EQST insight

AWS 클라우드 환경 내 ISMS 주요 인증항목 구현 전략

공공컨설팅/고도화팀 신관용 책임

■ 개요

출처 : KISA 한국인터넷진흥원 홈페이지

최근 IT 인프라 구축 시 온프레미스(On-Promise) 환경에서 클라우드 환경으로 전환하거나 하이브리드로 운영하는 기업이 늘고 있다. 시장조사업체 IDC 에 따르면 지난해 세계 클라우드 시장 규모는 전년 대비 20% 증가한 850 조 원이며, 향후 5 년간 연평균 19.4% 성장해 오는 2027 년에는 1,733 조 원에 달할 것으로 전망된다.

클라우드 환경은 디지털 전환에 따라 발생하는 대량의 데이터를 효과적으로 저장할 수 있도록 돕는다. 기업들은 이러한 클라우드 환경을 통해 가용성과 확장성을 높이고, 비용절감 및 효율성을 제고해 비즈니스 경쟁력을 확보할 수 있다. 특히, 클라우드 서비스 이용 시 예기치 못한 비상상황에서도 유연한 대응이 가능해 도입이 확대되고 있는 상황이다.

기업에서는 클라우드 환경에서의 보호대책 요구사항을 충족하도록 보안정책을 수립하고 관리하는 게 필요하다. 다만, 클라우드 서비스 제공업체(CSP)에서 제공하는 보안정책, 서비스와 비교했을 때 용어나 구성요소가 상이해 보안 관리자들이 많은 어려움을 겪고 있다.

따라서 이번 인사이트에서는 클라우드 환경에서 ISMS(정보보호관리체계) 인증을 준비하는 관리자들에게 도움을 제공하기 위해, 전 세계적으로 가장 사용자가 많은 아마존웹서비스(AWS) 클라우드 환경에서 ISMS 주요 인증항목에 대한 구현 방법을 제시하고자 한다.

■ ISMS 보호대책 요구사항 기술 인증항목과 AWS 내 제공서비스 매칭

ISMS 인증은 과학기술정보통신부 및 개인정보보호위원회가 공동 고시하는 국내 최고 권위의 정보보호 및 관리체계 인증이다. ISMS 인증을 받기 위해서는 관리체계 수립 및 운영(16 개), 보호 대책 요구사항(64 개) 등 총 80 개의 인증 기준과 234 개의 세부 점검 항목의 적합성을 모두 충족해야 한다. ISMS 인증을 획득한 기업은 해킹 및 개인정보 유출 발생 시 신속 대응이 가능한 기업으로 평가되고 있다.

먼저, ISMS 보호대책 요구사항 기술 인증항목과 AWS 내 제공서비스는 다음과 같다.

ISMS 항목	AWS 내 제공 서비스
2.1 정책, 조직, 자산 관리	해당사항 없음
2.2 인적 보안	
2.3 외부자 보안	
2.4 물리 보안	
2.5 인증 및 권한관리	**IAM**
2.6 접근통제	**VPC**
2.7 암호화 적용	**Key Management Service**
2.8 정보시스템 도입 및 개발 보안	해당사항 없음
2.9 시스템 및 서비스 운영관리	**CloudTrail, CloudWatch AWS System Manager**
2.10. 시스템 및 서비스 보안관리	**AWS WAF, AWS Firewall**
2.11. 사고 예방 및 대응	해당사항 없음
2.12 재해 복구	

출처 : ISMS-P 인증기준안내서 재가공

표 1. ISMS 보호대책 요구사항과 AWS 내 제공서비스 매칭

■ 주요 인증항목 구현방법

1. ISMS 인증항목 – 2.5 인증 및 권한관리

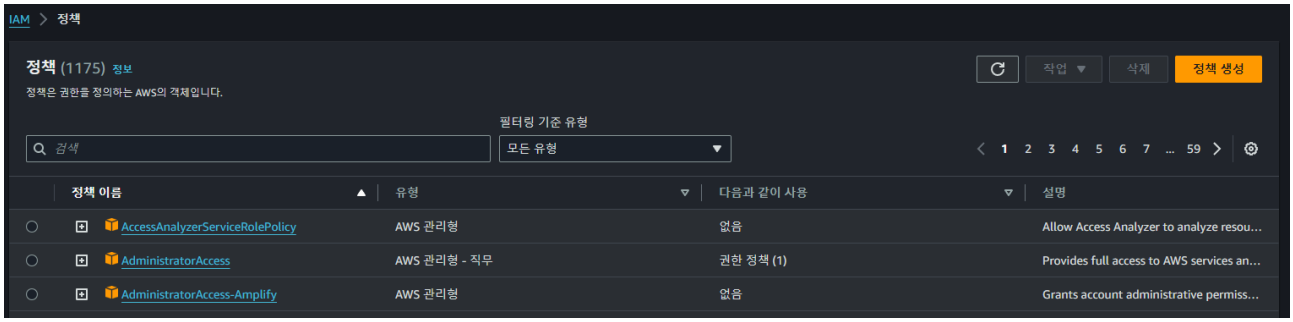
1) 2.5.1 사용자 계정관리 / 2.5.2 사용자 식별 / 2.5.6 접근권한 검토

AWS 서비스에서 사용되는 계정은 루트 사용자 계정, IAM 사용자 계정이 있다.

