K-Digital training
클라우드보안융합,
클라우드데이터보안
전문가 양성과정

클라우드 보안 가이드

2 조 청바지
강길웅 곽지선 김진현
배효린 박주희 임종배 하주연

목 차

0. 보안 진단 체크리스트 & 위험도 산정 기준

1. 클라우드 보안

- CloudTrail 3
- CloudWatch 6
- Inspector 10
- GuardDuty 13
- Config 15
- System Manager 18

2. 네트워크 보안

- Security Group 21
- ACL 24
- Network Firewall 27
- NAT Gateway 31
- WAF 33
- VPN 35
- Internet Gateway 38
- Routing Tables 39

3. 계정 보안

- Multi Factor 인증 41
- IAM(자격 증명 기반 정책) 44

4. RDS

- 다중 AZ 48
- 스냅샷 49
- 파라미터 스토어 50
- 프라이빗 액세스 52

5. 데이터 보안

- 가명처리 53
- KMS 62

0. 보안 진단 체크리스트 & 위험도 산정 기준

- AWS 보안진단 체크리스트

영역	항목명	중요도
클라우드 보안	CloudTrail	중
	CloudWatch	중
	Inspector	하
	GuardDuty	중
	Config	상
	System Manager	상
네트워크 보안	Security Group	중
	ACL	중
	Network Firewall	중
	NAT Gateway	하
	WAF	중
	VPN	하
	Internet Gateway	하
	Routing Tables	중
계정 보안	Multi Factor 인증	중
	IAM(자격 증명 기반 정책)	하
RDS	다중 AZ	중
	스냅샷	중
	파라미터 스토어	상
	프라이빗 액세스	중
데이터 보안	가명처리	상
	KMS	상

- 위험도 산정 기준

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

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

1. 클라우드 보안

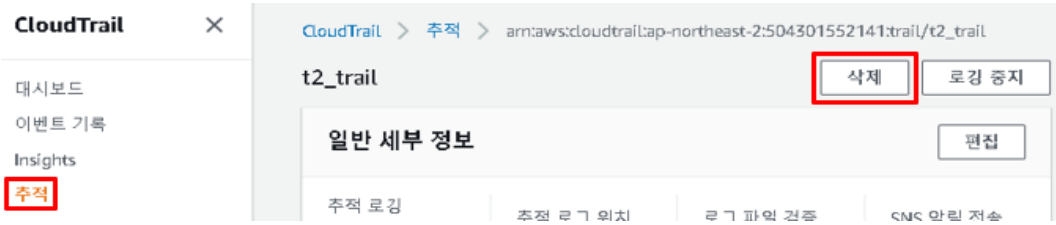
<table>
<tr><td>분류</td><td colspan="2">클라우드 보안</td><td>위험도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="4">CloudTrail</td></tr>
<tr><td>항목 설명</td><td colspan="4">AWS CloudTrail은 AWS 계정의 거버넌스, 규정 준수, 운영 감사, 위험 감사를 지원하는 서비스입니다. AWS 인프라에서 계정 활동과 관련된 작업을 기록하고 지속적으로 모니터링하며 보관합니다. 이러한 이벤트 기록을 통해 보안 분석, 리소스 변경 추적, 문제 해결을 간소화할 수 있습니다. 또한 AWS 계정의 비정상적인 활동을 탐지할 수 있습니다.

- 기능
• 보안 분석 및 문제 해결 - 지정된 기간 내에 AWS 계정에서 이루어진 변경 사항에 대한 포괄적인 기록을 캡처하여 보안 및 운영 문제를 발견하고 해결할 수 있습니다.
• 사용자 및 리소스 활동에 대한 가시성 - AWS Management Console 작업과 API 호출을 기록함으로써 사용자 및 리소스 활동에 대한 가시성을 높입니다. AWS 를 호출한 사용자와 계정, 호출이 이루어진 소스 IP 주소, 호출이 발생한 시간을 파악할 수 있습니다.
• 보안 자동화 - AWS 리소스 보안을 위협하는 계정 활동을 추적하고 자동으로 대응할 수 있습니다. Amazon CloudWatch Events 와 통합하면 보안 취약성을 초래할 수 있는 이벤트가 탐지될 때 실행되는 워크플로를 정의할 수 있습니다. 예를 들어 CloudTrail 이 해당 버킷을 공개로 전환하는 API 호출을 기록하는 경우 Amazon S3 버킷에 특정 정책을 추가하도록 워크플로를 생성할 수 있습니다.</td></tr>
<tr><td rowspan="10">세부 설명</td><td>조항</td><td>항목번호</td><td>항목</td><td>일부내용</td></tr>
<tr><td>ISMS-P</td><td>2.5.1</td><td>사용자 계정관리</td><td rowspan="2">개인정보 및 중요정보에 대한 비인가 접근을 통제하고 접근권한을 최소한으로 부여</td></tr>
<tr><td>CSAP</td><td>10.2.1</td><td>사용자 등록 및 권한부여</td></tr>
<tr><td>ISMS-P</td><td>2.9.4</td><td>로그 및 접속기록 관리</td><td rowspan="4">사용자 접속기록, 시스템로그 보존방법 정의. 정보시스템에 대한 사용자 접속기록, 시스템로그, 권한부여 내역 등의 로그유형, 보존기간, 보존방법 등을 정하고 위·변조, 도난, 분실 되지 않도록 안전하게 보존·관리</td></tr>
<tr><td>ISMS-P</td><td>2.9.5</td><td>로그 및 접속 기록 점검</td></tr>
<tr><td>CSAP</td><td>13.1.3</td><td>보안로그 기능</td></tr>
<tr><td>CSAP</td><td>10.1.2</td><td>접근기록 관리</td></tr>
<tr><td>ISMS-P</td><td>2.9.6</td><td>시간 동기화</td><td>로그 및 접속기록의 정확성을 보장하고 신뢰성 있는 로그분석을 위하여 관련 정보시스템의 시각을 표준시각으로 동기화하고 주기적으로 관리</td></tr>
<tr><td>CSAP</td><td>9.2.2</td><td>인터페이스 및 API 보안</td><td>가상 환경 접근을 위한 인터페이스 및 API에 대한 보호 방안 마련</td></tr>
<tr><td>CSAP</td><td>10.2.3</td><td>접근권한 검토</td><td>클라우드 시스템에 대한 접근권한 검토 이행</td></tr>
<tr><td colspan="4">항목 준수를 위해 cloudwatch를 통한 점검과 함께 사용자 계정에 대한 등록, 이용 접근권한의 부여, 변경 이력을 남기며 불필요한 정보와 중요정보 노출을 최소화하며 API에 대한 로그 및 접속기록을 관리하고 시스템 로그가 위·변조 되지않도록 안전하게 관리합니다.</td></tr>
<tr><td>설정 방법</td><td colspan="4">- CloudTrail 추적 생성
CloudTrail → 추적 → 추적 생성 → 추적 페이지에서 생성한 추적 이름 선택 → 추적의 행에</td></tr>
</table>

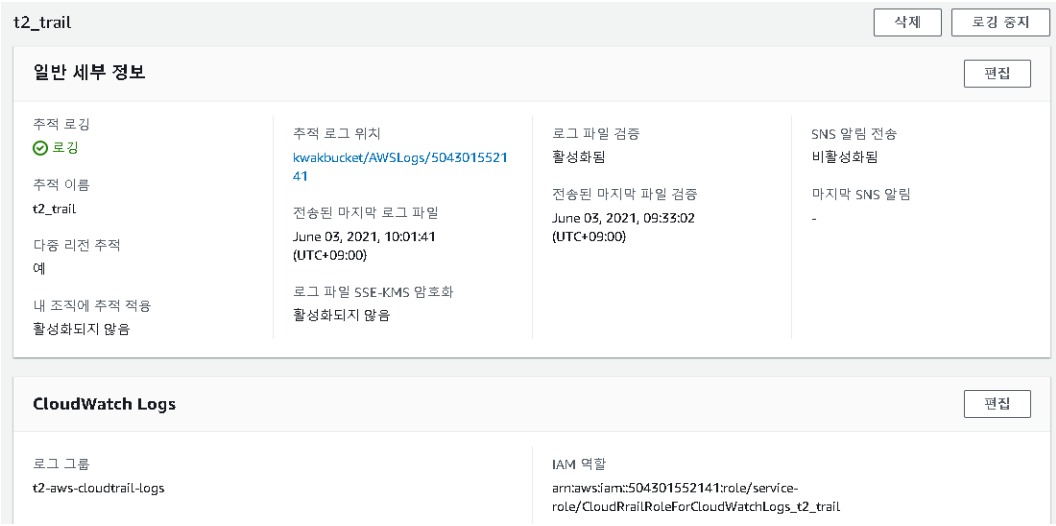
서 S3 버킷의 값을 선택 → 로그 파일을 검토하려는 AWS 리전의 폴더 선택 → 로그 파일을 검토하려는 연도, 월 및 일 선택

- CloudTrail 추적 삭제

CloudTrail → 추적 → 삭제하려는 추적 이름 선택 → 추적 세부 정보 페이지 상단에서 삭제



- CloudTrail 예시



※ 자세한 설명은

https://docs.aws.amazon.com/ko_kr/awscloudtrail/latest/userguide/cloudtrail-tutorial.html 참고

진단 기준	양호	CloudTrail의 추적기능을 활성화한 경우
	취약	CloudTrail의 추적기능을 활성화하지 않은 경우

적용 인증법	CSAP 9.2.2. 인터페이스 및 API 보안 CSAP 10.1.2. 접근기록 관리 CSAP 10.2.1. 사용자 등록 및 권한부여 CSAP 10.2.3. 접근권한 검토 CSAP 13.1.3. 보안로그 기능 ISMS-P 2.9.4 로그 및 접속 기록 관리

	ISMS-P 2.5.1 사용자계정관리 ISMS-P 2.9.4 로그 및 접속 기록 관리 ISMS-P 2.9.5 로그 및 접속 기록 점검 ISMS-P 2.9.6 시간 동기화

분류	클라우드 보안	위험도	중
항목명	CloudWatch		

항목 설명

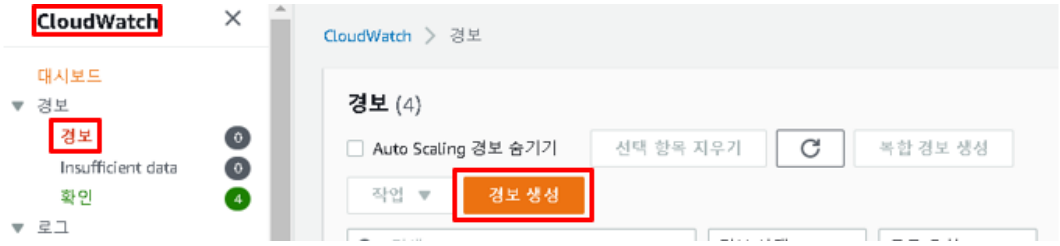
AWS 리소스와 AWS에서 실시간으로 실행 중인 애플리케이션을 모니터링합니다. 또한 리소스 및 애플리케이션에 대해 측정할 수 있는 변수인 지표를 수집하고 추적할 수 있습니다.

