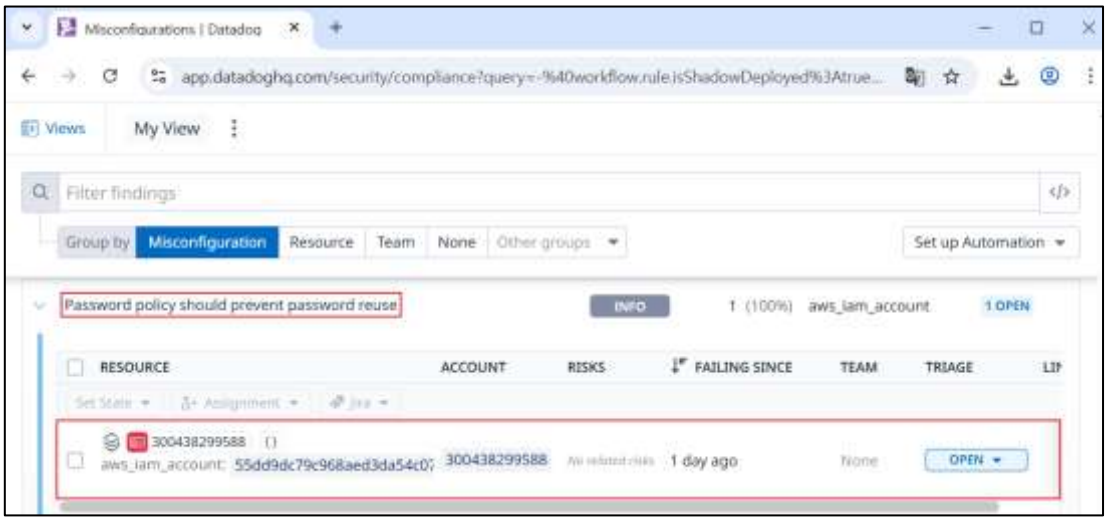
라. IAM 비밀번호 정책은 비밀번호 재사용을 방지해야 함 (INFO)

※ 암호 재사용 제한 횟수는 내부 정책 및 보안 수준에 따라 커스텀 사용 권고

1) IAM -> 엑세스 관리 -> 계정 설정-> 암호 정책 -> 편집

2) 암호 강도 설정 확인

3) Datadog Misconfiguration 탐지 확인

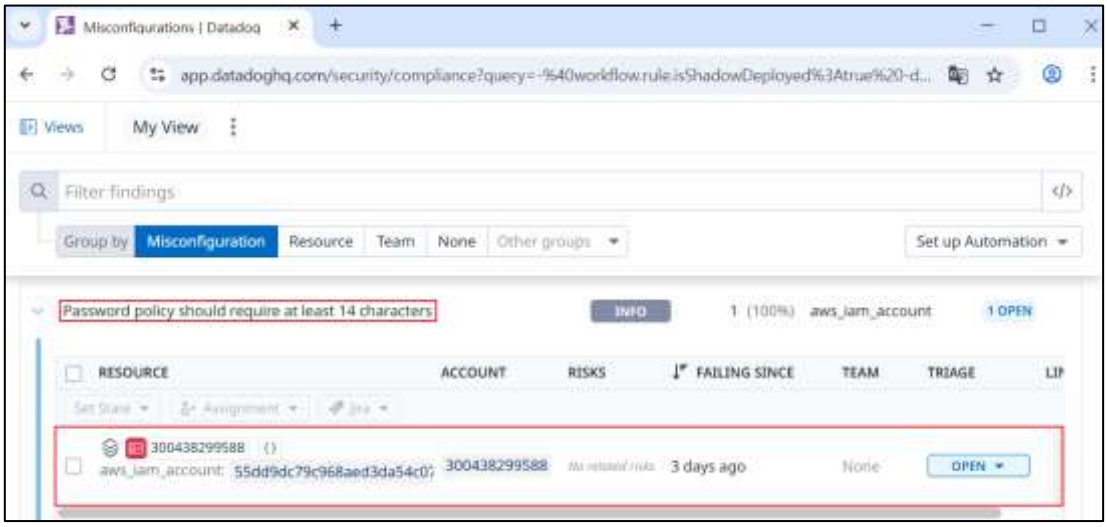


마. IAM 비밀번호 정책이 최소 14자 이상을 요구해야 함 (INFO)

1) IAM -> 엑세스 관리 -> 계정 설정-> 암호 정책 -> 편집

2) 암호 강도 설정 확인

3) Datadog Misconfiguration 탐지 확인

	
탐지 기준	**2mn-qgc-gka** : IAM 암호 정책에 "1개 이상의 숫자" 설정이 되어 있지 않은 경우 **r88-a34-ppx** : IAM 암호 정책에 "특수문자 1개 이상" 설정이 되어 있지 않은 경우 **ziw-w2v-e6z** : IAM 암호 정책에 "1개 이상의 알파벳 대문자" 설정이 되어 있지 않은 경우 **z23-f9p-six** : IAM 암호 정책에 직전 패스워드 사용을 검증하도록 설정이 되어 있지 않은 경우 **ayr-n9s-q87** : IAM 암호 정책에 "암호 최소 길이 14자 이상" 설정이 되어 있지 않은 경우
비고	기술 공식 문서 : https://docs.datadoghq.com/security/default_rules/2mn-qgc-gka/ https://docs.datadoghq.com/security/default_rules/r88-a34-ppx/ https://docs.datadoghq.com/security/default_rules/ziw-w2v-e6z/ https://docs.datadoghq.com/security/default_rules/z23-f9p-six/ https://docs.datadoghq.com/security/default_rules/ayr-n9s-q87/

2. 권한 관리

2.1 인스턴스 서비스 정책 관리

<table>
<tr><td>분류</td><td>권한 관리</td><td>중요도</td><td>상</td></tr>
<tr><td>항목명</td><td colspan="3">인스턴스 서비스 정책 관리</td></tr>
<tr><td>항목 설명</td><td colspan="3">AWS 인스턴스 서비스(EC2, RDS, S3 등)의 리소스 생성 또는 액세스 권한은 권한 정책에 따라 결정됩니다. 계정 관리자는 IAM 자격 증명(즉, 사용자, 그룹, 역할)에 권한 정책을 연결할 수 있으며 적절한 권한을 통한 서비스 관리가 이루어져야 합니다.

EC2 인스턴스는 공격자에게 인터넷에서 액세스 경로를 제공할 수 있는 인프라 내에 있는 경우 공개적으로 액세스가 가능합니다. EC2 인스턴스 역할은 EC2 인스턴스에서 실행되는 애플리케이션에 AWS API 접근 권한을 부여하는데 권한되는 방법입니다. 그러나 권한이 있는 IAM 역할에 연결된 EC2 인스턴스는 공격자가 인스턴스를 손상시킬 경우 전체 AWS 계정이 손상되는 위험이 발생할 수 있습니다.

1) 인스턴스 서비스 구분
<table>
<tr><th>서비스 구분</th><th>서비스 상세</th></tr>
<tr><td>EC2</td><td>가상 컴퓨팅 환경인 인스턴스를 제공하며 보안 및 네트워크 구성과 스토리지 관리가 가능함</td></tr>
<tr><td>ECS</td><td>Cluster에서 도커 컨테이너를 손쉽게 실행, 중지 및 관리 할 수 있게 해주는 컨테이너 관리가 가능함</td></tr>
<tr><td>ECR</td><td>컨테이너 이미지를 저장, 관리 및 배포 할 수 있게 지원하는 관리형 도커 레지스트리 서비스
레지스트리(이미지 레포지토리 생성 후 레포지토리에 이미지 저장), 사용자 권한 토큰(ECR 레지스트리 인증 시 Docker 클라이언트 활용)
레포지토리 정책(레포지토리 및 레포지토리 내 이미지에 대한 액세스 제어) 관리가 가능함</td></tr>
<tr><td>EKS</td><td>Kubernetes 제어 플레인을 설치하고 운영할 필요 없이 AWS에서 Kubernetes를 손쉽게 실행하도록 하는 관리형 서비스입니다.
Kubernetes는 컨테이너화된 애플리케이션의 배포, 조정 및 관리 자동화를 위한 오픈 소스 시스템임</td></tr>
<tr><td>EFS</td><td>AWS 클라우드 서비스와 온프레미스 리소스에서 사용할 수 있는 간단하고 확장 가능하며 탄력적인 완전 관리형 탄력적 NFS 파일 시스템</td></tr>
<tr><td>RDS</td><td>AWS 클라우드에서 관계형 데이터베이스를 더 쉽게 설치, 운영 및 확장할 수 있는 웹 서비스입니다. 이 서비스는 산업 표준 관계형 데이터베이스를 위한 경제적이고 크기 조절이 가능한 용량을 제공하고 공통 데이터베이스 관리 작업이 가능함</td></tr>
<tr><td>S3</td><td>Amazon Simple Storage Service(Amazon S3)는 인터넷용</td></tr>
</table>
</td></tr>
</table>

	스토리지입니다. Amazon S3을 사용하면 웹을 통해 언제 어디서든 원하는 양의 데이터를 저장하고 검색할 수 있습니다. 간편하고 직관적인 웹 인터페이스인 AWS Management 콘솔을 사용하여 이러한 작업을 수행할 수 있습니다.

(*) IAM 관리형 정책 권한 관리 List (예시)

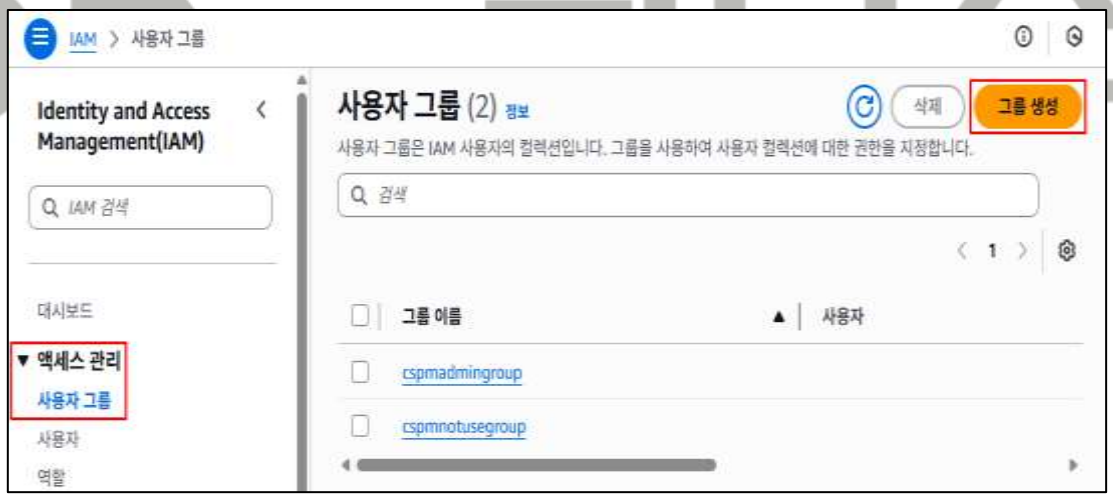
역할	계정 관리 (그룹 및 계정명)	AWS 관리형 정책	취약 유/무
AWS Admin Console 관리자	Ex)EC2_Admin (admin_accout)	Ex) EC2_Admin (AmazonC2FullAcces)	N/A
Infra 운영/관리자 및 담당자			N/A
Application 운영/관리자 및 담당자			N/A
개발 관리자 및 담당자			N/A
재무 / 비용 관리자 및 담당자			N/A

설정 방법

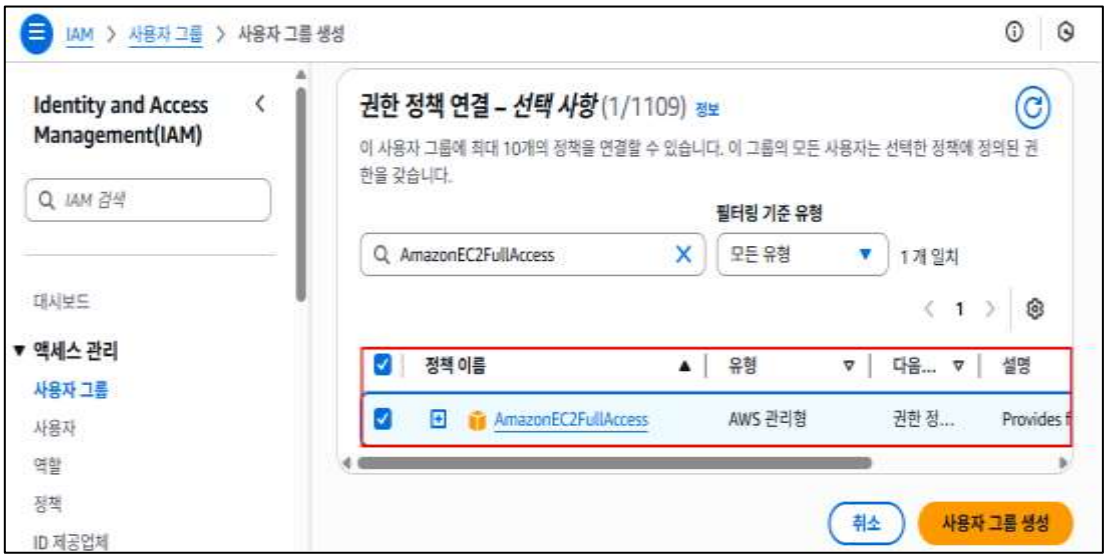
가. IAM 그룹/사용자/역할 인스턴스 권한 정책 관리 (HIGH)

※ 인스턴스 서비스 운영/관리에 필요한 IAMFullAccess 등의 권한과 같이 중요도가 높은 권한은 Infra 운영/관리자 및 담당자에게만 정책이 되도록 해야하며 최소한의 계정 수가 유지되어야 함

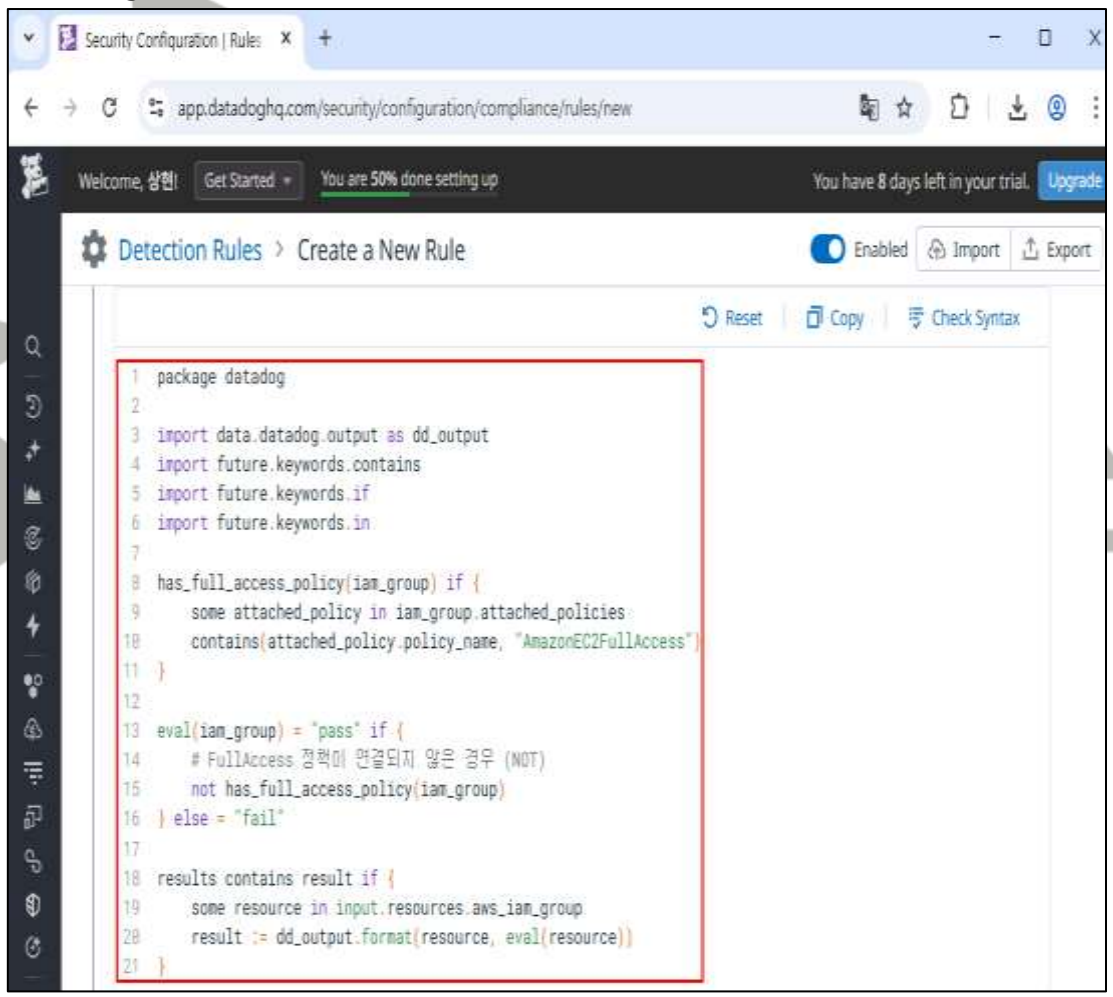
1) IAM -> 엑세스 관리 -> 사용자 -> 그룹 생성



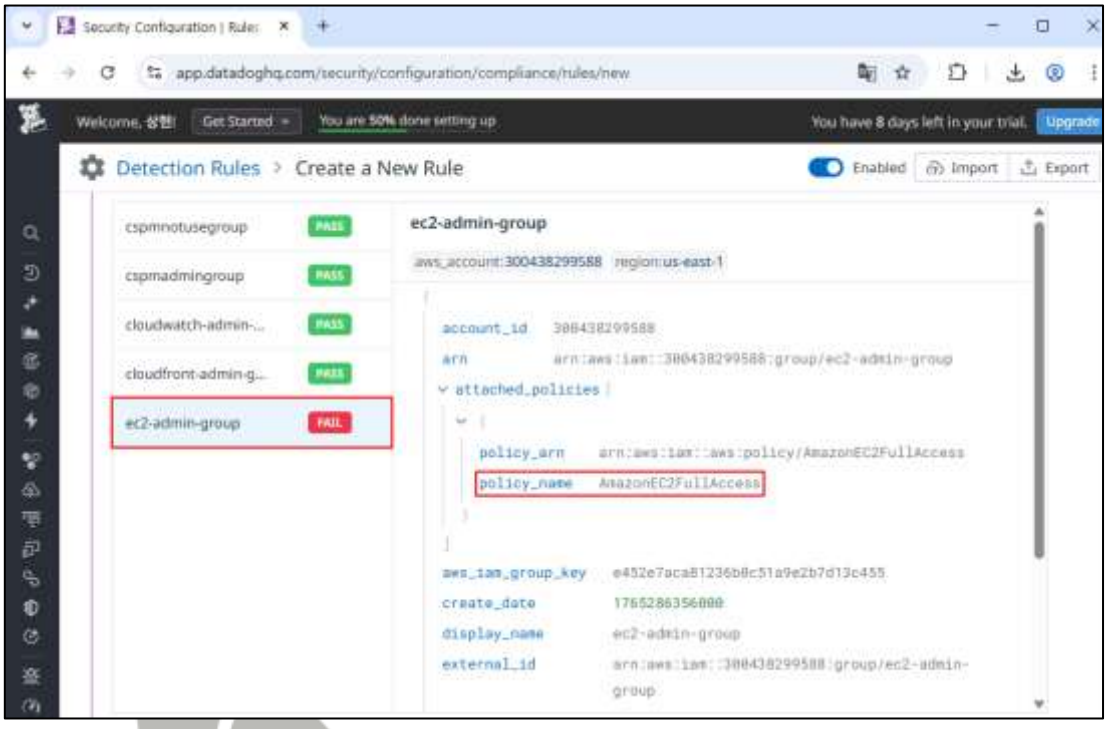
2) IAM 그룹 생성 시 "AmazoneEC2FullAccess" 정책 연결



3) Datadog Detection Rule 추가



4) Datadog Detection Rule 탐지 결과 확인

	
탐지 기준	**커스텀** : IAM 그룹/사용자/역할의 인스턴스 서비스 관리형 정책 연결 탐지
비고	

2.2 네트워크 서비스 정책 관리

분류	권한 관리	중요도	상
항목명	네트워크 서비스 정책 관리		

항목 설명

AWS 네트워크 서비스(VPC, Route 53, Direct Connect 등)의 리소스 생성 또는 액세스 권한은 권한 정책에 따라 결정됩니다. 계정 관리자는 IAM 자격 증명(즉, 사용자, 그룹, 역할)에 권한 정책을 연결할 수 있으며 적절한 권한을 통한 서비스 관리가 이루어져야 합니다.

1) 네트워크 서비스 구분

서비스 구분	서비스 상세
VPC	사용자가 정의한 가상 네트워크로 AWS 리소스를 시작할 수 있습니다. 이 가상 네트워크는 AWS의 확장 가능한 인프라를 사용한다는 이점과 함께 고객의 자체 데이터 센터에서 운영하는 기존 네트워크와 매우 유사합니다.
CloudFront	.html, .css, .js 및 이미지 파일과 같은 정적 및 동적 웹 콘텐츠를 사용자에게 더 빨리 배포하도록 지원하는 웹 서비스
Route 53	가용성과 확장성이 우수한 DNS(도메인 이름 시스템) 웹 서비스입니다. Route 53을 사용하여 세 가지 주요 기능, 즉 도메인 등록, DNS 라우팅, 상태 확인을 조합하여 실행할 수 있는 서비스
API Gateway	규모와 상관없이 REST 및 WebSocket API를 생성, 게시, 유지하고 모니터링 및 보안하기 위한 AWS 서비스
Direct Connect	표준 이더넷 광섬유 케이블을 통해 내부 네트워크를 AWS Direct Connect 위치에 연결할 수 있습니다. 케이블의 한쪽 끝을 사용자의 라우터에 연결하고 다른 쪽 끝을 AWS Direct Connect 라우터에 연결하는 서비스
AppMesh	애플리케이션의 모든 서비스에 대해 일관된 가시성과 네트워크 트래픽 제어를 제공하는 서비스
CloudMap	AWS Cloud Map를 사용하여 Amazon API Gateway에 배포된 API, Amazon EC2 인스턴스, Amazon DynamoDB 테이블, Amazon S3 버킷, Amazon Simple Queue Service(Amazon SQS) 대기열 등과 같은 모든 클라우드 리소스를 등록해 찾을 수 있는 서비스

2) 네트워크 서비스 별 관리형 정책 (예시)

서비스 구분	정책명	정책설명
VPC	AmazonVPCFullAccess	Amazon VPC에 대한 전체 액세스 권한
	AmazonVPCCrossAccount NetworkInterfaceOperations	네트워크 인터페이스를 생성하고 교차 계정 리소스에 연결할 수 있는 액세스 권한

	AmazonVPCReadOnlyAccess	Amazon VPC에 대한 읽기 전용 액세스 권한
CloudFront	CloudFrontFullAccess	전체 액세스 권한과 AWS Management 콘솔을 통해 Amazon S3 버킷을 나열하는 권한
	AWSCloudFrontLogger	CloudFront Logger에 CloudWatch Logs에 대한 쓰기 권한
	CloudFrontReadOnlyAccess	CloudFront 배포 구성 정보 및 목록 배포에 대한 액세스 권한
Route 53	AmazonRoute53FullAccess	Amazon Route 53에 대한 전체 액세스 권한
	AmazonRoute53DomainsFullAccess	모든 Route 53 도메인 작업 및 호스팅 영역 생성에 대한 전체 액세스 권한
	AmazonRoute53ReadOnlyAccess	Amazon Route 53에 대한 읽기 전용 액세스 권한
API Gateway	AmazonAPIGatewayAdministrator	Amazon API Gateway에서 API 생성/편집/삭제에 대한 전체 액세스 권한
	APIGatewayServiceRolePolicy	API Gateway가 고객을 대신하여 연결된 AWS 리소스를 관리하는 권한
	AmazonAPIGatewayInvokeFullAccess	Amazon API Gateway에서 API를 호출할 수 있는 전체 액세스 권한
Direct Connect	AWSDirectConnectFullAccess	AWS Direct Connect에 대한 전체 액세스 권한
	AWSDirectConnectServiceRolePolicy	리소스를 생성하고 관리할 수 있는 AWS Direct Connect 권한
	AWSDirectConnectReadOnlyAccess	AWS Direct Connect에 대한 읽기 전용 액세스 권한
AppMesh	AWSAppMeshFullAccess	AWS App Mesh API 및 관리 콘솔에 대한 전체 액세스 권한
	AWSAppMeshServiceRolePolicy	AWS App Mesh에서 사용하거나 관리하는 AWS 서비스 및 리소스에 대한 액세스 권한
	AWSAppMeshReadOnly	AWS App Mesh API 및 관리 콘솔에 대한 읽기 전용 액세스 권한
CloudMap	AWSCloudMapFullAccess	모든 AWS Cloud Map 작업에 대한

		전체 액세스 권한
	AWSCloudMapRegisterInstanceAccess	AWS Cloud Map 작업에 대한 등록자 수준 액세스 권한
	AWSCloudMapReadOnlyAccess	모든 AWS Cloud Map 작업에 대한 읽기 전용 액세스 권한

3) IAM 관리형 정책 권한 관리 List (예시)

역할	계정 관리 (그룹 및 계정명)	AWS 관리형 정책	취약 유/무
AWS Root 관리자	Ex)RDS_Admin (admin_accout)	Ex) RDS_Admin (AmazonRDSFullAccess)	
Infra 운영/관리자 및 담당자			
Application 운영/관리자 및 담당자			
개발 관리자 및 담당자			
재무 / 비용 관리자 및 담당자			

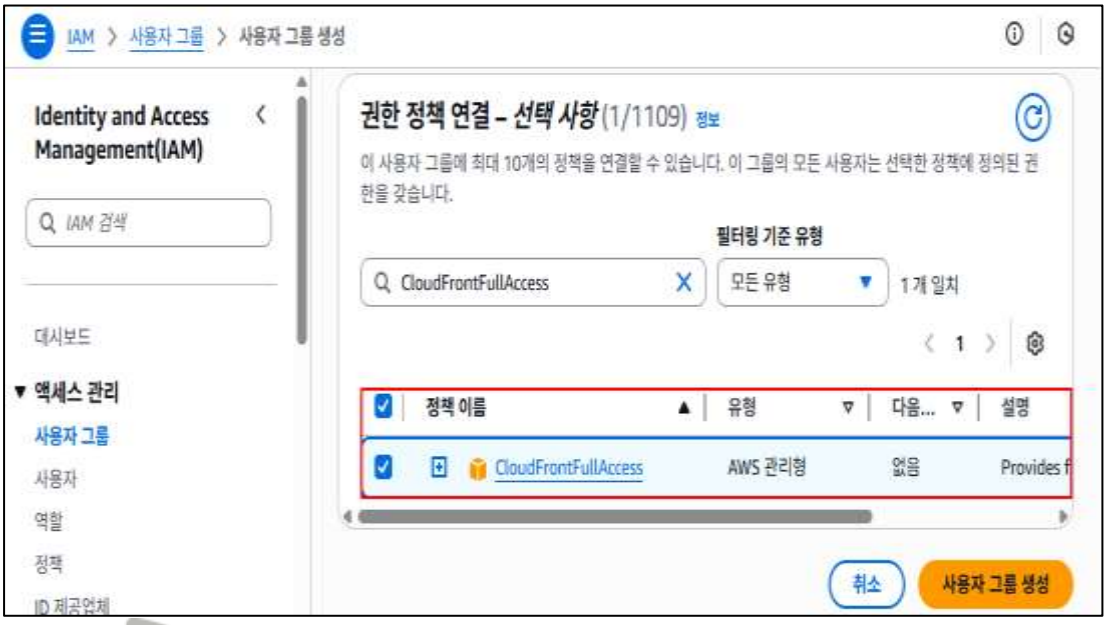
설정 방법

가. IAM 그룹/사용자 네트워크 권한 정책 관리 (HIGH)

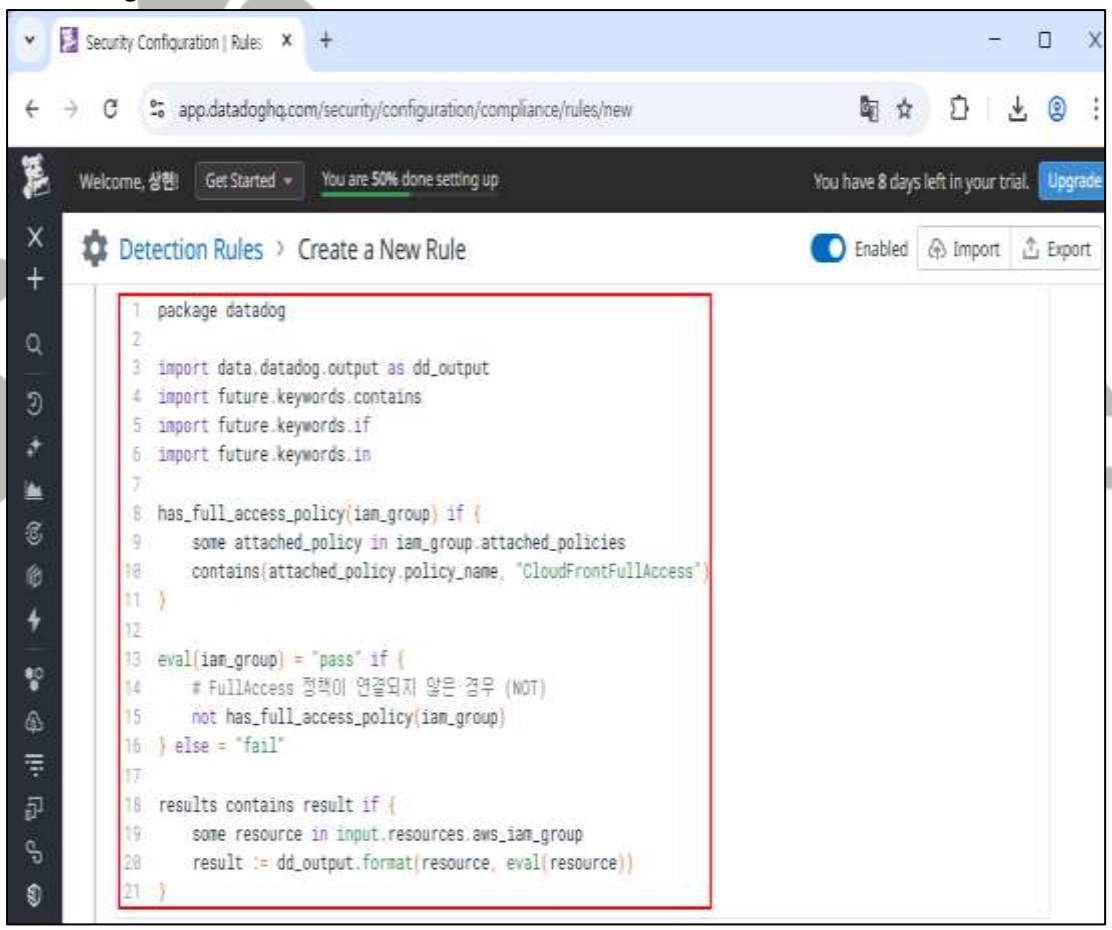
※ 네트워크 서비스 운영/관리에 필요한 IAMFullAccess 등의 권한과 같이 중요도가 높은 권한은 Infra 운영/관리자 및 담당자에게만 정책이 되도록 해야하며 최소한의 계정 수가 유지되어야 함

1) IAM -> 엑세스 관리 -> 사용자 -> 그룹 생성

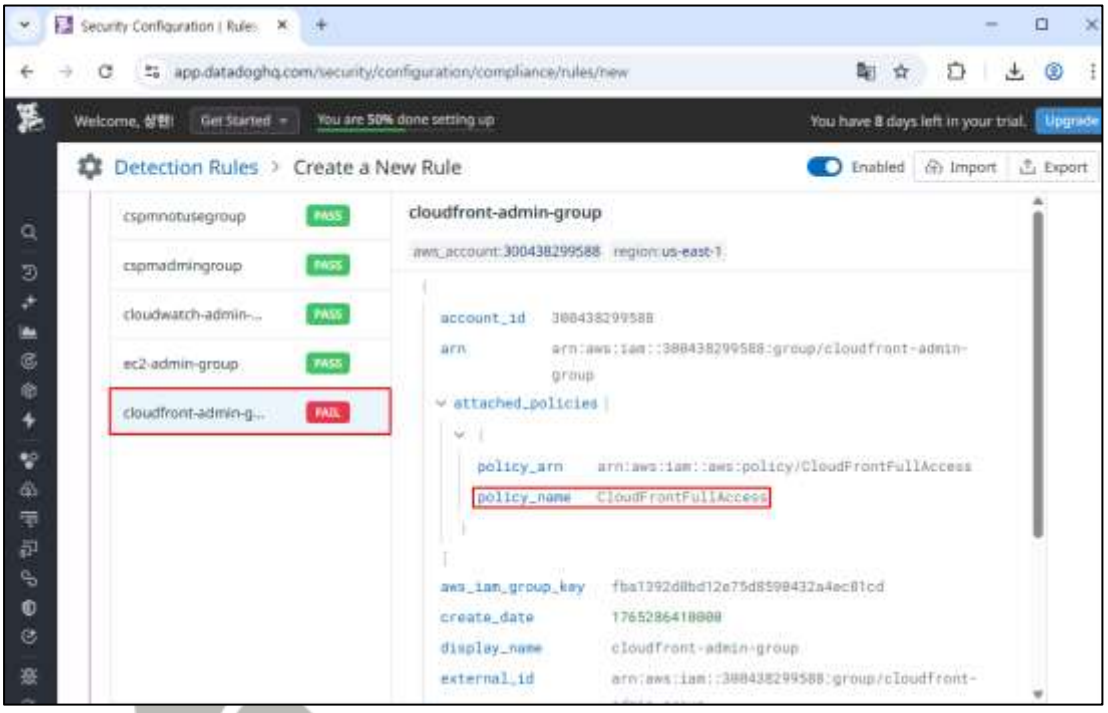
2) IAM 그룹 생성 시 "CloudFrontFullAccess" 정책 연결



3) Datadog Detection Rule 추가



4) Datadog Detection Rule 탐지 결과 확인

	
진단 기준	**커스텀** : IAM 그룹/사용자의 네트워크 서비스 관리형 정책 연결 탐지
비고	

2.3 기타 서비스 정책 관리

분류	권한 관리	중요도	상
항목명	기타 서비스 정책 관리		

항목 설명

AWS 기타 서비스(CloudWatch, CloudTrail, KMS 등)의 리소스 생성 또는 액세스 권한은 권한 정책에 따라 결정됩니다. 계정 관리자는 IAM 자격 증명(즉, 사용자, 그룹, 역할)에 권한 정책을 연결할 수 있으며 적절한 권한을 통한 서비스 관리가 이루어져야 합니다.