- AWS 루트 계정 : 모든 AWS 서비스 및 리소스에 액세스할 수 있는 슈퍼유저 계정이므로 서비스 운용 시 사용하지 않는 것을 권장
- AWS IAM(Identity and Access Management) : AWS 서비스에 접근하는 계정 생성 인증(로그인) 및 권한 부여 등 계정관리 서비스

※ 서비스별(EC2, RDS) 계정은 각 서비스에서 관리한다

기본적으로 IAM 을 통해 계정 생성/관리를 수행한다. 계정 권한은 사용자별, 그룹별로 부여할 수 있으며 AWS 에서는 '관리형 정책'을 통해 최고관리자/각 서비스별 관리자/사용자별 권한을 미리 정의하여 제공하고 있다. 또한, 직접 정책을 생성하여 원하는 권한을 선택하여 부여할 수 있다.



출처 : AWS 콘솔 홈페이지

그림 1. AWS 에서 제공하는 관리형 정책

★ Key Point

소수 계정을 사용할 경우 각 계정별로 권한을 부여하여 관리할 수 있지만, 다수의 계정을 생성한다면 직무별로 그룹 생성 후 권한을 부여하는 것이 관리/권한 검토 시 용이하다.

그림 2. 사용자 그룹 생성

출처 : AWS 콘솔 홈페이지

그림 3. 그룹 지정하여 권한 부여

2) 2.5.3 사용자 인증

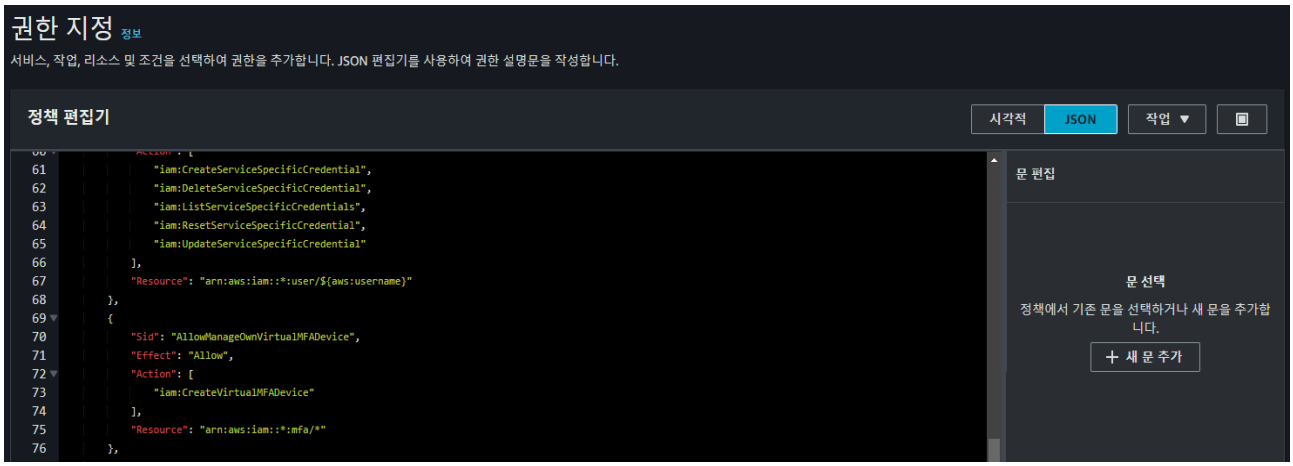
개인정보 및 중요정보에 접근하는 계정은 안전한 인증절차를 적용해야 한다. AWS 에서는 3 가지의 MFA(Multi Factor Authentication)를 제공하고 있다.

- 모바일 OTP 인증 : Google Authenticator APP으로 OTP 생성 및 인증
- FIDO 보안키 인증 : FIDO 표준을 지원하는 보안키를 이용한 인증
- 하드웨어 OTP 인증 : 하드웨어 방식의 OTP생성기를 이용한 인증

★ Key Point

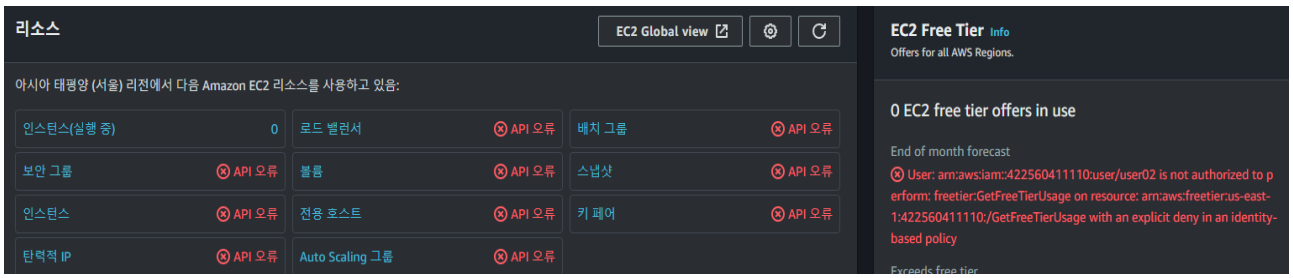
사용자 계정 생성 후 MFA 미설정 시 AWS 서비스에 접근할 수 없도록 IAM 정책으로 강제 적용할 수 있다. 아래 AWS 문서를 참고하여 MFA 강제인증 정책을 생성 후 그룹정책 또는 사용자에게 직접 정책을 적용하면 된다.