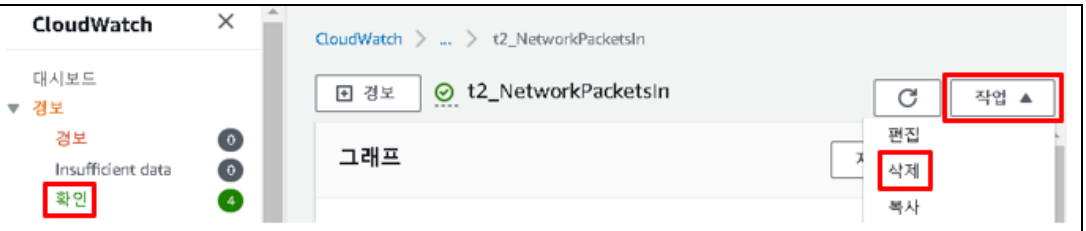
- **기능**

- **수집** - 리소스, 애플리케이션 및 서비스로부터 거의 실시간으로 로그를 수집하고 저장할 수 있습니다. 또한 사용자가 별도의 작업을 수행하지 않고도 Amazon EC2, Amazon DynamoDB, Amazon S3 등 70 개가 넘는 AWS 서비스에서 기본 지표를 수집할 수 있습니다. 또한 CPU, 메모리, 네트워크, 디스크 정보 같은 컴퓨팅 성능 지표를 각각의 컨테이너에서 성능 이벤트로 수집하고, 모니터링 및 경보 제공에 사용되는 사용자 지정 지표를 자동으로 생성합니다.
- **모니터링** - Amazon CloudWatch 대시보드를 사용하면 재사용 가능한 그래프를 생성하고 통합된 뷰에서 클라우드 리소스와 애플리케이션을 시각화할 수 있습니다. 하나의 대시보드에서 지표와 로그 데이터를 나란히 그래프로 표시하여 컨텍스트를 빠르게 확보하고 문제 진단에서 근본 원인 파악까지 진행할 수 있습니다. 또한 Amazon CloudWatch 이상 탐지는 기계 학습 알고리즘을 적용하여 지표 데이터를 지속적으로 분석하고 이상 행동을 식별합니다.
- **조치** - 주요 지표에 대한 경보를 받고 자동화된 Auto Scaling 작업을 트리거하도록 임계값을 설정할 수 있습니다. Amazon EKS 및 k8s 클러스터의 경우, Container Insights 를 사용하면 컴퓨팅 지표에 대한 경보를 제공하여 Amazon EC2 Auto Scaling 그룹에 대한 Auto Scaling 정책을 트리거하고 Amazon EC2 인스턴스를 중지, 종료, 재부팅, 복구할 수 있습니다.

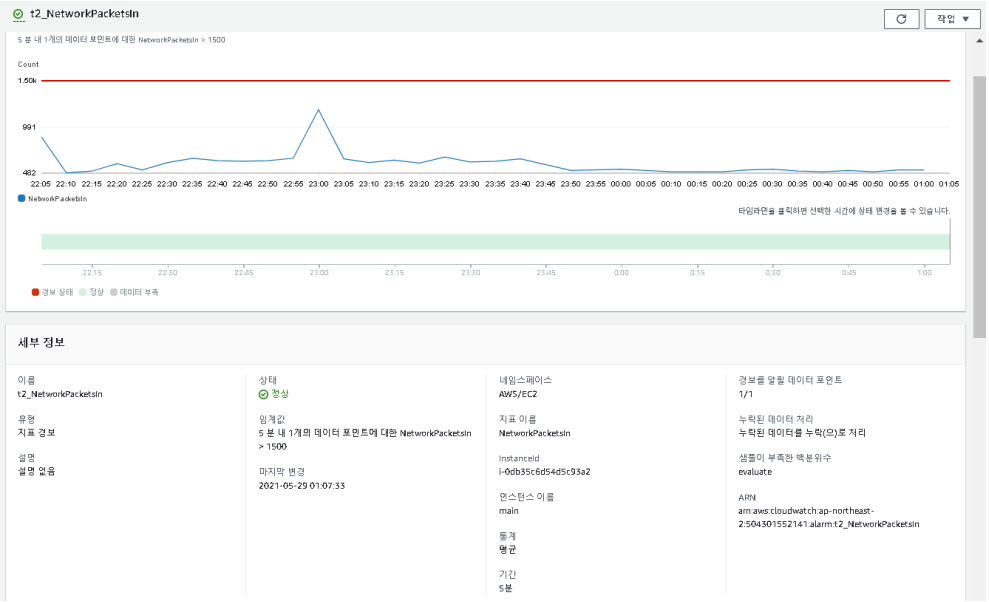
세부 설명

조항	항목번호	항목	일부내용
ISMS-P	2.5.3	사용자관리	클라우드 시스템에 대한 접근은 안전한 사용자 인증 절차에 의해 통제하고 계정 및 권한은 최소한으로 부여
ISMS-P	2.10.2	클라우드 보안	
CSAP	10..3.2	사용자 인증	
ISMS-P	2.6.1	네트워크 접근	DDoS, 비인가 접속 등으로 인한 서비스 중단 및 중요 정보 유출 등을 막기 위해 네트워크를 모니터링하고 통제. 내·외부에 의한 침해시도, 개인정보유출 시도, 부정행위 등을 신속하게 탐지·대응할 수 있도록 네트워크 및 데이터 흐름 등을 수집하여 분석
ISMS-P	2.10.1	보안시스템 운영	
ISMS-P	2.11.3	이상행위 분석 및 모니터링	
CSAP	11.1.2	네트워크 모니터링 및 통제	
ISMS-P	2.9.2	성능 및 장애 관리	관련 법률에서 규정한 클라우드컴퓨팅서비스의 중단으로부터 업무 연속성을 보장하기 위해 백업, 복구 등을 포함하는 장애 대응 절차를 마련 . 지속적으로 관리할 수 있는 모니터링 방법 또는 절차를 수립
CSAP	6.1.1	장애 대응절차 수립	
CSAP	6.1.2	장애 보고	
CSAP	6.1.3	장애 처리 및 복구	
CSAP	6.2.1	성능 및 용량 관리	
ISMS-P	2.9.3	백업 및 복구 관리	정보처리설비의 장애로 서비스가 중단되지 않도록 정보 처리설비를 이중화하고, 장애 발생
CSAP	6.2.2	이중화 및 백업	

				시 신속하게 복구를 수행하도록 백업 체계도 마련
	ISMS-P	2.9.4	로그 및 접속 기록 관리	클라우드 시스템 설계 시 사용자의 인증, 권한 변경, 중요정보 이용 및 유출 등에 대한 감사증적을 확보. 서버, 응용프로그램, 보안시스템, 네트워크시스템 등 정보시스템에 대한 사용자 접속기록, 시스템로그, 권한부여 내역 등의 로그 유형, 보존기간, 보존방법 등을 정하고 위·변조, 도난, 분실 되지 않도록 안전하게 보존·관리
	ISMS-P	2.9.5	로그 및 접속 기록 점검	
	CSAP	13.1.3	보안로그 기능	
	ISMS-P	2.11.1	사고 예방 및 대응체계 구축	침해사고 및 개인정보 유출 등을 예방하고 사고 발생 시 신속하고 효과적으로 대응할 수 있도록 내·외부 침해시도의 탐지·대응·분석 및 공유를 위한 체계와 절차를 수립
	CSAP	5.1.2	침해사고 대응 체계 구축	
	ISMS-P	2.11.5	사고 대응 및 복구	침해사고 및 개인정보 유출 징후나 발생을 인지한 때에는 법적 통지 및 신고 의무를 준수하여야 하며, 절차에 따라 신속하게 대응 및 복구하고 사고분석 후 재발방지 대책을 수립하여 대응체계에 반영
	CSAP	5.2.2	침해사고 처리 및 복구	
	CSAP	9.1.1	가상자원 관리	가상자원의 생성, 변경, 회수 등에 대한 관리 방안을 수립
	CSAP	9.2.1	악성코드 통제	바이러스, 웜, 트로이목마 등의 악성코드로부터 이용자의 가상 환경을 보호하기 위한 악성코드 탐지, 차단 등의 보안기술을 지원. 또한 이상 징후 발견 시 이용자 통지하고 사용 중지 및 격리 조치를 수행
	항목 준수를 위해 cloudtrail과 함께 네트워크, 보안시스템 등에서 발생한 네트워크 트래픽, 성능 및 용량등을 지속적으로 모니터링하며 업무연속성 보장과 침해시도나 웹기반 악성공격에 대해서도 모니터링을 합니다. 임계치를 초과하는 경우엔 이메일로 알람이 오도록 설정하며 신속한 복구를 수행하기위해 백업체계도 마련하여 장애발생에 대한 대응을 합니다.			
설정 방법	**- CloudWatch 경보 생성** CloudWatch → 경보 → 경보 생성 → 지표 수식 경보가 생성된 후 경보 확인란을 선택하고 대시보드에 추가  **- CloudWatch 경보 삭제** CloudWatch → 경보 확인 → 삭제하려는 경보 이름 선택 → 작업 → 삭제			

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


- **CloudWatch 예시**



※ 자세한 설명은
https://aws.amazon.com/ko/blogs/korea/create-a-metric-math-alarm-using-amazon-cloudwatch/
참고
https://docs.aws.amazon.com/ko_kr/AmazonCloudWatch/latest/monitoring/Edit-CloudWatch-Alarm.html 참고
</td>
</tr>
<tr>
<td rowspan="2">진단 기준</td>
<td>양호</td>
<td>적절한 임계치를 설정할 경우</td>
</tr>
<tr>
<td>취약</td>
<td>임계치를 너무 높게 설정할 경우</td>
</tr>
<tr>
<td>적용 인증법</td>
<td colspan="2">ISMS-P 2.5.3. 사용자관리
ISMS-P 2.6.1 네트워크 접근
ISMS-P 2.9.2 성능 및 장애 관리
ISMS-P 2.9.3 백업 및 복구 관리
ISMS-P 2.9.4 로그 및 접속 기록 관리
ISMS-P 2.9.5 로그 및 접속 기록 점검
ISMS-P 2.10.1 보안시스템 운영
ISMS-P 2.10.2 클라우드 보안
ISMS-P 2.11.1 사고 예방 및 대응체계 구축
ISMS-P 2.11.3 이상행위 분석 및 모니터링
ISMS-P 2.11.5 사고 대응 및 복구
CSAP 5.1.2. 침해사고 대응 체계 구축
CSAP 5.2.2. 침해사고 처리 및 복구</td>
</tr>
</table>

	CSAP 6.1.1. 장애 대응절차 수립 CSAP 6.1.2. 장애 보고 CSAP 6.1.3 장애 처리 및 복구 CSAP 6.2.1. 성능 및 용량 관리 CSAP 6.2.2. 이중화 및 백업 CSAP 9.1.1. 가상자원 관리 CSAP 9.2.1. 악성코드 통제 CSAP 10.3.2. 사용자 인증 CSAP 11.1.2. 네트워크 모니터링 및 통제 CSAP 13.1.3. 보안로그 기능

<table>
<tr><td>분류</td><td colspan="3">클라우드 보안</td><td>위험도</td><td>하</td></tr>
<tr><td>항목명</td><td colspan="5">Inspector</td></tr>
<tr><td>항목
설명</td><td colspan="5">웹서버와 WAS 를 기동하는 EC2 의 인스턴스에서 실행되는 어플리케이션 보안상태를 테스트하고 노출과 취약성에 대해 평가를 합니다. Inspector 가 평가를 수행한 후 세부 보안 평가결과 목록을 제공하며 이 목록은 심각도 수준에 따라 구성되어 있습니다.