1) 기타 서비스 구분

서비스 구분	서비스 상세
Organizations	AWS Organizations는 사용자가 생성해 중앙에서 관리하는 조직으로 여러 AWS 계정을 통합할 수 있는 계정 관리 서비스
CloudWatch	Amazon Web Services(AWS) 리소스와 AWS에서 실시간으로 실행 중인 애플리케이션을 모니터링하는 서비스
Auto Scaling	AWS Auto Scaling 콘솔은 단일 사용자 인터페이스가 여러 AWS 서비스의 자동 조정 기능 사용하는 서비스
CloudFormation	Amazon Web Services 리소스를 모델링하고 설정하여 리소스 관리 시간을 줄이고 AWS에서 실행되는 애플리케이션에 더 많은 시간을 사용하도록 해 주는 서비스
CloudTrail	계정의 거버넌스, 규정 준수, 운영 및 위험 감사를 활성화하도록 도와주는 서비스
Config	AWS 계정에 있는 AWS 리소스의 구성을 자세히 보여 줍니다. 이러한 보기에는 리소스 간에 어떤 관계가 있는지와 리소스가 과거에 어떻게 구성되었는지도 포함되므로, 시간이 지나면서 구성과 관계가 어떻게 변하는지 확인할 수 있는 서비스
Systems Manager	Systems Manager 콘솔을 사용하여, 여러 AWS 서비스의 운영 데이터를 볼 수 있고 AWS 리소스 전체에 걸쳐 운영 작업을 자동화할 수 있는 서비스
GuardDuty	VPC 흐름 로그, AWS CloudTrail 이벤트 로그, DNS 로그 같은 데이터 원본을 분석하고 처리하는 지속적 보안 모니터링 서비스
Inspector	Amazon EC2 instances의 네트워크 액세스 가능성 및 해당 인스턴스에서 실행되는 애플리케이션의 보안 상태를 확인할 수 있는 서비스
Single Sign-On	모든 AWS 계정 및 클라우드 애플리케이션에 대한 SSO 액세스를 중앙에서 쉽게 관리 할 수있는 클라우드 기반 싱글 사인온 (SSO) 서비스
Certificate Manager	AWS 기반 웹 사이트 및 애플리케이션에 대한 공인 SSL/TLS 인증서를 생성 및 관리하는 서비스
KMS	데이터 암호화에 사용하는 암호화 키를 쉽게 생성하고 제어할 수 있게 해주는 관리형 서비스

WAF	Amazon CloudFront 배포, Amazon API Gateway API 또는 Application Load Balancer에 전달되는 HTTP(S) 요청을 모니터링할 수 있게 해주는 웹 애플리케이션 방화벽 서비스
Shield	Amazon Elastic Compute Cloud 인스턴스, Elastic Load Balancing 로드 밸런서, Amazon CloudFront 배포 및 Amazon Route 53 호스팅 영역 및 AWS Global Accelerator에 확장 DDoS 공격 보호를 제공하는 서비스
Security Hub	AWS 계정, 서비스 및 지원되는 타사 파트너 제품 전반에 걸쳐 보안 데이터를 수집하고, 보안 동향을 분석하고 우선 순위가 가장 높은 보안 문제를 식별할 수 있는 서비스
Data Pipeline	데이터의 이동과 변환을 자동화하는 데 사용할 수 있는 웹 서비스
Glue	완전 관리형 ETL(추출, 변환, 로드) 서비스로, 효율적인 비용으로 간단하게 여러 데이터 스토어 간에 원하는 데이터를 분류, 정리, 보강, 이동할 수 있는 서비스
MSK	Amazon Managed Streaming for Apache Kafka(Amazon MSK)는 Apache Kafka를 사용해 스트리밍 데이터를 처리하는 애플리케이션을 빌드하고 실행할 수 있는 완전관리형 서비스
Backup	클라우드 및 온프레미스에서 AWS 서비스 전반에 걸쳐 데이터 백업을 중앙 집중화하고 자동화할 수 있는 완전 관리형 백업 서비스

2) IAM 관리형 정책 권한 관리 List (예시)

역할	계정 관리 (그룹 및 계정명)	AWS 고객관리형 정책	취약 유/무
AWS Root 관리자	Ex)S3_Admin (admin_accout)	Ex) S3_Admin (CustomS3FullAccess)	
Infra 운영/관리자 및 담당자			
Application 운영/관리자 및 담당자			
개발 관리자 및 담당자			
재무 / 비용 관리자 및 담당자			

설정 방법

가. IAM 그룹/사용자 기타 서비스 권한 정책 관리 (HIGH)

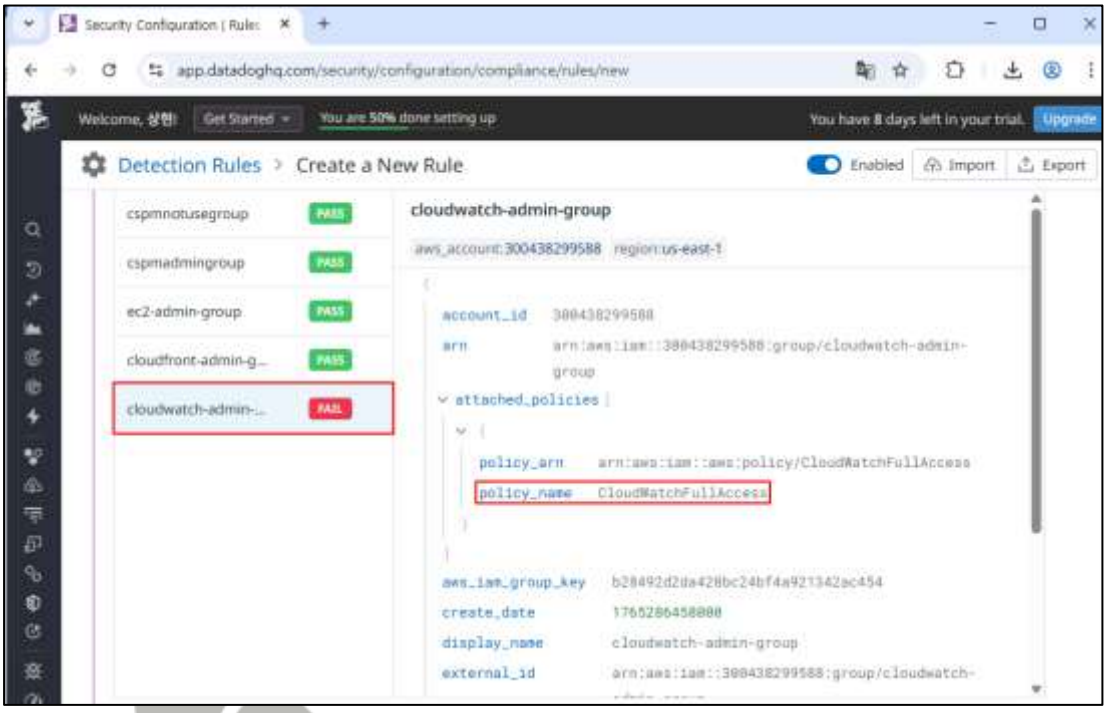
※ 기타 서비스 운영/관리에 필요한 IAMFullAccess 등의 권한과 같이 중요도가 높은 권한은 Infra 운영/관리자 및 담당자에게만 정책이 되도록 해야하며 최소한의 계정 수가 유지되어야 함

1) IAM -> 엑세스 관리 -> 사용자 -> 그룹 생성

2) IAM 그룹 생성 시 "CloudWatchFullAccess" 정책 연결

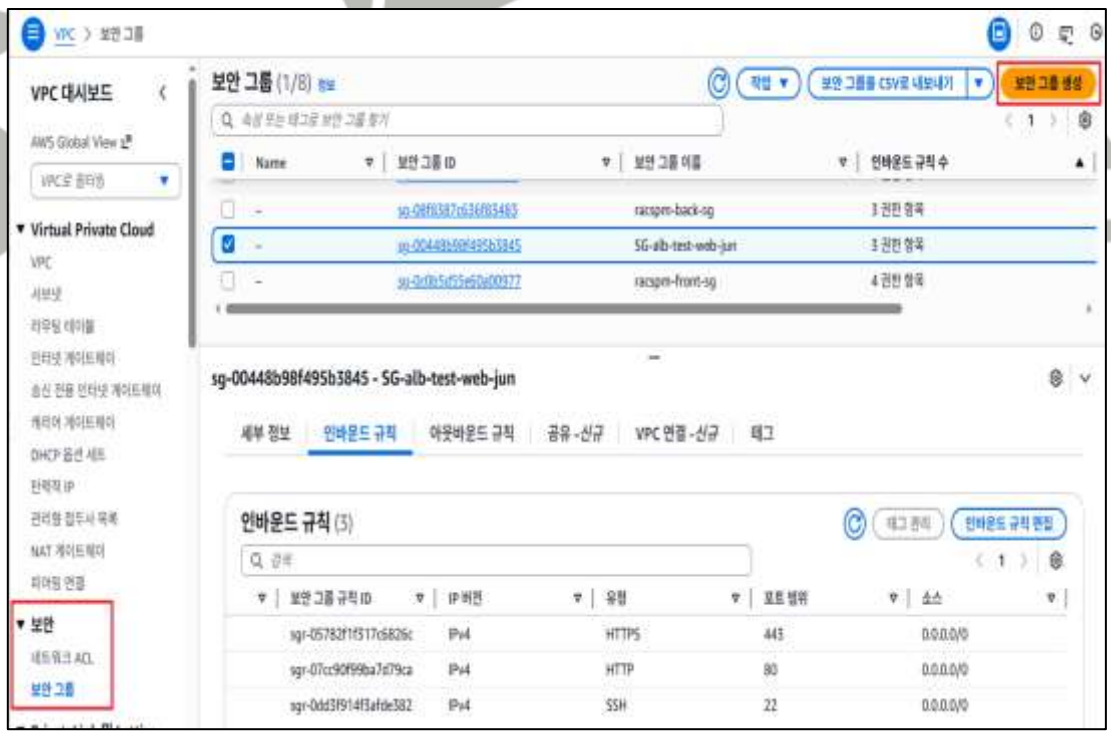
3) Datadog Detection Rule 추가

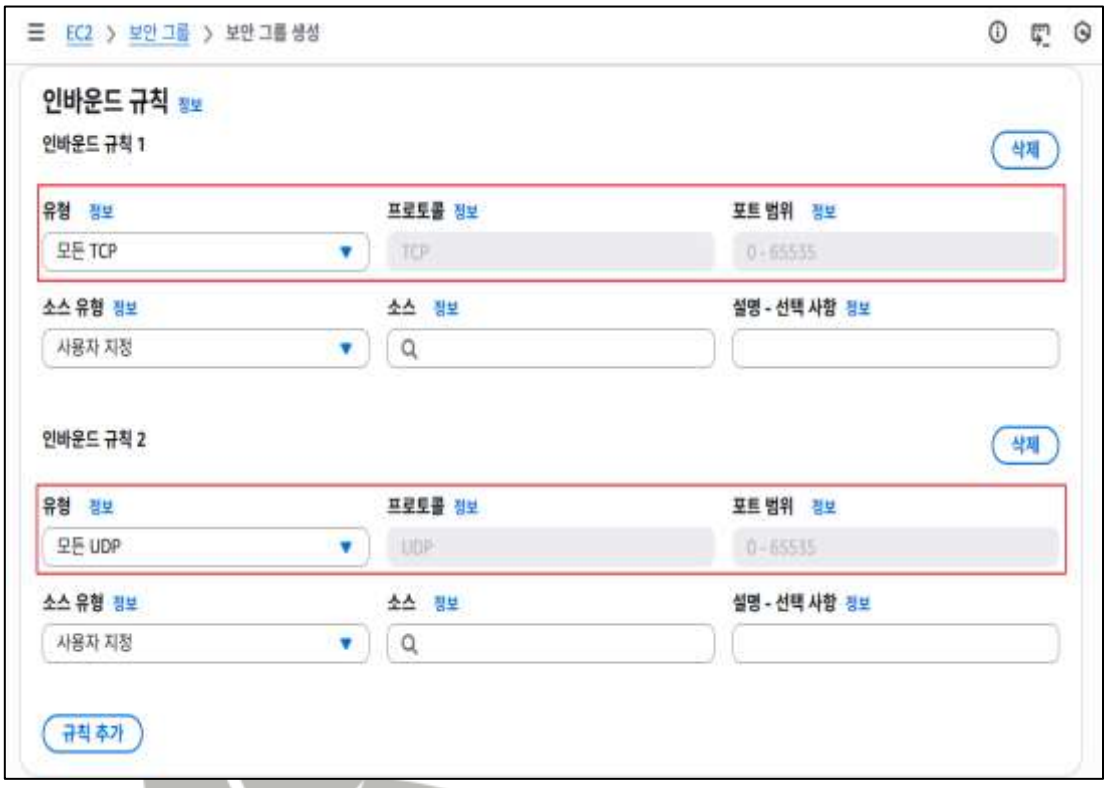
4) Datadog Detection Rule 탐지 결과 확인

	
진단 기준	**커스텀** : IAM 그룹/사용자의 기타 서비스 관리형 정책 연결 탐지
비고	

3. 가상 리소스 관리

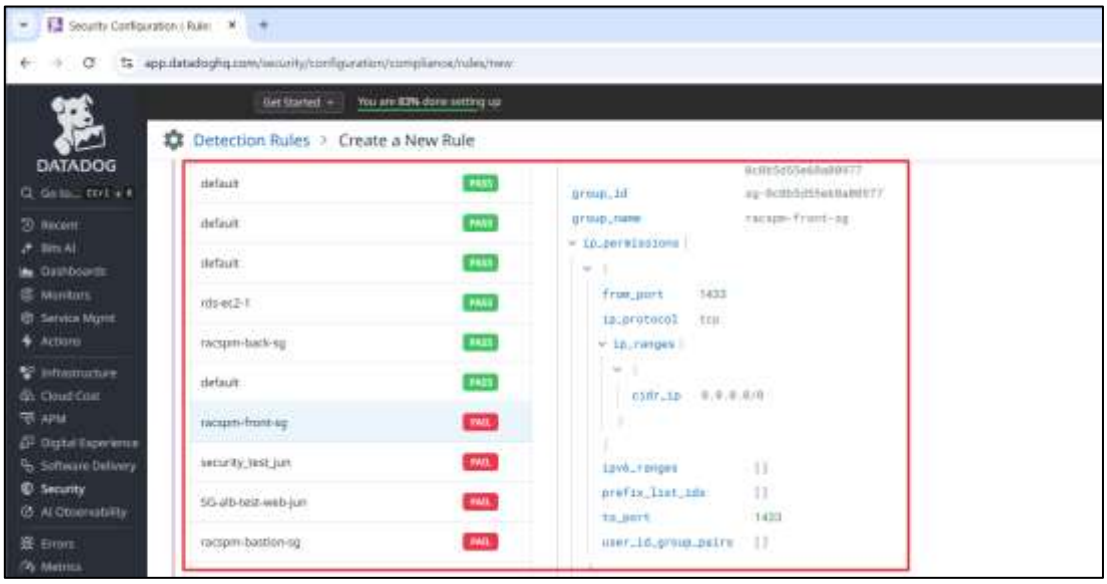
3.1 보안 그룹 인/아웃바운드 PORT ANY 설정 관리

분류	가상 리소스 관리	중요도	상
항목명	보안 그룹 인/아웃바운드 ANY 설정 관리		
항목 설명	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. 보안 그룹은 인/아웃바운드의 규칙 편집을 통해 특정 소스(출발지)에서의 통신이 가능하도록 유형(네트워크 프로토콜) 및 단일/범위 포트를 설정할 수 있습니다. [Defualt Port 정보] 20,21(FTP) / 22(SSH) / 23(Telnet) / 25(SMTP) / 110(POP3) / 135(RPC) / 143(IMAP) /445(CIFS) / 1433,1434(MSSQL) / 3000(Go, Node.js) / 3306(MySQL) / 3389(RDP) / 4333(ahsp) / 5000(Python web development) / 5432(postgresql) / 5500(fcp-addr-srvr1) / 5601(OpenSearch Dashboards) / 8080(Proxy) / 8088(legacy HTTP) / 8888(alternative HTTP) / 9200,9300(OpenSearch)		
설정 방법	**가. 보안 그룹은 위험도가 높은 포트에 대한 무제한 액세스를 제한해야 함 (MEDIUM)** 1) 보안 그룹 탭 접근 -> 보안 그룹 생성  2) 보안 그룹 생성 시 인바운드 규칙 추가 (불필요한 포트 허용)		

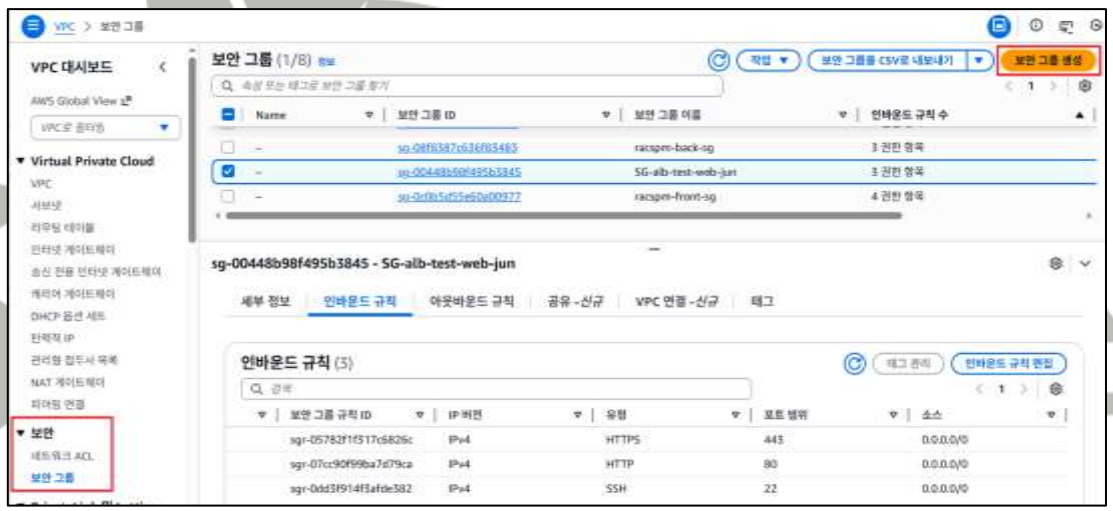
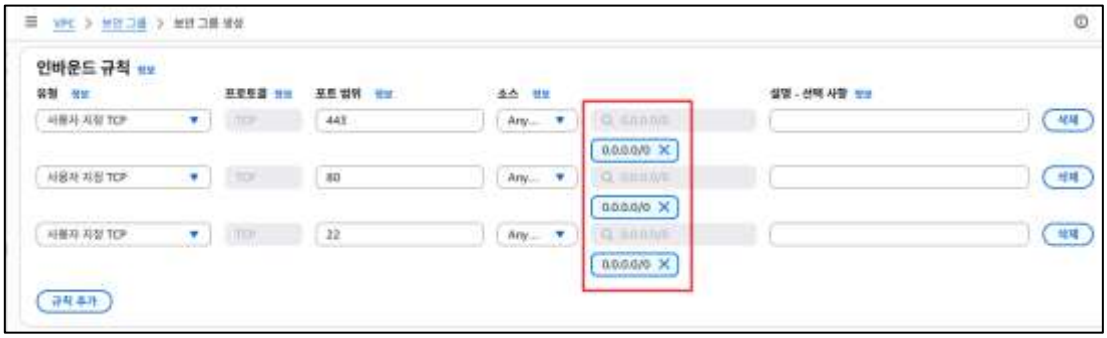


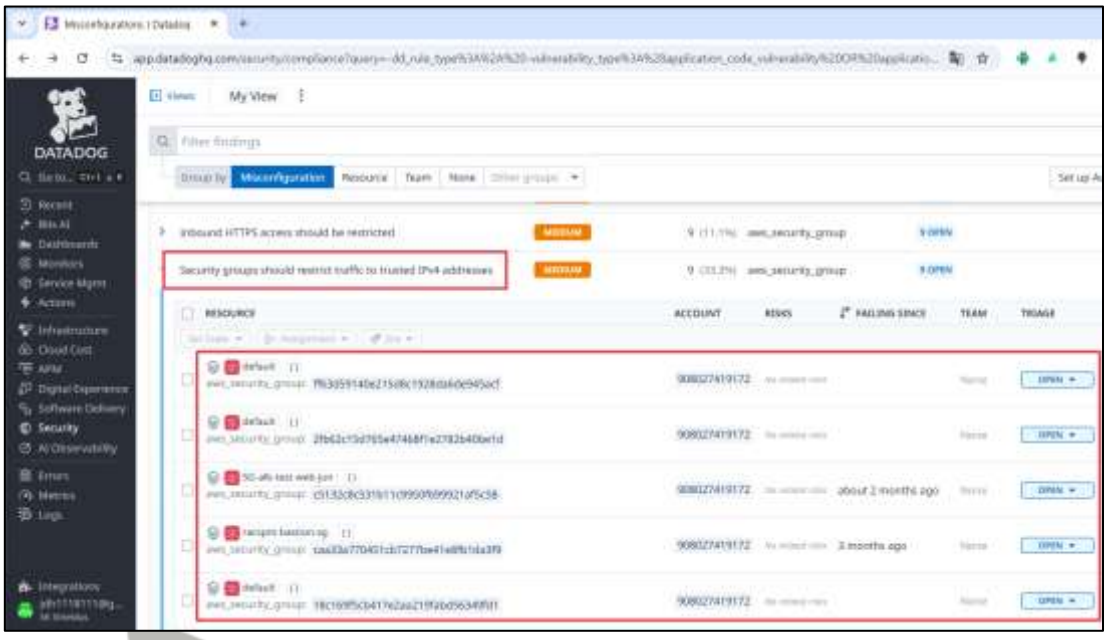
3) Datadog Detection Rule 추가

4) Datadog Detection Rule 탐지 여부 확인

	
탐지 기준	**커스텀** : 보안 그룹에 Default Port 외 Port ANY로 탐지될 경우
비고	

3.2 보안 그룹 인/아웃바운드 불필요 정책 관리

분류	가상 리소스 관리	중요도	상
항목명	보안 그룹 인/아웃바운드 불필요 정책 관리		
항목 설명	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. 보안 그룹은 인/아웃바운드의 규칙 편집을 통해 특정 소스(출발지)에서의 통신이 가능하도록 유형(네트워크 프로토콜) 및 단일/범위 정책을 설정할 수 있습니다. 보안 그룹은 AWS 리소스에 대한 수신 및 송신 네트워크 트래픽의 상태 기반 필터링을 제공합니다. SSH(Port 22) 및 RDP(Port 3389)와 같은 원격 서버 관리 포트에 대한 무제한 수신 액세스를 허용하면 표면 공격이 증가하고 리소스 손상 위험이 높아집니다.		
설정 방법	**가. 보안 그룹은 신뢰할 수 있는 IPv4 주소로 트래픽을 제한해야 함 (MEDIUM)** 1) 보안 그룹 탭 접근 -> 보안 그룹 생성  2) 보안 그룹 생성 시 IPv4 인바운드 규칙 추가  3) Datadog Misconfiguration 탐지 확인		

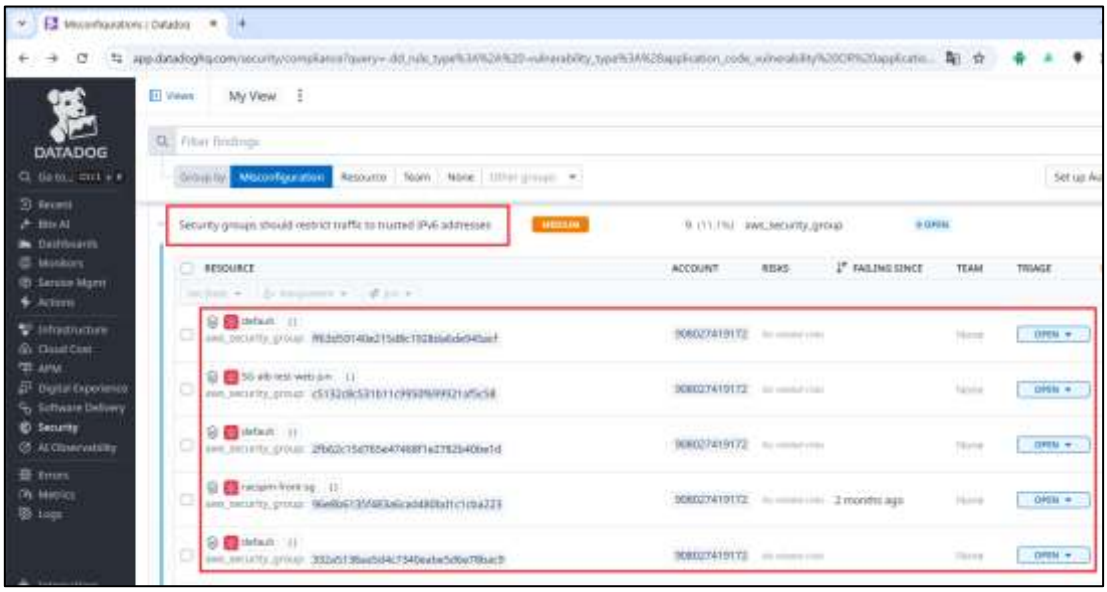


나. 보안 그룹은 신뢰할 수 있는 IPv6 주소로 트래픽을 제한해야 함 (MEDIUM)

1) 보안 그룹 탭 접근 -> 보안 그룹 생성

2) 보안 그룹 생성 시 IPv6 인바운드 규칙 추가

3) Datadog Misconfiguration 탐지 확인

	
탐지 기준	**tch-c9p-gh4** : 보안 그룹 IPv4에 대한 SourceIP가 ANY로 탐지될 경우 **def-000-9mn** : 보안 그룹 IPv6에 대한 SourceIP가 ANY로 탐지될 경우
비고	기술 공식 문서 : https://docs.datadoghq.com/security/default_rules/tch-c9p-gh4/ https://docs.datadoghq.com/security/default_rules/def-000-9mn/

3.3 네트워크 ACL 인/아웃바운드 트래픽 정책 관리

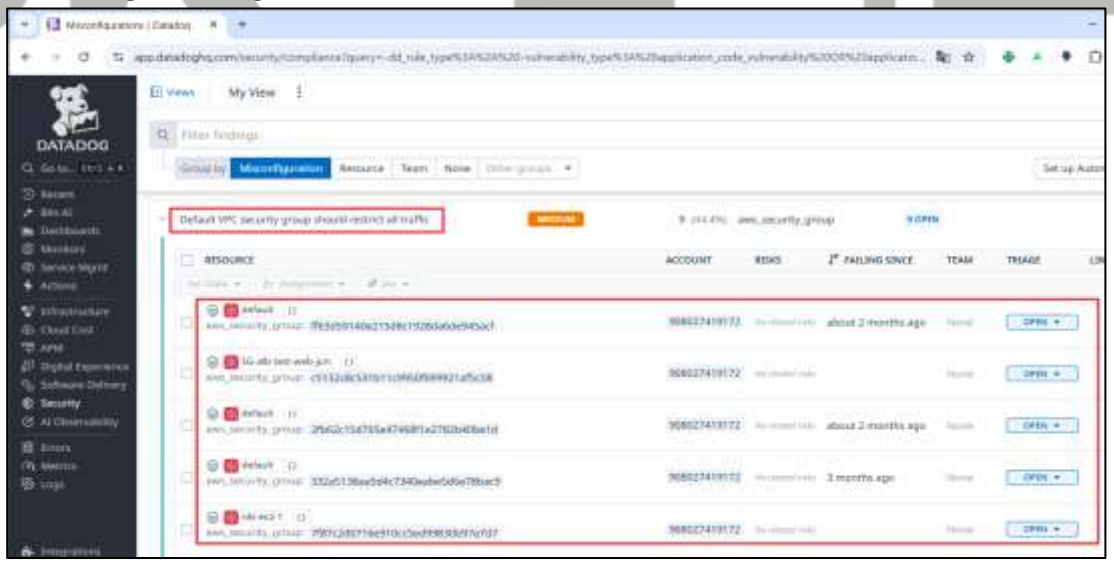
<table>
<tr><td>분류</td><td>가상 리소스 관리</td><td>중요도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">네트워크 ACL 인/아웃바운드 트래픽 정책 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">네트워크 ACL(Access Control List)은 1개 이상의 서브넷 내부와 외부의 트래픽을 제어하기 위한 방화벽 역할을 하는 VPC의 선택적 보안 계층입니다. 보안 그룹과 비슷한 규칙으로 네트워크 ACL을 설정하여 VPC에 보안 계층을 더 추가할 수 있습니다. ACL은 VPC 서브넷 계층에서 동작하며 VPC 서브넷과는 1:1로 대응합니다. 정책의 방식은 허용(Allow) 및 거부(deny) 정책(WhiteList or BlackList) 기능으로 Stateless 방식으로 사용이 됩니다.

VPC에는 기본적으로 모든 인바운드 트래픽을 거부하고, 모든 아웃바운트 트래픽을 허용하며, 그룹 내 인스턴스 간의 트래픽을 허용하는 기본 보안 그룹이 있습니다. 모든 트래픽을 제한하도록 기본 보안 그룹을 설정하면 리소스 노출을 최소화 할 수 있습니다.

(*) 기본 네트워크 ACL 규칙
기본 네트워크 ACL은 연결된 서브넷 트래픽 흐름을 모두 허용하도록 구성되어 있습니다. 각 네트워크 ACL에는 규칙 번호가 별표로 되어 있는 규칙도 포함되어 있습니다. 이 규칙은 패킷이 번호가 매겨진 다른 어떤 규칙과도 일치하지 않을 경우에는 거부되도록 되어 있습니다. 이 규칙을 수정하거나 제거할 수 없습니다.
<table>
<tr><th colspan="6">인바운드 정책</th></tr>
<tr><th>규칙 #</th><th>유형</th><th>프로토콜</th><th>포트</th><th>소스</th><th>허용/거부</th></tr>
<tr><td>100</td><td>모든 IPv4 트래픽</td><td>모두</td><td>모두</td><td>0.0.0.0/0</td><td>ALLOW</td></tr>
<tr><td>*</td><td>모든 IPv4 트래픽</td><td>모두</td><td>모두</td><td>0.0.0.0/0</td><td>DENY</td></tr>
</table>
<table>
<tr><th colspan="6">아웃바운드 정책</th></tr>
<tr><th>규칙 #</th><th>유형</th><th>프로토콜</th><th>포트</th><th>소스</th><th>허용/거부</th></tr>
<tr><td>100</td><td>모든 IPv4 트래픽</td><td>모두</td><td>모두</td><td>0.0.0.0/0</td><td>ALLOW</td></tr>
<tr><td>*</td><td>모든 IPv4 트래픽</td><td>모두</td><td>모두</td><td>0.0.0.0/0</td><td>DENY</td></tr>
</table>
</td></tr>
<tr><td>설정
방법</td><td colspan="3">가. 기본 VPC 보안 그룹은 모든 트래픽을 제한해야 함 (MEDIUM)
1) 보안 그룹 탭 접근 -> default 보안 그룹 -> 인바운드 규칙 확인</td></tr>
</table>

2) 보안 그룹 탭 접근 -> default 보안 그룹 -> 아웃바운드 규칙 확인

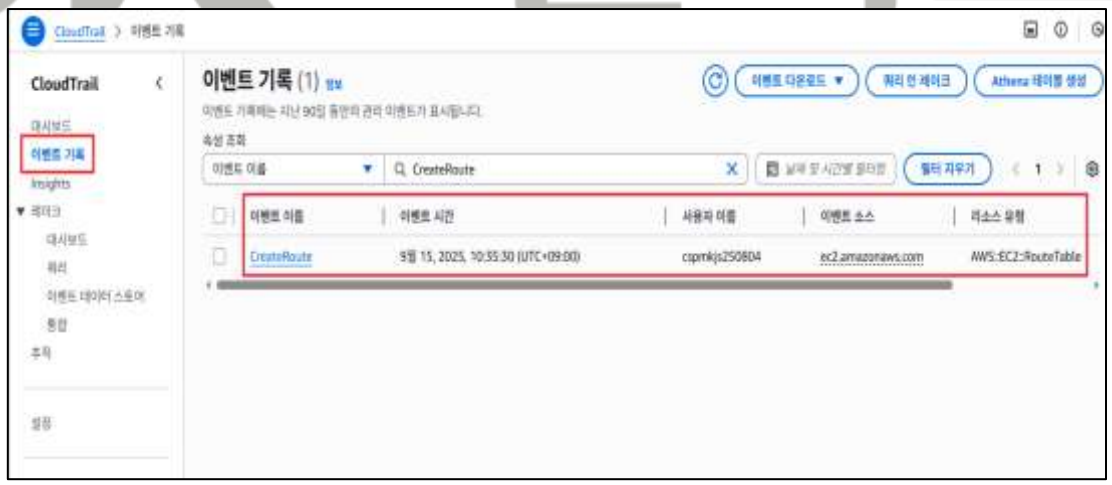
3) Datadog Misconfiguration 탐지 확인

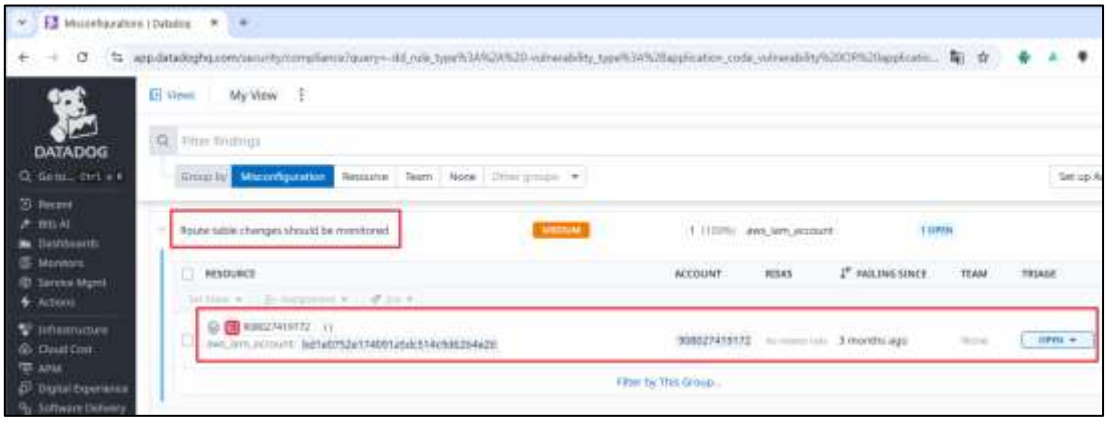


탐지	**rx9-tkr-e6b** : Default VPC 보안 그룹에서 인/아웃바운드 규칙이 All Traffic/Protocol이면 탐지

기준	
비고	기술 공식 문서 : https://docs.datadoghq.com/security/default_rules/rx9-tkr-e6b/

3.4 라우팅 테이블 정책 관리

분류	가상 리소스 관리	중요도	중
항목명	라우팅 테이블 정책 관리		
항목 설명	라우팅 테이블에는 네트워크 트래픽을 전달할 위치 결정 시 사용되는 규칙입니다. VPC의 각 서브넷을 라우팅 테이블에 연결해야 하며, 테이블에서는 서브넷에 대한 라우팅을 제어하게 됩니다. 서브넷을 한 번에 하나의 라우팅 테이블에만 연결 할 수 있지만 여러 서브넷을 동일한 라우팅 테이블에 연결하는 것은 가능합니다. 라우팅 테이블 변경 사항에 대한 메트릭 필터와 알람을 CloudWatch 로그로 전송하여 API 호출을 실시간으로 모니터링 할 수 있습니다.		
설정 방법	**가. 라우팅 테이블 변경 사항을 모니터링해야 함 (MEDIUM)** 1) 라우팅 테이블 탭 접근 -> 라우팅 테이블 생성/수정/삭제  2) CloudTrail 이벤트 기록 확인  3) Datadog Misconfiguration 탐지 확인		

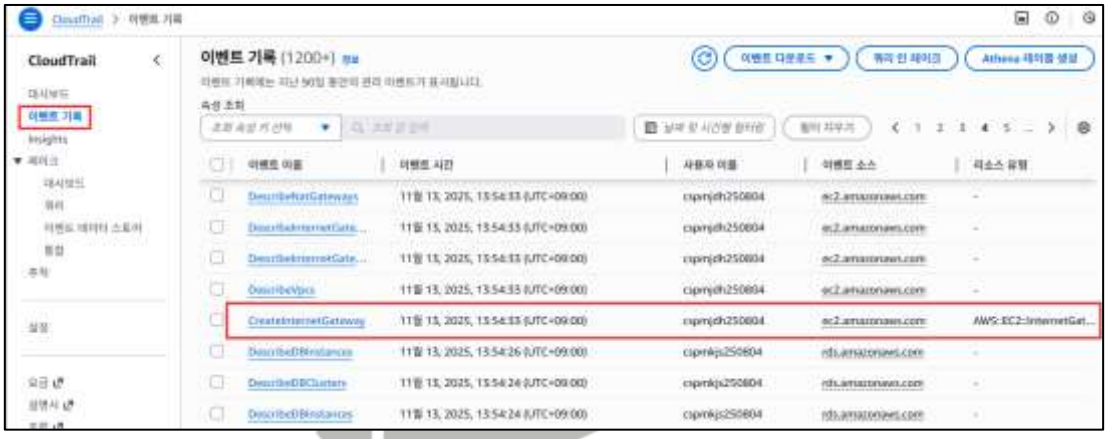
	
탐지 기준	**def-000-j0s** : CloudTrail 이벤트에서 VPC Route Table 변경이 감지될 경우 탐지
비고	기술 공식 문서 : https://docs.datadoghq.com/security/default_rules/def-000-j0s/

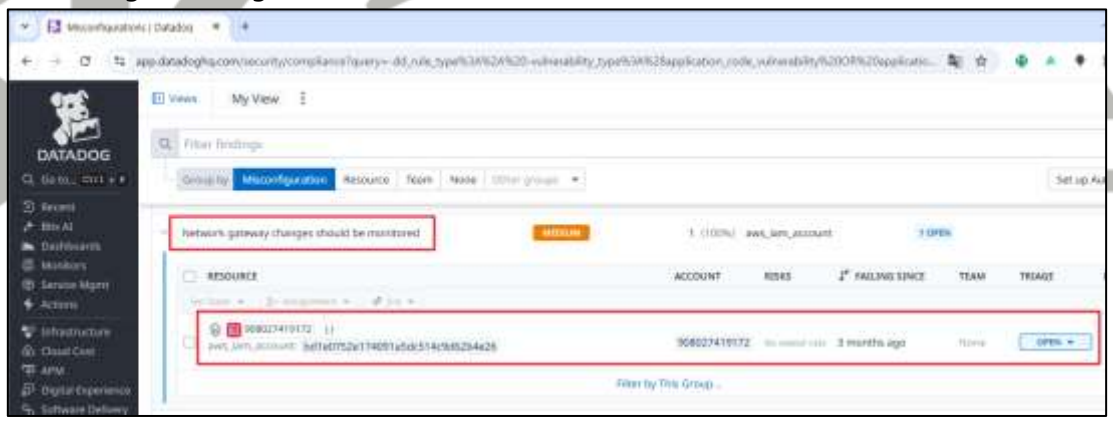
3.5 인터넷 게이트웨이 연결 관리

<table>
<tr><td>분류</td><td>가상 리소스 관리</td><td>중요도</td><td>하</td></tr>
<tr><td>항목명</td><td colspan="3">인터넷 게이트웨이 연결 관리</td></tr>
<tr><td>항목 설명</td><td colspan="3">인터넷 게이트웨이는 수평 확장되고 가용성이 높은 중복 VPC 구성요소로, VPC의 인스턴스와 인터넷 간에 통신이 가능할 수 있게 해주는 기능이며 네트워크 트래픽 가용성 위험이나 대역폭 제약조건이 별도로 발생하진 않습니다.
인터넷 게이트웨이에는 인터넷 Route 가능 트래픽에 대한 VPC 라우팅 테이블에 대상을 제공하고, 퍼블릭 IPv4 주소가 할당된 인스턴스에 대해 NAT(네트워크 주소 변환)를 수행하는 두 가지 목적이 있으며, IPv4, IPv6 트래픽을 모두 지원합니다.