※ 참고링크: https://docs.aws.amazon.com/ko_kr/IAM/latest/UserGuide/tutorial_users-self-manage-mfa-and-creds.html



출처 : AWS 콘솔 홈페이지

그림 4. IAM 정책생성에서 JSON 편집기를 통해 MFA 강제인증 정책 생성



출처 : AWS 콘솔 홈페이지

그림 5. MFA 강제인증 정책 적용시 MFA 활성화 전까지 AWS 서비스 이용이 제한됨

3) 2.5.4 비밀번호 관리

AWS 에서 Default 로 설정되어 있는 비밀번호 관리규칙은 아래와 같다.

- 암호 최소 길이 : 8자
- 대/소문자, 숫자, 특수문자 중 3가지 이상 포함
- AWS 계정이름 또는 이메일 주소와 동일한 문자 사용 금지
- 비밀번호 10 회 실패 시 5 초 로그인 제한

Default 값 이외 규칙은 다음과 같이 수동으로 설정해야 한다.

- 암호 만료기간 설정 : 90일 이하로 설정
- 사용자 자신의 암호 변경 허용 : 허용 활성화
- 암호 재사용 제한 : 동일 암호 재사용 제한, 4개 이상 기억 권장

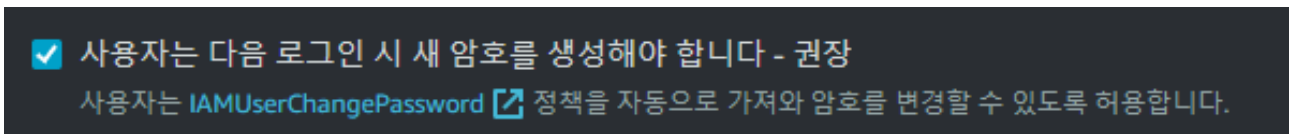
출처 : AWS 콘솔 홈페이지

그림 6. 기본 암호 정책

출처 : AWS 콘솔 홈페이지

그림 7. 추가로 제공하는 암호 정책

★ Key Point



출처 : AWS 콘솔 홈페이지

그림 8. 사용자 초기암호 강제변경 옵션

IAM 사용자에게 최초 계정 부여 또는 비밀번호 초기화 시 최초 비밀번호 강제 변경을 위해 위 옵션을 관리자가 직접 체크해야 한다.

4) 2.5.5 특수 계정 및 권한관리

AWS IAM 에서 설정할 수 있는 정책 중 특수권한(관리자 권한)은 아래와 같다.

정책이름	설 명
AdministratorAccess	AWS 내 모든 서비스와 리소스에 대한 모든 작업 허용 ※ 루트계정 대신 최고관리자로 권한을 부여할 계정에만 최소한으로 부여하여야 한다.
FullAccess	각 서비스별(EC2, RDS, S3 등) 모든 작업을 허용 ※ 서비스별 자원 생성/삭제/수정이 가능하므로 해당 직무를 수행하는 계정에게만 최소한으로 부여하여야 한다.

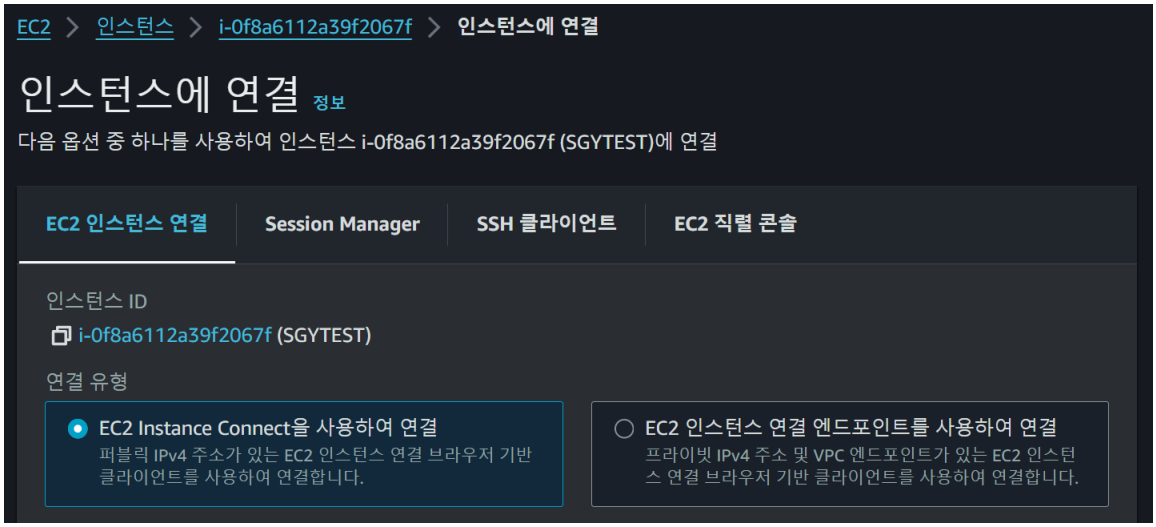
출처 : AWS 가이드 홈페이지 재가공

표 2. AWS IAM 관리자권한 정책

★ Key Point

AdministratorAccess, Ec2FullAccess 권한을 가지고 있는 경우 SSH 를 이용하지 않고 EC2 인스턴스 직접접속 기능으로 EC2 인스턴스에 직접 접근이 가능하다. SSH 이외 우회 접근을 제한하기 위해서는 아래 링크를 참고하여 EC2 인스턴스내 ec2-instance-connect 패키지를 제거해야 한다.