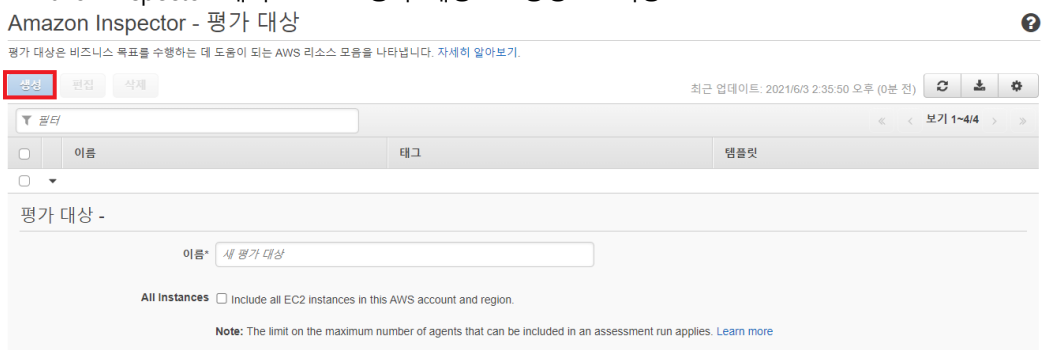
- 기능
• 구성 검색 및 활동 모니터링 엔진 - Amazon Inspector 에이전트는 시스템 및 리소스 구성을 분석합니다. 또한 활동을 모니터링하여 평가 대상의 모양, 작동 방식 및 종속성 구성 요소를 결정합니다. 이 원격 측정을 조합하면 평가 대상 및 잠재적인 보안 또는 규정 준수 문제의 전체적인 그림을 알 수 있습니다.
• 기본 제공되는 콘텐츠 라이브러리 - Amazon Inspector 에는 기본 제공되는 규칙 및 보고서의 라이브러리가 포함되어 있습니다. 여기에는 모범 사례, 공통 규정 준수 표준 및 취약성에 대한 검사가 포함됩니다. 이 검사에는 잠재적인 보안 문제를 해결하기 위한 상세한 권장 단계가 포함됩니다.
• API 를 통한 자동화 - Amazon Inspector 는 API 를 통해 완전히 자동화될 수 있습니다. 이를 통해 보안 테스트를 개발 및 설계 프로세스에 통합하고, 해당 테스트 결과를 선택, 실행 및 보고할 수 있습니다.</td></tr>
<tr><td rowspan="15">세부
설명</td><td>조항</td><td>항목번호</td><td>항목</td><td colspan="2">일부내용</td></tr>
<tr><td>ISMS-P</td><td>2.6.1</td><td>네트워크 모니터링 및 통제</td><td colspan="2" rowspan="4">DDoS, 비인가 접속 등으로 인한 서비스 중단 및 중요 정보 유출 등을 막기 위해 네트워크를 모니터링하고 통제. 내·외부에 의한 침해 시도, 개인정보유출 시도, 부정행위 등을 신속하게 탐지·대응할 수 있도록 네트워크 및 데이터 흐름 등을 수집하여 분석</td></tr>
<tr><td>ISMS-P</td><td>2.10.1</td><td>보안시스템 운영</td></tr>
<tr><td>ISMS-P</td><td>2.11.3</td><td>이상행위 분석 및 모니터링</td></tr>
<tr><td>CSAP</td><td>11.1.2</td><td>네트워크 모니터링 및 통제</td></tr>
<tr><td>ISMS-P</td><td>2.6.1</td><td>네트워크 접근</td><td colspan="2" rowspan="4">가상자원 및 서비스를 제공하기 위한 웹사이트 또는 공개서버를 제공하는 경우 기술적 보호대책을 수립. 클라우드컴퓨팅서비스 제공자의 관리 영역과 이용자의 서비스 영역, 이용자 간 서비스 영역의 네트워크 접근은 물리적 또는 논리적으로 분리하여야 하고, 취약점 점검, 접근통제, 인증, 정보 수집·저장·공개 절차 등 강화된 보호대책을 수립·이행</td></tr>
<tr><td>ISMS-P</td><td>2.10.3</td><td>공개서버 보안</td></tr>
<tr><td>CSAP</td><td>9.1.5</td><td>공개서버 보안</td></tr>
<tr><td>CSAP</td><td>11.1.5</td><td>네트워크 분리</td></tr>
<tr><td>ISMS-P</td><td>2.8.2</td><td>보안 요구사항 검토 및 시험</td><td colspan="2" rowspan="2">안전한 코딩방법에 따라 클라우드컴퓨팅서비스를 구현하고, 분석 및 설계 과정에서 도출한 보안요구사항이 정보시스템에 적용되었는지 확인하기 위하여 시험을 수행</td></tr>
<tr><td>CSAP</td><td>13.2.1</td><td>구현 및 시험</td></tr>
<tr><td>ISMS-P</td><td>2.9.3</td><td>백업 및 복구 관리</td><td colspan="2" rowspan="3">보안감사 증적(로그)은 식별할 수 있는 형태로 기록 및 모니터링 되어야 되고 비인가된 접근 및 변조로부터 보호</td></tr>
<tr><td>ISMS-P</td><td>2.9.4</td><td>로그 및 접속 기록 관리</td></tr>
<tr><td>CSAP</td><td>7.2.2</td><td>감사기록 및 모니터링</td></tr>
<tr><td>ISMS-P</td><td>2.11.2</td><td>취약점 점검 및 조치</td><td colspan="2">정보시스템의 취약점이 노출되어 있는지를</td></tr>
</table>

				확인하기 위하여 정기적으로 취약점 점검을 수행하고 발견된 취약점에 대해서는 신속하게 조치
	CSAP	7.2.1	독립적 보안감사	법적 요구사항 및 정보보호 정책 준수 여부를 보증하기 위해 독립적 보안감사 계획을 수립하여 시행하고 개선
	항목 준수를 위해 네트워크와 보안취약성 평가를 진행하며 네트워크기반 침해시도는 Network Reachability, 알려진 보안취약성에 대해서는 CVE를 사용하여 평가를 합니다. 또한 법적 요구사항 및 정보보호 정책 준수 여부를 보증하기 위해 독립적 보안감사 계획을 수립하며 보안요구사항이 정보시스템에 적용되었는지를 확인하기 위한 평가를 수행합니다. 평가된 항목에 대한 결과는 Amazon SNS를 통해 이메일로 결과를 보고 받을 수 있습니다.			

설정 방법

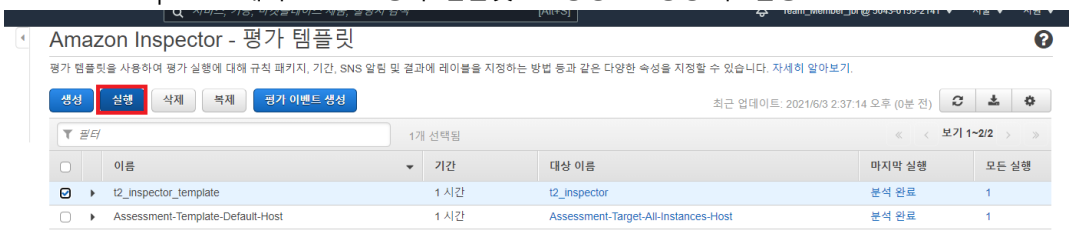
- 평가 대상 생성

Amazon Inspector 대시보드 → 평가 대상 → 생성 → 저장

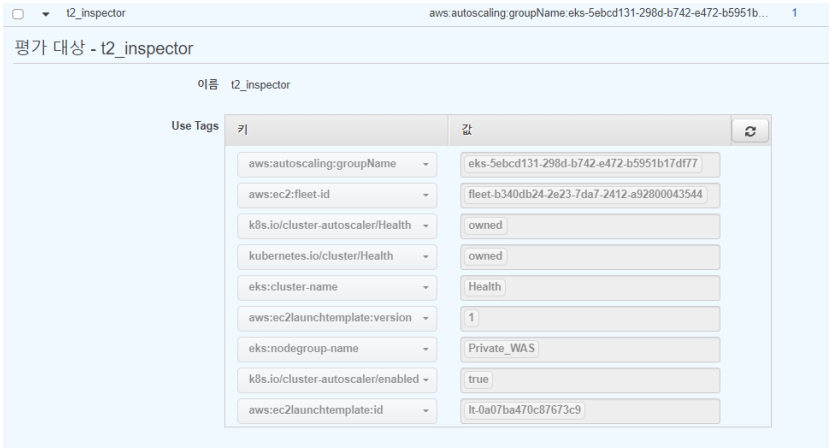


- 평가 탬플릿 생성

Amazon Inspector 대시보드 → 평가 템플릿 → 생성 → 생성 후 실행



- 평가 탬플릿 예시



※ 자세한 설명은

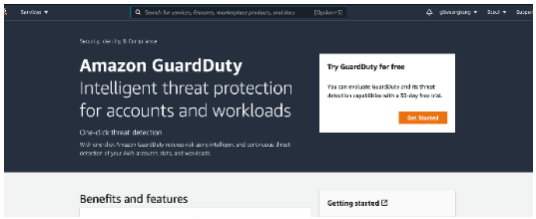
	https://docs.aws.amazon.com/ko_kr/inspector/latest/userguide/inspector_introduction.html 참고	
진단 기준	**양호**	Inspector 평가를 실시한 경우
	취약	Inspector 평가를 실시하지 않은 경우
적용 인증법	ISMS-P 2.6.1 네트워크 접근 ISMS-P 2.8.2 보안 요구사항 검토 및 시험 ISMS-P 2.9.3 백업 및 복구 관리 ISMS-P 2.9.4 로그 및 접속 기록 관리 ISMS-P 2.10.1 보안시스템 운영 ISMS-P 2.10.3 공개서버 보안 ISMS-P 2.11.2 취약점 점검 및 조치 ISMS-P 2.11.3 이상행위 분석 및 모니터링 CSAP 7.2.1. 독립적 보안감사 CSAP 7.2.2. 감사기록 및 모니터링 CSAP 9.1.5. 공개서버 보안 CSAP 11.1.2. 네트워크 모니터링 및 통제 CSAP 11.1.5. 네트워크 분리 CSAP 13.2.1. 구현 및 시험	

<table>
<tr><td>분류</td><td colspan="3">클라우드 보안</td><td>위험도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="5">GuardDuty</td></tr>
<tr><td>항목
설명</td><td colspan="5">회사의 적용되어 있는 클라우드 서비스에 대해서 분석하고 처리하는 지속적 보안 모니터링 서비스 입니다. CloudTrail 이벤트 로그, S3 데이터 로그, VPC Flow 로그, DNS 로그를 수집하여 자동으로 분석하고 해당 결과를 심각도로 나뉘어 나타냅니다.

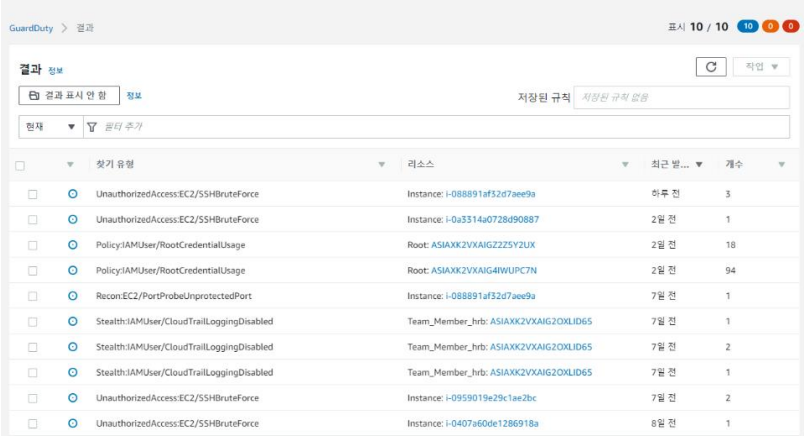
- 로그 종류
• AWS CloudTrail 이벤트로그 - AWS 서비스를 사용하여 만든 API 호출을 포함하여 계정에 대한 AWS API 호출 기록을 제공합니다.
• AWS CloudTrail 관리 이벤트 - 관리 이벤트를 컨트롤 플레인 이벤트라고도 하며, AWS 계정의 리소스에 대해 수행된 관리 작업을 파악할 수 있습니다.
• AWS CloudTrail S3 데이터 이벤트 - 데이터 이벤트, 또한 데이터 플레인 작업으로 알려진 데이터 이벤트를 통해 또는 리소스 내에서 수행된 리소스 작업을 파악할 수 있습니다.
• VPC FlowLog - VPC 의 Amazon EC2 네트워크 인터페이스에서 송수신되는 IP 트래픽에 대한 정보를 수집합니다.
• DNS 로그 - EC2 인스턴스에 대해 AWS DNS 해석기를 사용하는 경우 (기본 설정) 은(는) 내부 AWS DNS 해석기를 통해 요청 및 응답 DNS 로그에 액세스하고 처리할 수 있습니다.</td></tr>
<tr><td rowspan="14">세부
설명</td><td>조항</td><td>항목번호</td><td>항목</td><td colspan="2">일부내용</td></tr>
<tr><td>ISMS-P</td><td>2.6.1</td><td>네트워크 접근</td><td colspan="2" rowspan="4">DDoS, 비인가 접속 등으로 인한 서비스 중단 및 중요 정보 유출 등을 막기 위해 네트워크를 모니터링하고 통제. 내·외부에 의한 침해시도, 개인정보유출 시도, 부정행위 등을 신속하게 탐지·대응할 수 있도록 네트워크 및 데이터 흐름 등을 수집하여 분석</td></tr>
<tr><td>ISMS-P</td><td>2.10.1</td><td>보안시스템 운영</td></tr>
<tr><td>ISMS-P</td><td>2.11.3</td><td>이상행위 분석 및 모니터링</td></tr>
<tr><td>CSAP</td><td>11.1.2</td><td>네트워크 모니터링 및 통제</td></tr>
<tr><td>ISMS-P</td><td>2.9.2</td><td>성능 및 장애 관리</td><td colspan="2" rowspan="3">관련 법률에서 규정한 클라우드컴퓨팅서비스의 중단으로부터 업무 연속성을 보장하기 위해 장애 대응 절차를 마련</td></tr>
<tr><td>CSAP</td><td>6.1.1</td><td>장애 대응절차 수립</td></tr>
<tr><td>CSAP</td><td>6.1.2</td><td>장애 보고</td></tr>
<tr><td>ISMS-P</td><td>2.9.4</td><td>로그 및 접속 기록 관리</td><td colspan="2" rowspan="3">서버, 응용프로그램, 보안시스템, 네트워크시스템 등 정보시스템에 대한 사용자 접속기록, 시스템로그, 권한부여 내역 등의 로그유형, 보존기간, 보존방법 등을 정하고 위·변조, 도난, 분실 되지 않도록 안전하게 관리</td></tr>
<tr><td>ISMS-P</td><td>2.9.5</td><td>로그 및 접속 기록 점검</td></tr>
<tr><td>CSAP</td><td>13.1.3</td><td>보안로그 기능</td></tr>
<tr><td>ISMS-P</td><td>2.11.1</td><td>사고 예방 및 대응체계 구축</td><td colspan="2" rowspan="2">침해사고 발생 시 개인정보 유출 등을 예방하고 사고 발생 시 신속하고 효과적으로 대응할 수 있도록 내·외부 침해시도의 탐지·대응·분석</td></tr>
<tr><td>CSAP</td><td>5.1.2</td><td>침해사고 대응 체계 구축</td></tr>
<tr><td>ISMS-P</td><td>2.11.5</td><td>사고 대응 및 복구</td><td colspan="2" rowspan="2">침해사고 및 개인정보 유출 징후나 발생을 인지한 때에는 신속하게 대응 및 복구하고 사고 분석 후 재발방지 대책을 수립</td></tr>
<tr><td>CSAP</td><td>5.2.2</td><td>침해사고 처리 및 복구</td></tr>
</table>