(*) 기본 VPC와 기본이 아닌 VPC에 대한 인터넷 액세스
<table>
<tr><th>구분</th><th>기존 VPC</th><th>기본이 아닌 VPC</th></tr>
<tr><td>인터넷 게이트웨이</td><td>예</td><td>VPC 마법사의 첫 번째 또는 두 번째 옵션을 사용하여 VPC를 생성한 경우.
그렇지 않은 경우, 인터넷 게이트웨이를 수동으로 생성하여 연결해야 합니다.</td></tr>
<tr><td>IPv4 트래픽을 위한 인터넷 게이트웨이로 가는 경로가 있는 라우팅 테이블(0.0.0.0/0)</td><td>예</td><td>VPC 마법사의 첫 번째 또는 두 번째 옵션을 사용하여 VPC를 생성한 경우.
그렇지 않은 경우, 라우팅 테이블을 수동으로 생성하여 경로를 추가해야 합니다.</td></tr>
<tr><td>IPv6 트래픽을 위한 인터넷 게이트웨이로 가는 경로가 있는 라우팅 테이블(::/0)</td><td>아니요</td><td>VPC 마법사의 첫 번째 또는 두 번째 옵션을 사용하여 VPC를 생성한 경우, 그리고 IPv6 CIDR 블록을 VPC와 연결하기 위해 옵션을 지정한 경우.
그렇지 않은 경우, 라우팅 테이블을 수동으로 생성하여 경로를 추가해야 합니다.</td></tr>
<tr><td>서브넷에서 시작된 인스턴스에 자동 할당된 퍼블릭 IPv4 주소</td><td>예
(기본 서브넷)</td><td>아니요(기본이 아닌 서브넷)</td></tr>
<tr><td>서브넷에서 시작된 인스턴스에 자동 할당된 IPv6 주소</td><td>아니요
(기본 서브넷)</td><td>아니요(기본이 아닌 서브넷)</td></tr>
</table></td></tr>
<tr><td>설정 방법</td><td colspan="3">가. 네트워크 게이트웨이 변경 사항을 모니터링해야 함 (MEDIUM)
1) 인터넷 게이트웨이 탭 접근 -> 인터넷 게이트웨이 생성/수정/삭제</td></tr>
</table>

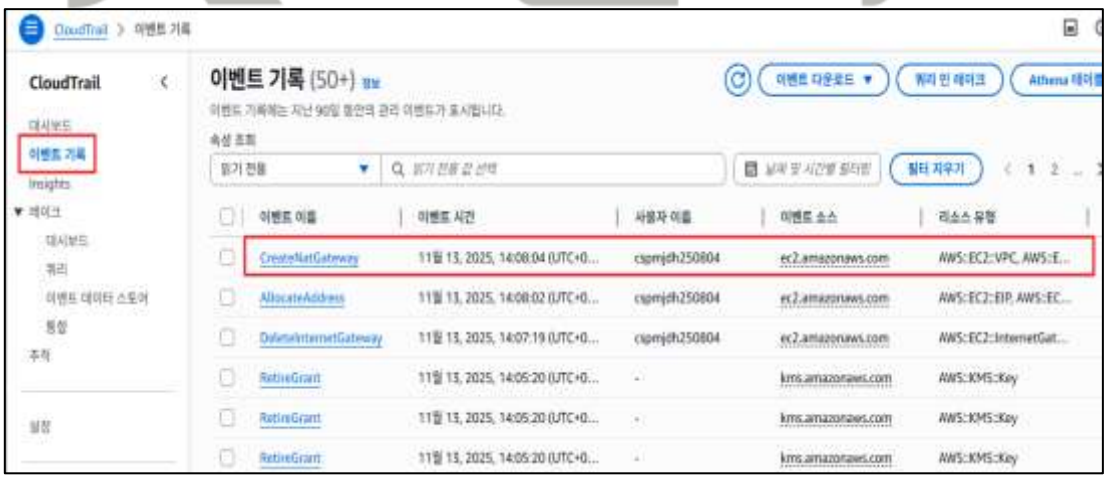
<table>
<tr>
<td></td>
<td>

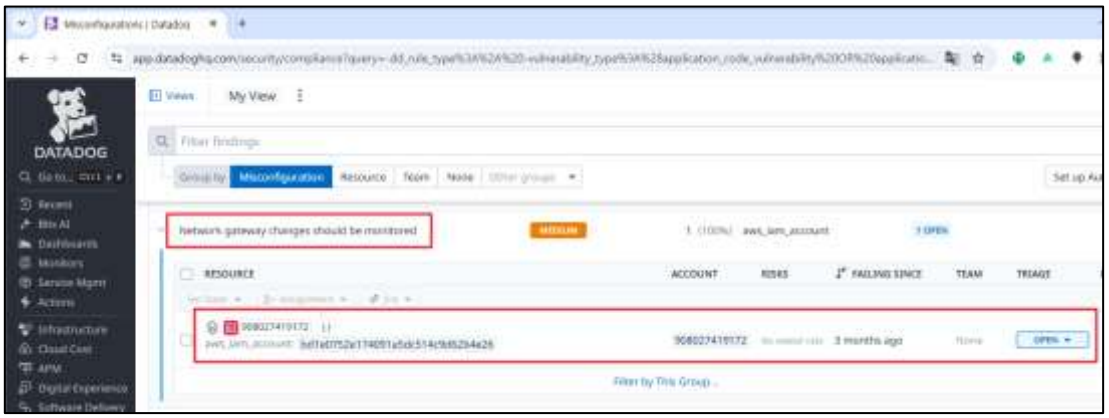

2) CloudTrail 이벤트 기록 확인


3) Datadog Misconfiguration 탐지 확인


</td>
</tr>
<tr>
<td>탐지 기준</td>
<td>def-000-k5x : 인터넷 게이트웨이에 대한 생성/삭제/연결 변경 이벤트가 감지될 경우 탐지</td>
</tr>
<tr>
<td>비고</td>
<td>기술 공식 문서 :
https://docs.datadoghq.com/security/default_rules/def-000-k5x/</td>
</tr>
</table>

3.6 NAT 게이트웨이 연결 관리

분류	가상 리소스 관리	중요도	중
항목명	NAT 게이트웨이 연결 관리		
항목 설명	NAT 게이트웨이는 NAT 디바이스를 사용하여 프라이빗 서브넷의 인스턴스를 인터넷(예: 소프트웨어 업데이트용) 또는 기타 AWS 서비스에 연결하는 한편, 인터넷에서 해당 인스턴스와의 연결을 시작하지 못하도록 할 수 있습니다. NAT 디바이스는 프라이빗 서브넷의 인스턴스에서 인터넷 또는 기타 AWS 서비스로 트래픽을 전달한 다음 인스턴스에 응답을 다시 보냅니다. 트래픽이 인터넷으로 이동하면 소스 IPv4 주소가 NAT 디바이스의 주소로 대체되고, 이와 마찬가지로 응답 트래픽이 해당 인스턴스로 이동하면 NAT 디바이스에서 주소를 해당 인스턴스의 프라이빗 IPv4 주소로 다시 변환합니다.		
설정 방법	**가. 네트워크 게이트웨이 변경 사항을 모니터링해야 함 (MEDIUM)** 1) NAT 게이트웨이 탭 접근 -> NAT 게이트웨이 생성/수정/삭제  2) CloudTrail 이벤트 기록 확인  3) Datadog Misconfiguration 탐지 확인		

	
탐지 기준	**def-000-k5x** : NAT 게이트웨이에 대한 생성/삭제/연결 변경 이벤트가 감지될 경우 탐지
비고	기술 공식 문서 : https://docs.datadoghq.com/security/default_rules/def-000-k5x/

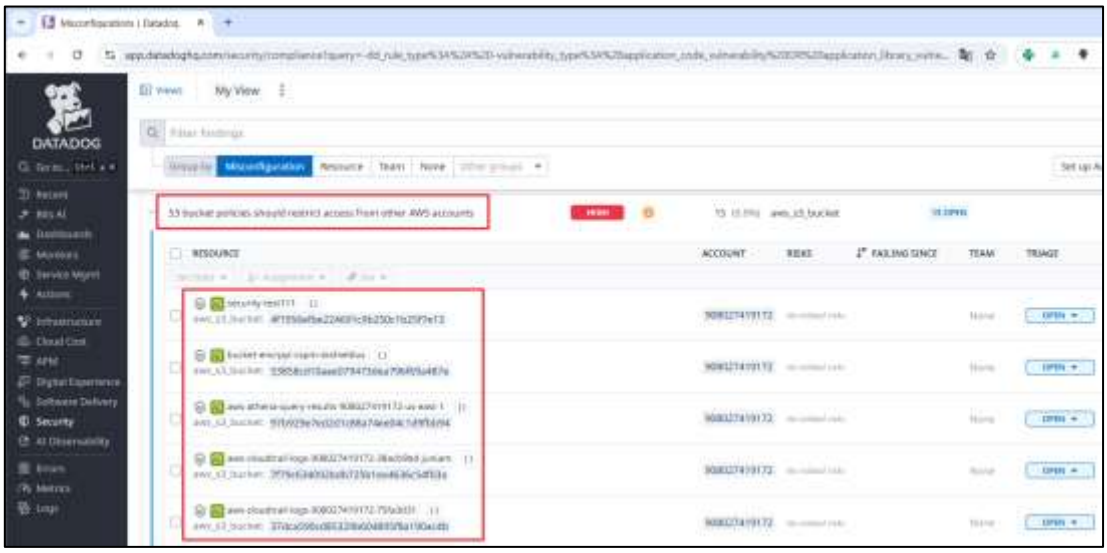
3.7 S3 버킷/객체 접근 관리

분류	가상 리소스 관리	중요도	중
항목명	S3 버킷/객체 접근 관리		
항목 설명	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 해야합니다. S3 범용 버킷 정책이 다른 AWS 계정의 보안 주체가 S3 버킷 내 리소스에 대해 무단 작업을 실행하는 것을 제한하는지 여부를 확인합니다. 최소 권한 원칙을 적용하는 것은 보안 위험을 완화하고 오류나 악의적인 활동의 영향을 최소화하는데 필수적입니다. S3 버킷 정책을 통해 외부 계정의 액세스를 허용하면 악의적인 내부자나 공격자에 의한 데이터 유출로 인해 보안 침해가 발생할 수 있습니다.		
설정 방법	**가. S3 버킷 정책은 다른 AWS 계정의 액세스를 제한해야 함 (HIGH)** 1) S3 탭 접근 -> 버킷 만들기  2) 신규 버킷 만들기  3) 생성된 S3 버킷 내 권한 설정		

4) ACL(액세스 제어 목록) 편집

5) 다른 AWS 계정에 대한 액세스 설정 확인

6) Datadog Misconfiguration 탐지 확인



나. S3 버킷 정책은 공개 쓰기 액세스를 방지해야 함 (HIGH)

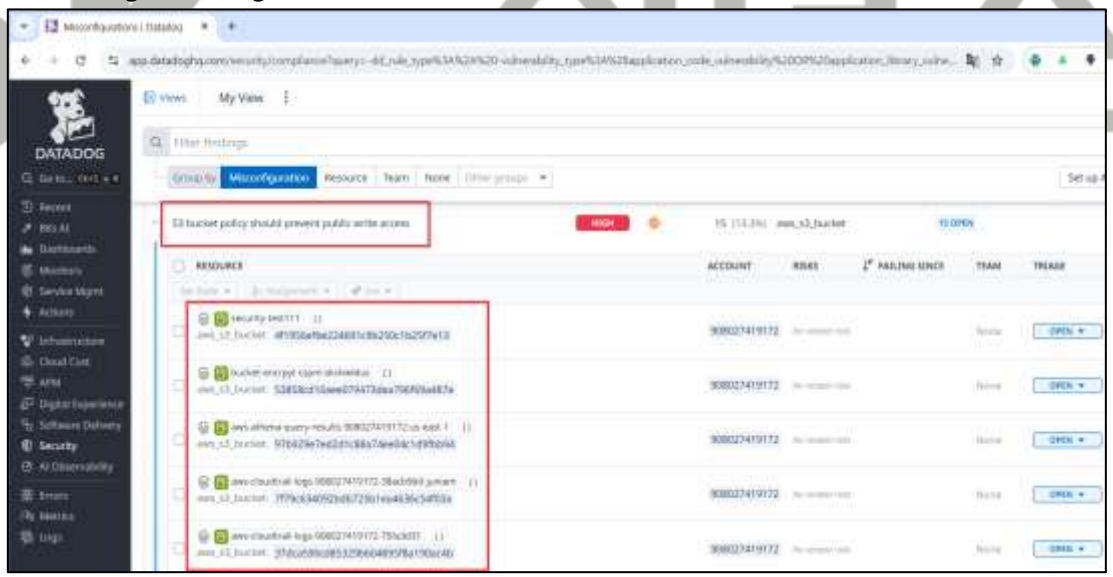
1) S3 탭 접근 -> 버킷 만들기

2) 신규 버킷 만들기

3) 생성된 S3 버킷 내 권한 설정

4) 버킷 정책(JSON) 설정 확인

5) Datadog Misconfiguration 탐지 확인



다. S3 버킷 ACL은 공개 쓰기 작업을 차단해야 함 (HIGH)

1) S3 탭 접근 -> 버킷 만들기

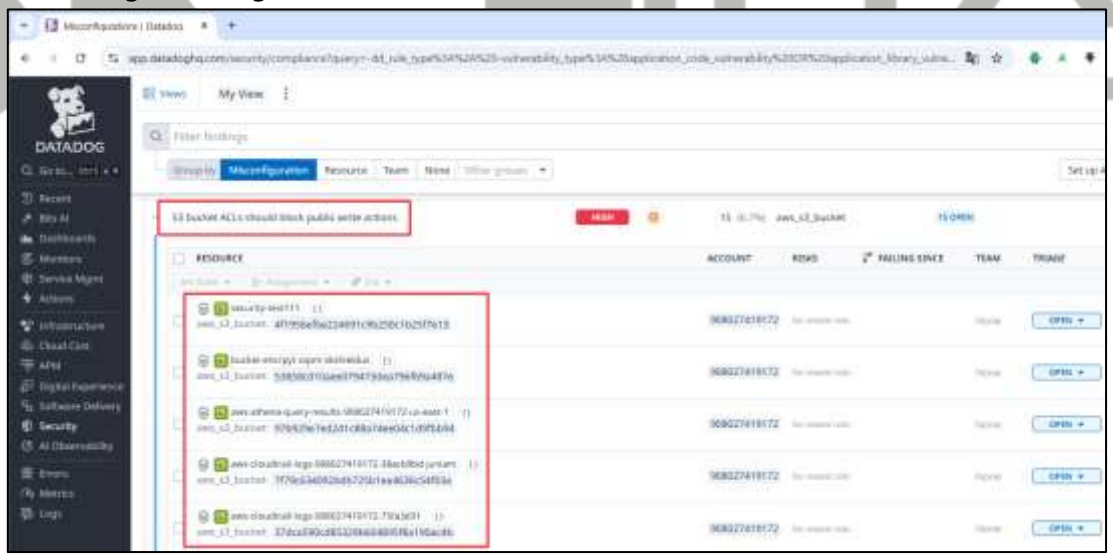
2) 신규 버킷 만들기

3) 생성된 S3 버킷 내 권한 설정

4) ACL(액세스 제어 목록) 설정

5) 모든 사람(퍼블릭 액세스) 쓰기 권한 설정 확인

6) Datadog Misconfiguration 탐지 확인



라. S3 버킷에는 '공개 액세스 차단' 기능이 활성화되어 있어야 함 (MIDIUM)

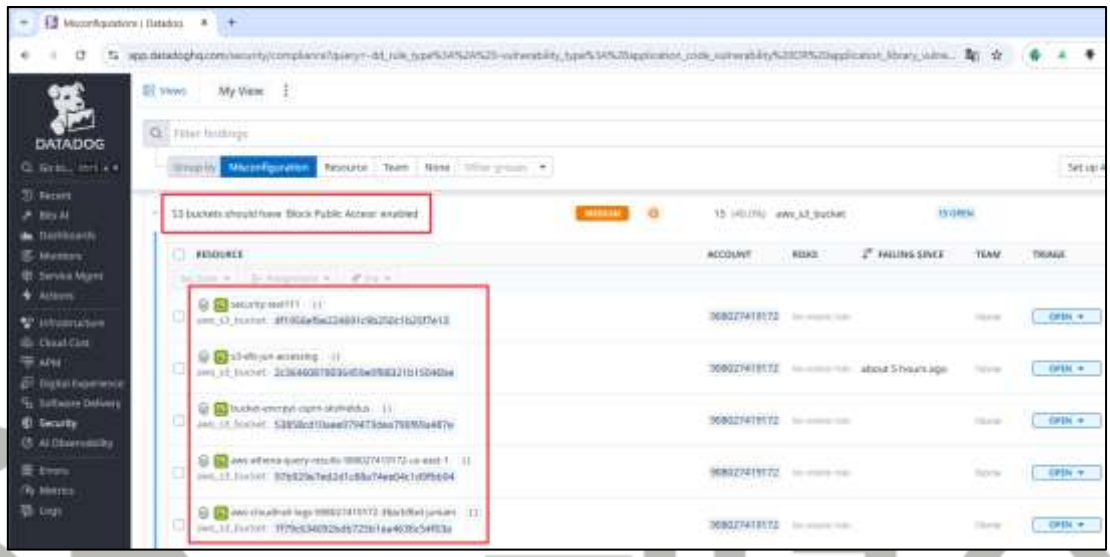
1) S3 탭 접근 -> 버킷 만들기

2) 신규 버킷 만들기

3) 생성된 S3 버킷 내 권한 설정

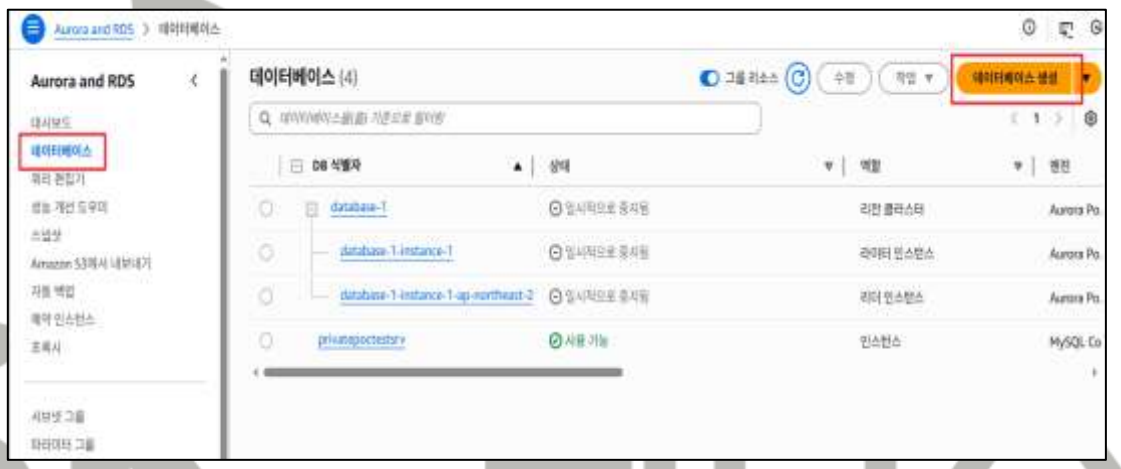
4) 퍼블릭 액세스 차단(버킷 설정) 설정

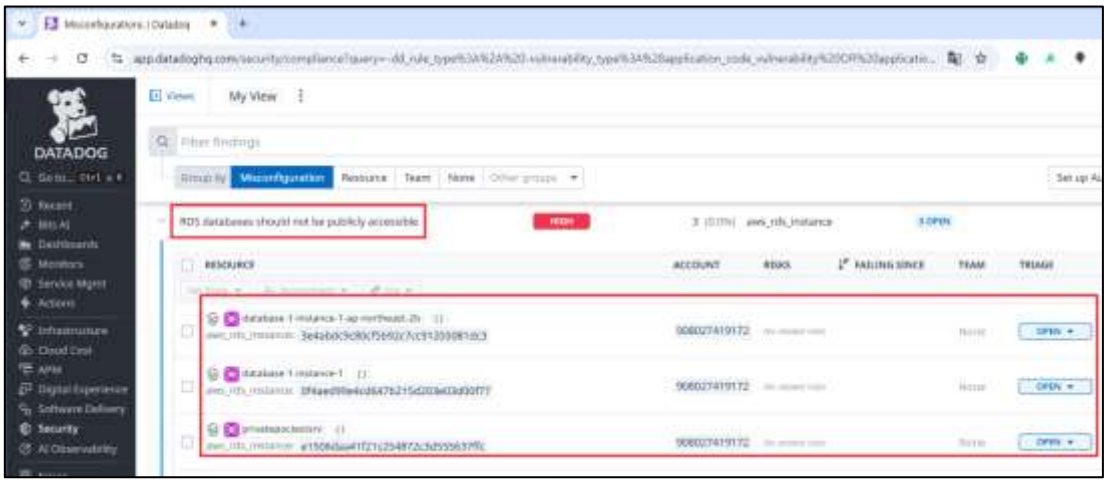
<table>
<tr><td></td><td>


5) Datadog Misconfiguration 탐지 확인


</td></tr>
<tr><td>탐지
기준</td><td>def-000-hb1 : 외부 AWS 계정이 S3 버킷의 주요 권한이 허용되어 있는 경우 탐지
def-000-0f1 : 버킷 정책(JSON)이 모든 사용자에게 쓰기권한이 허용되어 있는 경우 탐지
5yq-fi1-8pn : 버킷 ACL이 퍼블릭 그룹에 쓰기 권한이 부여되어 있으면 탐지
hkp-p6b-f7w : 버킷에 퍼블릭 액세스 차단 기능이 비활성화되어 있으면 탐지</td></tr>
<tr><td>비고</td><td>기술 공식 문서 :
https://docs.datadoghq.com/security/default_rules/def-000-hb1/
https://docs.datadoghq.com/security/default_rules/def-000-0f1/
https://docs.datadoghq.com/security/default_rules/5yq-fi1-8pn/
https://docs.datadoghq.com/security/default_rules/hkp-p6b-f7w/</td></tr>
</table>

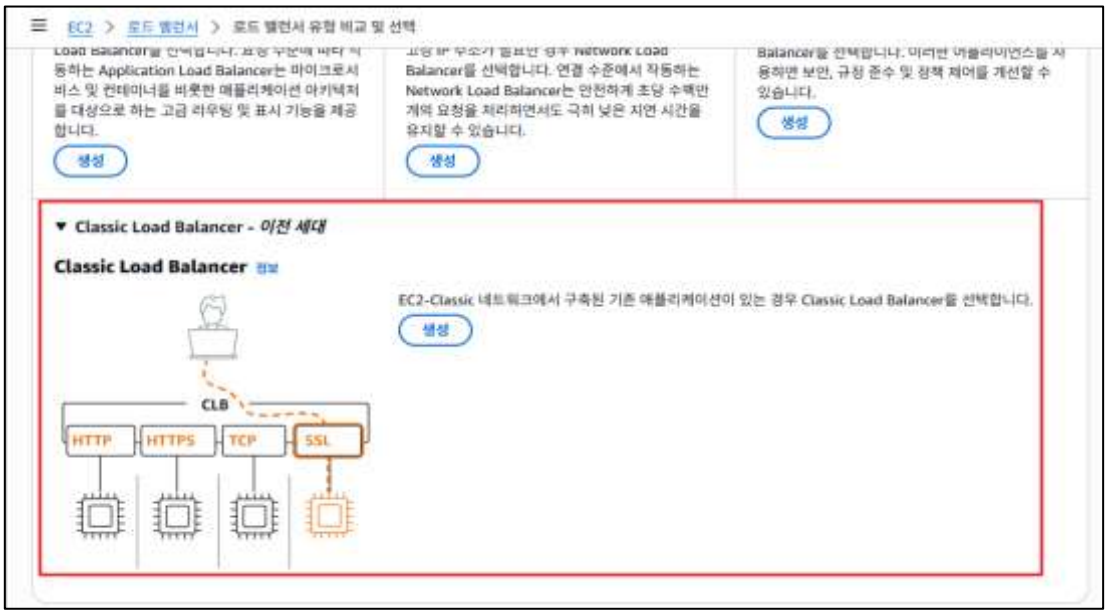
3.8 RDS 서브넷 가용 영역 관리

분류	가상 리소스 관리	중요도	중
항목명	RDS 서브넷 가용 영역 관리		
항목 설명	서브넷이란 하나의 IP 네트워크 주소를 지역적으로 나누어 이 하나의 네트워크 IP 주소가 실제로 여러 개의 서로 연결된 지역 네트워크로 사용할 수 있도록 하는 방법으로 EC2 인스턴스와 RDS 상호 통신 시 필요하나 불필요한 서브넷이 포함되어 있을 경우 보안성 위험을 발생시킬 수 있으므로 불필요한 서브넷의 유무를 관리해야 합니다. AWS 계정에 프로비저닝 된 RDS 데이터베이스 인스턴스의 무단 액세스를 제한하지 않을 경우 인터넷상의 누구에게나 데이터베이스를 노출시켜 무차별 대입 공격, SQL 인젝션, DoS/DDos 공격과 같은 악의적인 활동의 위험을 증가시길 수 있습니다.		
설정 방법	**가. RDS 데이터베이스는 공개적으로 액세스 할 수 없어야 함 (HIGH)** 1) RDS 데이터베이스 탭 접근 -> 데이터베이스 생성  2) 퍼블릭 액세스 기본 설정  3) Datadog Misconfiguration 탐지 확인		

	
탐지 기준	**fu0-rtv-2rb** : RDS 인스턴스 설정에서 PublicAccessible이 True로 설정되어 있고 퍼블릭 서브넷에 포함(IGW에 연결된 상태)되어 있는 경우 탐지
비고	기술 공식 문서 : https://docs.datadoghq.com/security/default_rules/fu0-rtv-2rb/

3.9 ELB(Elastic Load Balancing) 연결 관리

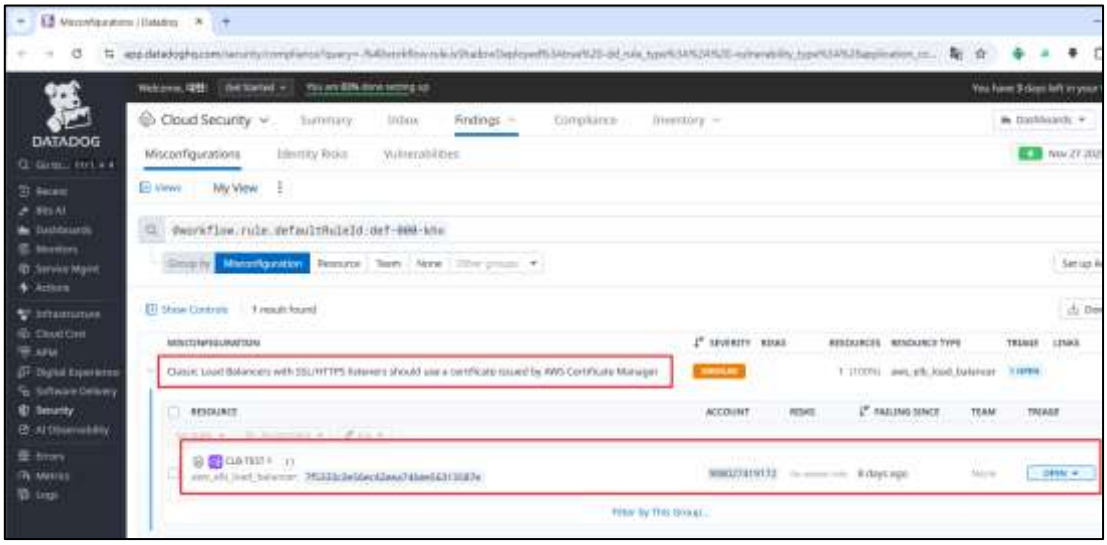
분류	가상 리소스 관리	중요도	중
항목명	ELB(Elastic Load Baclancing) 연결 관리		
항목 설명	Elastic Load Balancing은 둘 이상의 가용 영역에서 EC2 인스턴스, 컨테이너, IP 주소 등 여러 대상에 걸쳐 수신되는 트래픽을 자동으로 분산해주는 서비스 입니다. ELB의 종류로는 Application Load Balancers, Network Load Balancers, Gateway Load Balancers 및 Classic Load Balancer가 있으며 유형별로 살펴보면 ALB는 애플리케이션 트래픽을 리디렉션하기 위해 HTTP 헤더 또는 SSL 세션 ID와 같은 요청된 콘텐츠 검사 목적으로 사용되며 NLB는 IP 주소 및 기타 네트워크 정보를 검사해 트래픽을 최적으로 리디렉션하도록 도와줍니다. GLB는 네트워크 게이트웨이(모든 트래픽의 단일 진입점 및 종료점) 역할을 하며, 트래픽을 분산하는 동시에 수요에 따라 가상 어플라이언스의 규모를 조정하는 목적으로 사용됩니다. 차이점으로는 ALB, NLB 및 GLB는 네트워크 통신의 서로 다른 계층에서 작동합니다. ALB는 OSI 계층 7에서 작동하며 애플리케이션 수준의 트래픽 조작 및 라우팅을 지원합니다. NLB는 계층 4에서 작동하며 포트 및 IP 주소를 기반으로 하는 네트워크 수준 트래픽 관리를 지원합니다. GLB는 계층 3과 7에서 작동하며 게이트웨이 기능과 함께 네트워크 수준에서 밸런싱 및 라우팅 서비스를 제공합니다.		
설정 방법	**가. SSL/HTTPS 리스너가 있는 클래릭 로드 밸런서는 Certificate Manager에서 발급한 인증서를 사용해야 함 (MEDIUM)** 1) 로드밸런서 탭 접근 -> 로드 밸런서 생성  2) Classic Load Balancer 생성		



3) 리스너 설정

4) IAM 인증서 선택 후 생성

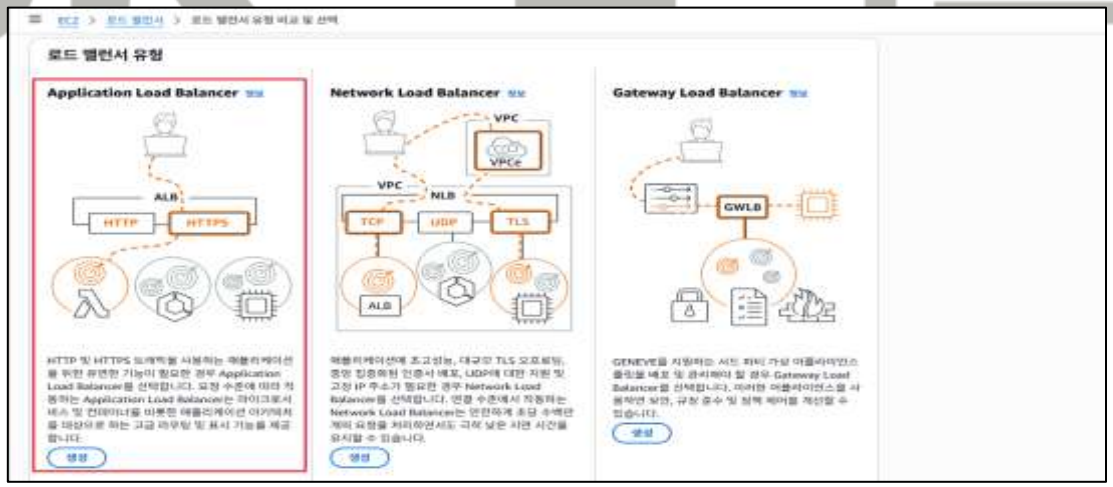
5) Datadog Misconfiguration 탐지 확인



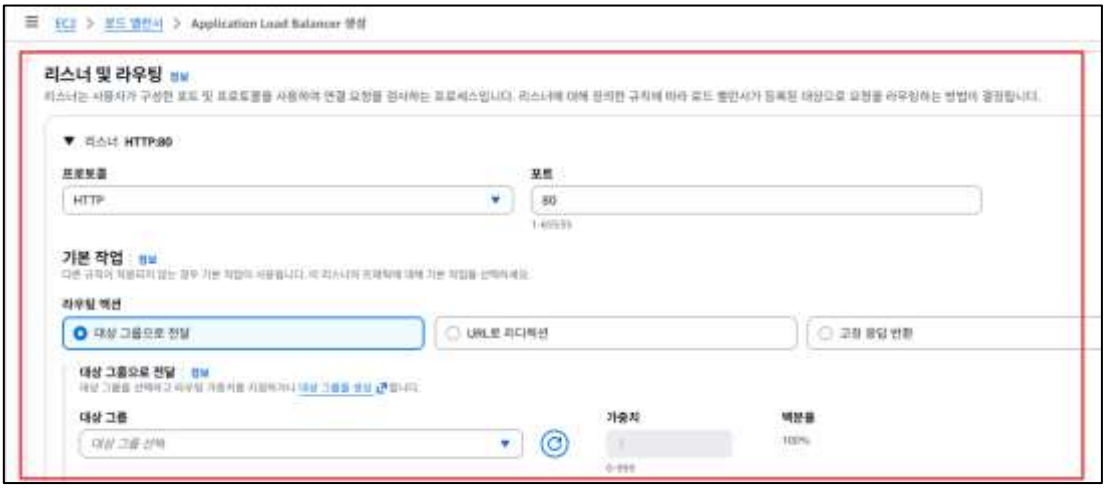
나. 삭제 보호 기능을 활성화해야 함 (MEDIUM)

1) 로드밸런서 탭 접근 -> 로드 밸런서 생성

2) Application Load Balancer 생성

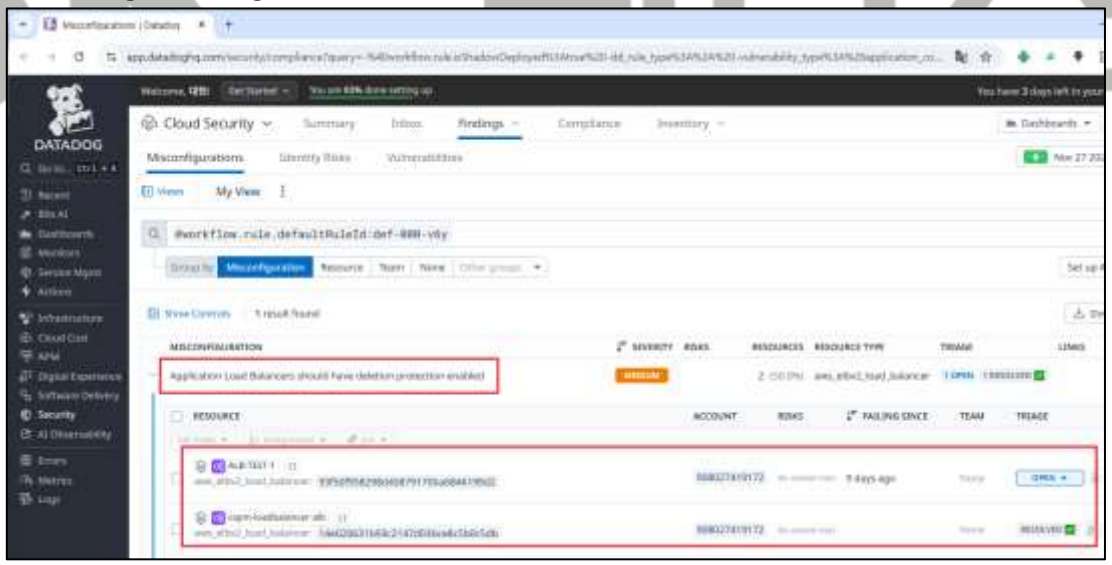


3) 기본 설정으로 로드 밸런서 생성



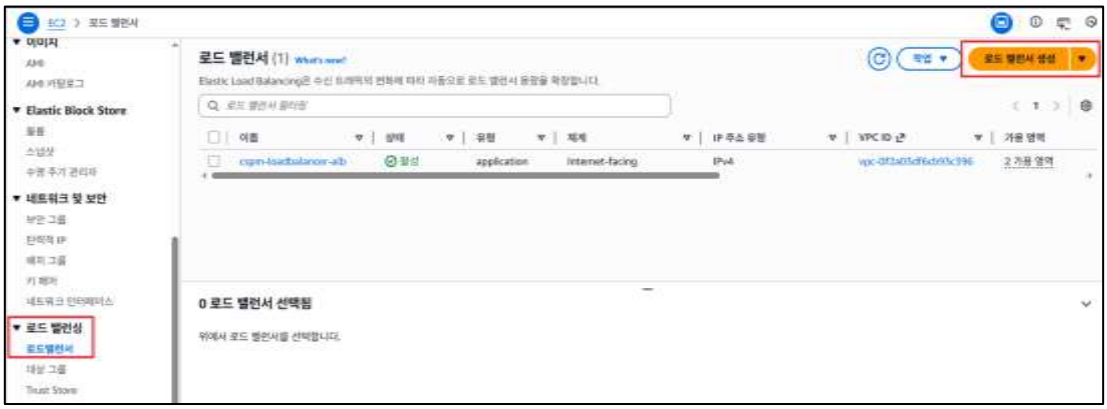
4) 삭제 방지 옵션 확인

5) Datadog Misconfiguration 탐지 확인

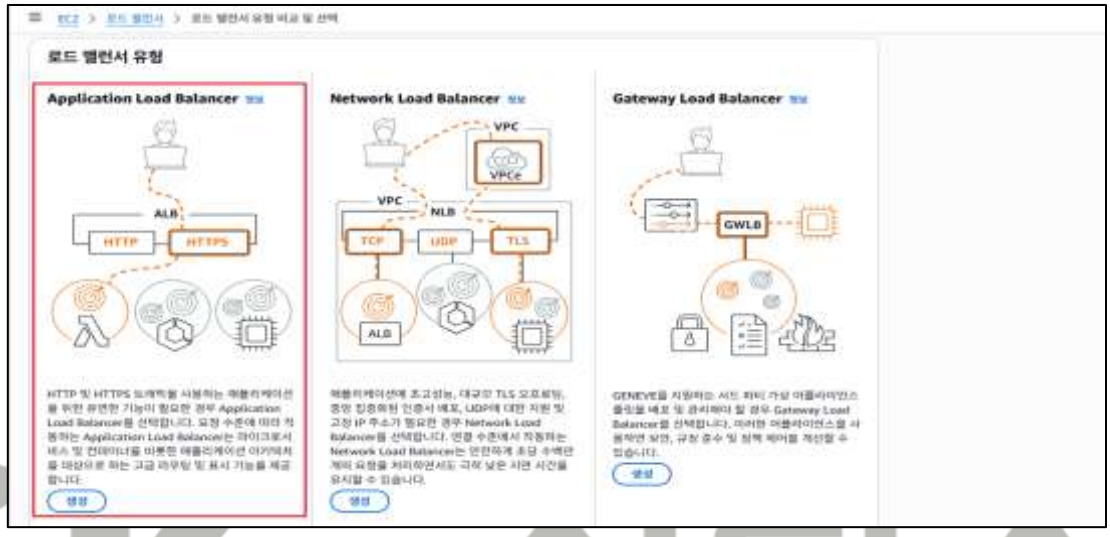


다. 잘못된 헤더 필드 삭제 설정 기능을 활성화해야 함 (MEDIUM)