※ 참고링크: https://docs.aws.amazon.com/ko_kr/AWSEC2/latest/UserGuide/ec2-instance-connect-uninstall.html



출처 : AWS 콘솔 홈페이지

그림 9. AWS 에서 제공하는 EC2 인스턴스 직접연결

```
[ec2-user ~]$ sudo yum remove ec2-instance-connect
```

출처 : AWS 가이드 홈페이지

그림 10. EC2 인스턴스에서 ec2-instance-connect 제거

2. ISMS 인증항목 – 2.6 접근통제

1) 2.6.1 네트워크 접근 / 2.6.7 인터넷 접속 통제

AWS 에서는 VPC(Virtual Private Cloud)라는 독립적인 네트워크를 구성한다.

VPC 내에서 네트워크 영역은 Public 과 Private 으로 구분된다.

- Public : 인터넷 게이트웨이를 통해 외부망과 통신가능한 네트워크 영역
- Private : 사설IP로 할당하여 내부망으로만 통신가능한 네트워크 영역

WEB 서비스 등 대외서비스를 위해 운용하는 인스턴스는 Public 으로 할당하고, 외부통신이 필요 없는 내부망 전용 인스턴스는 Private 으로 할당한다.

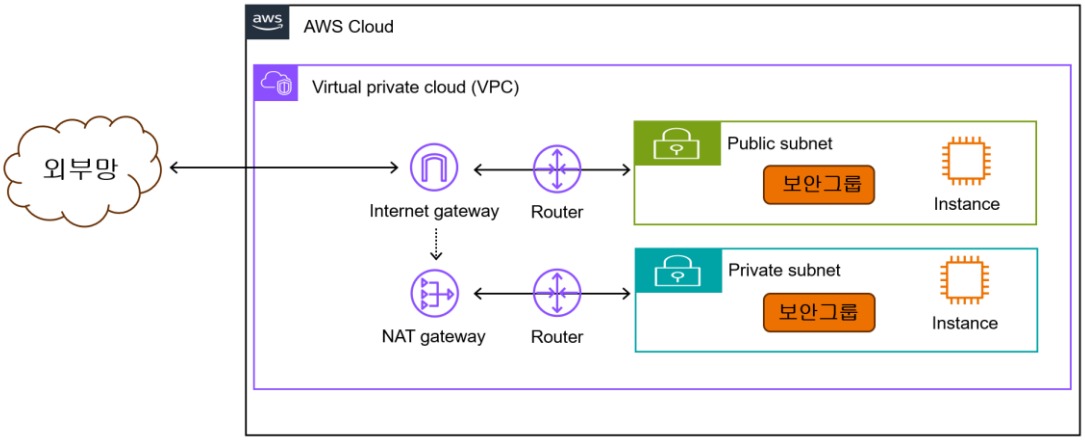
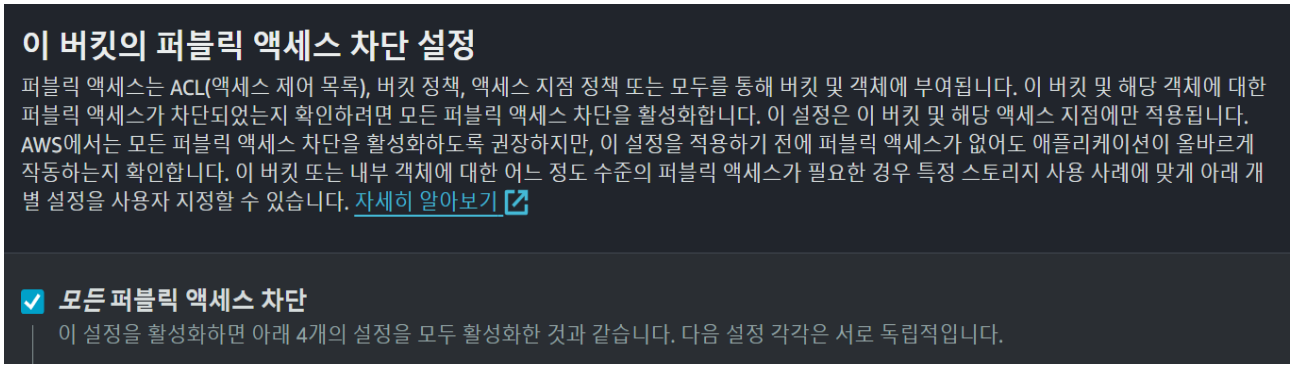


그림 11. AWS 네트워크 구성도

★ Key Point

AWS 에서 EC2, RDS, S3 생성 시 Public 액세스를 설정하면 라우팅과 관계없이 인스턴스/버킷이 직접 외부망과 통신이 가능한 상태가 되어 직접 접근이 가능하므로 인스턴스/버킷에 Public 액세스를 활성화하는 것은 권장하지 않는다.