<table>
<tr><td></td><td>항목 준수를 위해 정보를 수집하고 저장하기 위해 수집된 로그들을 S3 에 저장하고 정보시스템 취약점 점검을 자동으로 분석하여 결과를 보여주며 분석된 로그들을 위험도에 따라 나뉘어 분류하고 사후조치를 해야하는 항목에 대해 보여줍니다. 또한 침해시도 발생시 탐지하여 사고를 분석하고 네트워크 및 데이터 흐름 등을 수집하여 분석합니다.</td></tr>
<tr><td>설정
방법</td><td>

- **첫 설정 시작화면**



- **시작 후 수집된 결과**



※ 자세한 설명은
https://docs.aws.amazon.com/ko_kr/guardduty/latest/ug/what-is-guardduty.html 참고

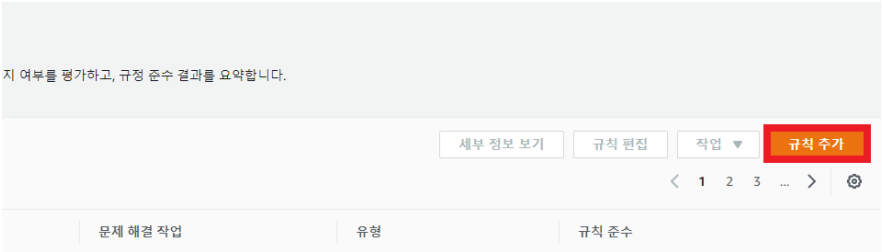
</td></tr>
<tr><td>진단
기준</td><td>

양호	GuardDuty를 설정한 경우
취약	GuardDuty를 설정하지 않은 경우

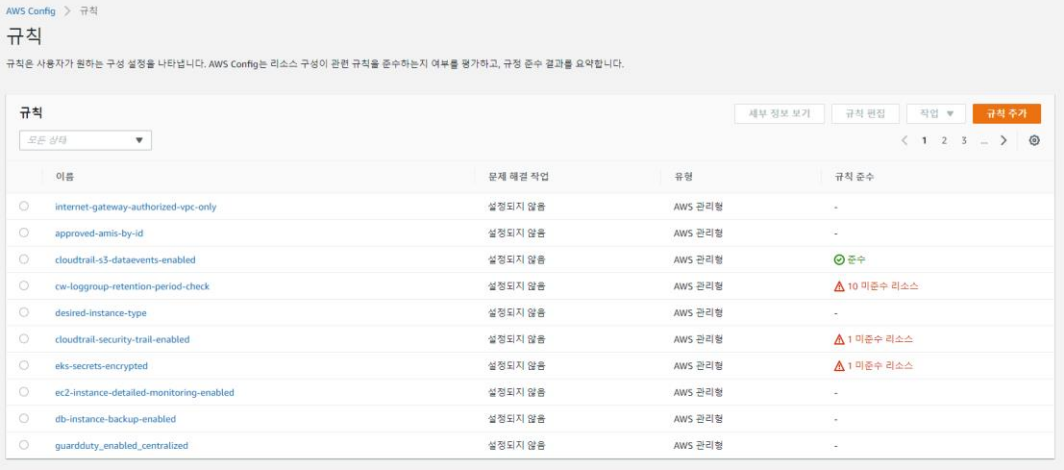
</td></tr>
<tr><td>적용
인증법</td><td>ISMS-P 2.6.1 네트워크 접근
ISMS-P 2.9.2 성능 및 장애 관리
ISMS-P 2.9.4 로그 및 접속 기록 관리
ISMS-P 2.9.5 로그 및 접속 기록 점검
ISMS-P 2.10.1 보안시스템 운영
ISMS-P 2.11.1 사고 예방 및 대응체계 구축
ISMS-P 2.11.3 이상행위 분석 및 모니터링
ISMS-P 2.11.5 사고 대응 및 복구
CSAP 5.1.2. 침해사고 대응 체계 구축
CSAP 5.2.2. 침해사고 처리 및 복구
CSAP 6.1.1. 장애 대응절차 수립
CSAP 6.1.2. 장애 보고
CSAP 11.1.2. 네트워크 모니터링 및 통제
CSAP 13.1.3. 보안로그 기능</td></tr>
</table>

<table>
<tr><td>분류</td><td colspan="2">클라우드 보안</td><td>위험도</td><td>상</td></tr>
<tr><td>항목명</td><td colspan="4">Config</td></tr>
<tr><td>항목 설명</td><td colspan="4">클라우드의 자원에 대해서 AWS 리소스의 구성을 상세하게 볼 수 있도록 합니다. 이러한 보기에는 리소스 간에 어떤 관계가 있는지와 리소스가 과거에 어떻게 구성되었는지도 포함되므로, 시간이 지나면서 구성과 관계가 어떻게 변하는지 확인할 수 있습니다.

- AWS Config 사용 방법
• 리소스 관리 - 리소스 구성을 보다 효과적으로 관리하고 리소스 구성 오류를 발견하려면, 존재하는 리소스 및 이러한 리소스의 구성 방식을 언제든 세부적으로 파악할 수 있어야 합니다.
• 감사, 보안 및 규정 준수 - 내부 정책 및 모범 사례를 준수하는지 확인하기 위해 감사가 자주 필요한 데이터를 작업할 수 있습니다. 보안 및 규정 준수를 입증하려면 리소스의 기록 구성에 액세스해야 합니다. 이 정보는 AWS Config 에서 제공합니다.
• 구성 변경 관리 및 문제 해결 – 서로 의존 관계에 있는 AWS 리소스를 여러 개 사용하는 경우, 한 리소스의 구성 변경으로 인해 관련 리소스에 의도하지 않은 결과가 발생할 수 있습니다. AWS Config 란 수정하고자 하는 리소스가 다른 리소스와 어떤 관계에 있는지 보고, 변경 영향을 평가할 수 있습니다.
• 보안 분석 - 잠재적 보안 취약성을 분석하려면 사용자에게 부여된 AWS ID 및 액세스 관리 (IAM) 권한 또는 리소스에 대한 액세스를 제어하는 Amazon EC2 보안 그룹 규칙 등 AWS 리소스 구성에 대한 세부 기록 정보가 필요합니다.</td></tr>
<tr><td rowspan="13">세부 설명</td><td>조항</td><td>항목번호</td><td>항목</td><td>일부내용</td></tr>
<tr><td>ISMS-P</td><td>1.4.1</td><td>법적 요구사항 준수 검토</td><td>조직이 준수하여야 할 정보보호 및 개인정보보호 관련 법적 요구사항을 주기적으로 파악하여 규정에 반영하고, 준수 여부를 지속적으로 검토</td></tr>
<tr><td>ISMS-P</td><td>2.11.2</td><td>취약점 점검 및 조치</td><td>정기적으로 취약점 점검을 수행하고 발견된 취약점에 대해서는 신속하게 조치</td></tr>
<tr><td>ISMS-P</td><td>2.5.3</td><td>사용자관리</td><td rowspan="3">클라우드 시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제</td></tr>
<tr><td>ISMS-P</td><td>2.10.2</td><td>클라우드 보안</td></tr>
<tr><td>CSAP</td><td>10.3.2</td><td>사용자 인증</td></tr>
<tr><td>ISMS-P</td><td>2.5.4</td><td>비밀번호관리</td><td rowspan="2">사용자 패스워드 관리절차를 수립·이행하고 패스워드 관리 책임이 사용자에게 있음을 주의시켜야 함. 특히 관리자 패스워드는 별도 보호대책을 수립하여 관리</td></tr>
<tr><td>CSAP</td><td>10.3.4</td><td>사용자 패스워드 관리</td></tr>
<tr><td>ISMS-P</td><td>2.6.1</td><td>네트워크 접근</td><td rowspan="4">DDoS, 비인가 접속 등으로 인한 서비스 중단 및 중요 정보 유출 등을 막기 위해 네트워크를 모니터링하고 통제. 내·외부에 의한 침해시도, 개인정보유출 시도, 부정행위 등을 신속하게 탐지·대응할 수 있도록 네트워크 및 데이터 흐름 등을 수집하여 분석하며, 모니터링 및 점검 결과에 따른 사후 조치는 적시에 이루어져야 함</td></tr>
<tr><td>ISMS-P</td><td>2.10.1</td><td>보안시스템 운영</td></tr>
<tr><td>ISMS-P</td><td>2.11.3</td><td>이상행위 분석 및 모니터링</td></tr>
<tr><td>CSAP</td><td>11.1.2</td><td>네트워크 모니터링 및 통제</td></tr>
</table>