1) 로드밸런서 탭 접근 -> 로드 밸런서 생성



2) Application Load Balancer 생성



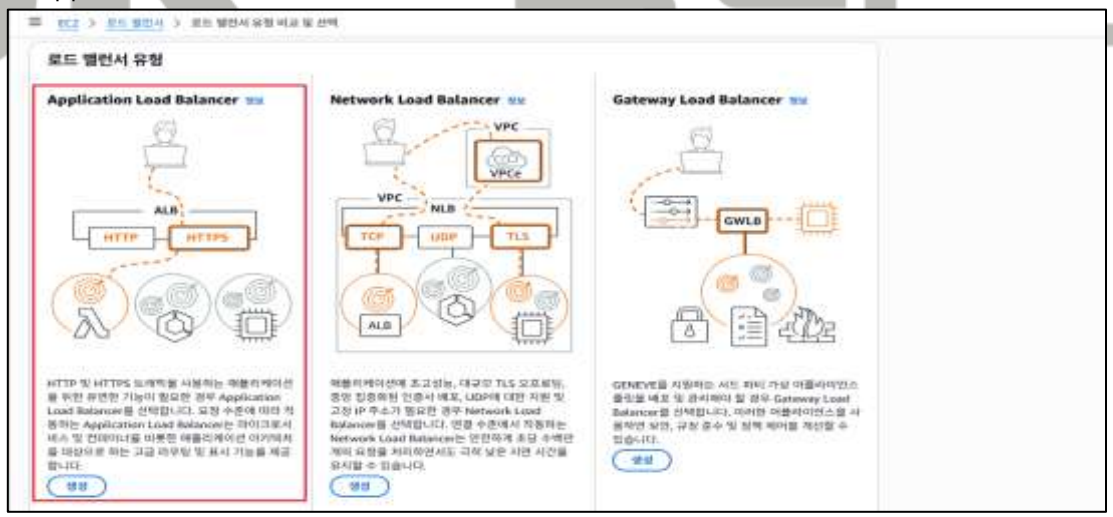
3) 기본 설정으로 로드 밸런서 생성

4) 잘못된 헤더 필드 삭제 옵션 확인

라. HTTPS 리스너를 사용해야 함 (LOW)

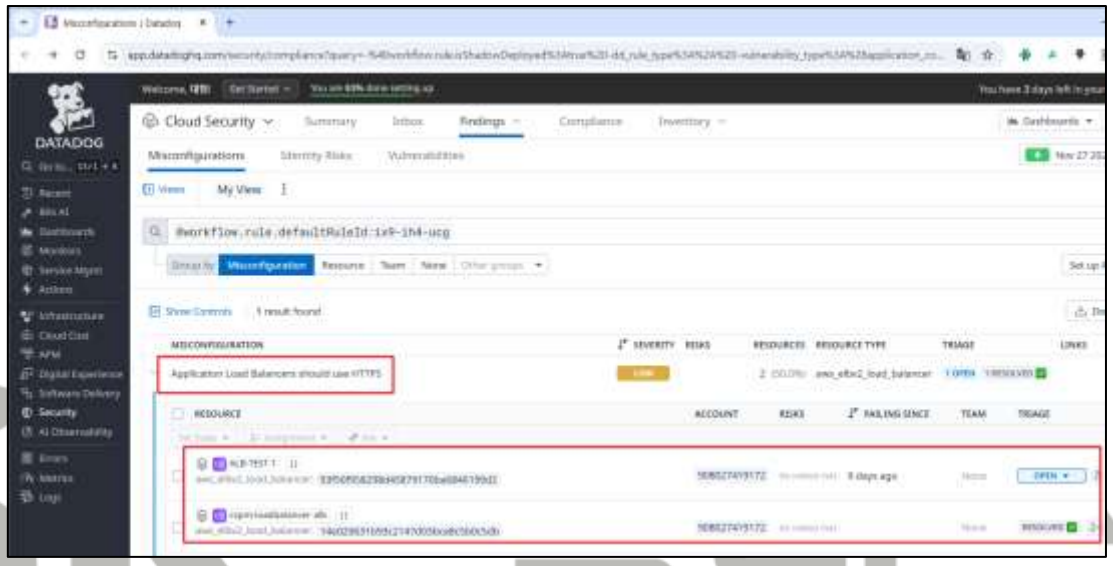
1) 로드밸런서 탭 접근 -> 로드 밸런서 생성

2) Application Load Balancer 생성



3) 기본 설정으로 로드 밸런서 생성

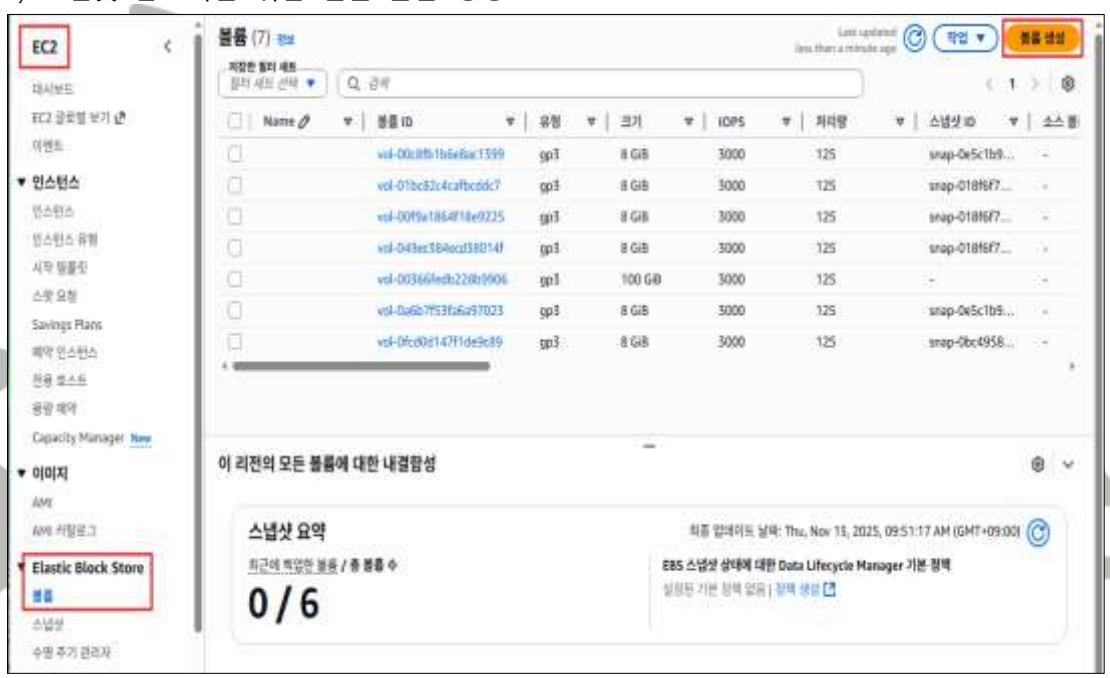
<table>
<tr>
<td></td>
<td>

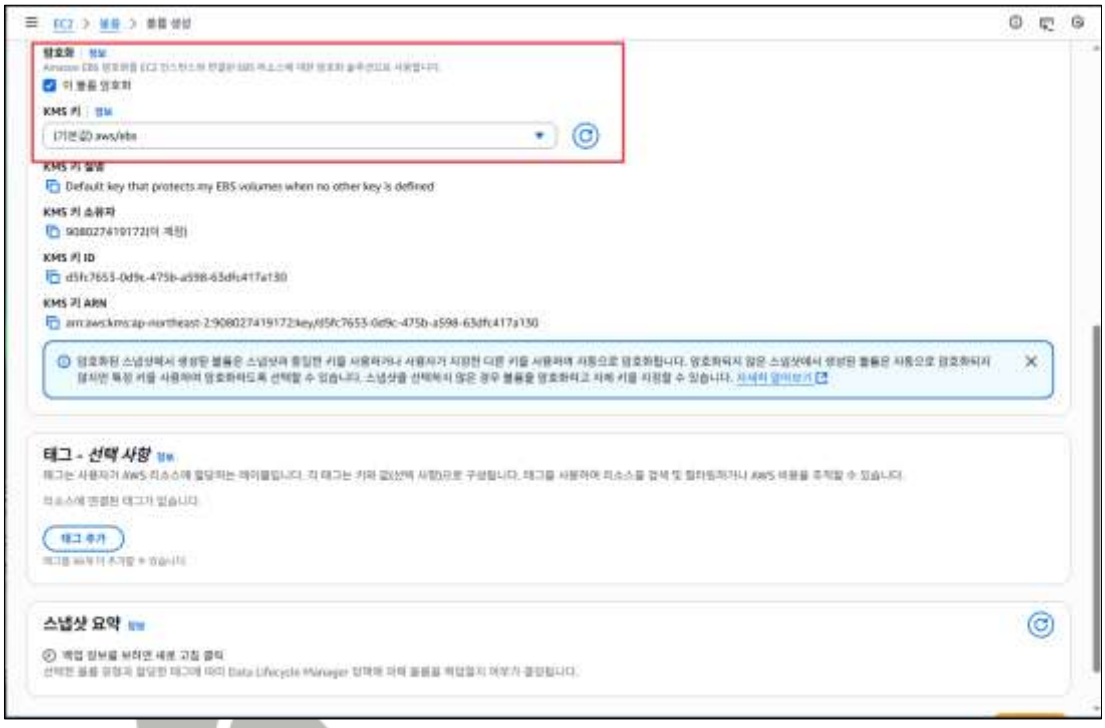

4) Datadog Misconfiguration 탐지 확인


</td>
</tr>
<tr>
<td>탐지
기준</td>
<td>
def-000-khx : HTTPS 리스너 사용 시 인증서를 ACM에서 가져오지 않은 경우 탐지
def-000-v6y : ALB 삭제 보호 기능이 비활성화되어 있는 경우 탐지
def-000-v86 : Public ALB가 잘못된 헤더 필드 삭제 설정이 비활성화되어 있는 경우 탐지
ix9-ih4-ucg : 생성된 ALB 리스너가 HTTP인 경우 탐지
</td>
</tr>
<tr>
<td>비고</td>
<td>
기술 공식 문서 :
https://docs.datadoghq.com/security/default_rules/def-000-khx/
https://docs.datadoghq.com/security/default_rules/def-000-v6y/
https://docs.datadoghq.com/security/default_rules/def-000-v86/
https://docs.datadoghq.com/security/default_rules/ix9-ih4-ucg/
</td>
</tr>
</table>

4. 운영 관리

4.1 EBS 및 볼륨 암호화 설정

분류	운영 관리	중요도	중
항목명	EBS 및 볼륨 암호화 설정		
항목 설명	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.		
설정 방법	**가. EBS 스냅샷은 암호화해야 함 (MEDIUM)** ***※ 스냅샷 암호화의 경우 사용하려는 볼륨 또는 인스턴스의 암호화 설정을 그대로 따름 별도 커스텀 설정이 불가능*** 1) 스냅샷 암호화를 위한 샘플 볼륨 생성  2) 볼륨 생성 시 암호화 설정		



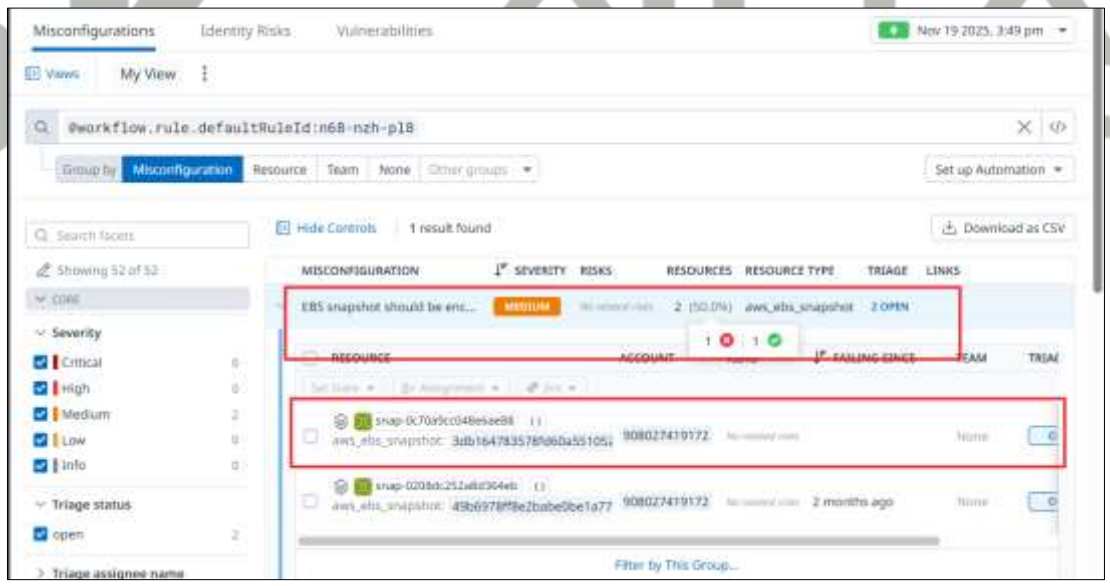
3) 생성된 볼륨 확인 (암호화 설정 확인)

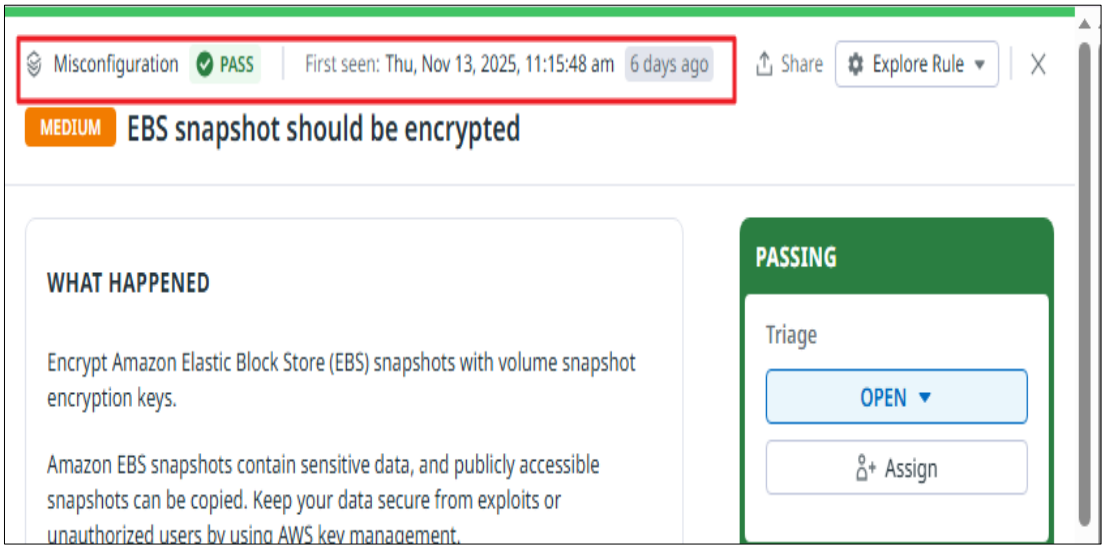
4) 스냅샷 생성 시도

5) 스냅샷 생성 시 "1) ~ 3)" 과정에서 생성한 암호화 설정된 볼륨 사용

6) 스냅샷 암호화 적용 확인

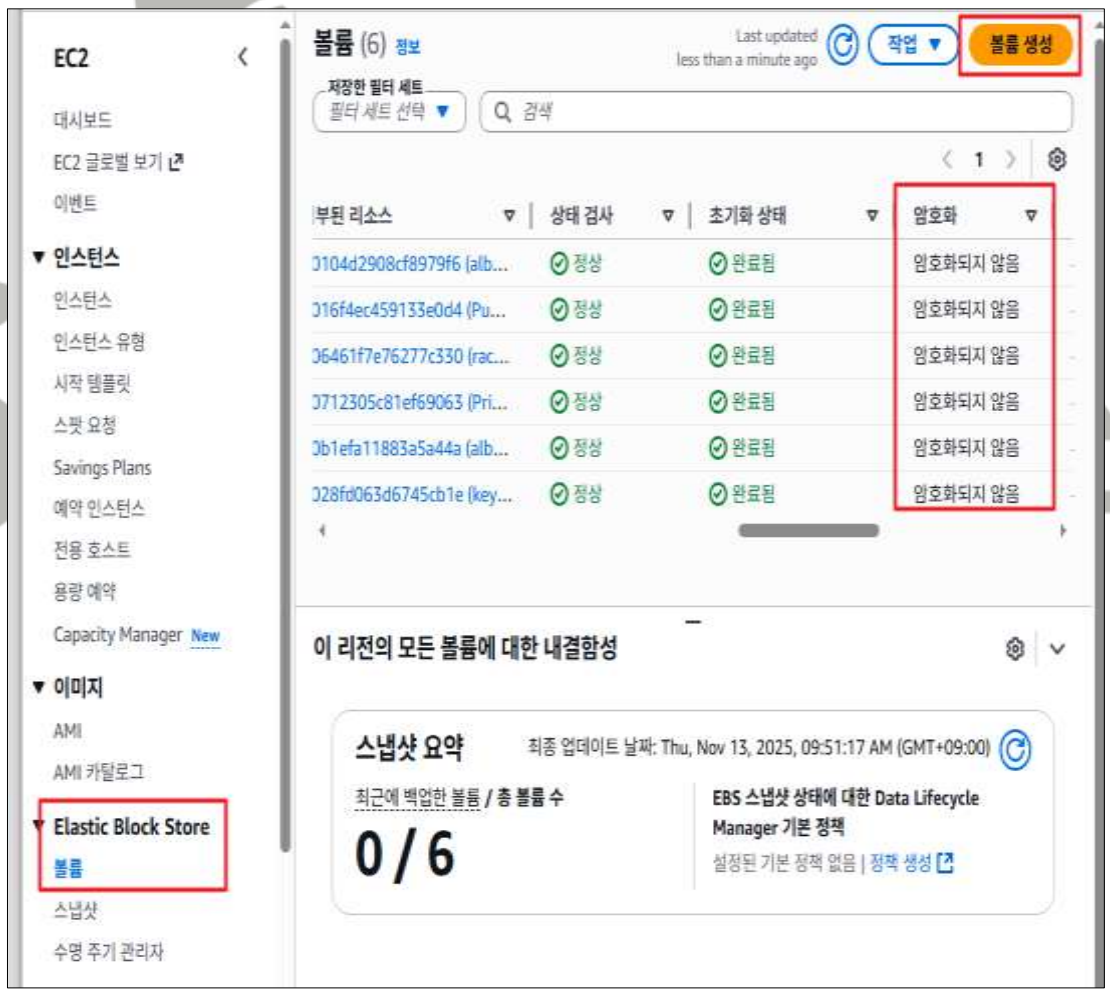
7) Datadog 내 스냅샷 암호화 탐지 확인



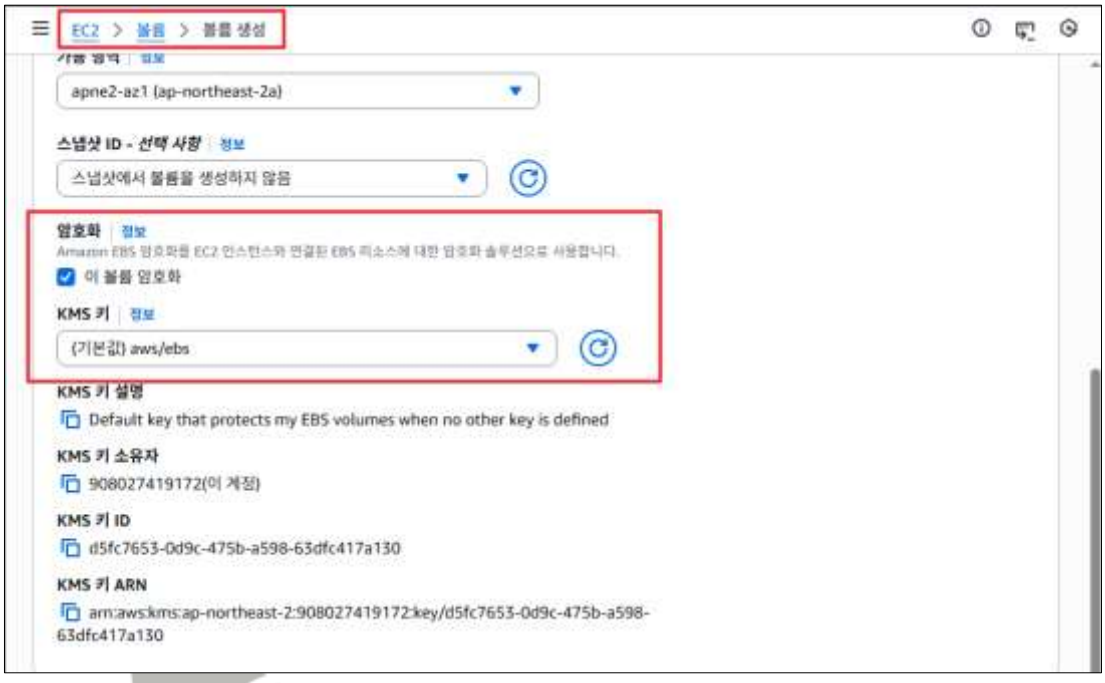


나. EBS 볼륨은 암호화해야 함 (LOW)

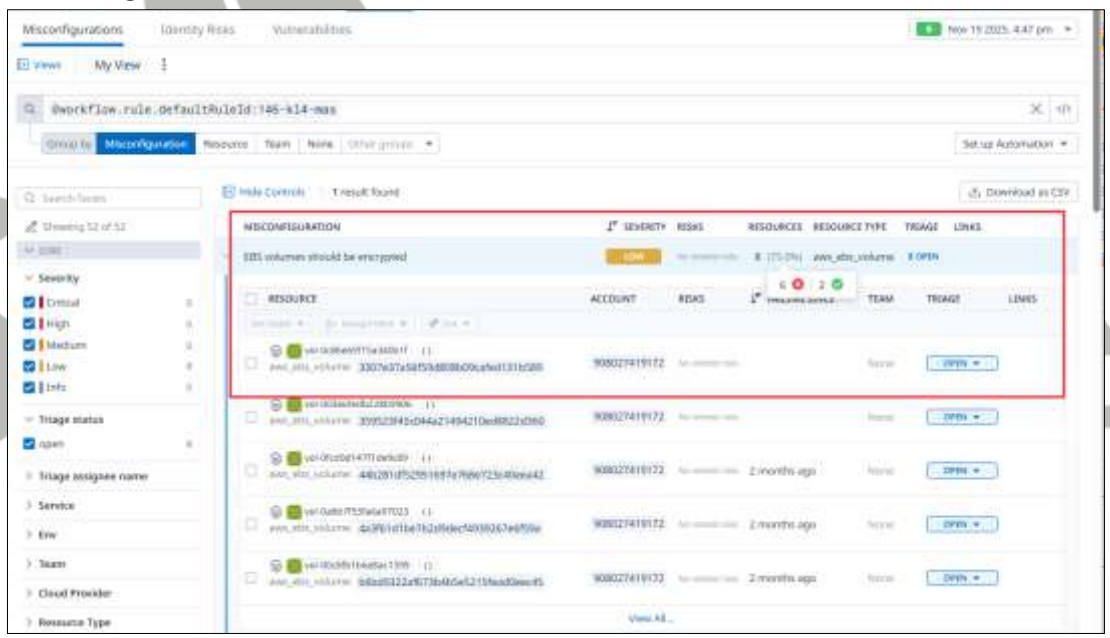
1) EC2 > EBS > 볼륨 > 볼륨 생성

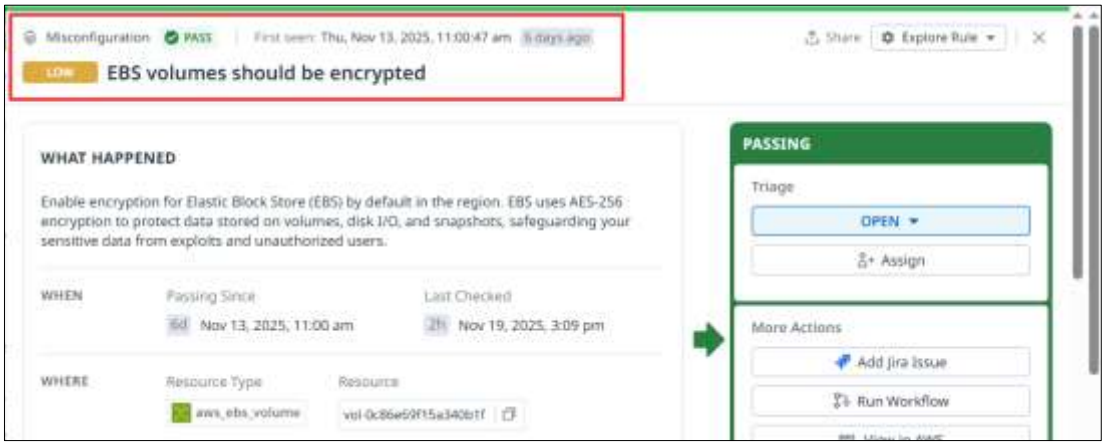


2) 볼륨 생성 메뉴 내 "암호화" 활성화 후 KMS 키 값을 추가하여 설정해야 함

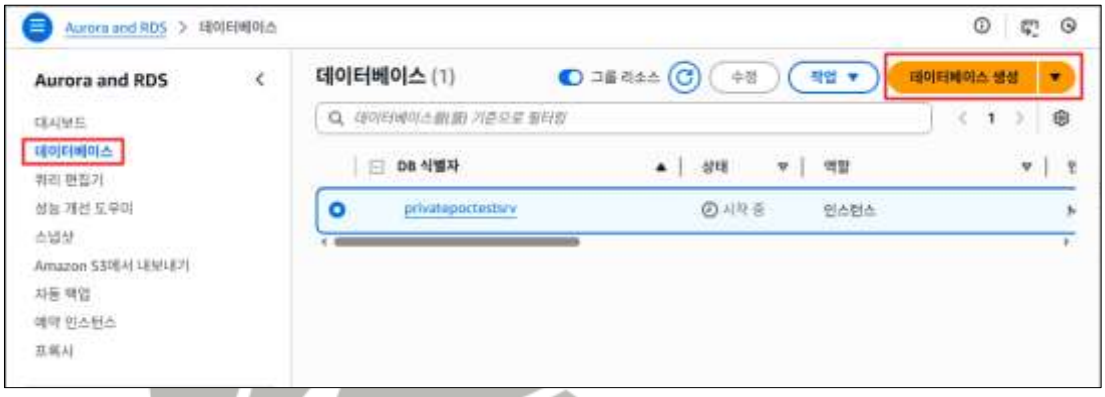


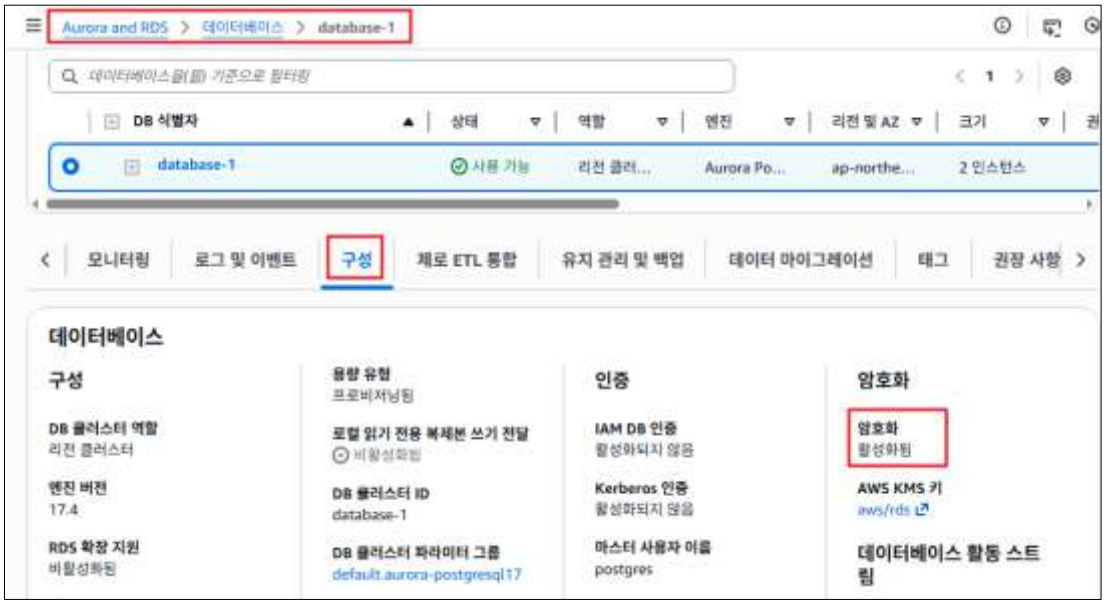
3) Datadog 내 볼륨 암호화 탐지 확인



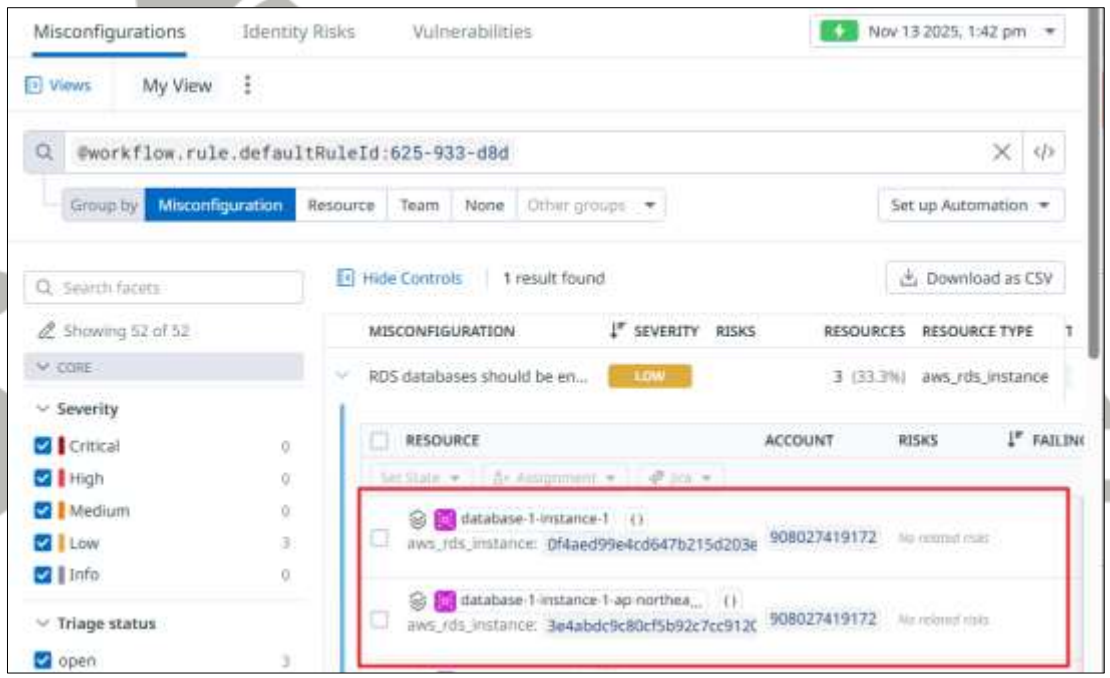
	
탐지 기준	**n68-nzh-pl8** : 스냅샷 암호화 설정이 비활성화되어 있는 경우 탐지 **146-kl4-mas** : EBS 볼륨 암호화 설정이 비활성화되어 있는 경우 탐지
비고	기술 공식 문서 : https://docs.datadoghq.com/security/default_rules/n68-nzh-pl8/ https://docs.datadoghq.com/security/default_rules/146-kl4-mas/

4.2 RDS 암호화 설정

분류	운영 관리	중요도	중
항목명	RDS 암호화 설정		
항목 설명	RDS는 데이터 보호를 위해 DB 인스턴스에서 암호화 옵션 기능을 제공하며 암호화 시 AES-256 암호화 알고리즘을 이용하여 DB 인스턴스의 모든 로그, 백업 및 스냅샷 암호화가 가능합니다.		
설정 방법	**가. RDS 데이터베이스 인스턴스는 암호화해야 함 (LOW)** ***※ 데이터베이스 인스턴스가 생성된 이후에 암호화 설정 변경 불가*** 1) 데이터베이스 생성 시도  2) DB 생성 시 인스턴스 암호화 설정 가능  3) 데이터베이스 인스턴스 암호화 확인 (DB 인스턴스 > 구성)		

<table>
<tr><td></td><td>


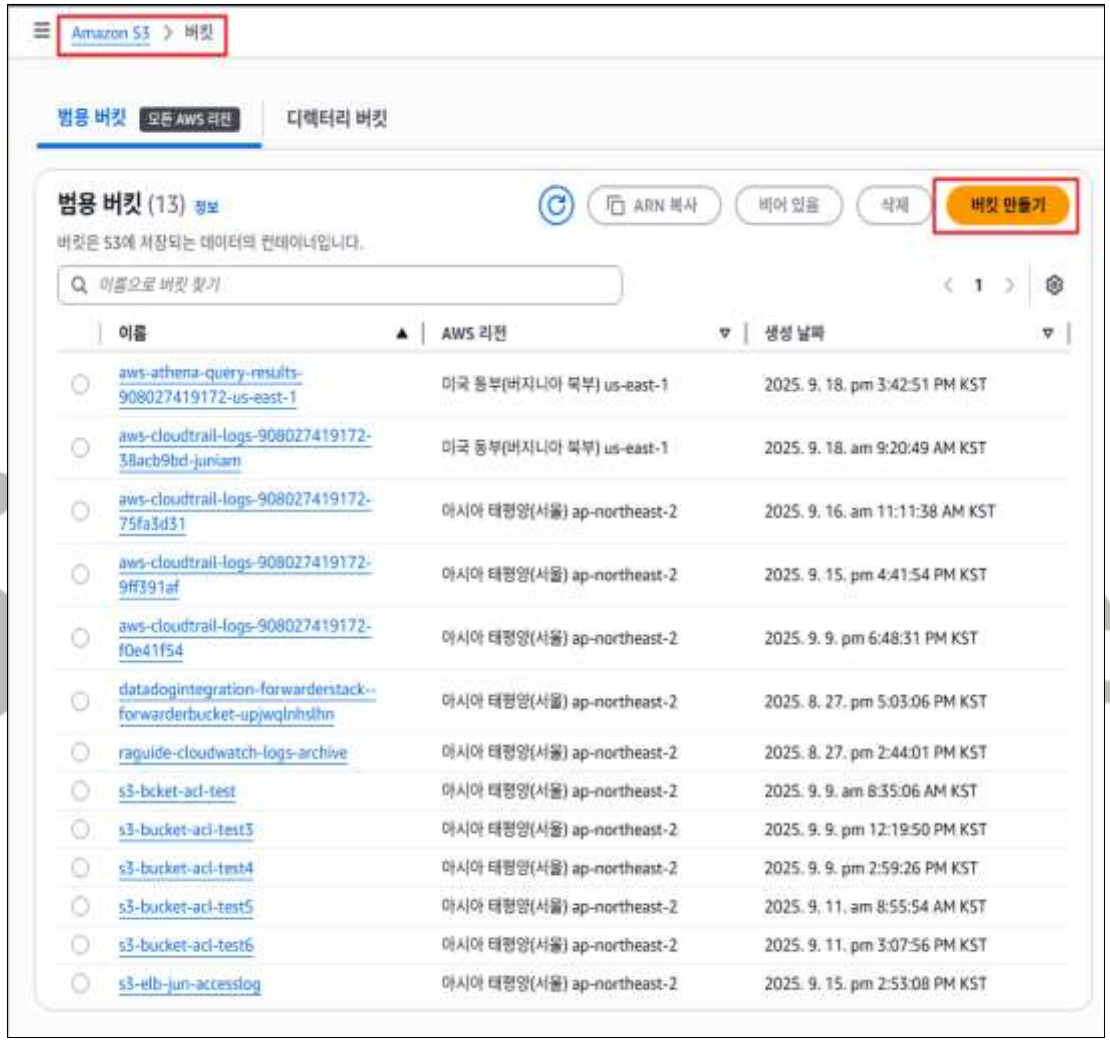
4) Datadog 내 데이터베이스 암호화 탐지 확인

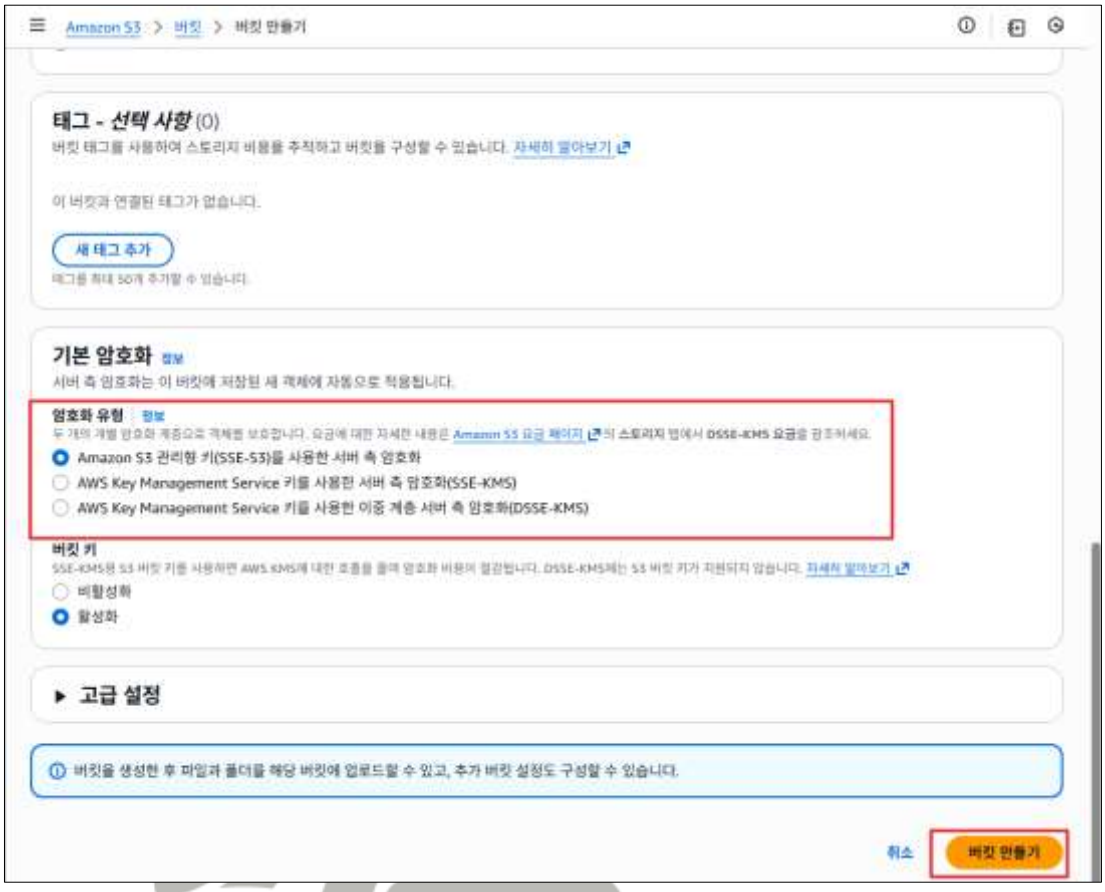


</td></tr>
<tr><td>탐지 기준</td><td>625-933-d8d : RDS 인스턴스 암호화 설정이 비활성화되어 있는 경우 탐지</td></tr>
<tr><td>비고</td><td>기술 공식 문서 :
https://docs.datadoghq.com/security/default_rules/625-933-d8d/</td></tr>
</table>