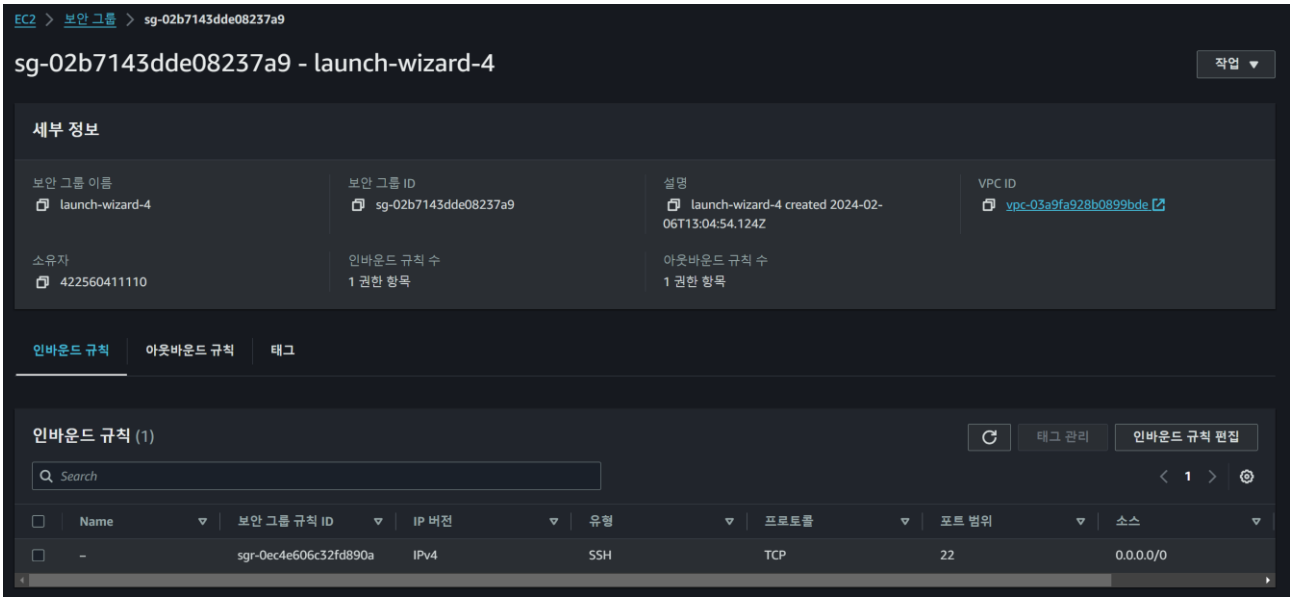


출처 : AWS 콘솔 홈페이지

그림 12. S3 버킷 퍼블릭 액세스 차단설정

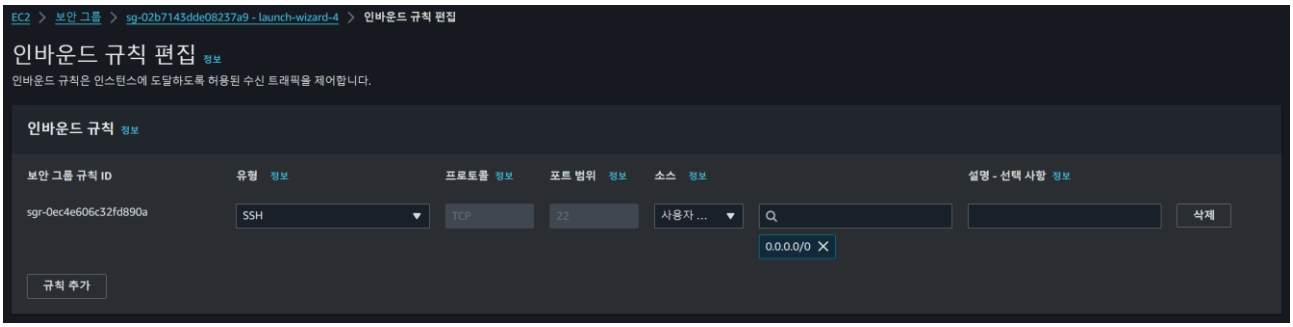
2) 2.6.2 정보시스템 접근

AWS VPC 에서는 각 인스턴스에 대한 접근제어를 위해 방화벽 역할을 수행하는 보안그룹(Security Group)을 제공한다. 보안그룹은 아무 정책을 추가하지 않으면 ALL DENY 로 동작하며 허용이 필요한 IP/PORT 정책을 등록하여 운용한다.



출처 : AWS 콘솔 홈페이지

그림 13. AWS 보안그룹



출처 : AWS 콘솔 홈페이지

그림 14. AWS 보안그룹 정책 편집

★ Key Point

보안그룹 최초 생성 시 인바운드 규칙에는 SSH 허용정책, 아웃바운드에는 모든 트래픽 허용 정책이 기본으로 설정되어 있다. 따라서 접근이 필요한 IP/PORT 정책 추가 후 기본 정책은 제거해야 한다.

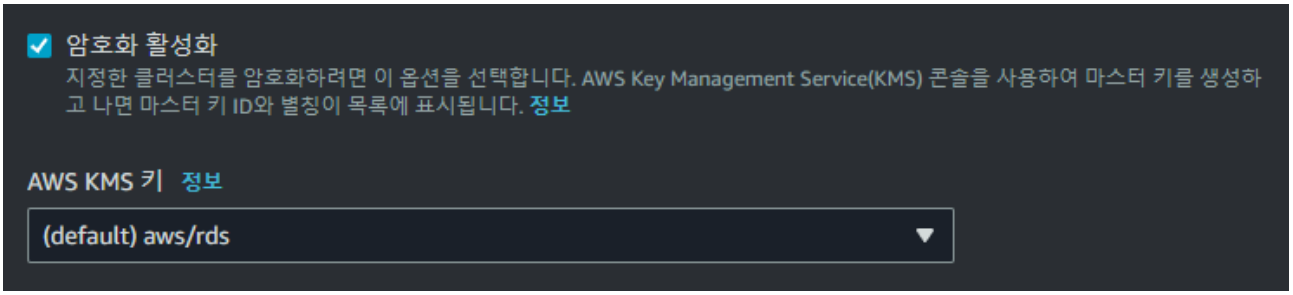
3. ISMS 인증항목 – 2.7 암호화 적용

1) 2.7.1 암호정책 적용 / 2.7.2 암호키 관리

EC2 스토리지, RDS, S3 등 데이터가 저장되는 서비스는 암호화 설정이 가능하다. EC2, RDS 는 인스턴스 생성시 암호화 여부를 설정할 수 있고, S3 버킷은 2023 년 1 월 5 일부터 기본값으로 S3 관리형 키를 이용한 암호화가 자동 적용된다.