<table>
<tr><td rowspan="15"></td><td>ISMS-P</td><td>2.7.1</td><td>암호정책 적용</td><td rowspan="2">클라우드컴퓨팅서비스에 저장 또는 전송 중인 데이터를 보호하기 위해 암호화 대상, 암호 강도, 키 관리, 암호 사용에 대한 정책을 마련</td></tr>
<tr><td>CSAP</td><td>12.2.1</td><td>암호정책 수립</td></tr>
<tr><td>ISMS-P</td><td>2.8.1</td><td>보안 요구사항 정의</td><td rowspan="2">신규 시스템 개발 및 기존 시스템 변경 시 정보보호 관련 법적 요구사항, 최신 보안취약점, 정보보호 기본요소 등을 고려하여 보안요구사항을 명확히 정의하고 이를 적용</td></tr>
<tr><td>CSAP</td><td>13.1.1</td><td>보안 요구사항 정의</td></tr>
<tr><td>ISMS-P</td><td>2.8.2</td><td>보안 요구사항 검토 및 시험</td><td rowspan="2">안전한 코딩방법에 따라 클라우드컴퓨팅서비스를 구현하고, 분석 및 설계 과정에서 도출한 보안요구사항이 정보시스템에 적용되었는지 확인하기 위하여 시험을 수행</td></tr>
<tr><td>CSAP</td><td>13.2.1</td><td>구현 및 시험</td></tr>
<tr><td>ISMS-P</td><td>2.9.2</td><td>성능 및 장애 관리</td><td rowspan="2">장애 관련 정보를 활용하여 유사한 서비스 중단이 반복되지 않도록 장애 재발방지 대책을 수립하고, 필요한 경우 장애 대응 절차도 변경</td></tr>
<tr><td>CSAP</td><td>6.1.4</td><td>재발방지</td></tr>
<tr><td>ISMS-P</td><td>2.9.3</td><td>백업 및 복구 관리</td><td rowspan="3">보안감사 증적(로그)은 식별할 수 있는 형태로 기록 및 모니터링 되어야 되고 비인가된 접근 및 변조로부터 보호</td></tr>
<tr><td>ISMS-P</td><td>2.9.4</td><td>로그 및 접속 기록 관리</td></tr>
<tr><td>CSAP</td><td>7.2.2.</td><td>감사기록 및 모니터링</td></tr>
<tr><td>ISMS-P</td><td>2.9.4</td><td>로그 및 접속 기록 관리</td><td rowspan="3">서버, 응용프로그램, 보안시스템, 네트워크시스템 등 정보시스템에 대한 사용자 접속기록, 시스템로그, 권한부여 내역 등의 로그유형, 보존기간, 보존방법 등을 정하고 위·변조, 도난, 분실 되지 않도록 안전하게 보존·관리</td></tr>
<tr><td>ISMS-P</td><td>2.9.5</td><td>로그 및 접속 기록 점검</td></tr>
<tr><td>CSAP</td><td>13.1.3</td><td>보안로그 기능</td></tr>
<tr><td>CSAP</td><td>7.1.1</td><td>법적요구사항 준수</td><td>정보보호 관련 법적 요구사항을 식별하고 준수</td></tr>
<tr><td>CSAP</td><td>7.2.1</td><td>독립적 보안감사</td><td>법적 요구사항 및 정보보호 정책 준수 여부를 보증하기 위해 독립적 보안감사 계획을 수립하여 시행하고 개선</td></tr>
<tr><td colspan="4">항목 준수를 위해 config규칙을 통해 준수할 항목에 대해 분석하고 미준수 규칙과 리소스를 보여줌으로써 정보자산을 식별하고 자산의 변경내역을 알려줍니다. 또한 암호화와 암호 대상에 대한 정책을 마련하고 보안요구사항이 정보시스템에 적용되었는지 검사를 수행하여 결과를 보여주고 장애 관련 정보를 활용하여 장애 재발방지대책을 수립하고 대응절차를 알려줍니다. 그리고 법적 요구사항 및 정보보호 정책 준수 여부를 확인하기 위해 독립적 보안감사 계획을 수립하여 수행합니다.</td></tr>
<tr><td>설정 방법</td><td colspan="4">- config 설정 방법
config 대시보드 → 규칙 → 규칙 추가 → 완료
 

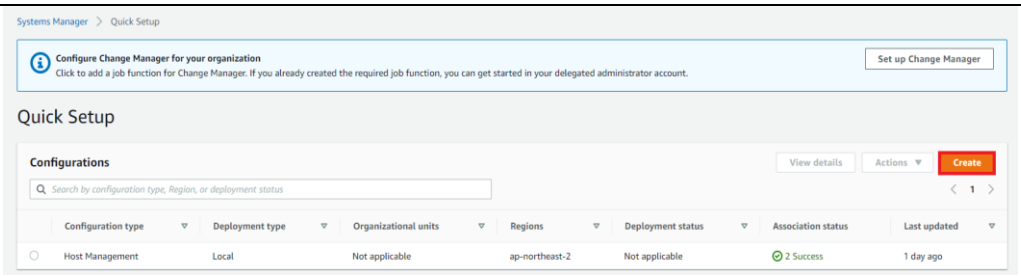
- config 예시</td></tr>
</table>

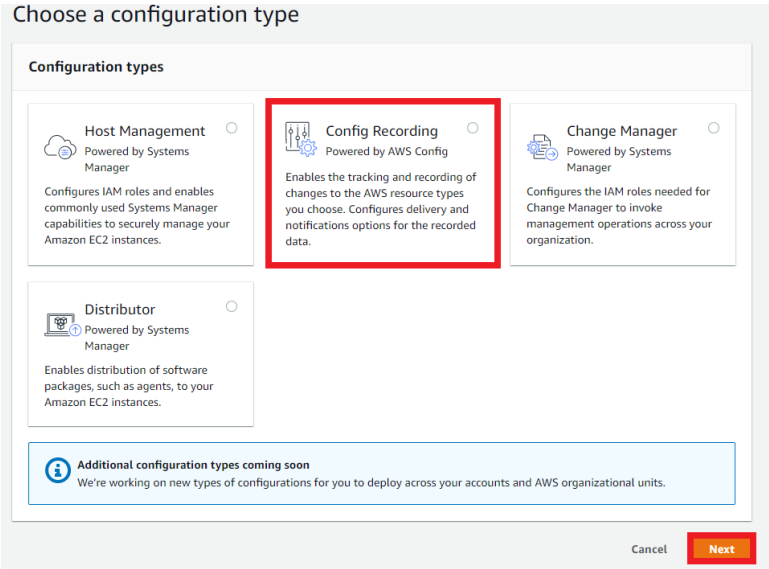
<table>
<tr><td></td><td>


※ 자세한 설명은
https://docs.aws.amazon.com/ko_kr/config/latest/developerguide/WhatIsConfig.html 참고
</td></tr>
<tr><td rowspan="2">진단 기준</td><td>양호</td><td>준수할 사항에 대해 config를 설정한 경우</td></tr>
<tr><td>취약</td><td>준수할 사항에 대해 config를 설정하지 않은 경우</td></tr>
<tr><td>적용 인증법</td><td colspan="2">ISMS-P 1.2.1 정보자산 식별
ISMS-P 2.1.3 정보자산 관리
ISMS-P 2.5.3 사용자관리
ISMS-P 2.5.4 비밀번호관리
ISMS-P 2.7.1 암호정책 적용
ISMS-P 2.8.1 보안 요구사항 정의
ISMS-P 2.8.2 보안 요구사항 검토 및 시험
ISMS-P 2.9.1 변경관리
ISMS-P 2.9.2 성능 및 장애 관리
ISMS-P 2.9.4 로그 및 접속 기록 관리
ISMS-P 2.10.2 클라우드 보안
ISMS-P 2.11.2 취약점 점검 및 조치
CSAP 4.1.1 공급망 관리 정책 수립
CSAP 6.1.4 재발방지
CSAP 7.1.1 법적요구사항 준수
CSAP 7.2.1 독립적 보안감사
CSAP 7.2.2 감사기록 및 모니터링
CSAP 10.3.2 사용자 인증
CSAP 10.3.4 사용자 패스워드 관리
CSAP 12.2.1 암호 정책 수립
CSAP 13.1.1 보안요구사항 정의
CSAP 13.1.3 보안로그 기능
CSAP 13.2.1 구현 및 시험</td></tr>
</table>

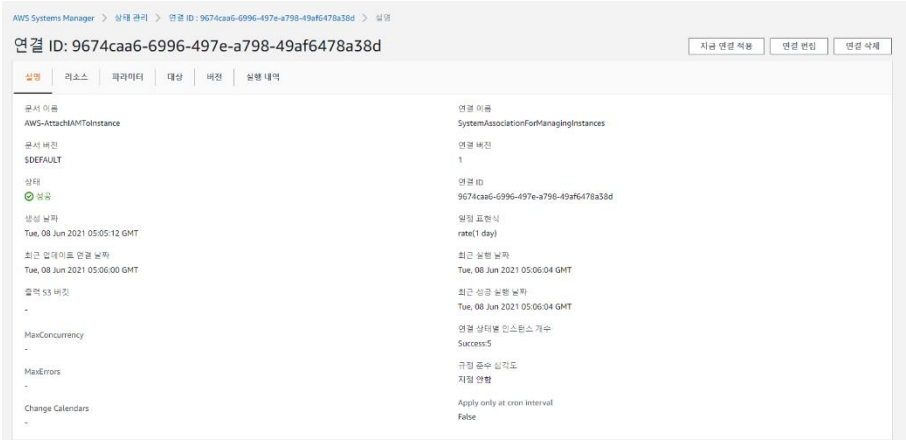
<table>
<tr><td>분류</td><td colspan="3">클라우드 보안</td><td>위험도</td><td>상</td></tr>
<tr><td>항목명</td><td colspan="5">Systems Manager</td></tr>
<tr><td>항목
설명</td><td colspan="5">클라우드에서 사용될 리소스를 관리하고 제어하기위해 사용되는 서비스입니다. Systems Manager 를 사용하면 보안 및 규정 준수를 유지 관리할 수 있습니다.

- Systems Manager 기능
• 애플리케이션, 환경, 리전, 프로젝트, 캠페인, 사업부 또는 소프트웨어 수명 주기 등 선택한 목적 또는 활동에 따라 AWS 리소스를 그룹화합니다.
• 관리형 인스턴스를 위한 구성 옵션 및 정책을 중앙 집중식으로 정의합니다.
• AWS 리소스와 관련된 운영 작업 항목을 중앙에서 보고 조사하고 해결합니다.
• 다양한 유지 관리 및 배포 작업을 자동화하거나 예약합니다.</td></tr>
<tr><td rowspan="11">세부
설명</td><td>조항</td><td>항목번호</td><td>항목</td><td colspan="2">일부내용</td></tr>
<tr><td>ISMS-P</td><td>1.4.1</td><td>법적 요구사항 준수 검토</td><td colspan="2">법적 요구사항을 파악하여 규정에 반영</td></tr>
<tr><td>ISMS-P</td><td>2.6.1</td><td>네트워크 접근</td><td colspan="2">네트워크에 대한 비인가 접근을 통제하기 위하여 IP관리, 단말인증 등 관리절차를 수립·이행</td></tr>
<tr><td>ISMS-P</td><td>2.8.1</td><td>보안 요구사항 정의</td><td colspan="2">정보보호 및 개인정보보호 관련 법적 요구사항을 정의하고 적용</td></tr>
<tr><td>ISMS-P</td><td>2.10.1</td><td>보안시스템 운영</td><td colspan="2">보안시스템 유형별로 최신 정책 업데이트, 룰셋 변경 등의 운영절차를 수립·이행하고 보안시스템별 정책적용 현황을 관리</td></tr>
<tr><td>ISMS-P</td><td>2.11.2</td><td>취약점 점검 및 조치</td><td colspan="2">취약점이 노출되어 있는지를 확인하기 위하여 취약점 점검을 수행</td></tr>
<tr><td>ISMS-P</td><td>2.11.3</td><td>이상행위 분석 및 모니터링</td><td colspan="2">내·외부에 의한 침해시도를 탐지·대응할 수 있도록 모니터링 및 점검</td></tr>
<tr><td>CSAP</td><td>12.1.5</td><td>데이터 추적성</td><td colspan="2">이용자에게 데이터를 추적하기 위한 방안을 제공하고, 이용자가 요구하는 경우 구체적인 제공정보를 공개</td></tr>
<tr><td>CSAP</td><td>13.1.1</td><td>보안요구사항 정의</td><td colspan="2">신규 시스템 개발 및 기존 시스템 변경 시 정보보호 관련 법적 요구사항, 최신 보안취약점, 정보보호 기본요소들을 고려하여 보안요구사항을 명확히 정의</td></tr>
<tr><td colspan="5">항목준수를 위해 어플리케이션을 검색하고, 운영데이터를 보고 수정작업이 가능하며 보안과 규정준수 유지를 위해 패치기준선을 정의하고 데이터를 대시보드를 통해 모니터링합니다. 또한 취약점노출이 되었는지 확인하며 보안요구사항을 명확히 정의하여 비인가 접근에 대한 통제를 합니다.</td></tr>
<tr><td>설정
방법</td><td colspan="5">- Systems Manager 규정준수 설정
Systems Manager 대시보드 → 빠른 설정 → 만들기(create) → Config Recording → 완료</td></tr>
</table>





- Systems Manager 예시



※ 자세한 설명은
https://docs.aws.amazon.com/ko_kr/systems-manager/latest/userguide/what-is-systems-manager.html참고

진단 기준	양호	Systems manager를 통한 config 규정준수를 실행한 경우
	취약	Systems manager를 통한 config 규정준수를 실행하지 않은 경우
적용 인증법	ISMS-P 1.4.1 법적 요구사항 준수 검토 ISMS-P 2.6.1 네트워크 접근 ISMS-P 2.8.1 보안 요구사항 정의	

	ISMS-P 2.10.1 보안시스템 운영 ISMS-P 2.11.2 취약점 점검 및 조치 ISMS-P 2.11.3 이상행위 분석 및 모니터링 CSAP 12.1.5 데이터 추적성 CSAP 13.1.1 보안요구사항 정의

2. 네트워크 보안

<table>
<tr><td>분류</td><td colspan="3">네트워크 보안</td><td>위험도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="5">Security Group</td></tr>
<tr><td>항목
설명</td><td colspan="5">

- 기능

- VPC에서의 Security Group은 EC2 인스턴스에 대한 인/아웃바운드 트래픽을 제어하는 가상 방화벽 역할을 합니다. VPC에서 EC2 인스턴스를 시작할 때 최대 5개의 Security Group에 인스턴스를 할당할 수 있습니다. Security Group은 서브넷 수준이 아니라 인스턴스 수준에서 작동하므로 VPC에 있는 서브넷의 각 인스턴스를 서로 다른 Security Group 세트에 할당할 수 있습니다.
- Security Group 은 인/아웃바운드의 규칙 편집을 통해 특정 소스(출발지)에서의 통신이 가능하도록 유형(네트워크 프로토콜) 및 단일/범위 Port 를 설정할 수 있습니다.