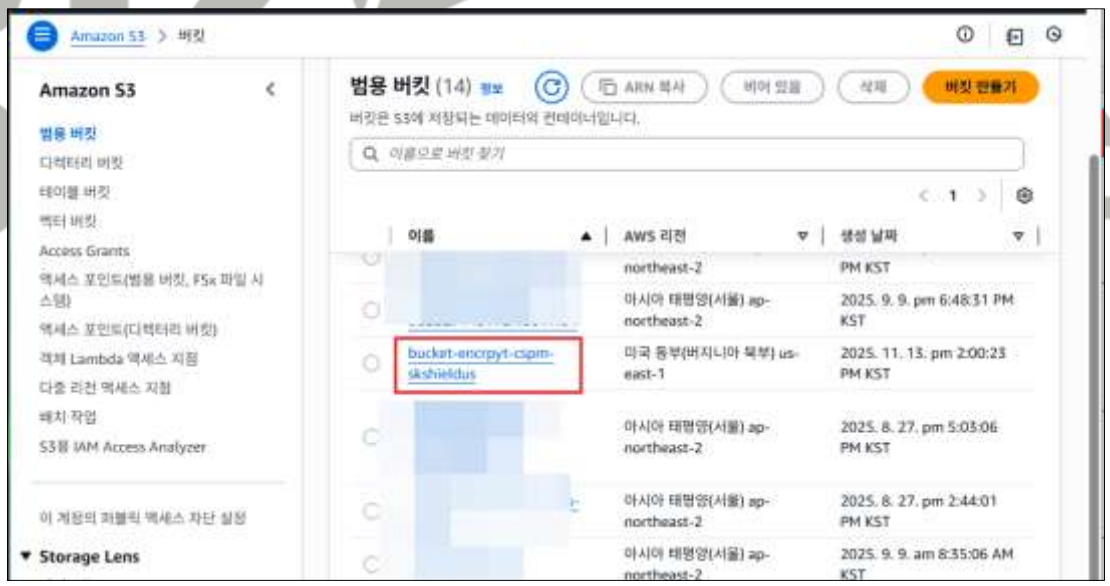
4.3 S3 암호화 설정

분류	운영 관리	중요도	중
항목명	S3 암호화 설정		

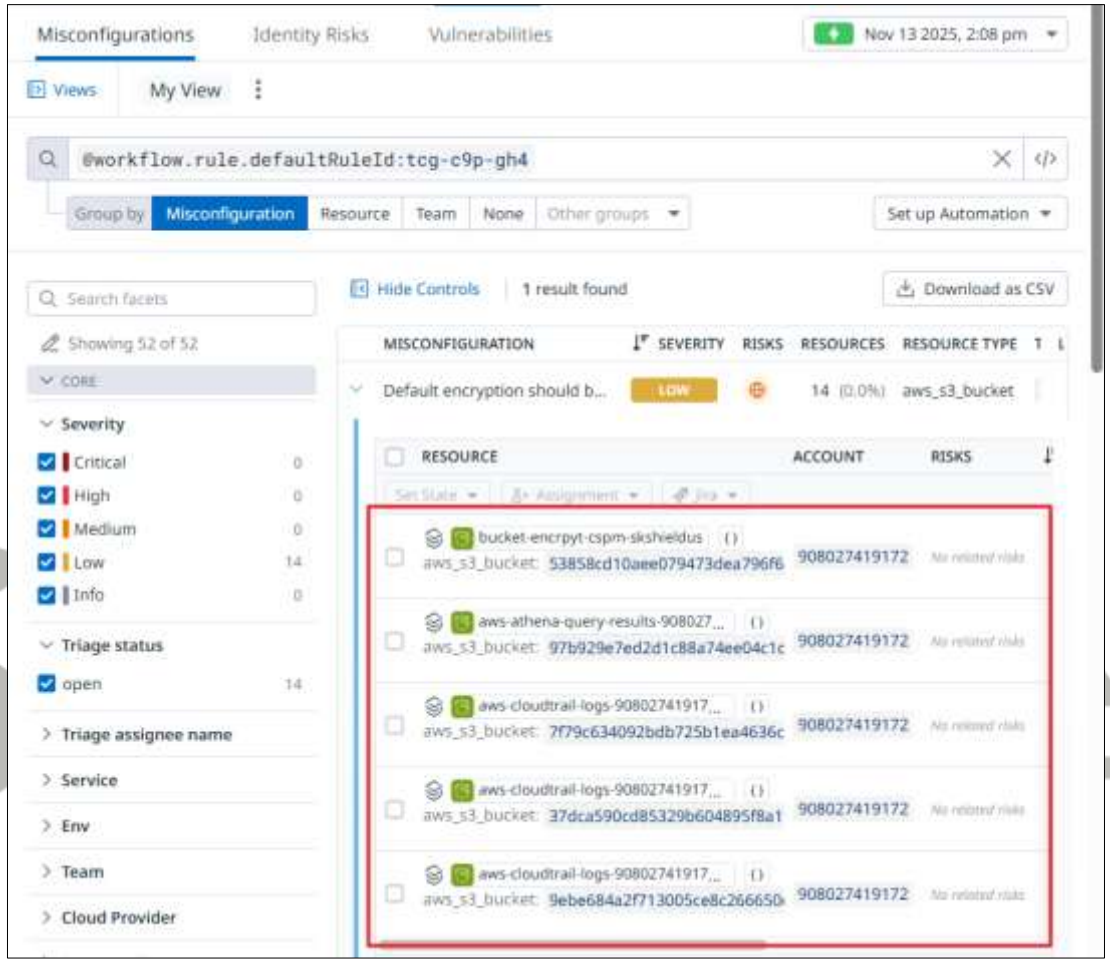
항목 설명	버킷 기본 암호화 설정은 S3 버킷에 저장되는 모든 객체를 암호화 되도록 하는 설정이며 Amazon S3 관리형 키(SSE-S3) 또는 AWS KMS 관리형 키(SSE-KMS)로 서버 측 암호화를 사용하여 객체를 암호화합니다. **※ S3 버킷 신규 생성 시 기본 암호화 (SSE-S3, SSE-KMS)를 설정할 수 있으며, 버킷에 기본 암호화가 적용된 상태에서 객체가 저장될 경우 하위 객체까지 자동으로 암호화 설정이 가능함**
설정 방법	**가. S3 버킷은 기본 암호화를 활성화해야 함 (LOW)** ***※ 버킷 내 암호화 설정 사용은 필수이며 AWS 관리형 키 적용 권고*** 1) S3 버킷 선택  2) S3 버킷 생성 시 기본 암호화 설정 확인



3) S3 버킷 속성 확인 (기본 암호화 설정 확인)

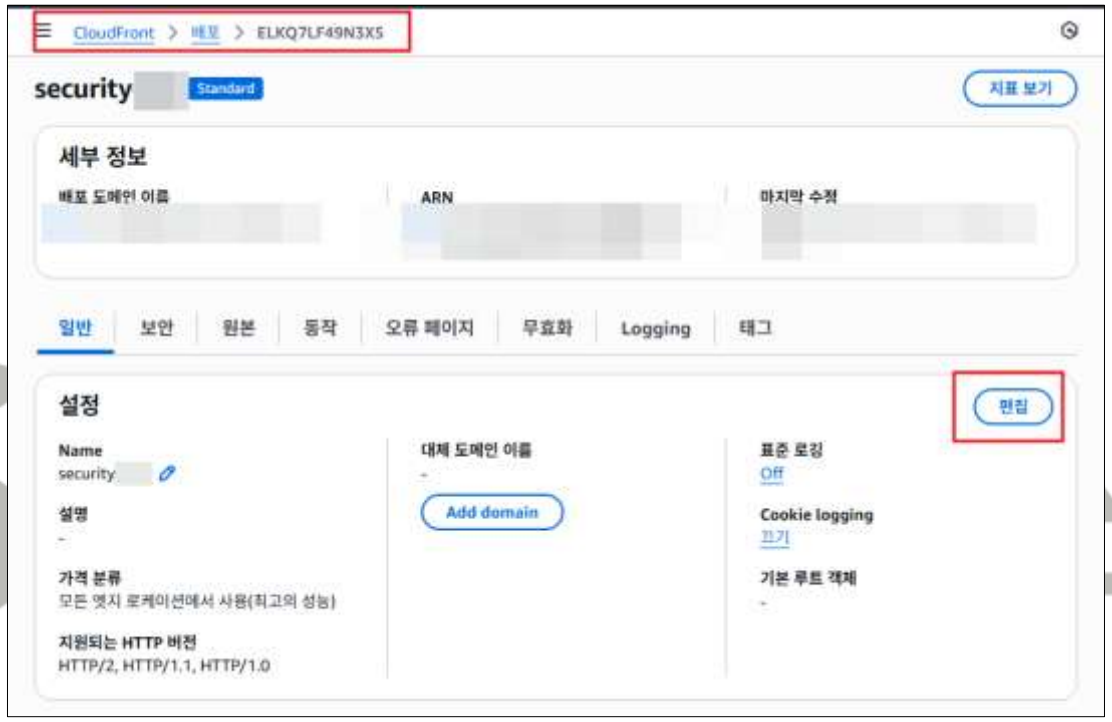


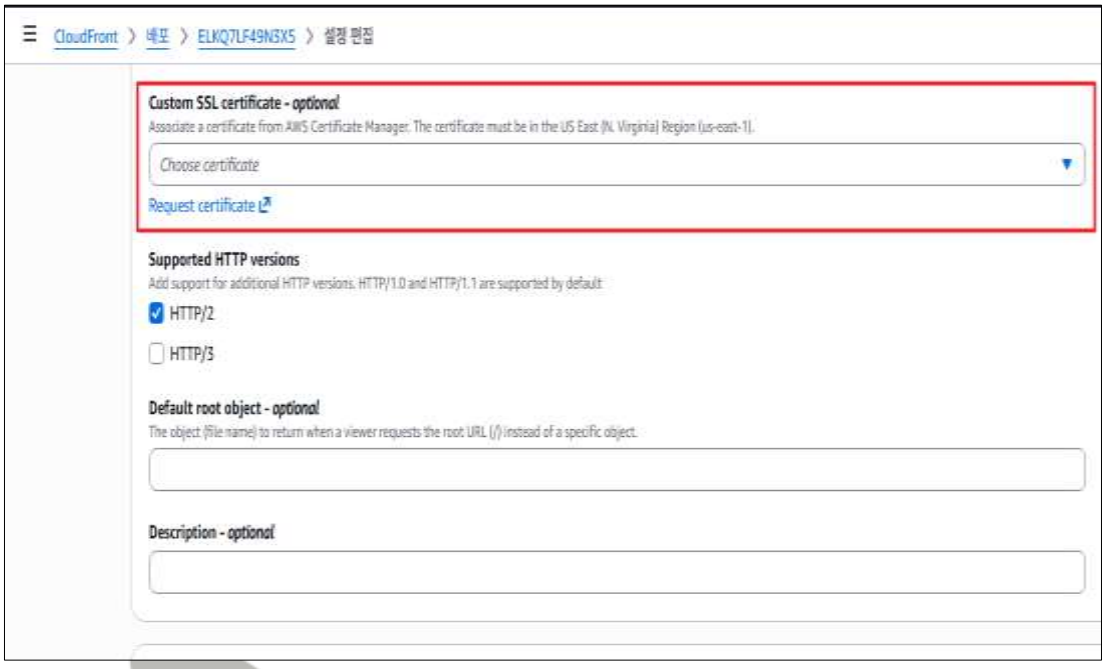
4) Datadog 내 S3 버킷 암호화 탐지 확인



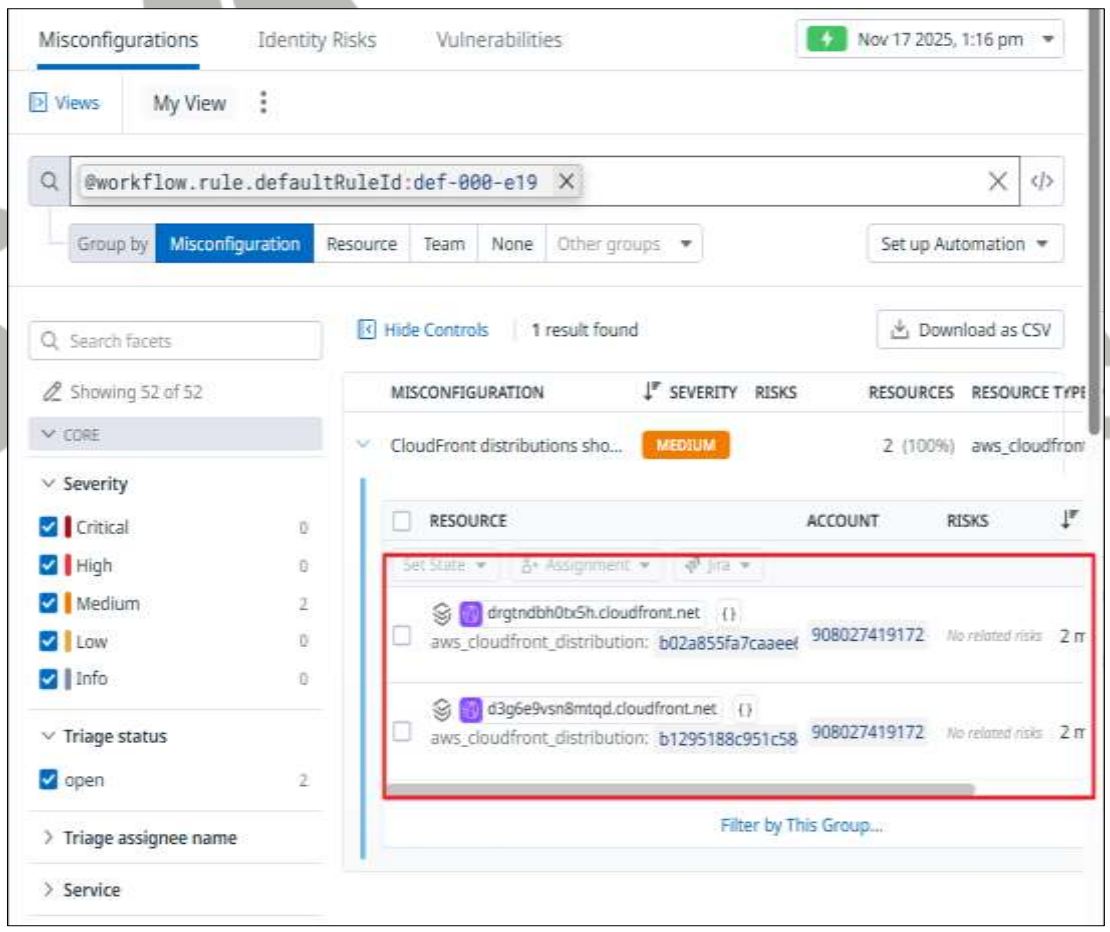
탐지 기준	**tcg-c9p-gh4** : S3 기본 암호화 유형 탐지
비고	기술 공식 문서 : https://docs.datadoghq.com/security/default_rules/tcg-c9p-gh4/

4.4 통신구간 암호화 설정

분류	운영 관리	중요도	중
항목명	통신구간 암호화 설정		
항목 설명	클라우드 리소스를 통해 대/내외 서비스에서 정보를 송, 수신 하는 경우 중간에서 공격자가 패킷을 가로채어 공격에 활용할 수 없도록 통신구간을 암호화하여 설정하여야 합니다. CloudFront 배포판이 사용자 지정 SSL/TLS 인증서를 사용하고 있으며 HTTPS 요청 처리에 서버 이름 표시(SNI)를 사용하도록 설정되어 있는지 확인합니다. 사용자 지정 SSL/TLS 인증서가 연결되어 있지만 SSL/TLS 지원 방식에 전용 IP주소가 포함된 경우 해당 검사가 실패할 수 있습니다.		
설정 방법	**가. CloudFront 배포 시 SNI를 사용하여 HTTPS 요청을 처리해야 함 (MEDIUM)** 1) HTTPS 적용을 위한 배포 편집  2) HTTPS 적용을 위한 Custom SSL 인증서 설정 ***※ HTTPS 요청을 적용하기 위해서 실제 소유권이 확인된 도메인이 존재해야함***		

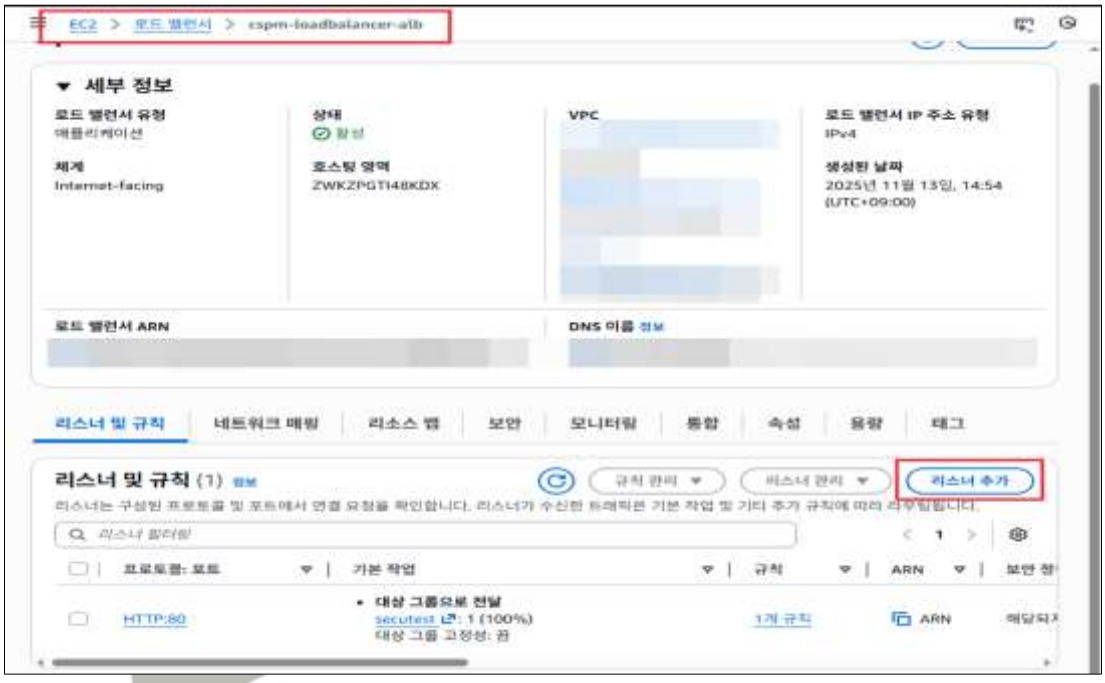


3) Datadog 내 CloudFront 배포 HTTPS 설정

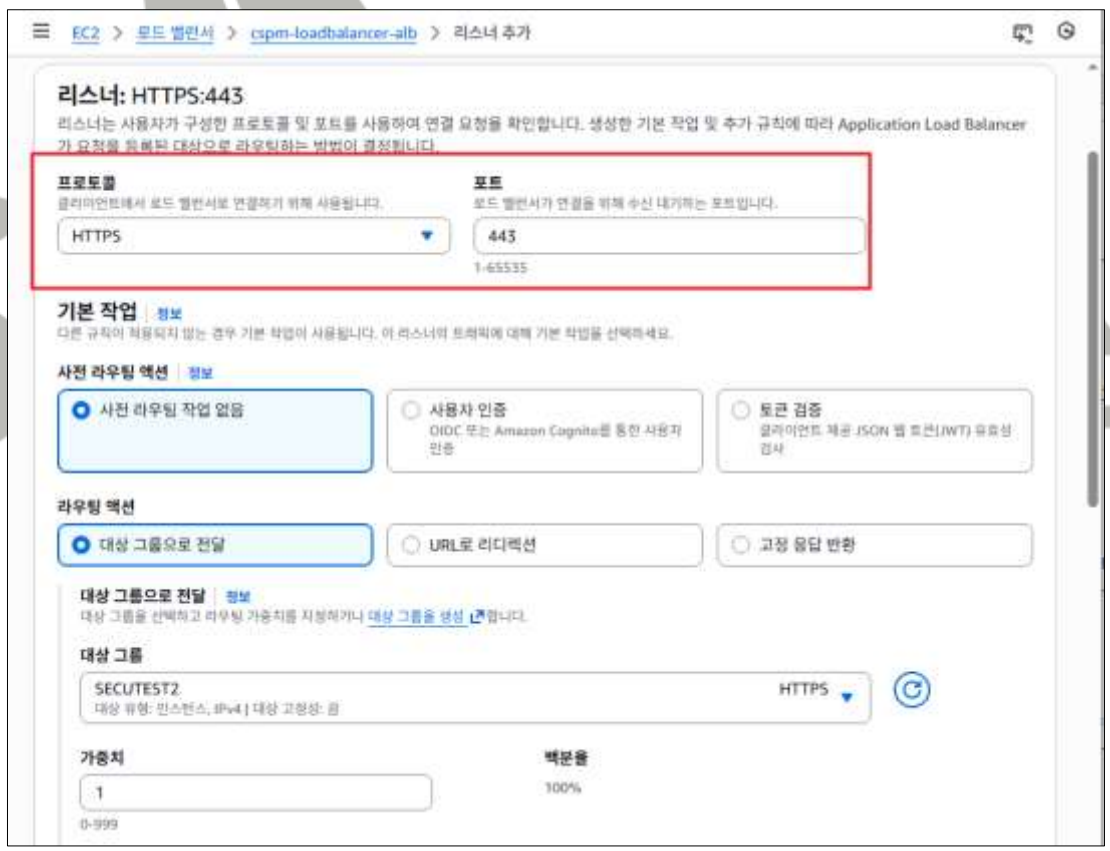


나. ALB 통신 시 HTTPS 사용해야 함 (LOW)

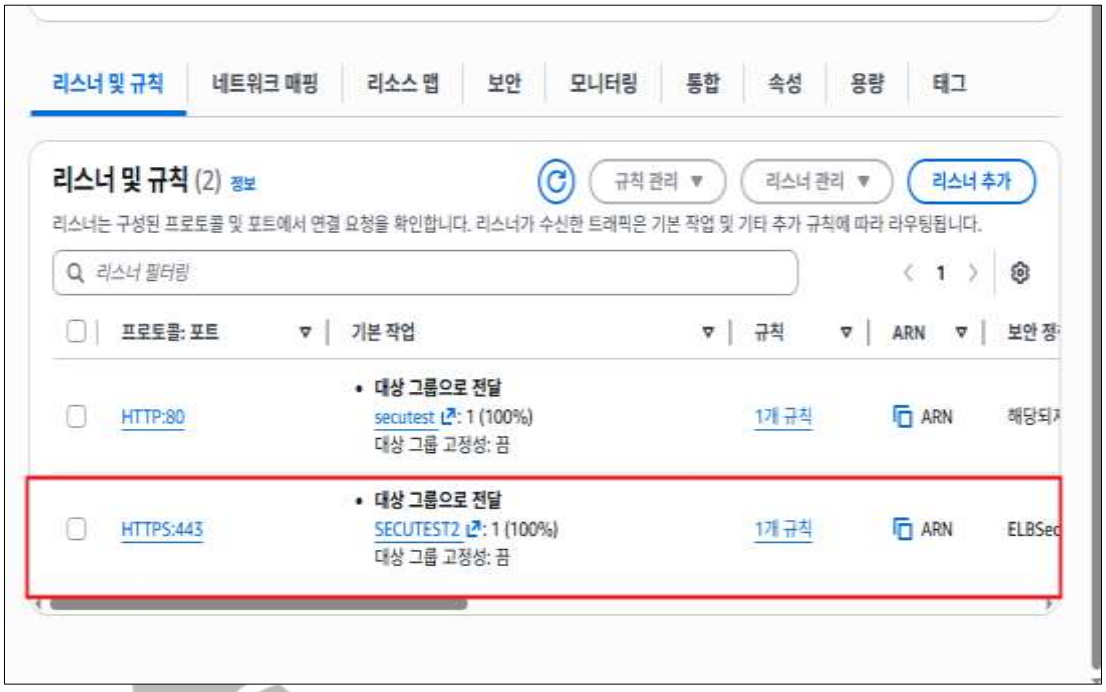
1) HTTPS 설정을 위한 ALB 리스너 추가



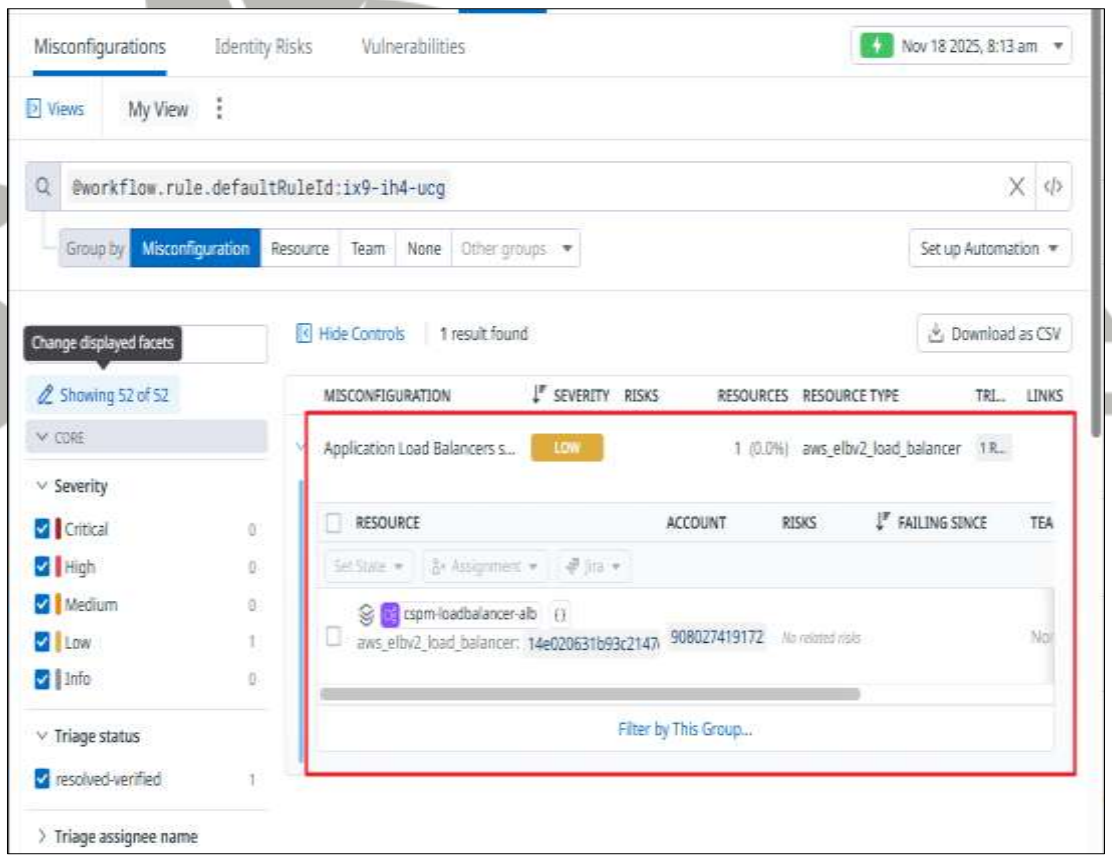
2) 암호화 프로토콜(HTTPS) 설정



3) 리스너 추가 확인 및 암호화 설정 확인



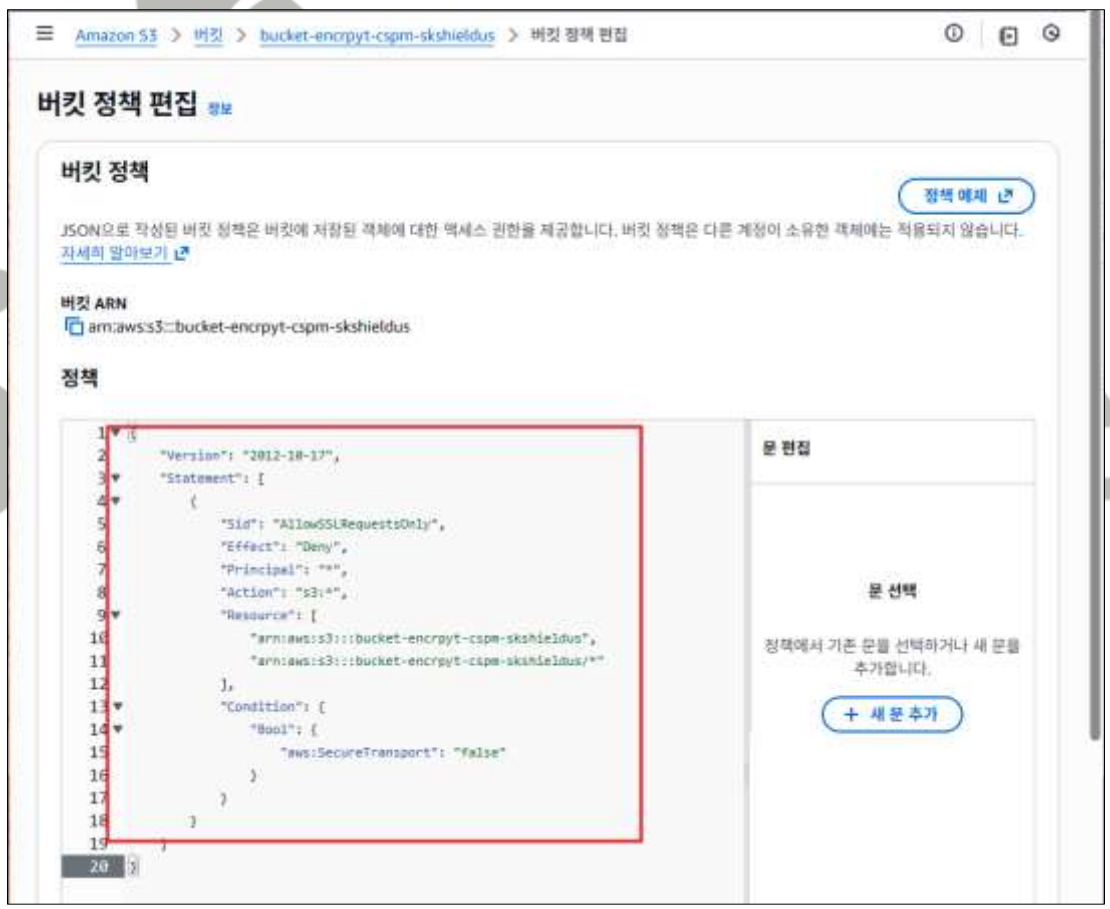
4) Datadog 내 로드밸런서 HTTPS 설정 탐지



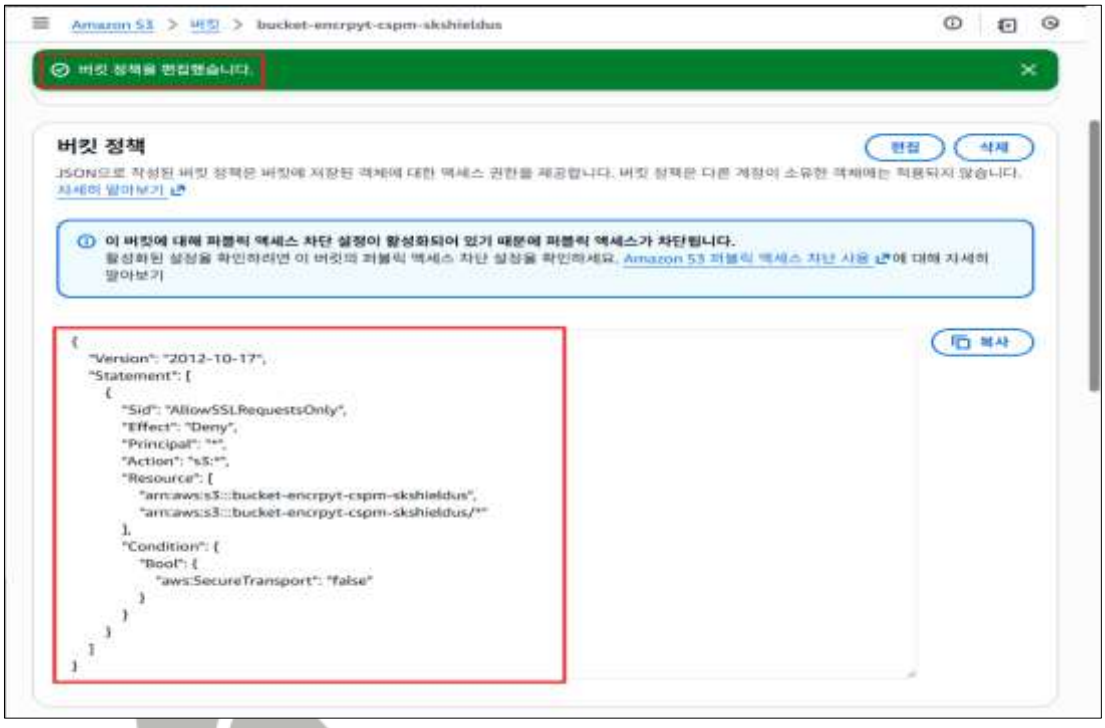
다. S3 버킷 정책은 HTTP 요청을 거부해야 함 (LOW)