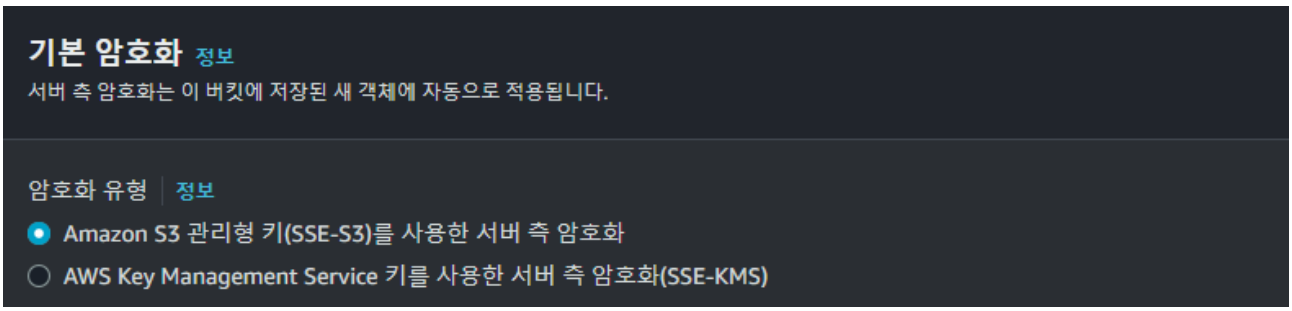
출처 : AWS 콘솔 홈페이지

그림 15. EC2 스토리지 암호화 설정



출처 : AWS 콘솔 홈페이지

그림 16. RDS 생성 시 암호화 설정

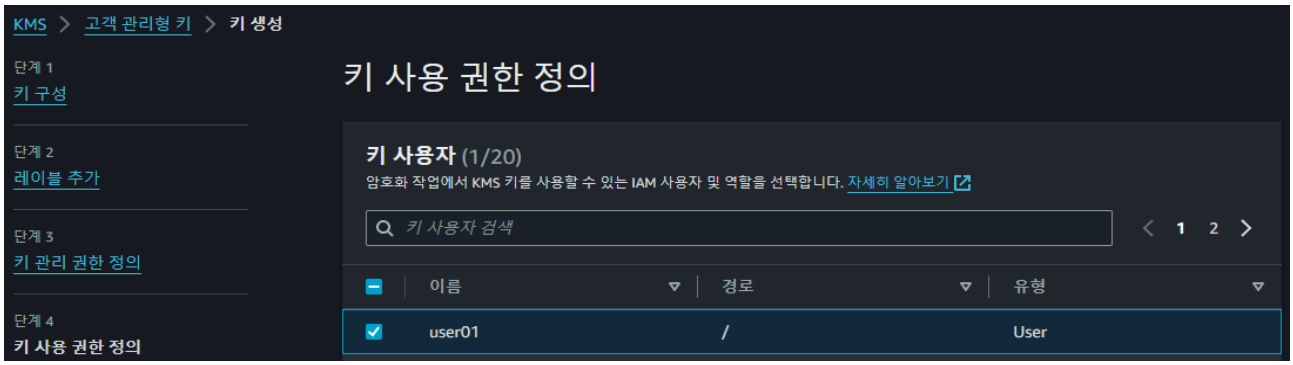


출처 : AWS 콘솔 홈페이지

그림 17. S3 버킷 암호화 설정 (기본 암호화 적용되어 있음)

★ Key Point

특정 사용자에게만 중요데이터 접근을 허용하려면 Key Management Service 에서 Key 를 생성하여 해당 키를 사용할 계정을 지정하여 암호화를 적용한다.