- 규칙

- **VPC Security Group 생성 시 Default 규칙**
  - 인바운드 : 모든 프로토콜, 포트에 대해 동일한 Security Group 에 지정된 EC2 인스턴스 간의 통신을 허용함
  - 아웃바운드 : Security Group 에 지정된 EC2 인스턴스에서 외부로의 IPv4, IPv6 트래픽을 허용함
- **Security Group 규칙** - 보안 그룹의 규칙을 추가하거나 제거할 수 있습니다. 규칙은 인바운드 트래픽(수신)이나 아웃바운드 트래픽(송신)에 적용되며, 특정 CIDR 범위 또는 VPC 나 피어 VPC(VPC 피어링 연결 필요)의 다른 보안 그룹에 대한 액세스 권한을 부여할 수 있습니다. 추가하는 규칙의 종류는 인스턴스의 용도에 따라 다를 수 있습니다.

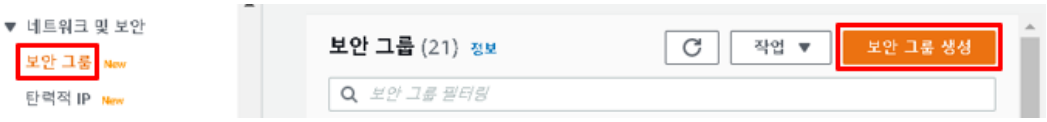
</td></tr>
<tr><td>세부
설명</td><td colspan="5">
<table>
<tr><th>조항</th><th>항목번호</th><th>항목</th><th>일부내용</th></tr>
<tr><td>ISMS-P</td><td>2.6.1</td><td>네트워크 접근</td><td>네트워크에 대한 비인가 접근을 통제하기 위하여 IP관리등 관리절차를 수립·이행하고, 업무목적 및 중요도에 따라 네트워크 분리와 접근통제를 적용</td></tr>
<tr><td>ISMS-P</td><td>2.6.2</td><td>정보시스템 접근</td><td>서버, 네트워크시스템 등 정보시스템에 접근을 허용하는 사용자, 접근제한 방식 정의하여 통제</td></tr>
<tr><td>ISMS-P</td><td>2.6.4</td><td>데이터베이스 접근</td><td>데이터베이스의 접근통제 정책을 수립</td></tr>
<tr><td>ISMS-P</td><td>2.10.1</td><td>보안시스템 운영</td><td>보안시스템 유형별로 룰셋 변경등의 운영절차를 수립·이행</td></tr>
<tr><td>ISMS-P</td><td>2.10.2</td><td>클라우드 보안</td><td>비인가 접근등에 대한 보호대책을 수립</td></tr>
<tr><td>ISMS-P</td><td>2.10.3</td><td rowspan="2">공개서버 보안</td><td rowspan="2">외부 네트워크에 공개되는 서버의 경우 내부 네트워크와 분리하고 접근통제 등 보호대책을 수립·이행</td></tr>
<tr><td>CSAP</td><td>9.1.5</td></tr>
<tr><td>CSAP</td><td>10.1.1</td><td>접근통제 정책 수립</td><td>비인가자의 접근을 통제, 접근통제 영역 및 범위, 접근통제 규칙, 접근통제 정책을 수립</td></tr>
</table>
</td></tr>
</table>

	CSAP	11.1.1	네트워크 보안 정책 수립	클라우드컴퓨팅서비스와 관련된 내·외부 네트워크에 대해 룰셋 변경등의 운영절차를 수립·이행
	CSAP	11.1.2	네트워크 모니터링 및 통제	DDoS, 비인가 접속 등으로 인한 서비스 중단 및 중요 정보 유출 등을 막기 위해 네트워크를 통제
	CSAP	11.1.3	네트워크 정보보호시스템 운영	클라우드컴퓨팅서비스와 관련된 내·외부 네트워크를 보호하기 위하여 정보보호시스템을 운영
	CSAP	11.1.5	네트워크 분리	클라우드컴퓨팅서비스 제공자의 관리 영역과 이용자의 서비스 영역, 이용자 간 서비스 영역의 네트워크 접근은 물리적 또는 논리적으로 분리
	CSAP	12.1.4	데이터 보호	데이터에 대한 접근제어, 위·변조 방지 등 데이터 처리에 대한 보호 기능을 이용자에게 제공
	CSAP	13.2.2	개발과 운영환경 분리	개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소하기 위해 원칙적으로 분리
	CSAP	13.2.4	소스 프로그램 보안	소스 프로그램에 대한 인가된 사용자만이 소스 프로그램에 접근할 수 있도록 통제절차를 수립하여 이행
	항목 준수를 위해 각 보안 그룹에 대해 인바운드 및 아웃바운드 트래픽을 제어하는 규칙을 설정하여 비인가 접근을 차단하고 서비스 영역의 네트워크 접근을 논리적으로 분리하는식으로 네트워크를 통제합니다.			

설정 방법

- 보안 그룹 생성

EC2 → 보안 그룹 → 보안 그룹 생성



- 보안 그룹 삭제

EC2 → 보안 그룹 → 삭제하려는 보안 그룹 선택 → 작업 → 보안 그룹삭제

- 보안 그룹 예시

<table>
<tr><td></td><td colspan="2">

※ 자세한 설명은 https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/VPC_SecurityGroups.html#CreatingSecurityGroups 참고</td></tr>
<tr><td rowspan="2">진단 기준</td><td>양호</td><td>1) EC2 인스턴스에 대한 인/아웃바운드의 Port가 Any로 허용되어 있지 않을 경우
2) EC2 인스턴스에 대한 인/아웃바운드 소스와 목적지의 설정 규칙이 Any로 허용되어 있지 않을 경우</td></tr>
<tr><td>취약</td><td>1) EC2 인스턴스에 대한 인/아웃바운드의 Port가 Any로 허용되어 있을 경우
2) EC2 인스턴스에 대한 인/아웃바운드 소스와 목적지의 설정 규칙이 Any로 허용되어 있을 경우</td></tr>
<tr><td>적용 인증법</td><td colspan="2">ISMS-P 2.6.1 네트워크 접근
ISMS-P 2.6.2 정보시스템 접근
ISMS-P 2.6.4 데이터베이스 접근
ISMS-P 2.10.1 보안시스템 운영
ISMS-P 2.10.2 클라우드 보안
ISMS-P 2.10.3 공개서버 보안
CSAP 9.1.5. 공개서버 보안
CSAP 10.1.1. 접근통제 정책 수립
CSAP 11.1.1. 네트워크 보안 정책 수립
CSAP 11.1.2. 네트워크 모니터링 및 통제
CSAP 11.1.3. 네트워크 정보보호시스템 운영
CSAP 11.1.5. 네트워크 분리
CSAP 12.1.4. 데이터 보호
CSAP 13.1.4. 접근권한 기능
CSAP 13.2.2. 개발과 운영환경 분리
CSAP 13.2.4. 소스 프로그램 보안</td></tr>
</table>

<table>
<tr><td>분류</td><td>네트워크 보안</td><td>위험도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">네트워크 ACL</td></tr>
<tr><td>항목
설명</td><td colspan="3">

- **기능**
  - ACL(Access Control List)은 1 개 이상의 서브넷 내부와 외부의 트래픽을 제어하기 위한 방화벽 역할을 하는 VPC 의 선택적 보안 계층입니다. 보안 그룹과 비슷한 규칙으로 네트워크 ACL 을 설정하여 VPC 에 보안 계층을 더 추가할 수 있습니다. ACL 은 VPC 서브넷 계층에서 동작하며 VPC 서브넷과는 1:1 로 대응합니다. 정책의 방식은 허용(Allow) 및 거부(Deny) 정책(화이트 및 블랙리스트) 기능으로 Stateless 방식이 사용됩니다.
  - VPC 에 있는 각 서브넷을 네트워크 ACL 과 연결하여 사용할 수 있으며, 서브넷을 네트워크 ACL 에 명시적으로 연결하지 않을 경우, 서브넷은 기본 네트워크 ACL 에 자동적으로 연결합니다. (단, 하나의 네트워크 ACL 은 다수의 서브넷과 연결할 수 있지만 하나의 서브넷 은 하나의 ACL 에만 연결할 수 있음)

- **규칙**
  - **기본 네트워크 ACL 규칙** - 기본 네트워크 ACL 은 연결된 서브넷을 드나드는 트래픽 흐름을 모두 허용하도록 구성되어 있습니다. 각 네트워크 ACL 에는 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.

</td></tr>
<tr><td>세부
설명</td><td colspan="3">
<table>
<tr><th>조항</th><th>항목번호</th><th>항목</th><th>일부내용</th></tr>
<tr><td>ISMS-P</td><td>2.6.1</td><td>네트워크 접근</td><td>네트워크에 대한 비인가 접근 통제</td></tr>
<tr><td>ISMS-P</td><td>2.6.2</td><td>정보시스템 접근</td><td>서버, 네트워크시스템 등 정보시스템에 접근을 허용하는 사용자, 접근제한 방식, 안전한 접근수단 등을 정의하여 통제</td></tr>
<tr><td>ISMS-P</td><td>2.6.4</td><td>데이터베이스 접근</td><td>데이터베이스의 접근통제 정책을 수립</td></tr>
<tr><td>ISMS-P</td><td>2.6.7</td><td>인터넷 접속 통제</td><td>인터넷 접속 통제 정책을 수립</td></tr>
<tr><td>ISMS-P</td><td>2.8.3</td><td>시험과 운영 환경 분리</td><td>개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 원칙적으로 분리</td></tr>
<tr><td>ISMS-P</td><td>2.10.2</td><td>클라우드 보안</td><td>관리자 접근 및 보안 설정 등에 대한 보호대책 수립</td></tr>
<tr><td>ISMS-P</td><td>2.10.3</td><td rowspan="2">공개서버 보안</td><td rowspan="2">외부 네트워크에 공개되는 서버의 경우 접근통제등 강화된 보호대책을 수립</td></tr>
<tr><td>CSAP</td><td>9.1.5</td></tr>
<tr><td>CSAP</td><td>10.1.1</td><td>접근통제 정책 수립</td><td>비인가자의 접근을 통제할 수 있도록 접근통제 영역 및 범위, 접근통제 규칙, 방법 등을 포함하여 접근통제 정책을 수립하여야 한다.</td></tr>
<tr><td>CSAP</td><td>11.1.2</td><td>네트워크 모니터링 및 통제</td><td>DDoS, 비인가 접속 등으로 인한 서비스 중단 및 중요 정보 유출 등을 막기 위해 통제</td></tr>
<tr><td>CSAP</td><td>11.1.3</td><td>네트워크 정보보호 시스템 운영</td><td>클라우드컴퓨팅서비스와 관련된 내·외부 네트워크를 보호하기 위하여 정보보호시스템(방화벽, IPS, IDS, VPN 등)을 운영하여야 한다.</td></tr>
</table>
</td></tr>
</table>

	CSAP	13.2.2	개발과 운영환경 분리	개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소하기 위해 원칙적으로 분리
	항목 준수를 위해 보안 그룹과 비슷한 규칙으로 각각의 서브넷 내부와 외부의 트래픽 제어하는 네트워크 ACL 을 설정하고, RDS 관련 접근통제를 위한 네트워크 ACL 을 설정하여 비인가자의 접근을 통제하며 중요정보 노출을 막는 역할을 합니다.			