1) HTTPS 설정을 위한 S3 버킷 정책 수정 시도

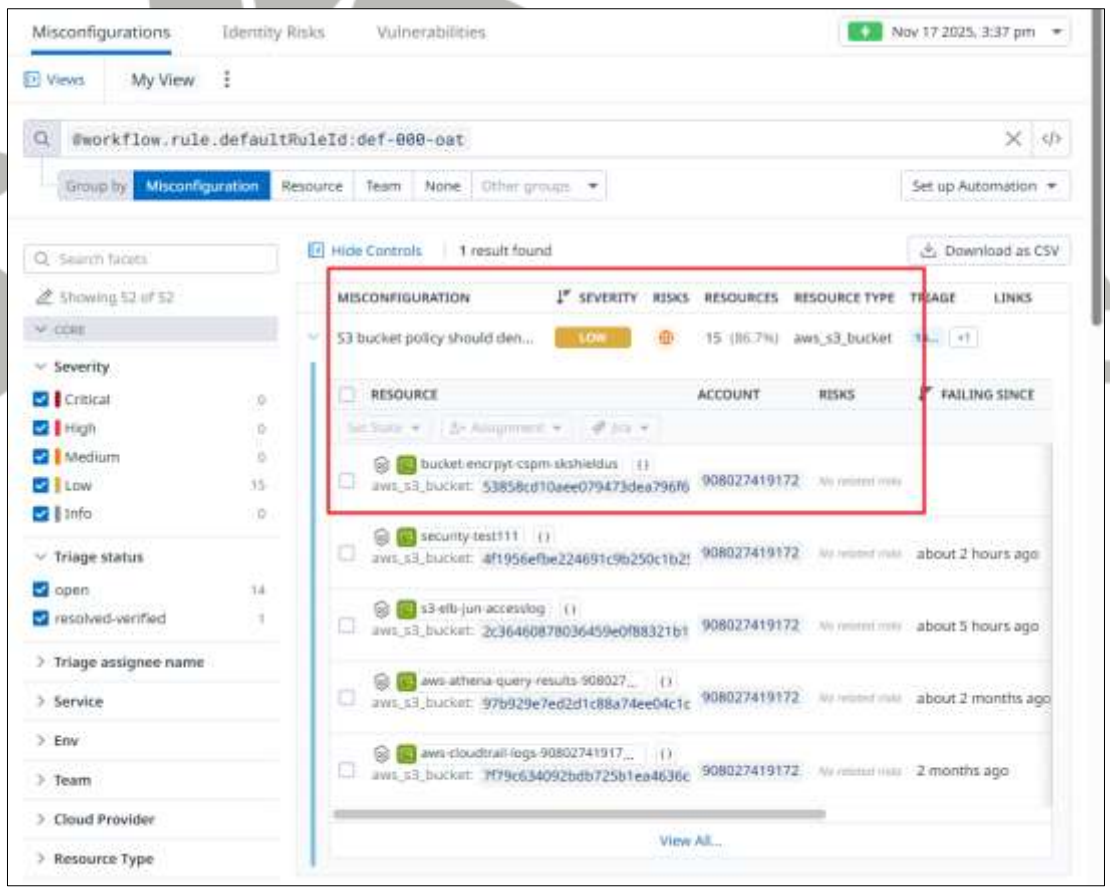
2) 버킷 정책 편집 - HTTP 요청 거부 설정



3) 정책 편집 완료



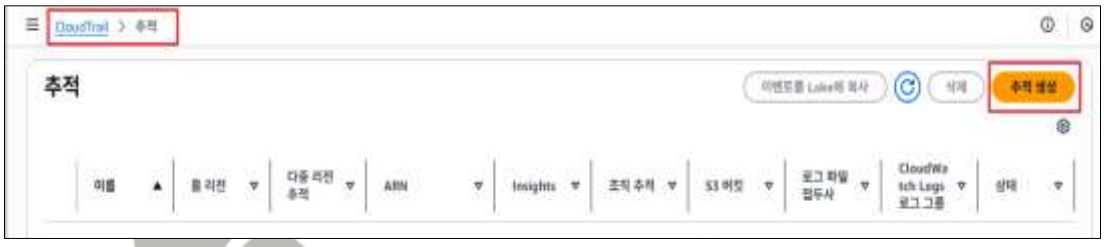
4) Datadog 내 S3 HTTP 요청 deny 정책 적용 확인



탐지 기준	**def-000-e19** : CloudFront 사용 시 사용자 정의 인증서(SSL/TLS) 사용 여부 탐지 **ix9-ih4-ucg** : ALB 리스너 Rule에서 HTTPS 사용 여부 탐지

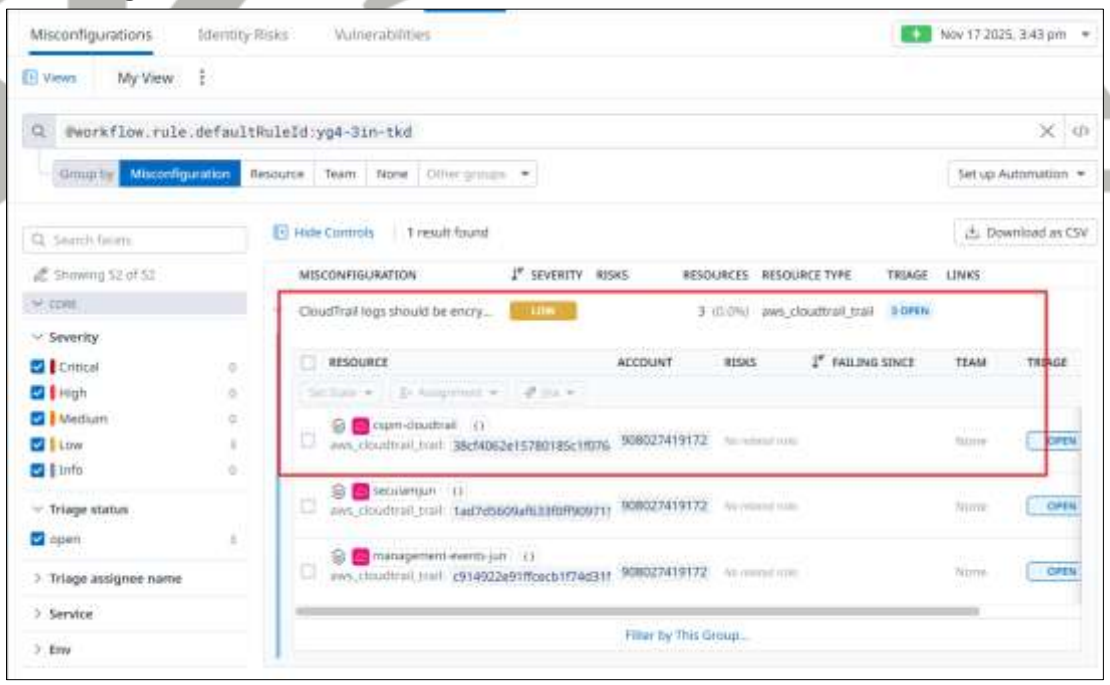
	def-000-oat : S3 버킷 내 HTTP 요청 거부 정책 존재여부 탐지
비고	기술 공식 문서 : https://docs.datadoghq.com/security/default_rules/def-000-e19/ https://docs.datadoghq.com/security/default_rules/ix9-ih4-ucg/ https://docs.datadoghq.com/security/default_rules/def-000-oat/

4.5 CloudTrail 암호화 설정

분류	운영 관리	중요도	중
항목명	CloudTrail 암호화 설정		
항목 설명	CloudTrail 이 버킷에 제공하는 로그 파일은 Amazon S3 가 관리하는 암호화 키(SSE-S3)를 사용하는 서버 측 암호화를 사용하여 암호화됩니다. 직접 관리할 수 있는 보안 계층을 제공하려면 CloudTrail 로그 파일에 대한 AWS KMS 관리형 키(SSE-KMS)를 사용하는 서버 측 암호화를 대신 사용하면 됩니다.		
설정 방법	**가. CloudTrail 로그는 KMS CMK를 사용하여 저장 시 암호화해야 함 (MEDUIM)** 1) CloudTrail 추적 생성  2) CloudTrail 추적 내 로그 파일 SSE-KMS 암호화 설정  3) CloudTrail 추적 생성 완료		

4) CloudTrail 암호화 설정 확인

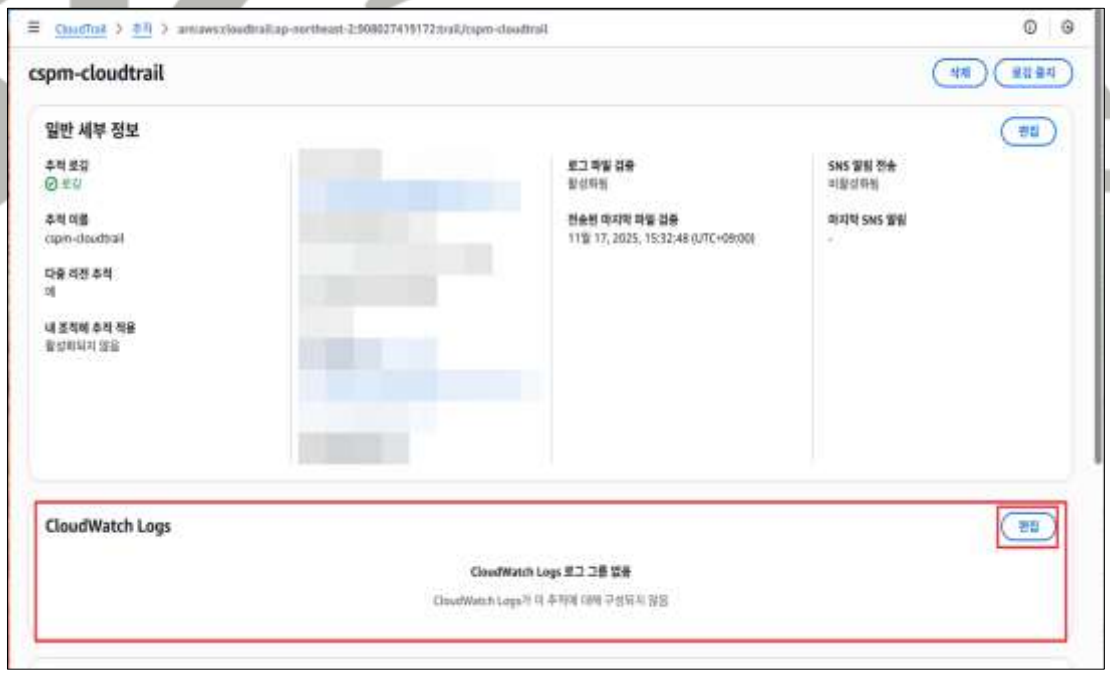
5) Datadog 내 CloudTrail 로그 추적 암호화 확인

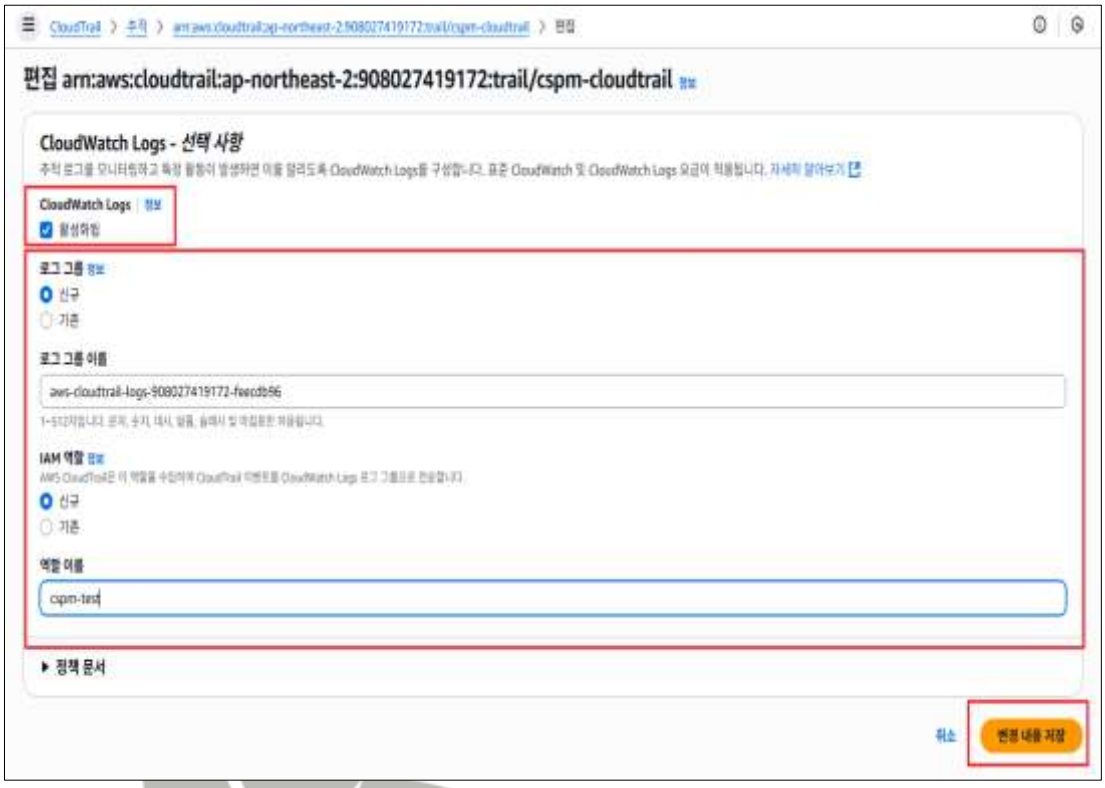


탐지 기준	**yg4-3in-tkd** : CloudTrail 추적 내 "로그파일 SSE-KMS" 암호화가 활성화되어 있는 경우 탐지

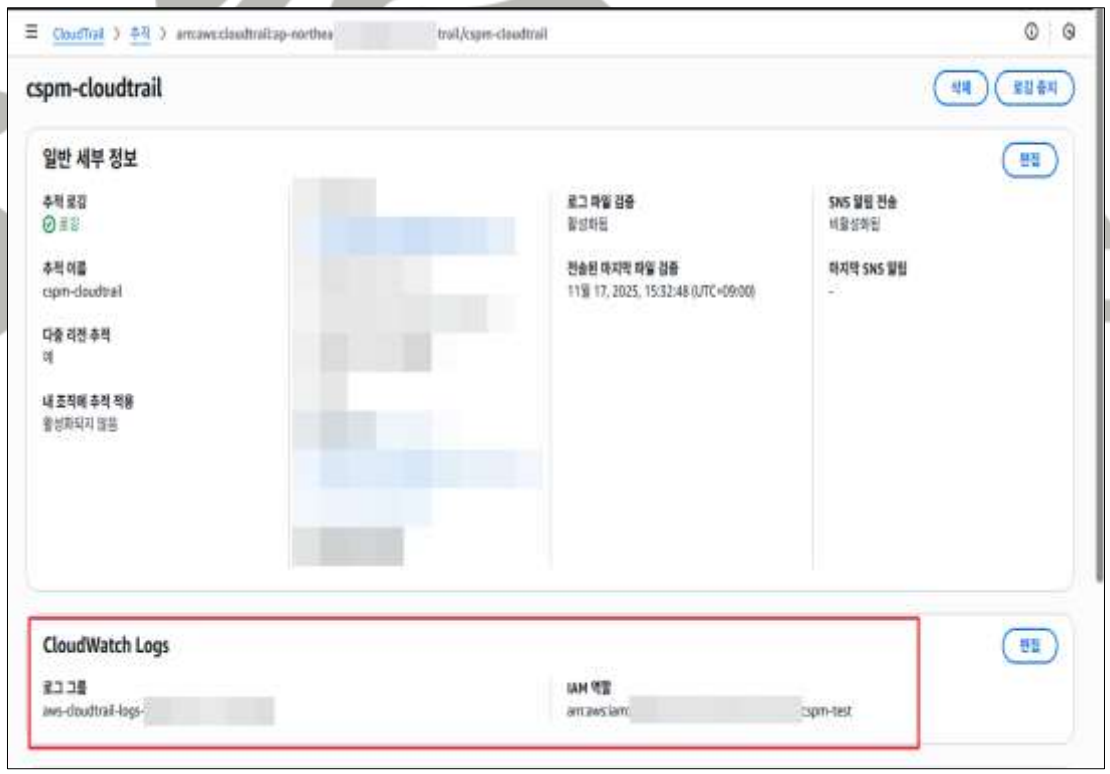
비고	기술 공식 문서 : https://docs.datadoghq.com/security/default_rules/yg4-3in-tkd/

4.6 AWS 사용자 계정 로깅 설정

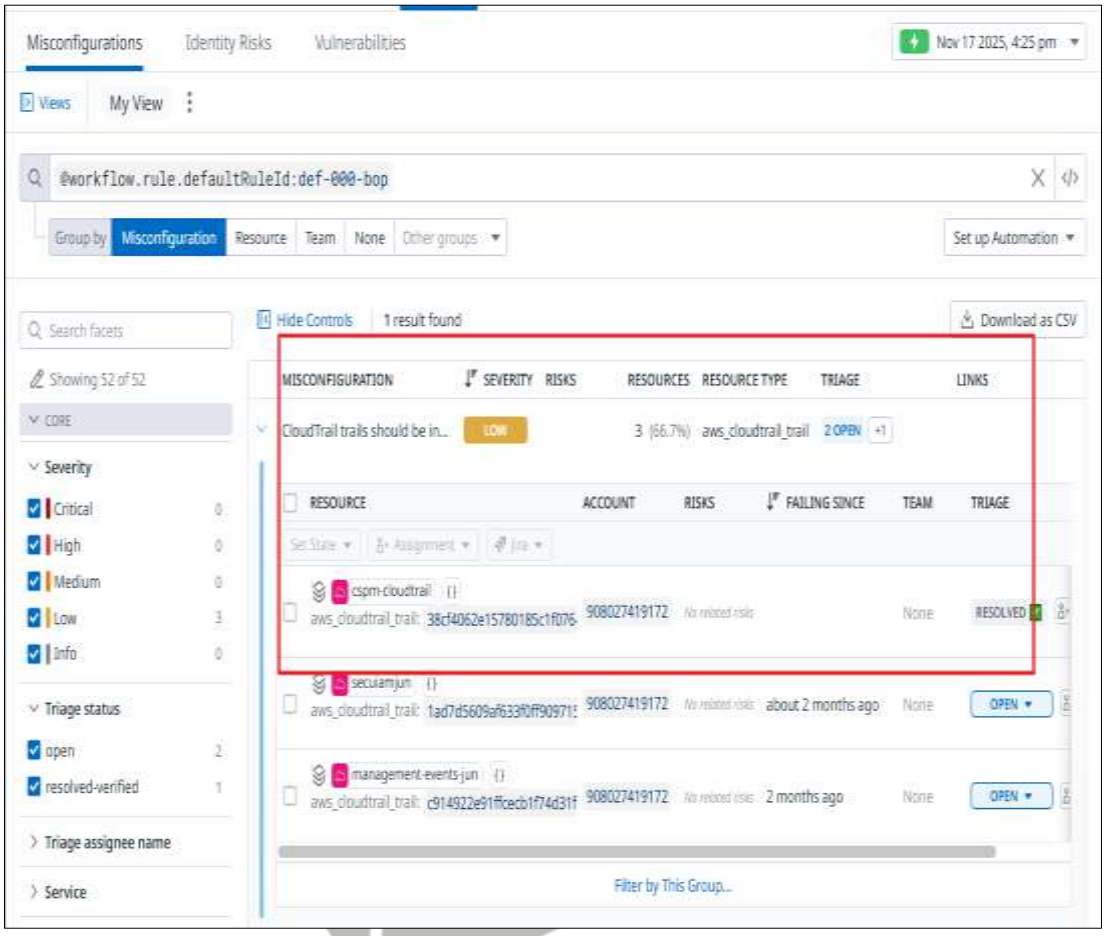
분류	운영 관리	중요도	상
항목명	AWS 사용자 계정 로깅 설정		
항목 설명	AWS CloudTrail 은 계정의 거버넌스, 규정 준수, 운영 및 위험 감사를 활성화하도록 도와주는 서비스로서 사용자, 역할 또는 AWS 서비스가 수행하는 작업들의 이벤트가 기록됩니다. 또한 CloudTrail 은 생성 시 AWS 계정에서 활성화됩니다. 활동이 AWS 계정에서 이루어지면 해당 활동이 CloudTrail 이벤트에 기록됩니다.		
설정 방법	**가. CloudTrail은 CloudWatch와 통합 설정해야 함 (LOW)** 1) CloudTrail 대시보드 진입 및 관리 이벤트 추적 확인  2) CloudWatch Logs 속성 확인 및 편집 시도 (현재: 빈값)  3) CloudWatch Logs 활성화 및 로그 그룹 설정		



4) CloudTrail 내 CloudWatch Logs 설정 확인



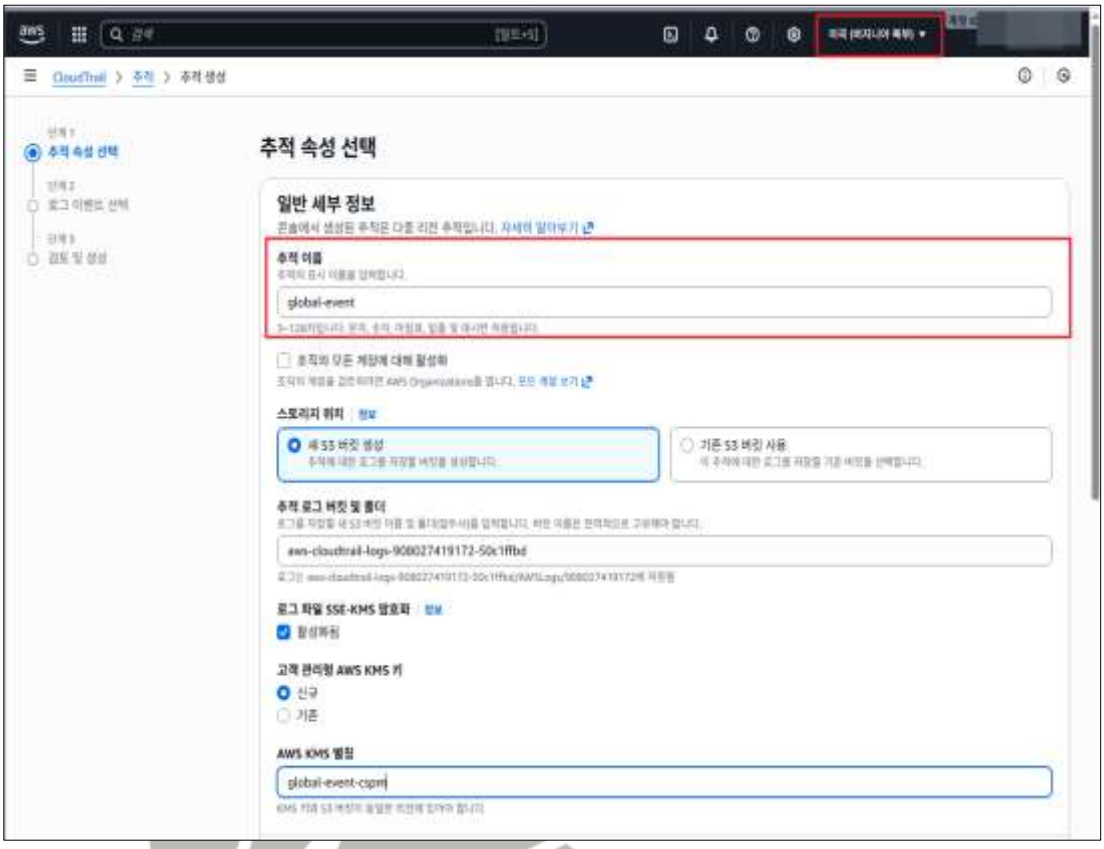
5) Datadog 내 CloudTrail <> CloudWatch 통합 연결 탐지 확인



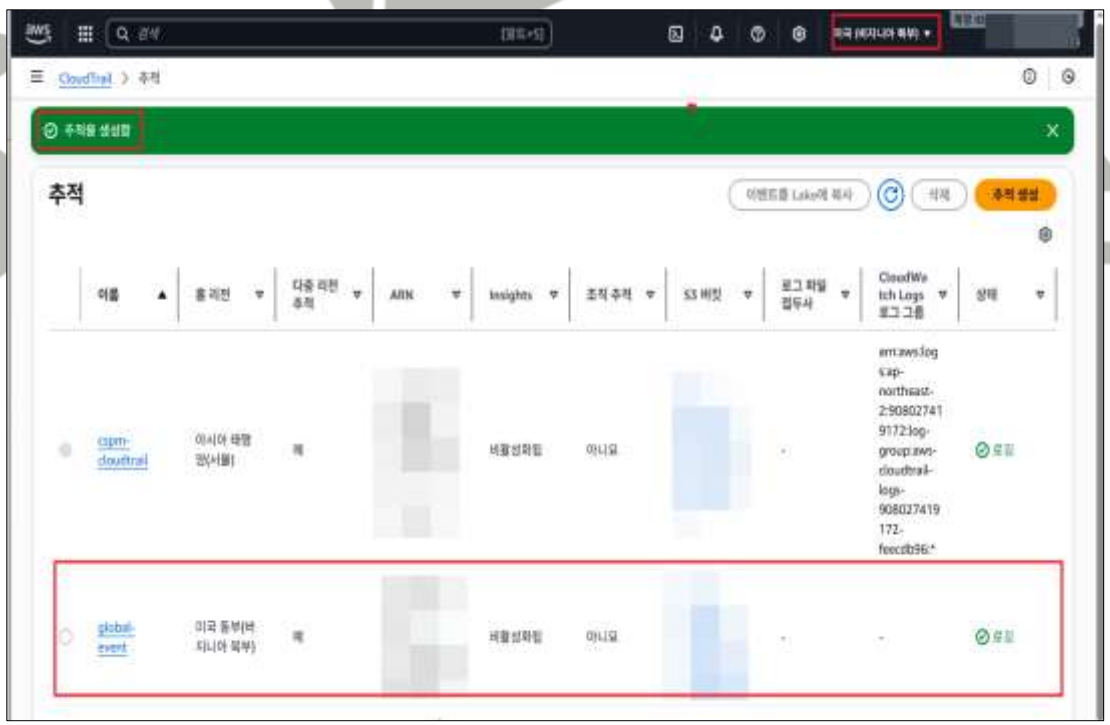
나. AWS CloudTrail 내 글로벌 서비스 이벤트 활성화해야 함 (LOW)

1) 글로벌 서비스 이벤트 로깅을 위한 us-east-1 리전 내 추적 생성

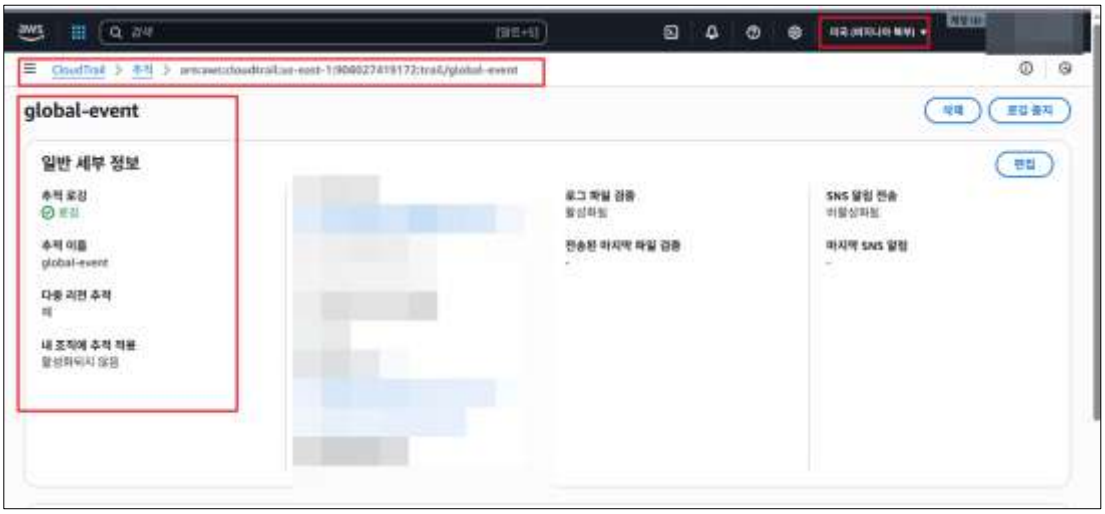
2) 추적 생성 시도



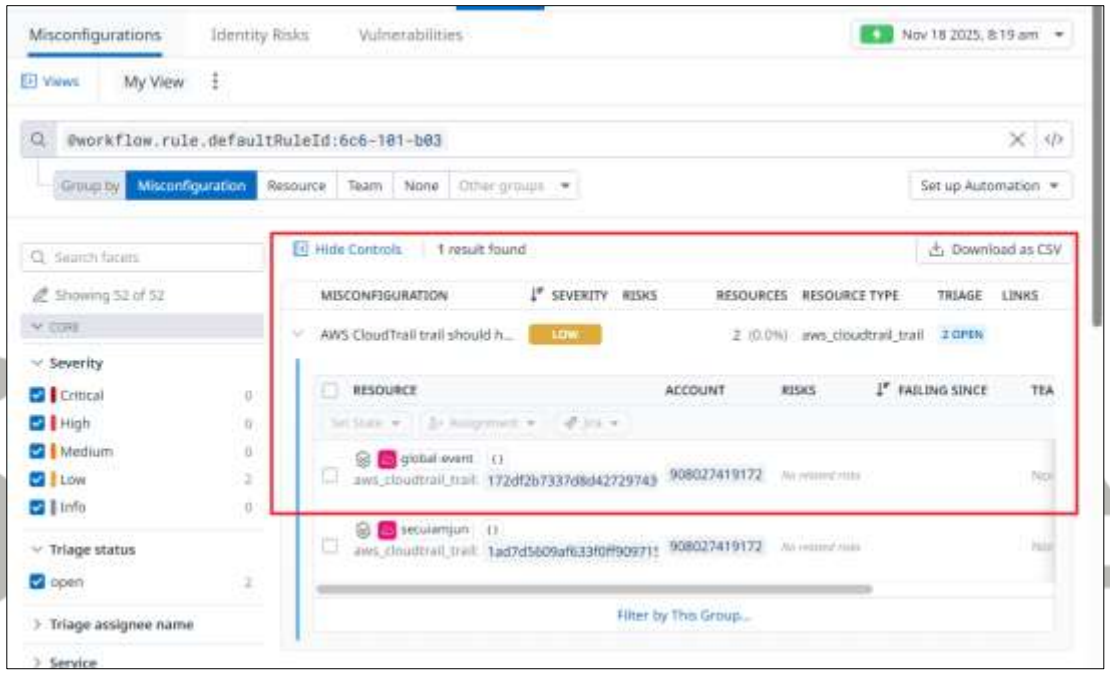
3) 추적 생성 완료



4) 글로벌 이벤트용 추적 생성 완료 확인

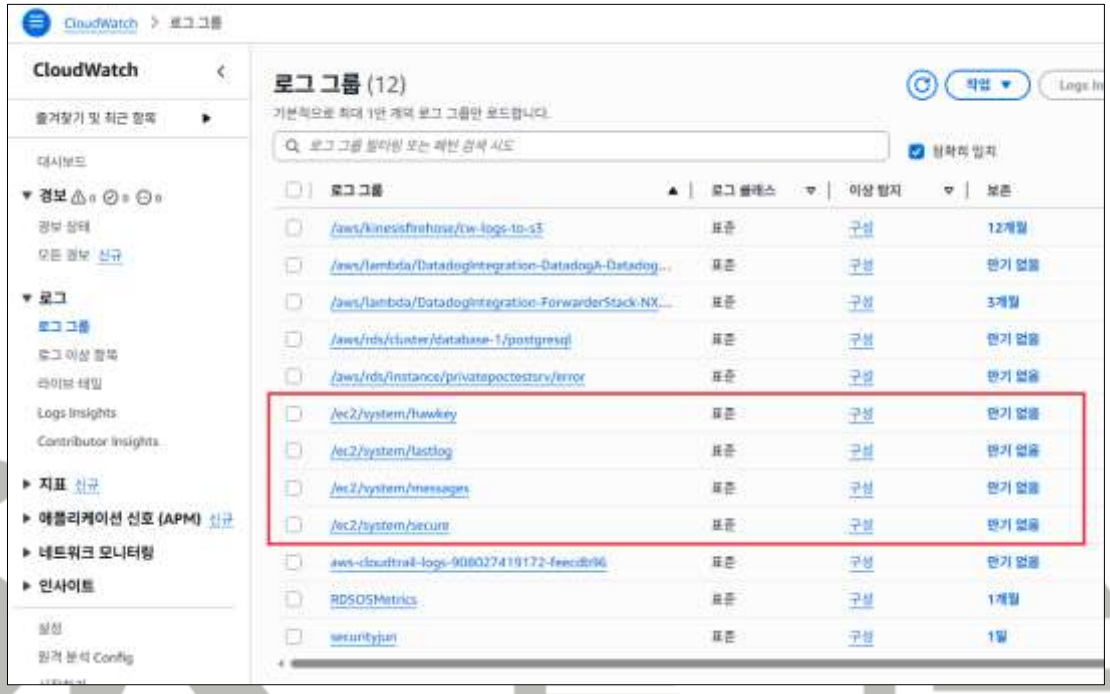
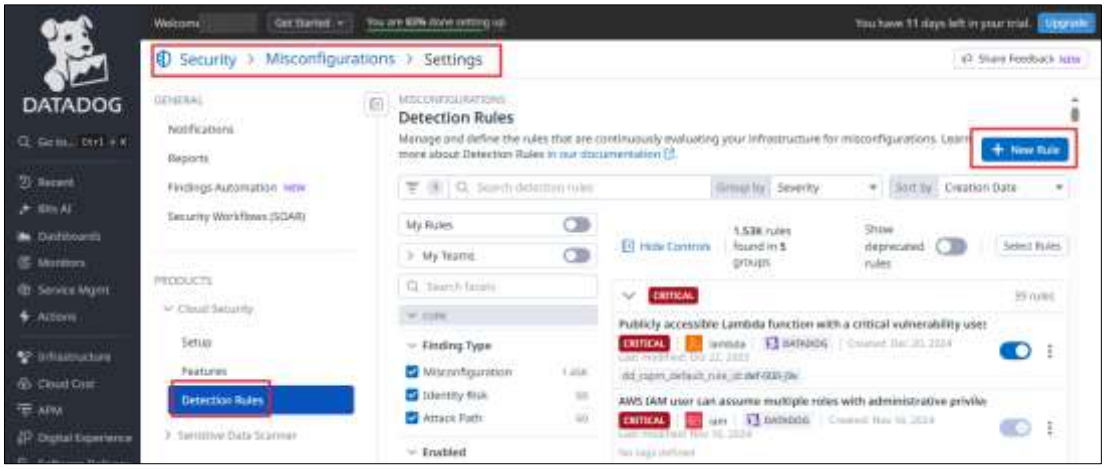


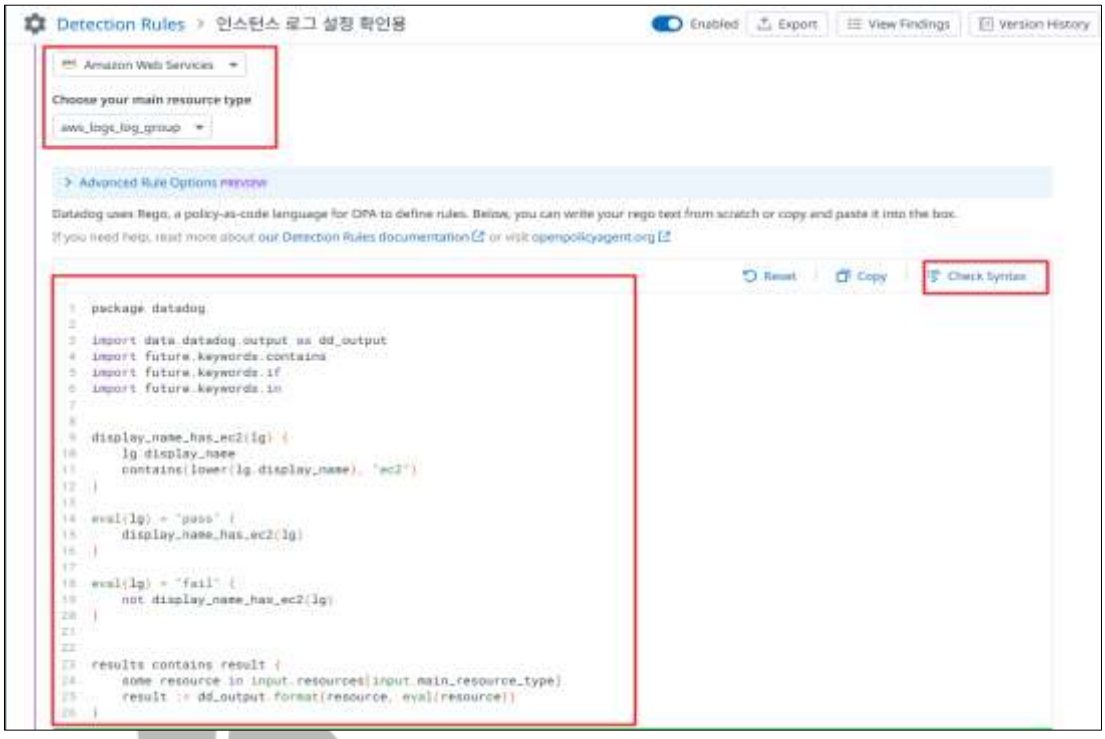
5) Datadog 내 CloudTrail 글로벌 이벤트 수집 추적 탐지 확인



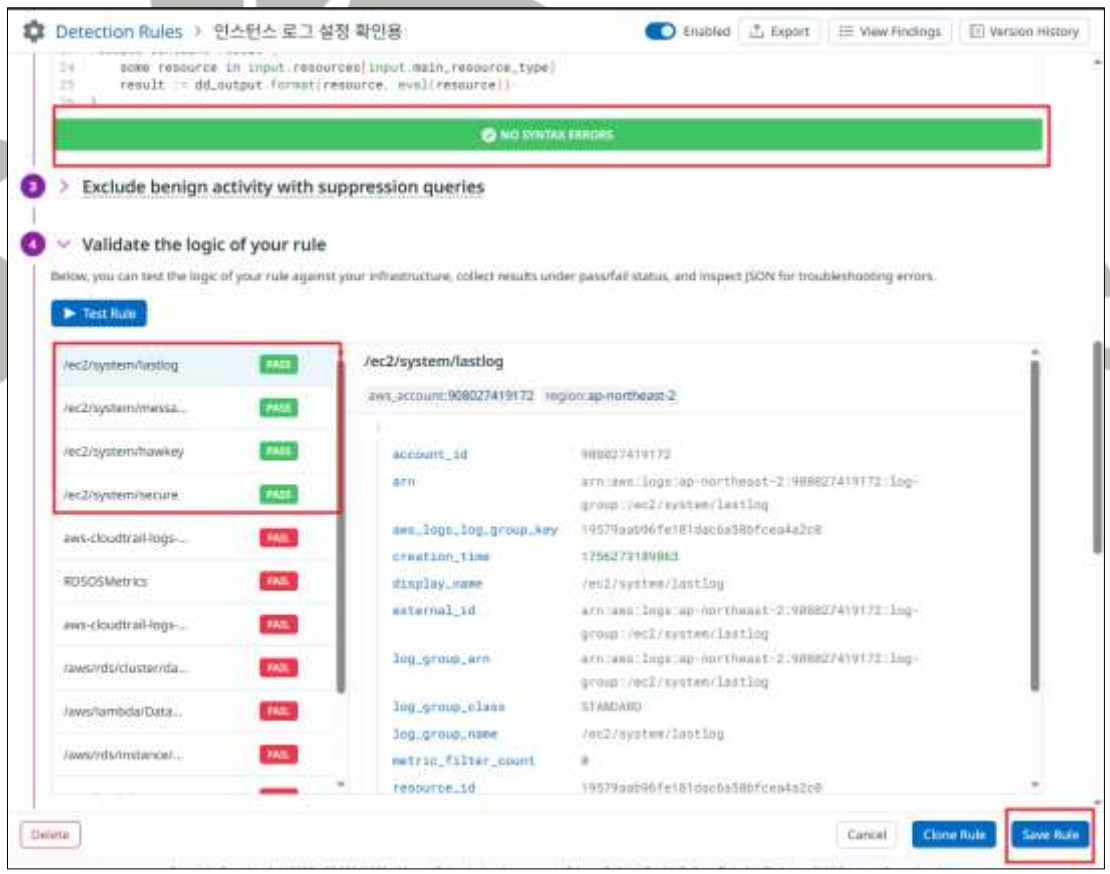
탐지 기준	**def-000-bop** : CloudTrail 추적 내 CloudWatch Logs가 활성화되어 있는 경우 탐지 **6c6-101-b03** : CloudTrail 추적 관리이벤트가 활성화되어 있는 경우 탐지
비고	기술 공식 문서 : https://docs.datadoghq.com/ko/security/default_rules/def-000-bop https://docs.datadoghq.com/security/default_rules/6c6-101-b03/