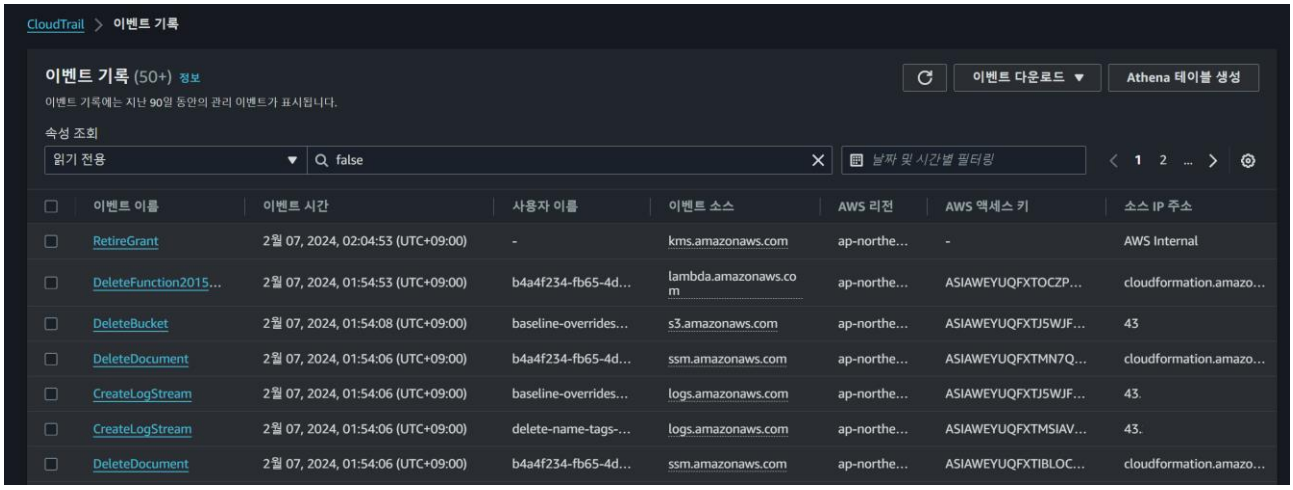
출처 : AWS 콘솔 홈페이지

그림 18. KMS 에서 Key 생성 시 사용자 지정 화면

4. ISMS 인증항목 – 2.9 시스템 및 서비스 운영관리

1) 2.9.4 로그 및 접속기록 관리

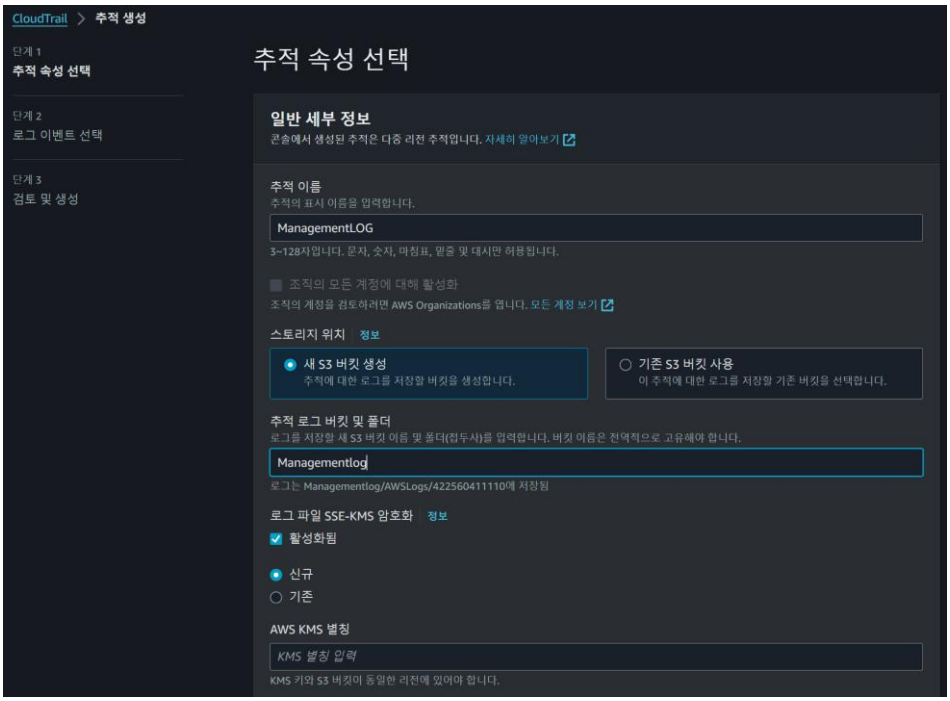
AWS 계정의 모든 활동로그는 CloudTrail 에 자동으로 기록된다. 최대 90 일 동안의 이벤트 로그가 저장되며, 90 일 이상 보관을 위해서는 추적을 생성하여 S3 버킷에 저장해야 한다.



출처 : AWS 콘솔 홈페이지

그림 19. AWS CloudTrail 이벤트 기록

추적을 생성하여 CloudTrail 이벤트 로그를 S3 버킷으로 저장할 수 있으며, SSE-KMS 암호화 설정을 하면 해당로그는 암호화되어 저장된다.