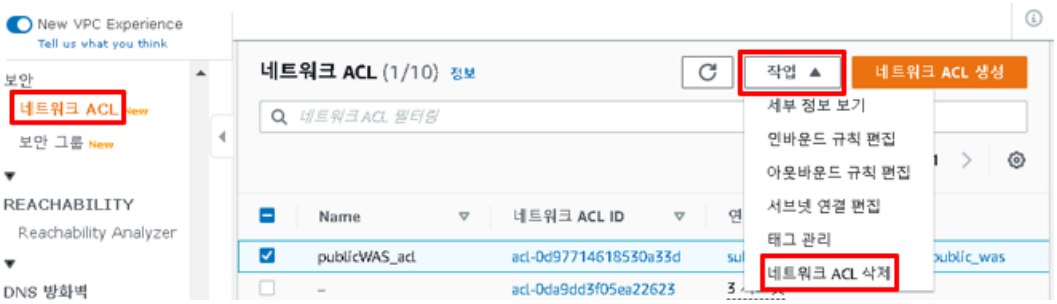
설정 방법

- Network ACL 생성

VPC → 네트워크 ACL → 네트워크 ACL 생성

- Network ACL 삭제

VPC → 네트워크 ACL → 삭제하려는 네트워크 ACL 선택 → 작업 → 네트워크 ACL 삭제



- Network ACL 예시

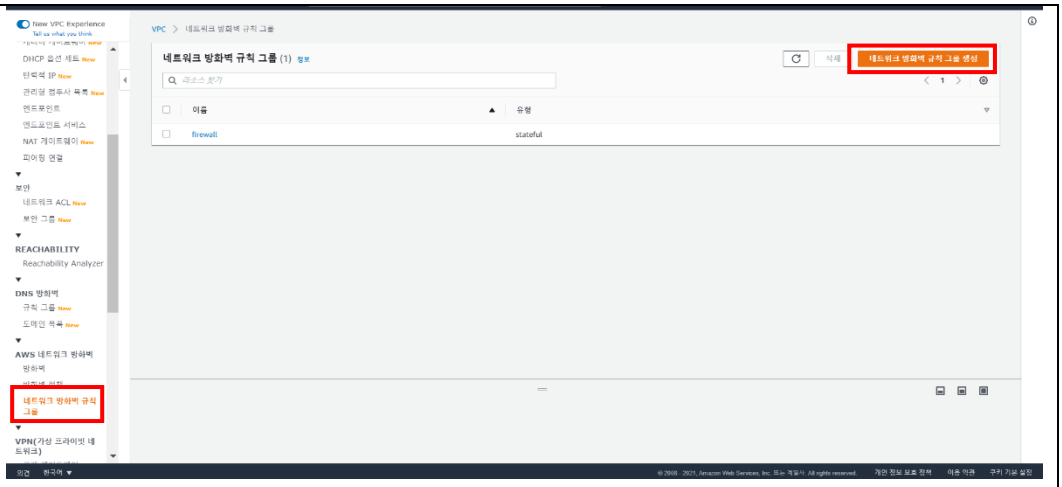
※ 자세한 설명은

https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/vpc-network-acls.html 참고

진단 기준	양호	인/아웃바운드에 대한 모든 트래픽이 허용되어 있지 않을 경우
	취약	인/아웃바운드에 대한 모든 트래픽이 허용되어 있을 경우
적용 인증법	ISMS-P 2.6.1 네트워크 접근 ISMS-P 2.6.2 정보시스템 접근 ISMS-P 2.6.4 데이터베이스 접근 ISMS-P 2.6.7 인터넷 접속 통제 ISMS-P 2.8.3 시험과 운영 환경 분리 ISMS-P 2.10.1 보안시스템 운영 ISMS-P 2.10.2 클라우드 보안 ISMS-P 2.10.3 공개서버 보안 ISMS-P 2.11.3 이상행위 분석 및 모니터링 CSAP 9.1.5 공개서버 보안 CSAP 10.1.1 접근통제 정책 수립 CSAP 11.1.2 네트워크 모니터링 및 통제 CSAP 11.1.3 네트워크 정보보호시스템 운영 CSAP 13.2.2 개발과 운영환경 분리	

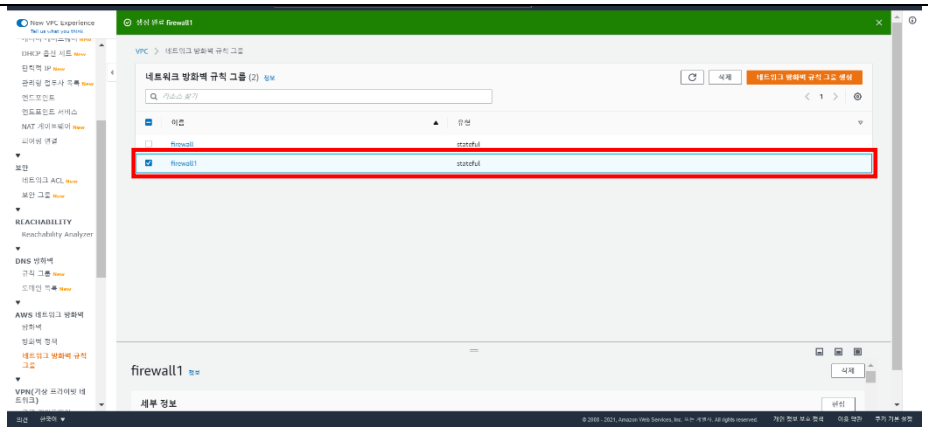
<table>
<tr><td>분류</td><td colspan="2">네트워크 보안</td><td>위험도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="4">Network firewall</td></tr>
<tr><td>항목 설명</td><td colspan="4">AWS Network Firewall은 일반적인 네트워크 위협에 대한 보호 기능을 포함하고 있습니다. AWS Network Firewall의 상태 기반 방화벽은 트래픽 흐름에 연결 추적 및 프로토콜 식별과 같은 컨텍스트를 통합하여 VPC가 승인되지 않은 프로토콜을 사용하여 도메인에 액세스하는 것을 방지하는 등의 정책을 적용할 수 있습니다. AWS Network Firewall의 IPS(침입 방지 시스템)는 취약성 공격을 식별 및 차단할 수 있도록 서명 기반 탐지에 기반한 능동적인 트래픽 흐름 검사를 제공합니다. 또한 AWS Network Firewall은 알려진 악성 URL에 대한 트래픽을 중지시키고 정규화된 도메인 이름을 모니터링할 수 있는 웹 필터링을 제공합니다.

- 구성
• 방화벽 - 방화벽은 방화벽 정책의 네트워크 트래픽 필터링 동작을 보호하려는 VPC에 연결합니다. 방화벽 구성에는 방화벽 엔드포인트가 배치되는 가용 영역 및 서브넷에 대한 사양이 포함됩니다. 또한 AWS 방화벽 리소스의 방화벽 로깅 구성 및 태그 지정과 같은 상위 수준 설정을 정의합니다.
• 방화벽 정책 - 방화벽 정책은 방화벽에 대한 모니터링 및 보호 동작을 정의합니다. 동작의 세부 정보는 정책에 추가하는 규칙 그룹과 일부 정책 기본 설정에 정의됩니다. 방화벽 정책을 사용하려면 하나 이상의 방화벽과 연결합니다.
• 규칙 그룹 - 규칙 그룹은 네트워크 트래픽을 검사하고 처리하기 위한 재사용 가능한 기준 세트입니다. 정책 구성의 일부로 방화벽 정책에 하나 이상의 규칙 그룹을 추가합니다. 상태 비저장 규칙 그룹을 정의하여 각 네트워크 패킷을 격리 상태에서 검사할 수 있습니다. 상태 비저장 규칙 그룹은 Amazon VPC 네트워크 액세스 제어 목록(ACL)과 동작 및 사용법이 유사합니다. 상태 저장 규칙 그룹을 정의하여 트래픽 흐름의 컨텍스트에서 패킷을 검사할 수도 있습니다. 상태 저장 규칙 그룹은 Amazon VPC 보안 그룹과 동작 및 사용법이 유사합니다.</td></tr>
<tr><td rowspan="6">세부 설명</td><td>조항</td><td>항목번호</td><td>항목</td><td>일부내용</td></tr>
<tr><td>ISMS-P</td><td>2.6.2</td><td>정보시스템 접근</td><td>서버, 네트워크시스템 등 정보시스템에 접근을 허용하는 사용자, 안전한 접근수단 등을 정의하여 통제</td></tr>
<tr><td>ISMS-P</td><td>2.10.3</td><td rowspan="2">공개서버 보안</td><td rowspan="2">외부 네트워크에 공개되는 서버의 경우 내부 네트워크와 분리하고 접근통제 , 인증 강화된 보호대책을 수립, 이행</td></tr>
<tr><td>CSAP</td><td>9.1.5</td></tr>
<tr><td>CSAP</td><td>9.2.1</td><td>악성코드 통제</td><td>가상환경을 보호하기 위한 보안기술을 지원, 이상 징후 발견시 이용자 통지하고 격리조치 수행</td></tr>
<tr><td>CSAP</td><td>11.1.3</td><td>네트워크 정보보호시스템 운영</td><td>클라우드컴퓨팅서비스와 관련된 내외부 네트워크를 보호하기 위하여 정보보호시스템을 운영하여야한다.</td></tr>
<tr><td colspan="4">항목 준수를 위해 사용자가 웹서버에 접속할 때 VPC 경계에서 Network firewall을 사용하여 네트워크 트래픽을 필터링하고 악성 IP 주소를 차단하거나 시그니처 기반 탐지를 사용하여 악의적인 활동을 식별할 수 있으며 이상 징후 발견시 Amazon SNS를 통해 경보를 알려줍니다.</td></tr>
<tr><td>설정 방법</td><td colspan="4">VPC → AWS 네트워크 방화벽 → 네트워크 방화벽 규칙 그룹 → 네트워크 방화벽 규칙 그룹 생성</td></tr>
</table>

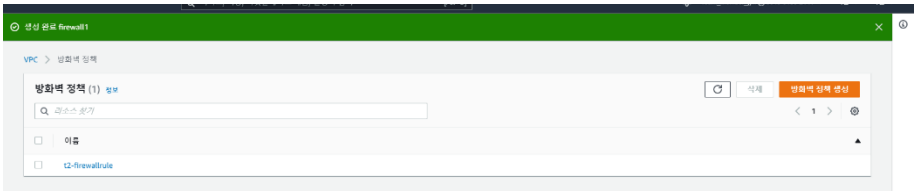


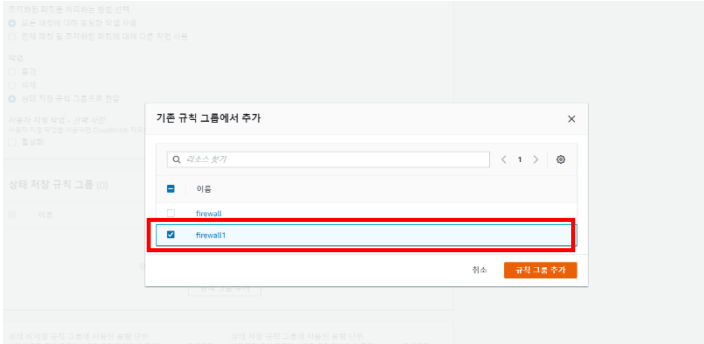
네트워크 방화벽 규칙 그룹 생성 → 규칙 추가 → 상태 저장 규칙 그룹 생성