4.7 인스턴스 로깅 설정

분류	운영 관리	중요도	중
항목명	인스턴스 로깅 설정		
항목 설명	Amazon CloudWatch Logs 는 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.		
설정 방법	**가. CloudWatch 로그 스트림 설정해야 함 (MEDIUM)** 1) EC2 인스턴스 로깅을 위한 로그 그룹 생성 및 확인 ***※ 로그 그룹 생성 과정은 생략 (EC2 생성 시 아래 로그 그룹은 자동생성)***  2) 인스턴스 로깅 기록 확인을 위한 DataDog 내 커스텀 정책 생성 시도  3) CSP (Resource) 선택 및 식별하려는 커스텀 코드 작성 (하기 코드는 샘플 코드임)		



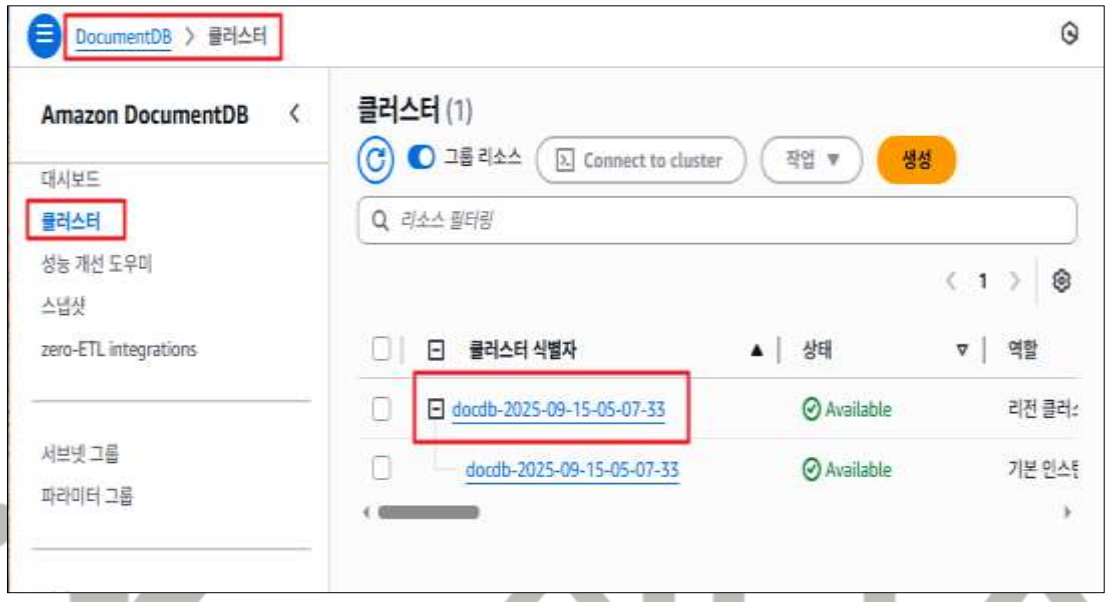
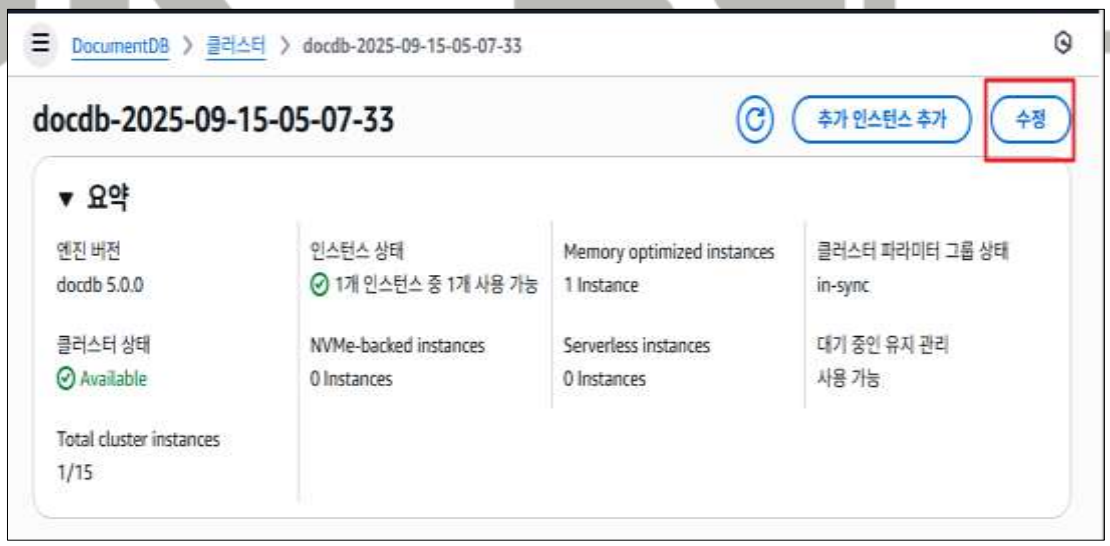
4) Custom Code Syntax 확인, 정책 Rule Test 및 정책 저장



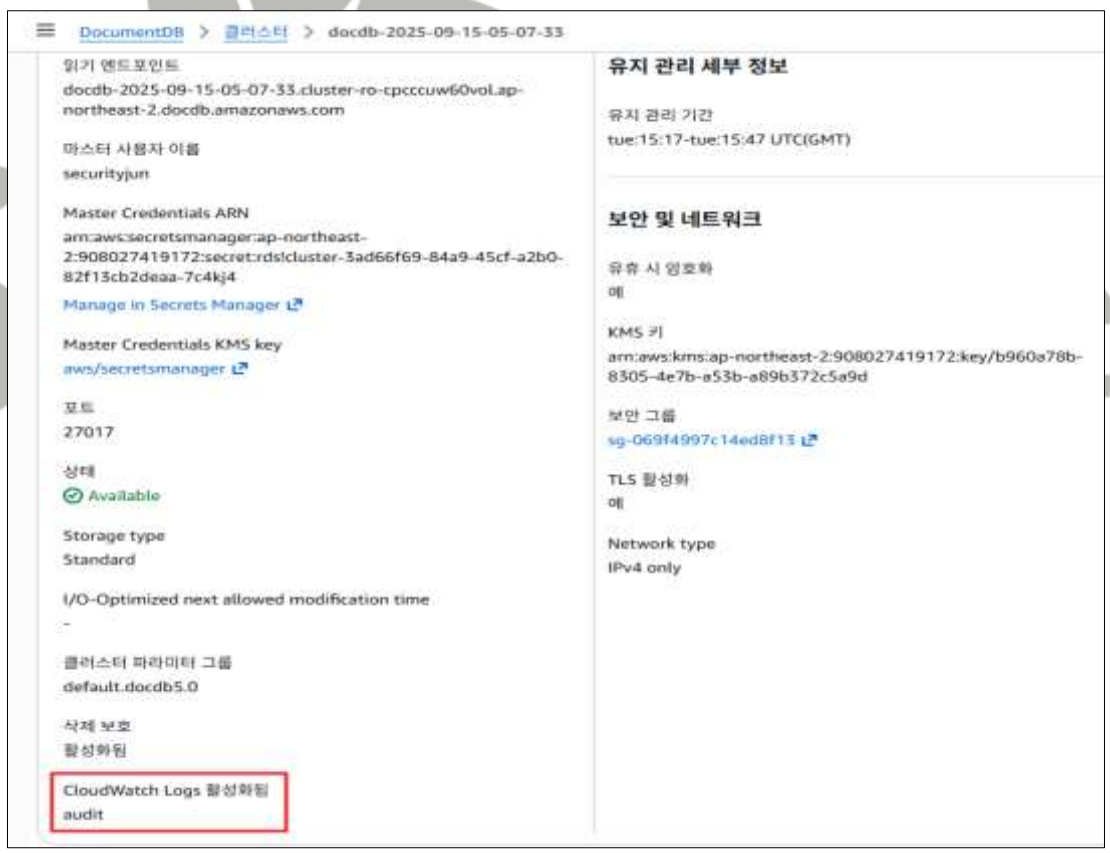
탐지 기준	**커스텀** : CloudWatch 로그 스트림 설정 유무를 확인하여 탐지

비고	

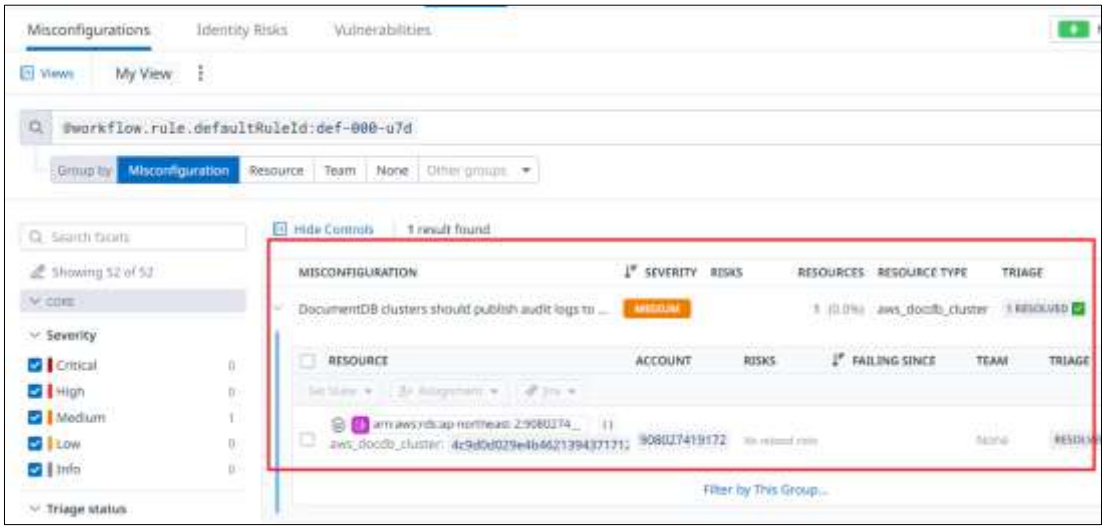
4.8 RDS 로깅 설정

분류	운영 관리	중요도	중
항목명	RDS 로깅 설정		
항목 설명	Amazon CloudWatch Logs 는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스, AWS CloudTrail, Route 53 및 기타 소스에서 로그 파일을 모니터링, 저장 및 액세스할 수 있습니다. 또한, 데이터베이스 옵션(로그 내보내기)을 수정하여 로그 그룹에 등록된 로그 스트림을 통해 RDS 로그를 확인할 수 있습니다.		
설정 방법	**가. DocumentDB 클러스터 내 감사로그를 설정해야 함 (MEDIUM)** 1) DocumentDB 클러스터 조회  2) 감사로그 설정을 위한 DocumentDB 클러스터 수정  3) 로그 내보내기 > 감사로그 설정		

4) 로그 설정 확인

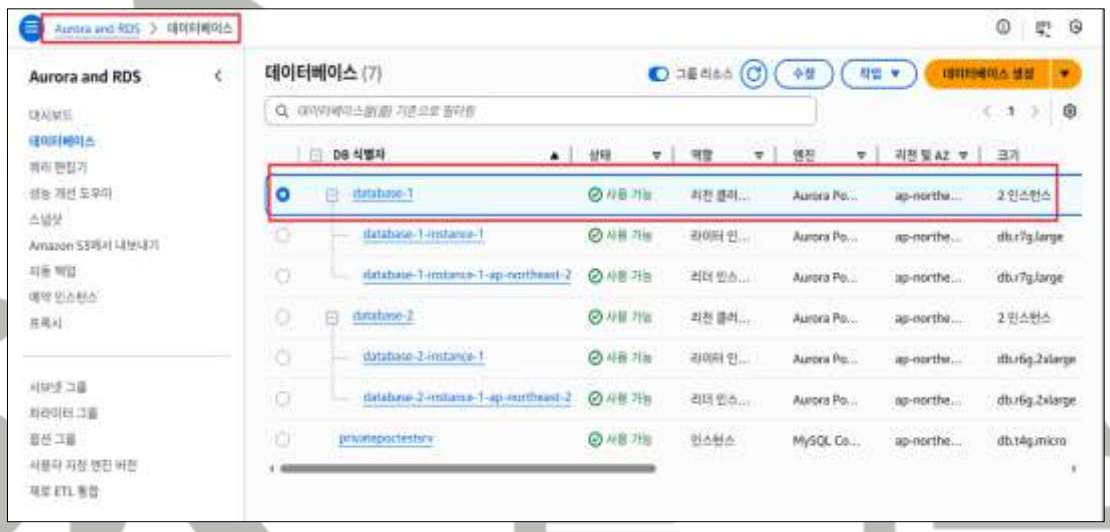


5) Datadog 내 DocumentDB 감사로그 정책 탐지 확인



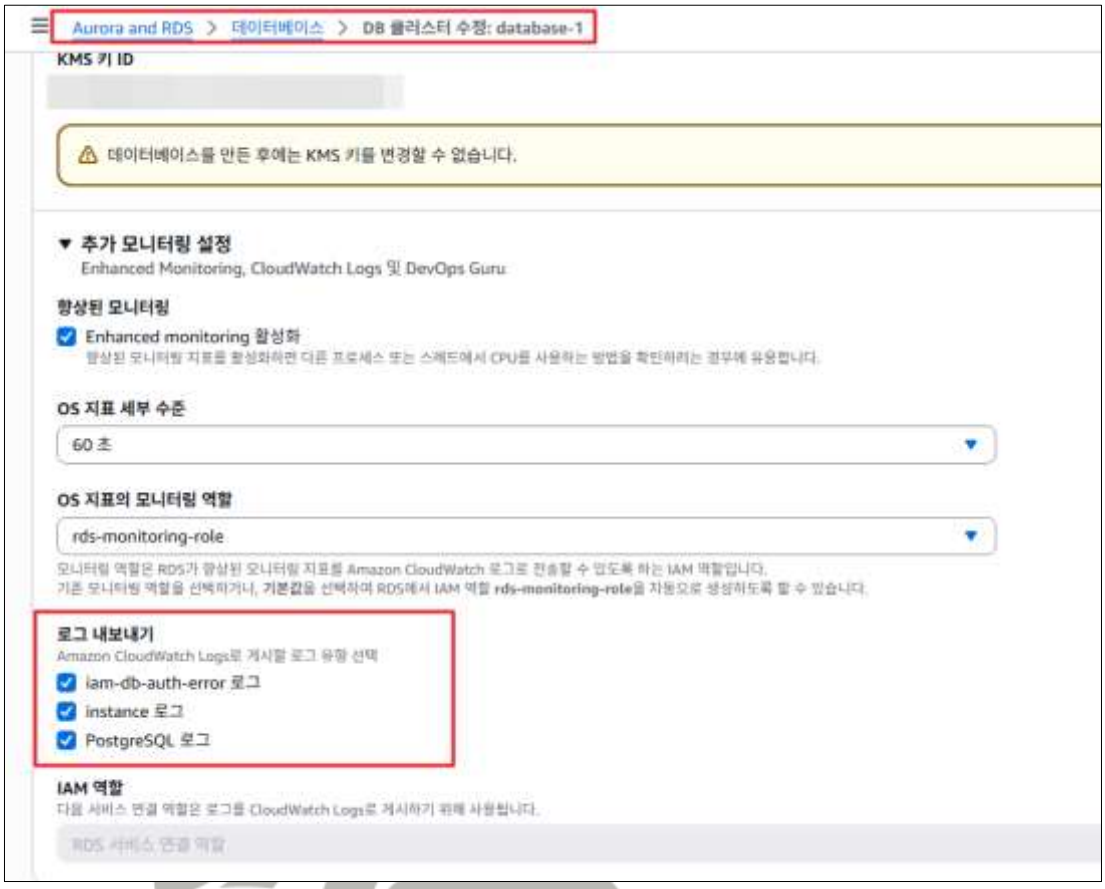
나. RDS 인스턴스 CloudWatch Logs에 로그 내보내기 설정해야 함 (MEDIUM)

1) RDS 내 데이터베이스 수정

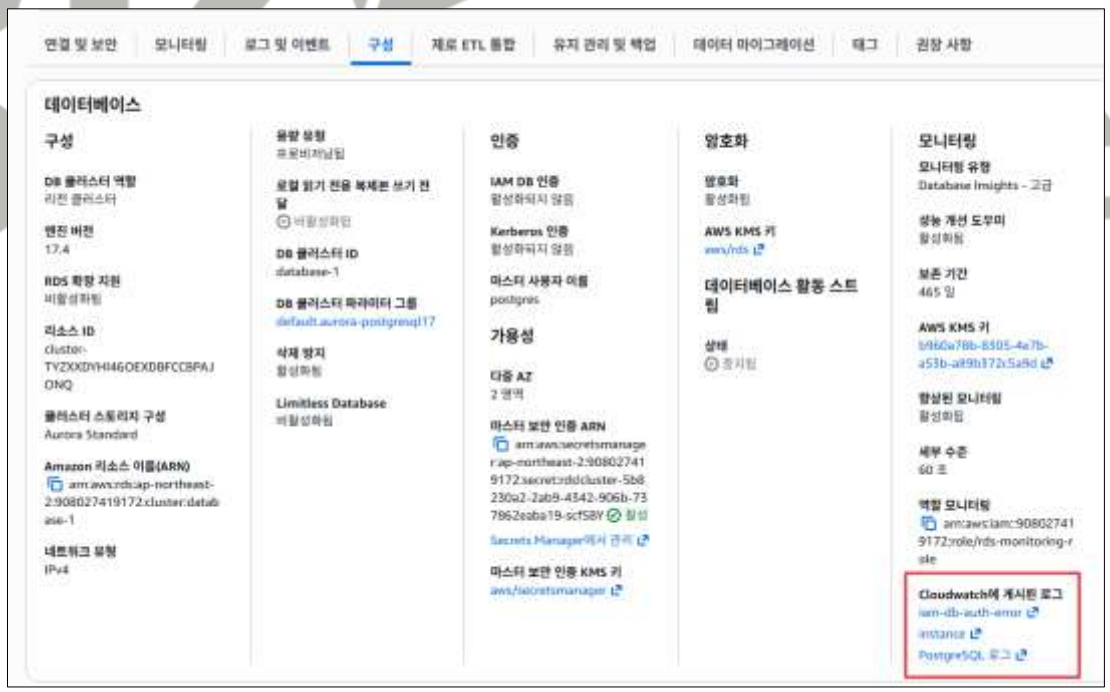


2) 데이터베이스 수정 페이지 접근

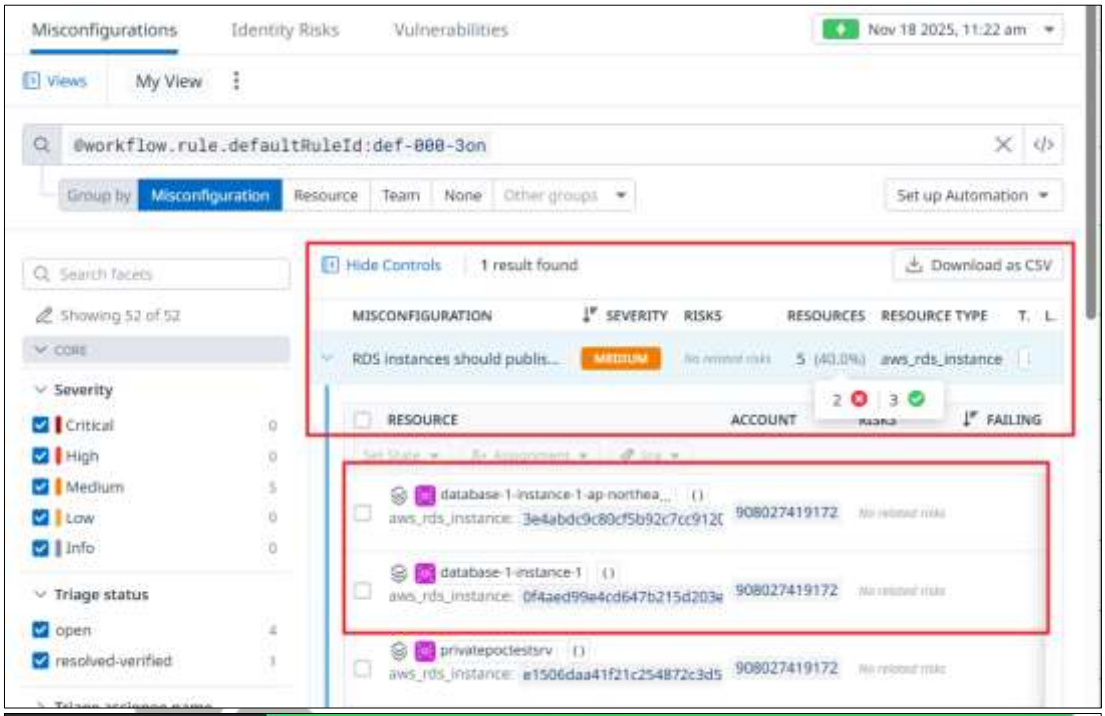
3) 로그 내보내기 옵션 선택

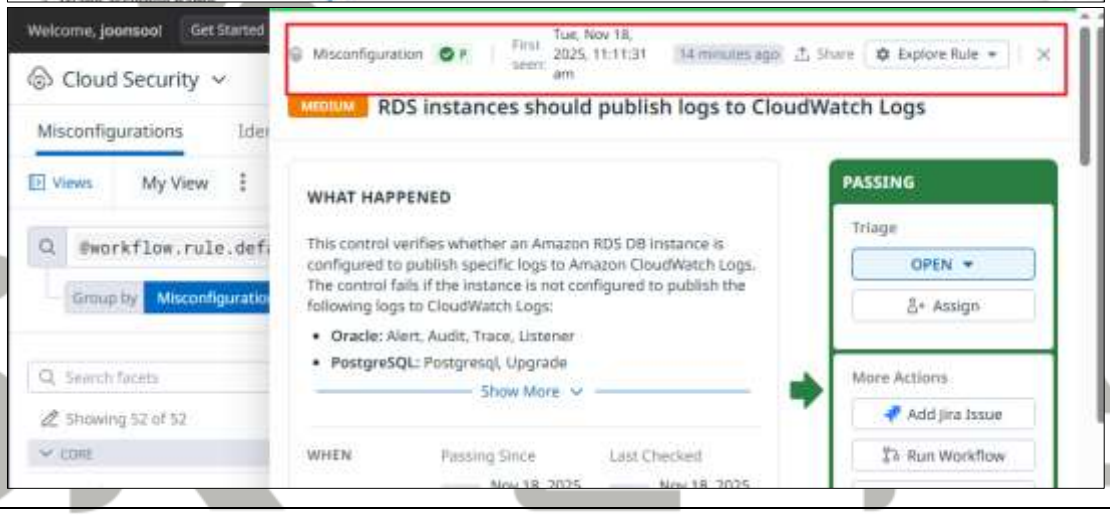


4) CloudWatch로의 로그 설정 확인



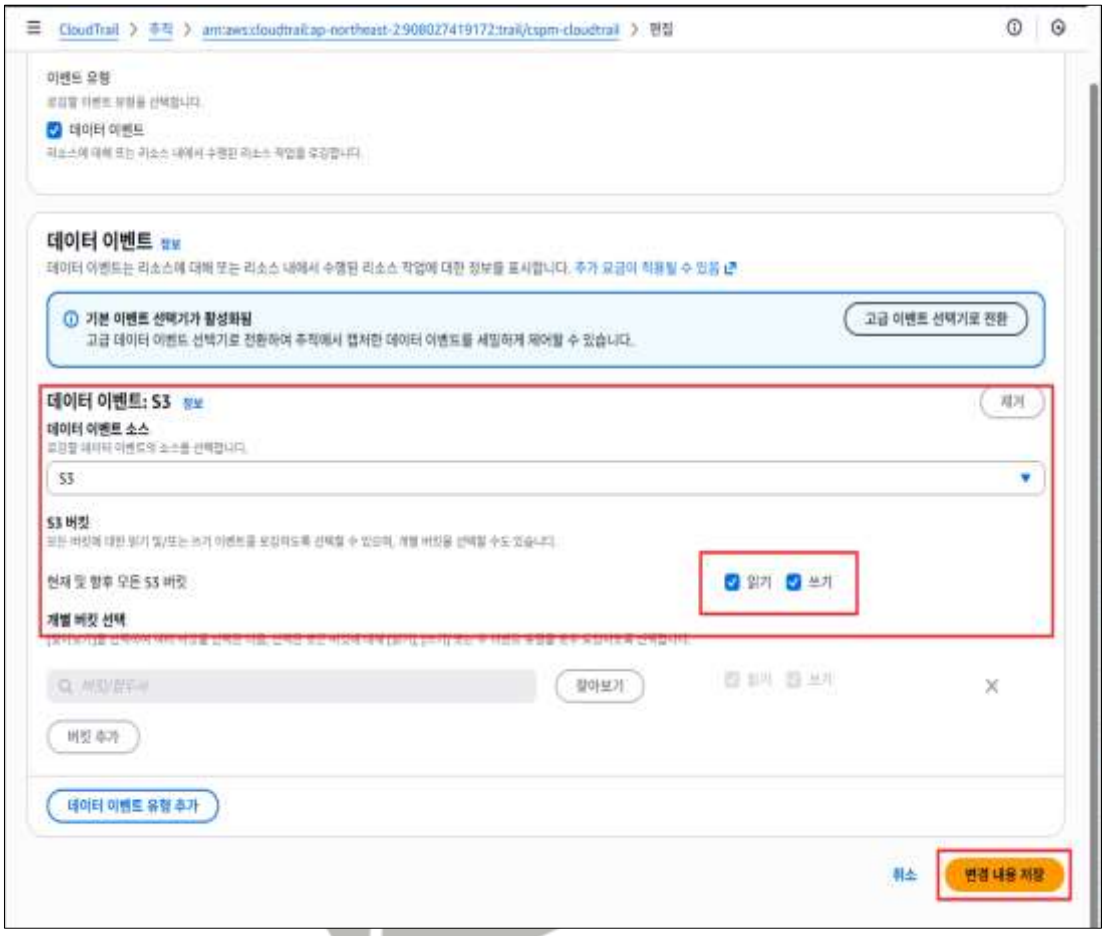
5) Datadog 내 RDS 인스턴스 감사로그 정책 탐지 확인

<table>
<tr><td></td><td> 


</td></tr>
<tr><td>탐지 기준</td><td>def-000-3on : RDS 내 로그 설정이 활성화되어 있는 경우 탐지
def-000-u7d : 클러스터 로그 내보내기 설정 내 감사로그 설정여부에 따라 탐지</td></tr>
<tr><td>비고</td><td>기술 공식 문서 :
https://docs.datadoghq.com/ko/security/default_rules/def-000-3on
https://docs.datadoghq.com/security/default_rules/def-000-u7d/</td></tr>
</table>

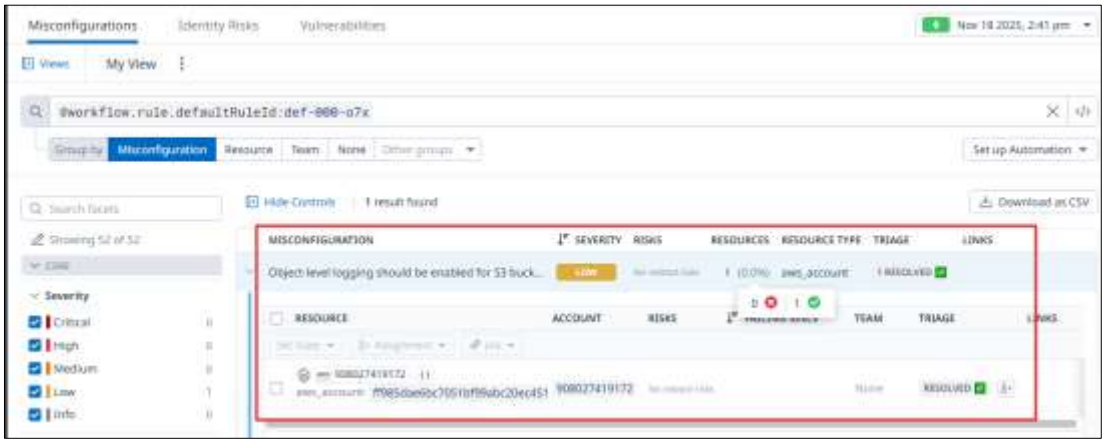
4.9 S3 버킷 로깅 설정

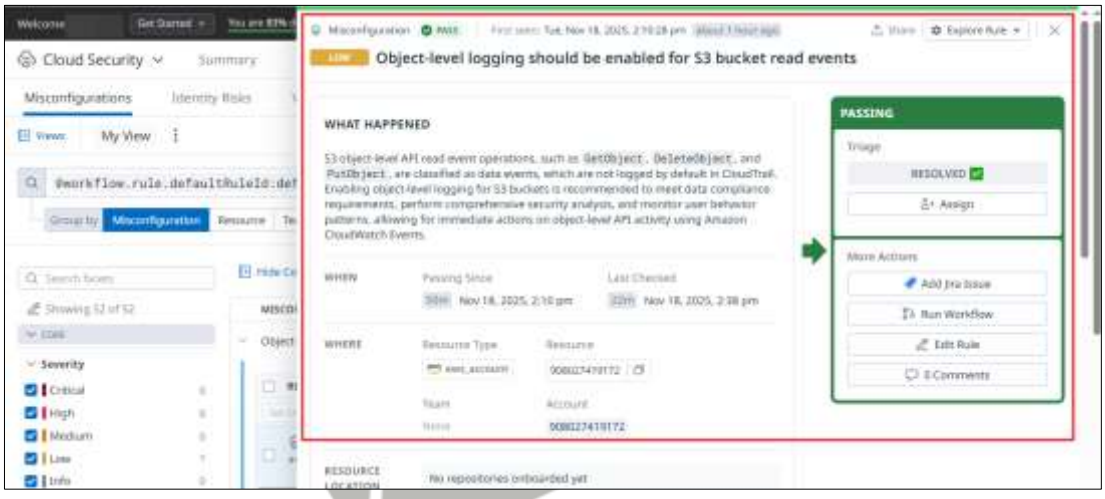
분류	운영 관리	중요도	중
항목명	S3 버킷 로깅 설정		
항목 설명	S3(Simple Storage Service)는 기본적으로 서버 액세스 로그를 수집하지 않으며, AWS Management 콘솔을 통해 S3 버킷에 대한 서버 액세스 로깅을 활성화시킬 수 있습니다. 로깅을 활성화하면 S3 액세스 로그를 사용자가 선택한 대상 버킷에 전달되며, 액세스 로그 레코드에는 요청 유형, 요청에 지정된 리소스, 요청을 처리한 날짜 및 시간 등이 포함됩니다. 대상 버킷은 원본 버킷과 동일한 AWS 리전에 존재해야 하며, 서버 액세스 로깅을 활성화 시 설정이 적용될 때까지 몇 시간이 소요될 수 있습니다.		
설정 방법	**가. S3 데이터 이벤트 읽기/쓰기 로깅을 설정해야 함 (LOW)** 1) CloudTrail 대시보드 진입 및 추적 확인  2) CloudTrail > 추적 내 데이터 이벤트 확인 및 편집  3) 데이터 이벤트 > 리소스 선택(S3) 및 읽기/쓰기 로깅 설정		



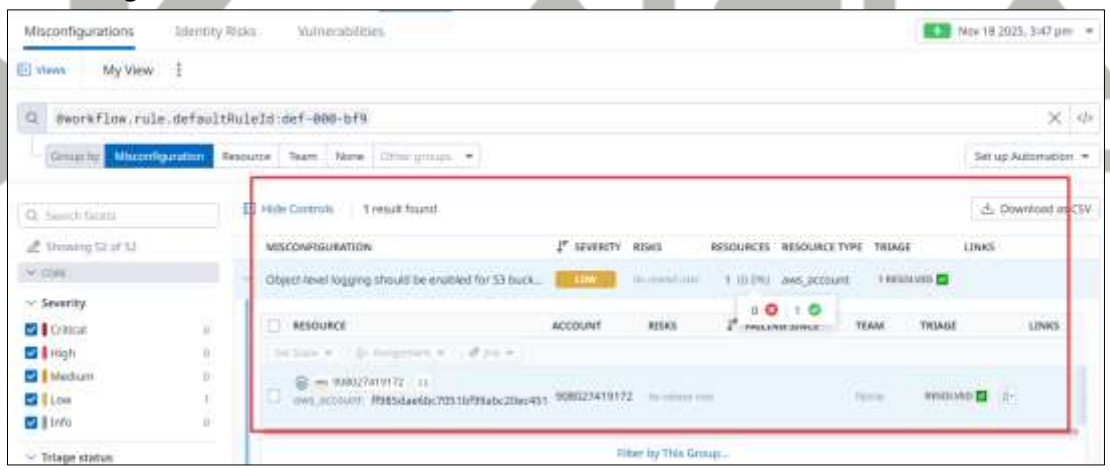
4) 데이터 이벤트 로깅 설정 적용 확인

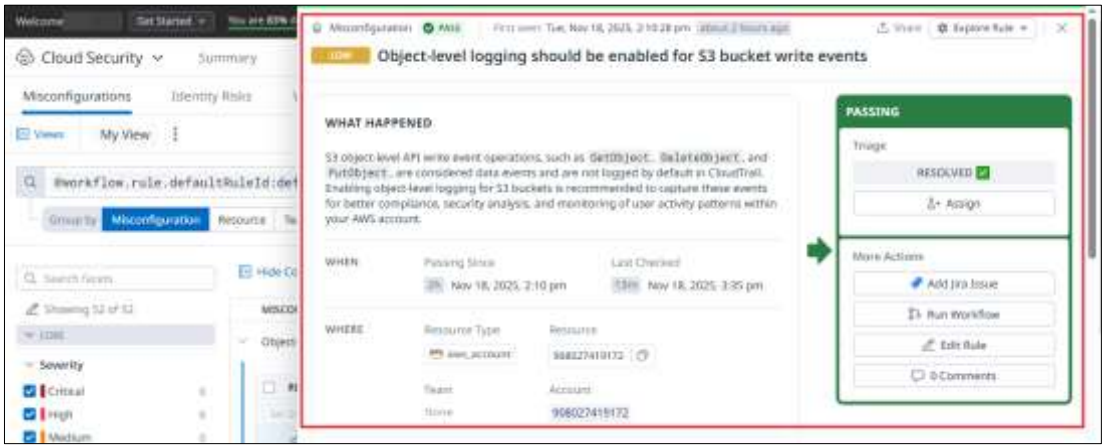
5) Datadog 내 S3 데이터 이벤트 정책 확인 (읽기 – Read)





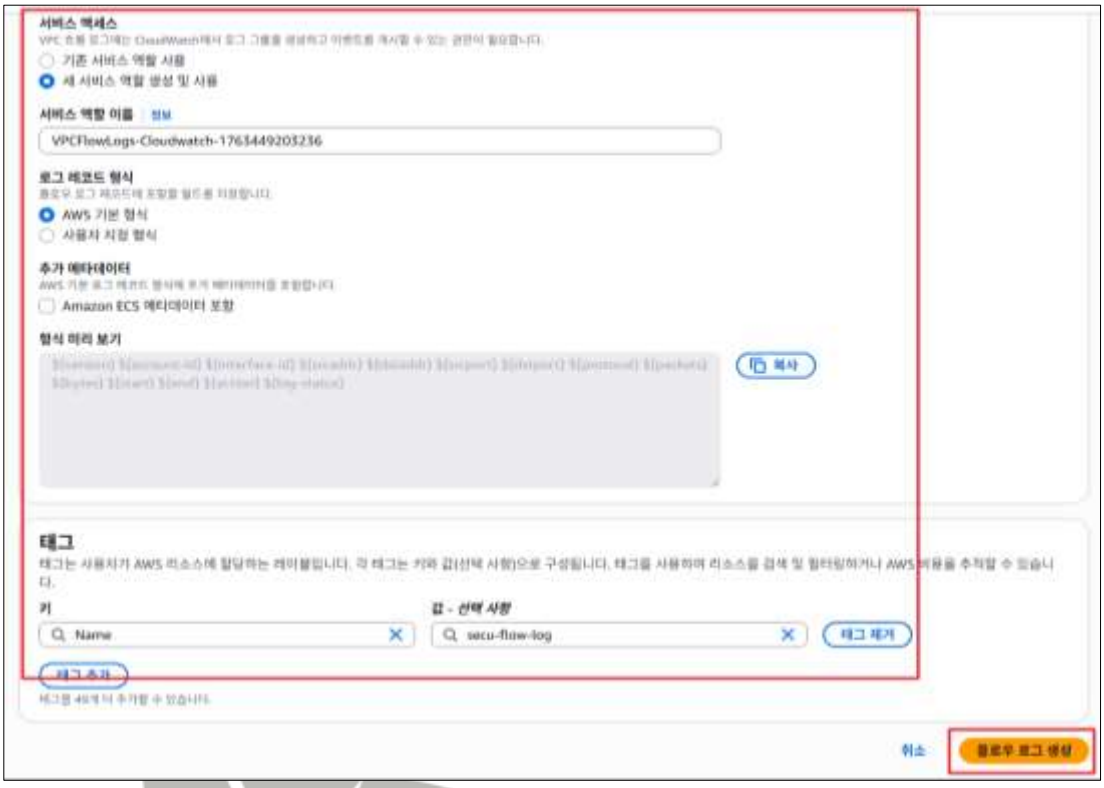
6) Datadog 내 S3 데이터 이벤트 정책 확인 (쓰기-Write)