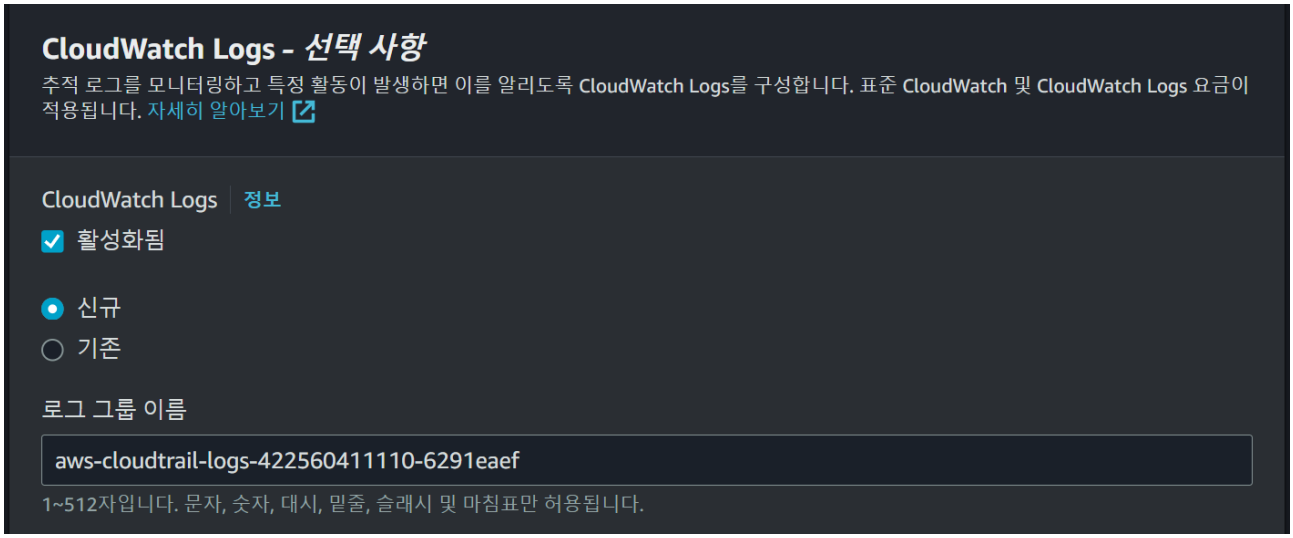


출처 : AWS 콘솔 홈페이지

그림 20. AWS CloudTrail 추적 생성

★ Key Point

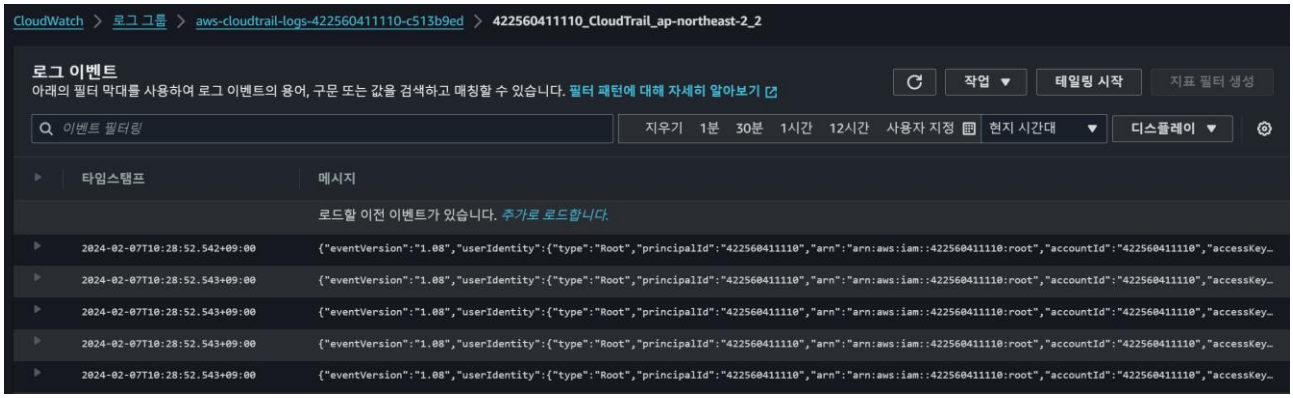
CloudTrail 로그를 S3 버킷으로만 저장하면 실시간 조회는 불가능하다. 수시로 조회해야 할 경우 CloudWatch 와 연동하여 로그를 확인할 수 있다.



출처 : AWS 콘솔 홈페이지

그림 21. CloudWatch 연동 설정

연동설정이 완료되면 CloudWatch 로그 그룹에 추가되며, 로그보존 기간을 설정하고 조회할 수 있다.



출처 : AWS 콘솔 홈페이지

그림 22. AWS CloudWatch 로그 이벤트 조회

■ 맺음말

지금까지 주요 ISMS 보호대책 구현을 위한 AWS 설정을 알아봤다. 클라우드 자산의 자동화된 위험평가를 위해 AWS Config 서비스, AWS Inspector 서비스 이용을 고려할 수 있다.

국내 1 위 보안 컨설팅 사업자 SK 쉴더스는 20 년간의 컨설팅 노하우가 집약된 노하우를 기반으로 클라우드 환경의 체계적인 보안 관리를 위해 정보보호관리체계(ISMS) 인증 컨설팅 서비스를 제공하고 있다. 업계 최다 전문 컨설턴트를 보유하고 있으며, 이들의 풍부한 컨설팅 수행 경험을 토대로 기업별 최적의 개선방안을 제공한다.

또한, SK 쉴더스는 공익 목적의 정보보안 정보 공유 활동에도 앞장서고 있다. 지난 2019 년 클라우드 보안 사업 수행에서 축적한 노하우를 기반으로 2021 년 클라우드 보안 가이드를 발간한 바 있으며, 지난해에는 두 번째 개정판을 발간했다. 기업의 보안 관계자는 '2023 클라우드 보안 가이드'를 통해 관리 영역에서 위협에 효과적으로 대응하고, 변화된 관리 영역 및 컴플라이언스 기준을 충족할 수 있는 방안을 확인할 수 있다. 이를 통해, 보안 관리자는 자체적으로 보안상 안전한 설정을 적용할 수 있으며, 추후 발생 가능한 위협에 대해 사전 대응 가능 여부를 점검해 볼 수 있다.

이러한 보안 가이드와 SK 쉴더스 컨설팅을 통해 클라우드 환경에서 ISMS 인증에 효과적이고 체계적으로 대응하길 바란다. 보다 자세한 내용은 SK 쉴더스 공식 블로그를 통해 확인할 수 있다.