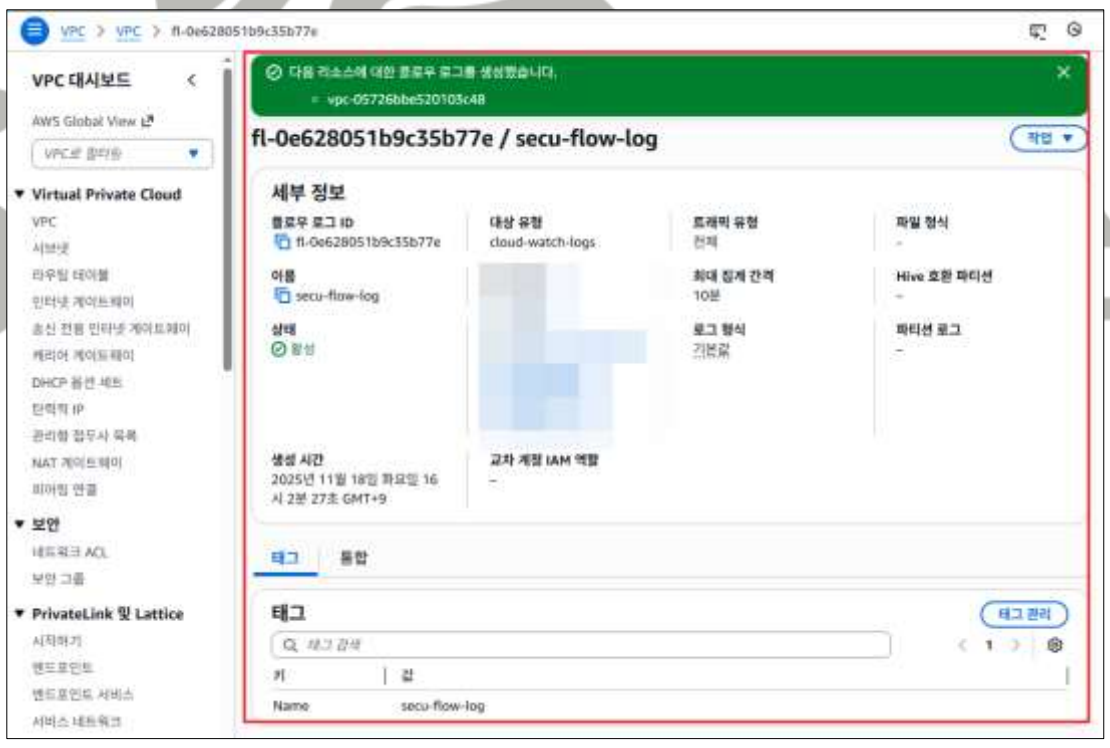
	
탐지 기준	**def-000-o7x** : 추적 내 데이터 쓰기에 대한 이벤트 값이 활성화되어 있는 경우 탐지 **def-000-bf9** : 추적 내 데이터 읽기에 대한 이벤트 값이 활성화되어 있는 경우 탐지
비고	기술 공식 문서 : https://docs.datadoghq.com/security/default_rules/def-000-o7x/ https://docs.datadoghq.com/security/default_rules/def-000-bf9/

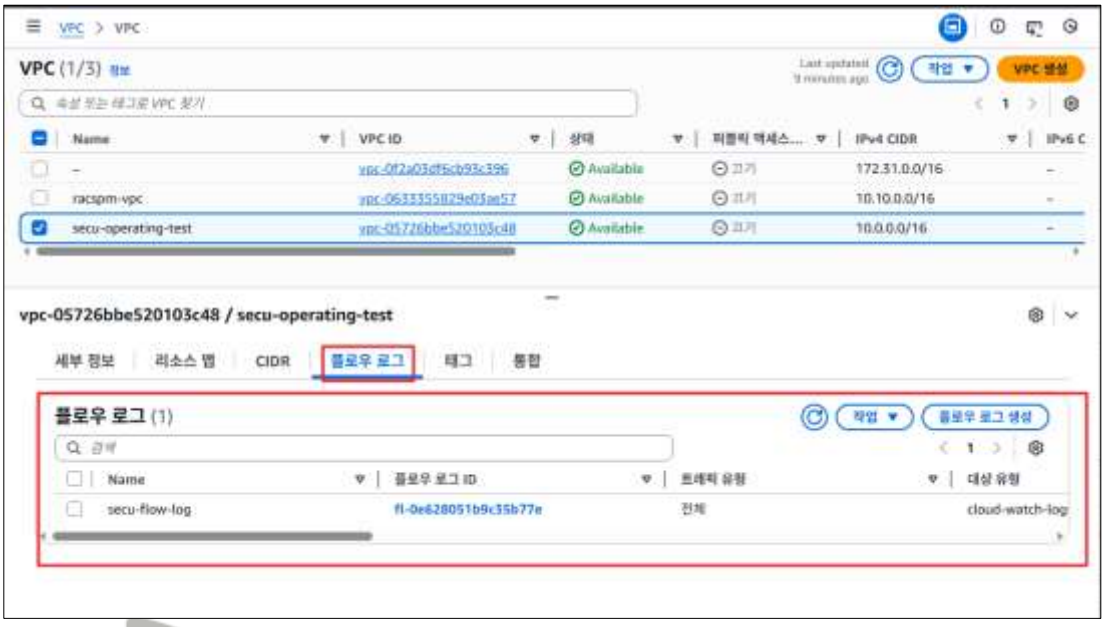
4.10 VPC 플로우 로깅 설정

분류	운영 관리	중요도	중
항목명	VPC 플로우 로깅 설정		
항목 설명	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.		
설정 방법	**가. VPC 플로우 로그를 설정해야 함 (MEDIUM)** 1) VPC 플로우 로그 설정 확인  2) VPC 플로우 로그 생성 ①  3) VPC 플로우 로그 생성 ②		

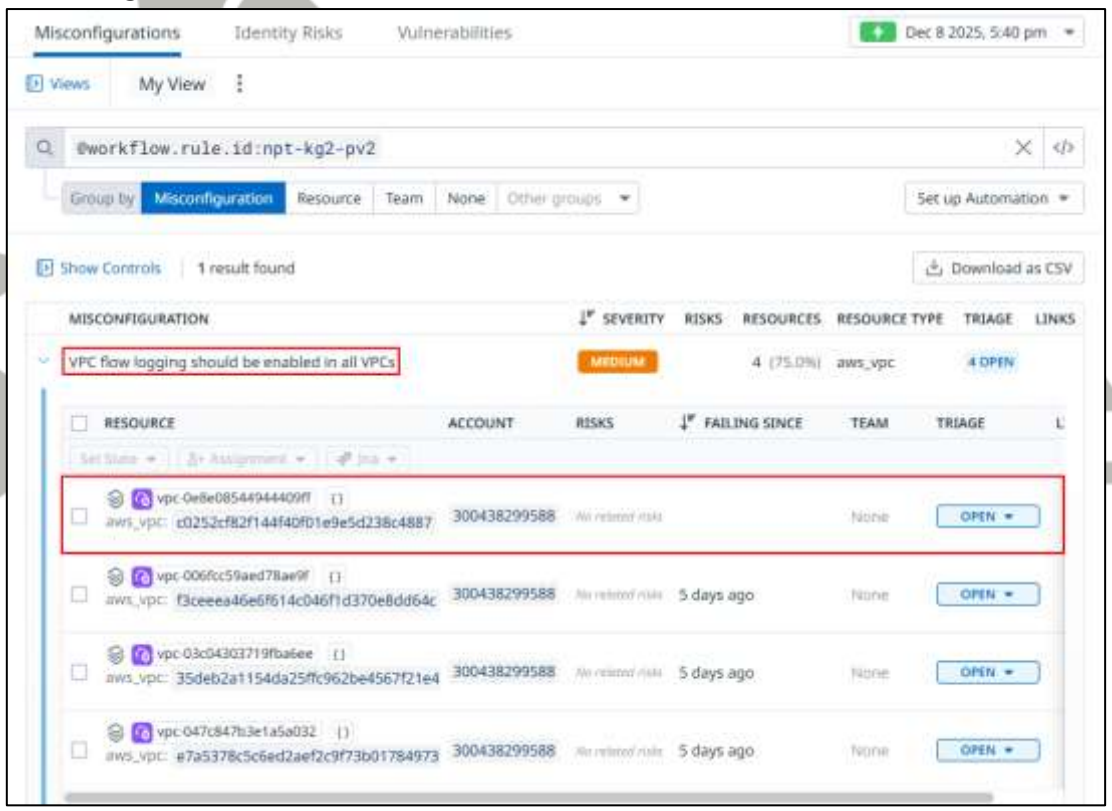


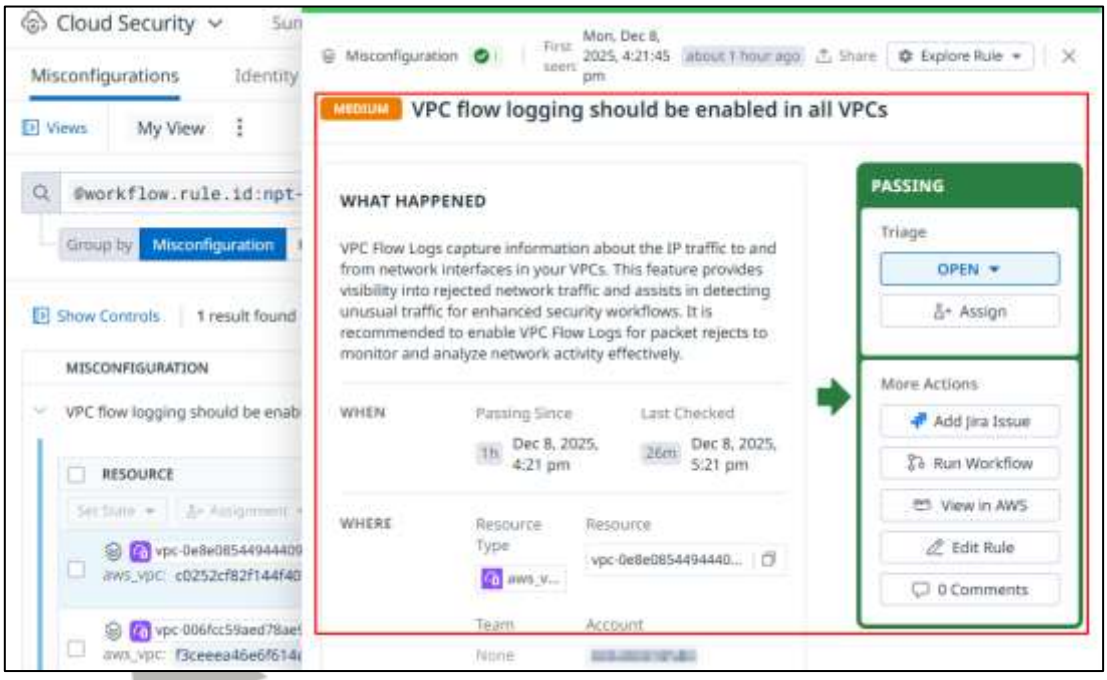
4) VPC 플로우 로그 설정 및 저장 확인





5) Datadog 내 VPC 플로우 로그 설정 탐지 확인

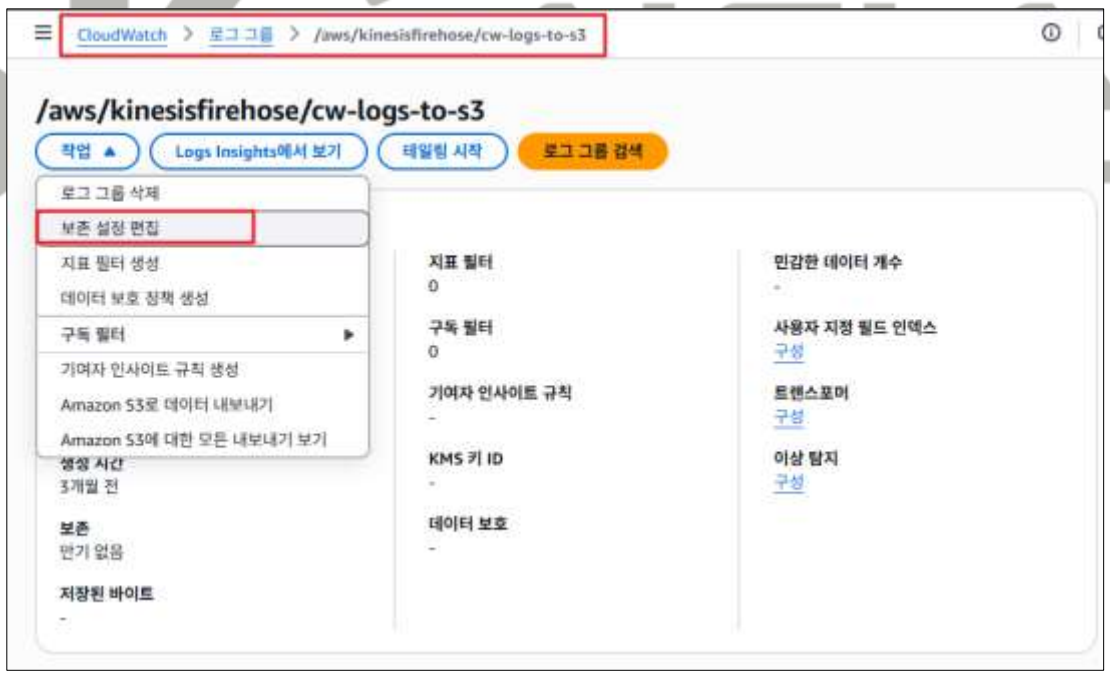


	
탐지 기준	**npt-kg2-pv2** : VPC 플로우 로그가 활성화되어 있는 경우 탐지
비고	기술 공식 문서 : https://docs.datadoghq.com/security/default_rules/npt-kg2-pv2/

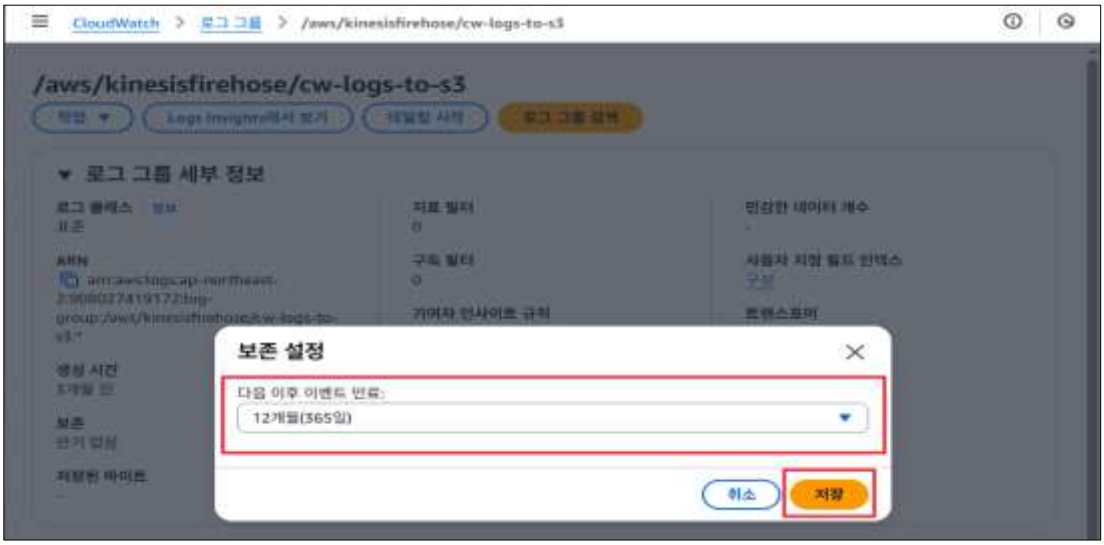
4.11 로그 보관 기간 설정

분류	운영 관리	중요도	중
항목명	로그 보관 기간 설정		
항목 설명	CloudWatch Logs에 저장되는 로그 데이터는 기본적으로 무기한 저장되므로, 기업 내부 정책 및 컴플라이언스 준수 등에 부합하도록 로그 데이터 저장 기간을 설정해주어야 하며, AWS Management 콘솔의 CloudWatch 로그 그룹에서 저장 기간 설정이 가능합니다. 국내에서 시행 중인 클라우드 보안인증제에서 보안감사 로그(접근기록 등)는 1년 이상 보존하도록 되어 있으며, 개인정보의 안전성 확보 조치 기준 8조(19.6, 행안부)에서도 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하도록 명시되어 있습니다. **(*) 로그 분류** 1) 개인정보처리시스템 접근 기록 고객 주요 정보, 임직원 주요 정보 등 관련 서비스: S3, RDS, EFS, EBS, FSX, DynamoDB 등 2) 보안관련 감사 로그 사용자 접속 기록, 인증 성공/실패, 계정 생성/삭제 등 관련 서비스: CloudTrail, S3 등 3) 시스템 이벤트 로그 운영체제 구성요소에 의해 발생되는 로그(시스템 시작, 종료, 상태, 에러코드 등) 주요 서버, 네트워크, 보안 장비 등의 로그(접근기록 및 이벤트 로그 등) 관련 서비스: S3, CloudWatch 등 **※ 법적 근거** **국가정보보안기본지침 제55조(로그기록 유지) - 2019/03** **개인정보의 안전성 확보조치 기준 제8조(접속 기록의 보관 및 점검) - 2019/06**		
설정 방법	**가. CloudWatch 로그 보존 기간 설정해야 함 (MEDIUM)** 1) CloudWatch 내 로그그룹 및 보존기간 확인		

2) 로그 그룹 내 보존 기간 설정 시도

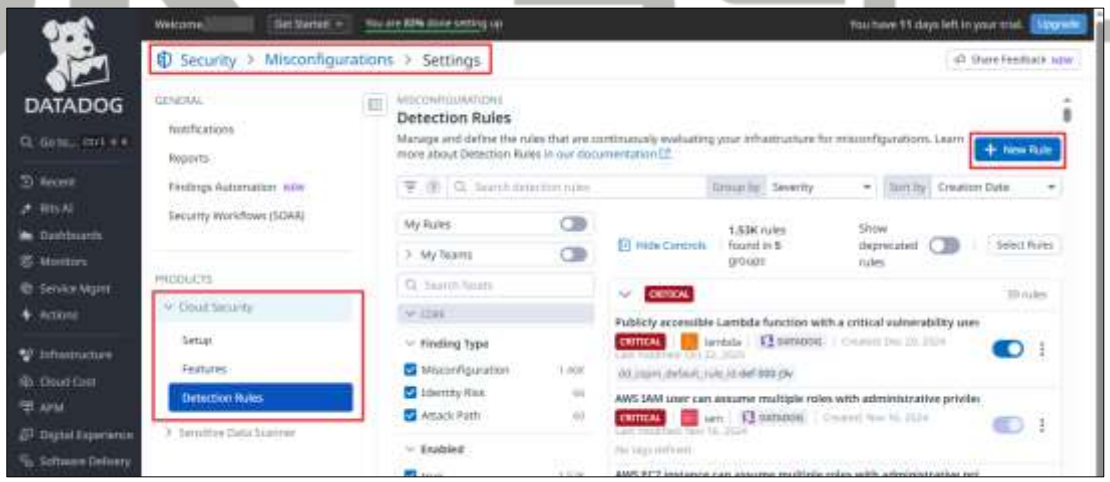


3) 보존 기간 설정 (1년 이상)

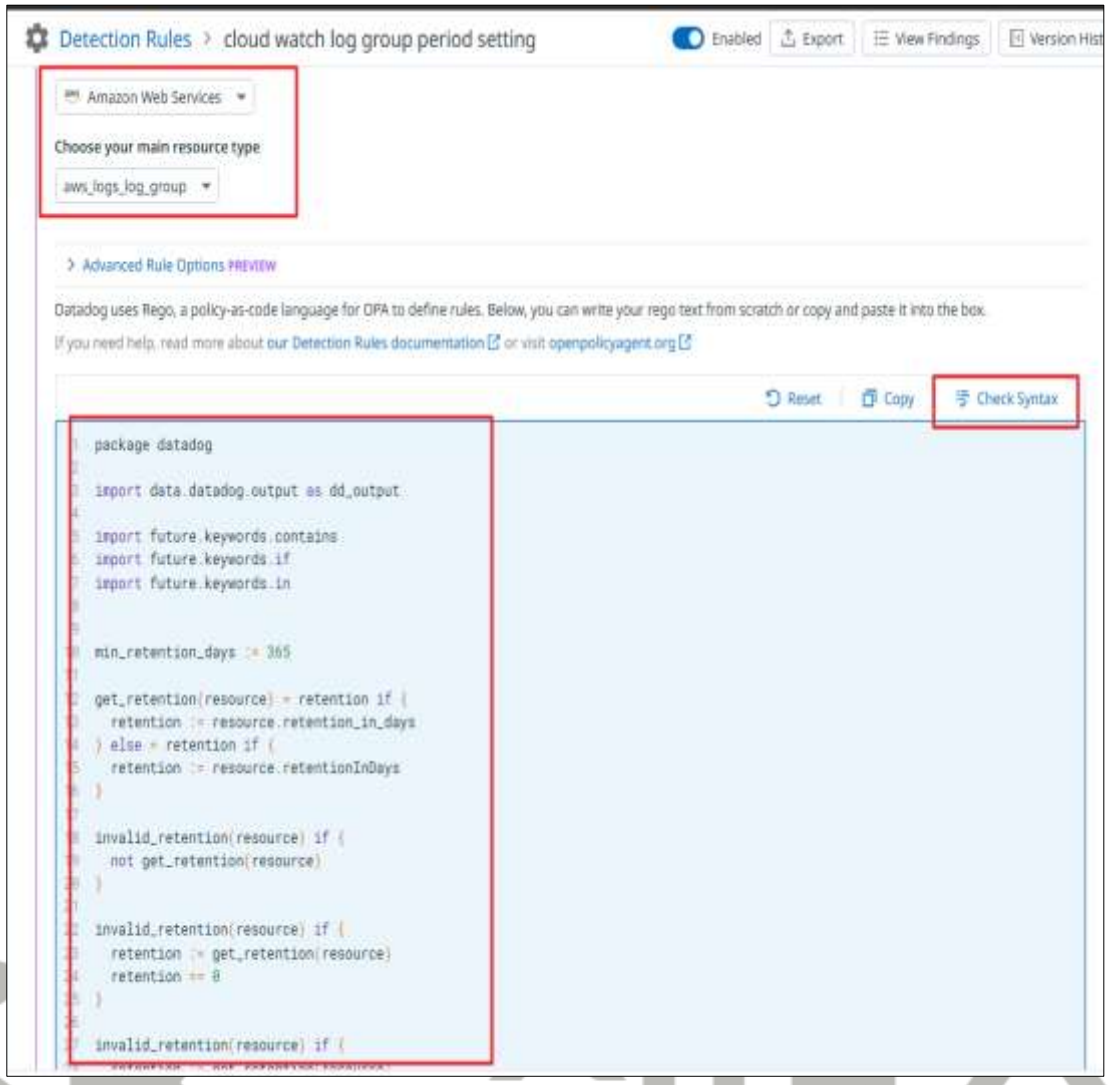


4) CloudTrail 보존 설정 기간 설정

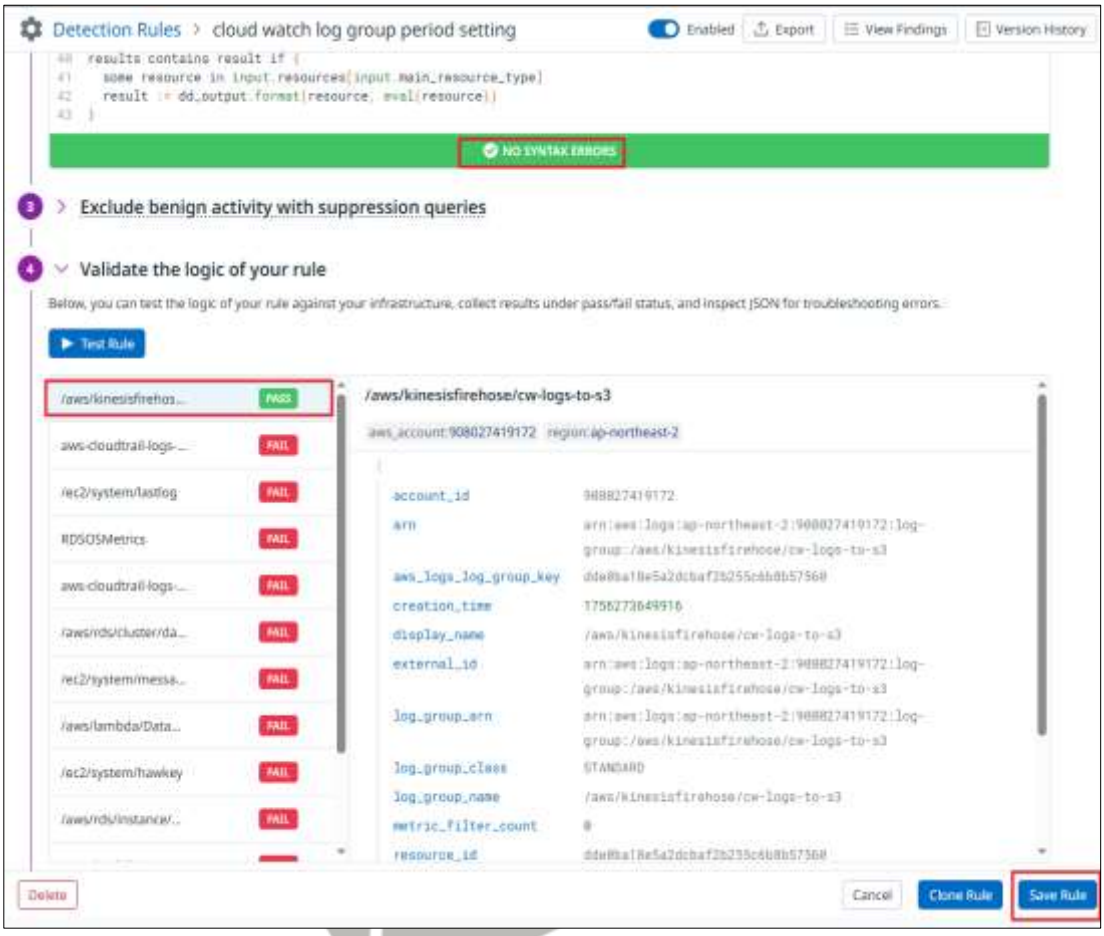
5) DataDog 내 커스텀 설정 생성



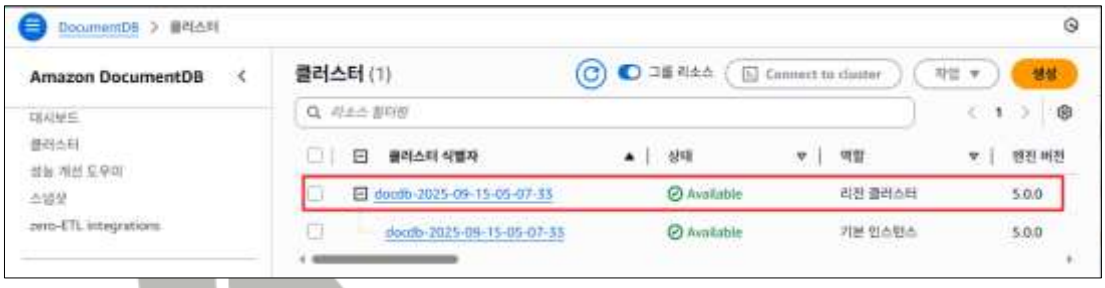
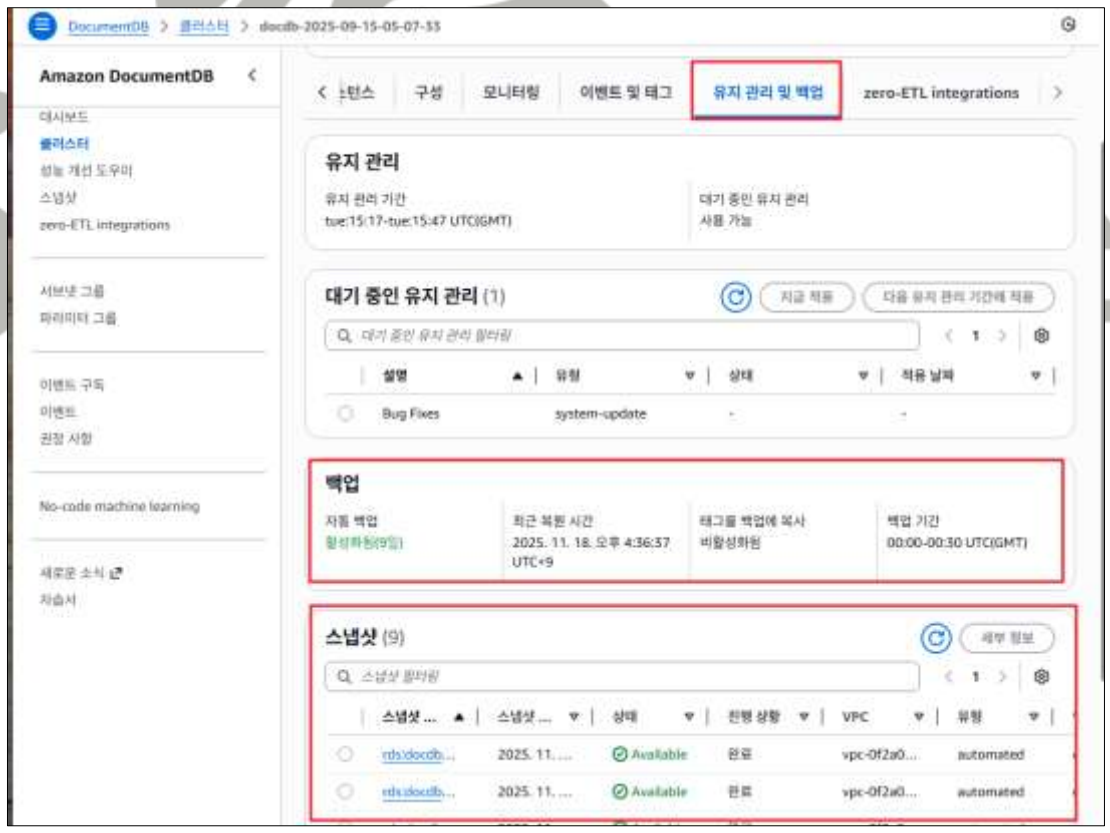
6) CSP (Resource) 및 식별하려는 커스텀 코드 작성



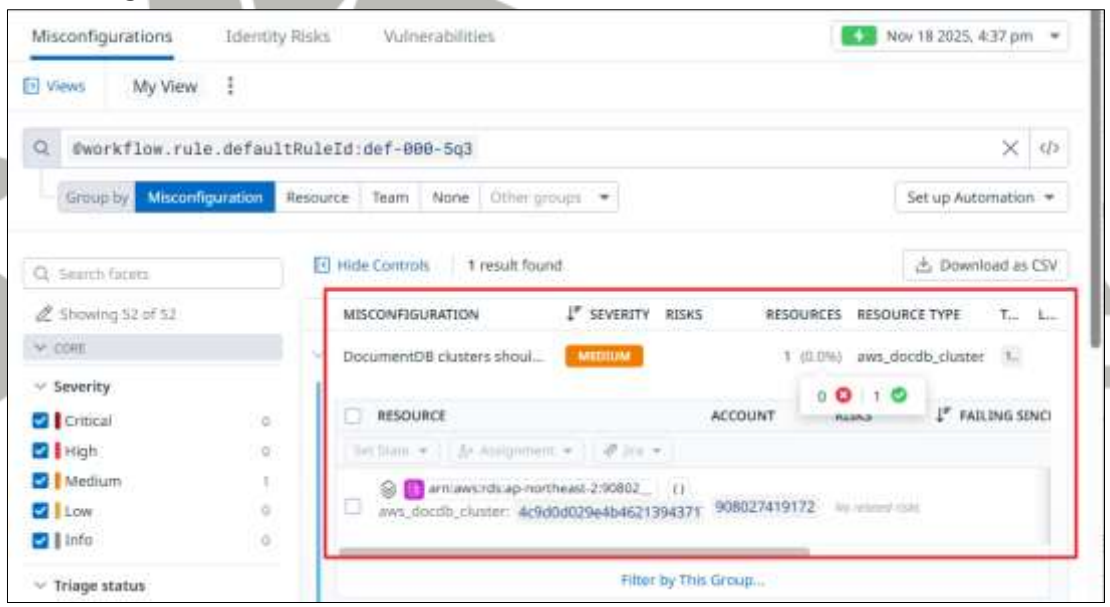
7) Custom Code Syntax 확인, 정책 Rule Test 및 정책 저장

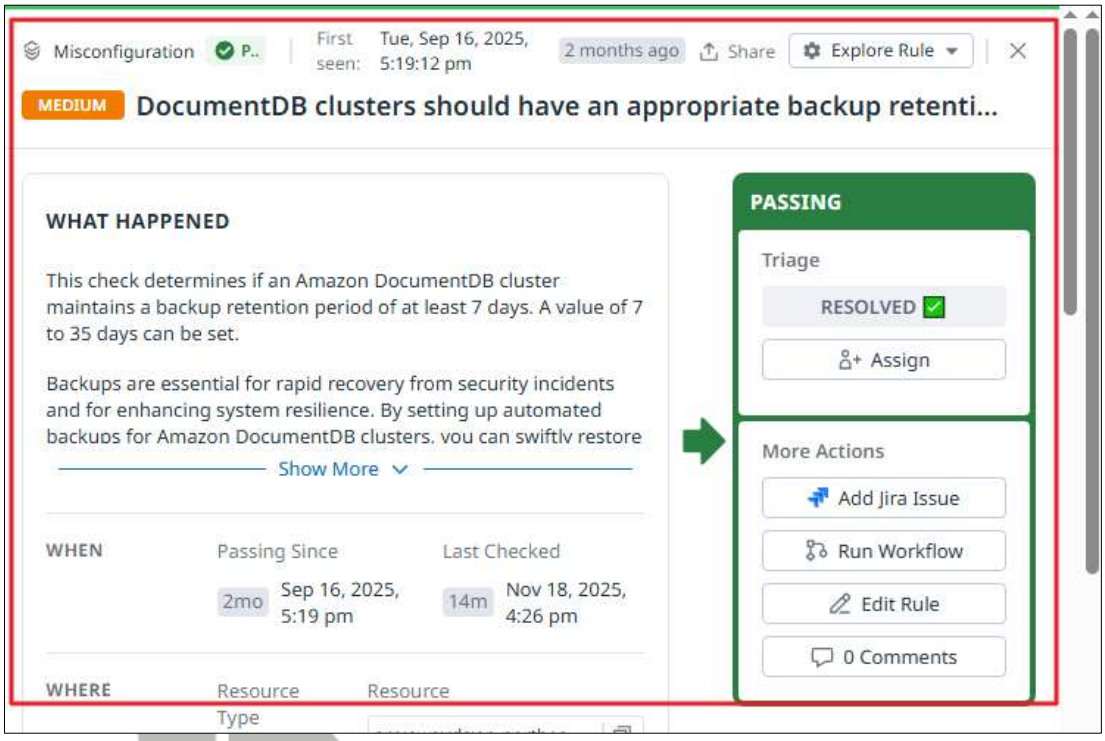
	
탐지 기준	**커스텀** : 로그 보관 기간 설정 유무를 확인하여 탐지
비고	

4.12 백업 사용 여부

분류	운영 관리	중요도	중
항목명	백업 사용 여부		
항목 설명	운영중인 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.		
설정 방법	**가. DocumentDB 클러스터에는 적절한 백업 보존 기간이 설정되어야 함 (MEDIUM)** 1) DocumentDB 클러스터 확인  2) DocumentDB 클러스터 내 백업 정책 확인 ***※ 클러스터 생성 시 기본 백업 설정 (Default) – 최소 1일***  3) DocumentDB 클러스터 내 백업 보존기간 설정 확인		

4) Datadog 내 DocumentDB 백업 정책 탐지 확인



	
탐지 기준	**def-000-5q3** : 클러스터 내 백업 보관기간에 따라 탐지
비고	기술 공식 문서 : https://docs.datadoghq.com/security/default_rules/def-000-5q3/

안녕을 지키는 기술 | SK 쉴더스

SK쉴더스㈜ 13486 경기도 성남시 분당구 판교로227번길 23, 4&5층
https://www.skshieldus.com

발행인 : SK쉴더스 ICT취약점진단팀