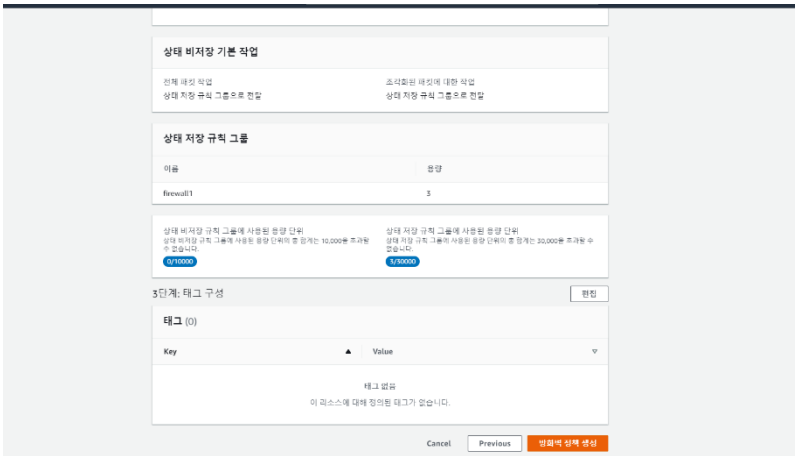
- **네트워크 방화벽 규칙 그룹 예시**



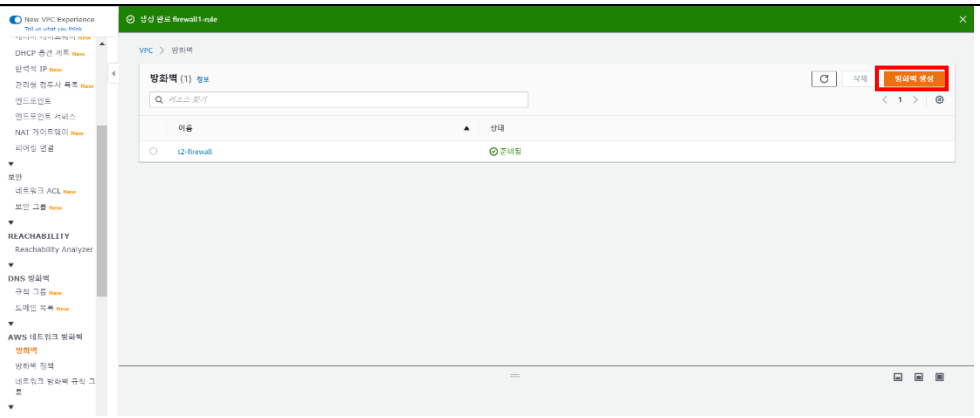
AWS 네트워크 방화벽 → 방화벽 정책 → 방화벽 정책 생성 → 전 과정에서 생성한 규칙 그룹 추가 → 방화벽 정책 생성



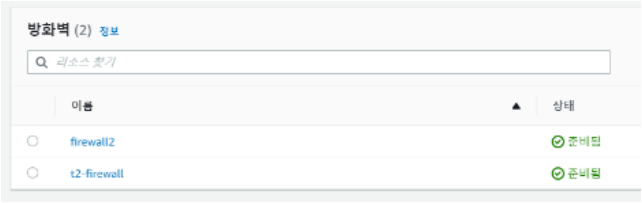




AWS 네트워크 방화벽 → 방화벽 → 방화벽 생성 → 이름, VPC, 방화벽 서브넷 선택 → 전 과정에서 생성한 방화벽 정책 선택 → 방화벽 생성

<table>
<tr><td></td><td colspan="2">


- **Network Firewall 예시**



</td></tr>
<tr><td rowspan="2">진단 기준</td><td>양호</td><td>네트워크 방화벽 규칙 그룹에서 허용한 Port 외 불필요한 Port가 Open 되어 있지 않을 경우</td></tr>
<tr><td>취약</td><td>네트워크 방화벽 규칙 그룹에서 허용한 Port 외 불필요한 Port가 Open 되어 있을 경우</td></tr>
<tr><td>적용 인증법</td><td colspan="2">ISMS-P 2.6.2 정보시스템 접근
ISMS-P 2.10.3 공개서버 보안
CSAP 9.1.5 공개서버 보안
CSAP 9.2.1 악성코드 통제
CSAP 11.1.3 네트워크 정보보호시스템 운영</td></tr>
</table>

분류	네트워크 보안	위험도	하
항목명	NAT Gateway		

항목 설명

헬스케어 데이터에 접근하려는 이용자들이 Internet Gateway를 통해 클라우드에 접근하게 되면 DMZ를 통해 들어오게 되고 Web server에 접근하기 전 외부인터넷에서 사용되는 공인 IP에서 VPC에서 사용되는 사설 IP로 변환시킵니다.

- 규칙 및 제한

- 하나의 탄력적 IP주소(Elastic IP)에 하나의 NAT Gateway를 연결할 수 있으며 연결된 후에는 NAT Gateway에서 탄력적 IP주소의 연결을 끊을 수 없습니다.
- NAT 게이트웨이는 TCP, UDP, ICMP 등의 프로토콜을 지원합니다.
- 보안 그룹을 NAT 게이트웨이와 연결할 수 없습니다. 프라이빗 서브넷의 인스턴스에 대한 보안 그룹을 사용하여 해당 인스턴스에서 주고받는 트래픽을 제어할 수 있습니다.
- 네트워크 ACL 을 사용하여 NAT 게이트웨이가 위치하고 있는 서브넷에서 주고받는 트래픽을 제어할 수 있습니다. 네트워크 ACL 은 NAT 게이트웨이의 트래픽에 적용됩니다. NAT 게이트웨이는 포트 1024 - 65535 를 사용합니다.
- NAT 게이트웨이가 생성되면 서브넷의 IP 주소 범위에 속하는 프라이빗 IP 주소가 자동으로 할당된 네트워크 인터페이스를 받습니다. Amazon EC2 콘솔에서 NAT 게이트웨이의 네트워크 인터페이스를 볼 수 있습니다.
- VPC 와 연결된 ClassicLink 연결을 통해서는 NAT 게이트웨이에 액세스할 수 없습니다.

세부 설명

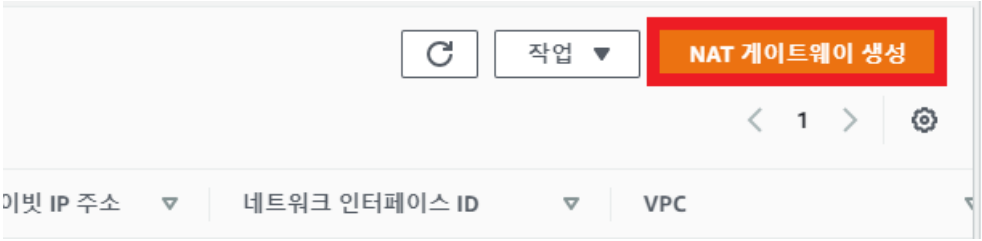
조항	항목번호	항목	일부내용
ISMS-P	2.6.2	정보시스템 접근	서버,네트워크 시스템...접근제한 방식...통제
CSAP	11.1.3	네트워크 정보보호 시스템 운영	클라우드컴퓨팅서비스와 관련된 내·외부 네트워크를 보호하기 위하여 정보보호시스템을 운영

항목 준수를 위해 외부인터넷, 외부에서의 원격접근을 할 시 NAT Gateway를 통해 퍼블릭으로 접근이 가능할 지 프라이빗으로 접근할 지를 정해 접근을 제한하고 원격접근에 대해서도 허용 범위를 정할 수 있습니다.

설정 방법

- NAT Gateway 생성 방법

VPC → NAT Gateway → NAT Gateway 선택 → 작업 → NAT Gateway 생성

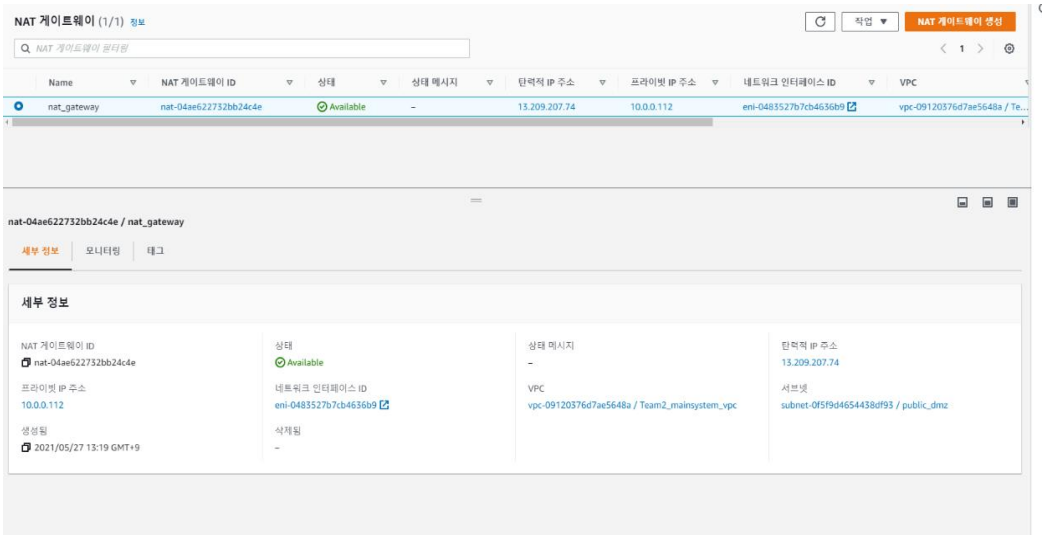


- NAT Gateway 삭제 방법

VPC → NAT Gateway → 삭제할 NAT Gateway 선택 → 작업 → NAT Gateway 삭제

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

- NAT Gateway 예시



※ 자세한 설명은
https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/vpc-nat-gateway.html#nat-gateway-working-with 참고
</td>
</tr>
<tr>
<td rowspan="2">진단 기준</td>
<td>양호</td>
<td>NAT Gateway가 설정되어 있지 않거나 사용 중인 private서브넷 인스턴스를 연결한 경우</td>
</tr>
<tr>
<td>취약</td>
<td>NAT Gateway를 사용할 때 사용하지 않는 private서브넷 인스턴스를 연결하지 않은 경우</td>
</tr>
<tr>
<td>적용 인증법</td>
<td colspan="2">ISMS-P 2.6.2 정보시스템 접근
CSAP 11.1.3 네트워크 정보보호시스템 운영</td>
</tr>
</table>

분류	네트워크 보안	위험도	중
항목명	WAF		

항목 설명

헬스케어 데이터를 조회하기위해 접근하는 이용자가 인터넷 게이트웨이를 통해 들어올 때 SQL Injection과 같은 웹 기반 공격을 차단하는 목적으로 WAF를 사용합니다.

- **구성 요소**
  - **웹 ACL -** 웹 액세스 제어 목록 (ACL) 을 사용하여 AWS 리소스 집합을 보호합니다. 규칙을 추가하여 웹 ACL 을 생성하고 보호 전략을 정의합니다. 규칙은 웹 요청을 검사하기 위한 기준을 정의하고 조건과 일치하는 요청을 처리하는 방법을 지정합니다. 규칙 검사를 통과하는 요청을 차단할지 또는 허용할지 여부를 나타내는 웹 ACL 에 대한 기본 작업을 설정합니다.
  - **규칙** - 각 규칙에는 검사 기준을 정의하는 문과 웹 요청이 기준을 충족하는 경우 수행할 작업이 포함됩니다. 웹 요청이 이 기준을 충족하면 일치하는 것입니다. 규칙을 사용하여 일치 요청을 차단하거나 일치 요청을 허용할 수 있습니다. 일치하는 요청의 개수를 세기 위해 규칙을 사용할 수도 있습니다.
  - **규칙 그룹** - 규칙을 개별적으로 사용하거나 재사용 가능한 규칙 그룹에서 사용할 수 있습니다. AWS 관리형 규칙 및 AWS Marketplace 판매자가 사용할 수 있는 관리형 규칙 그룹을 제공합니다. 사용자 고유의 규칙 그룹을 정의할 수도 있습니다.

세부 설명

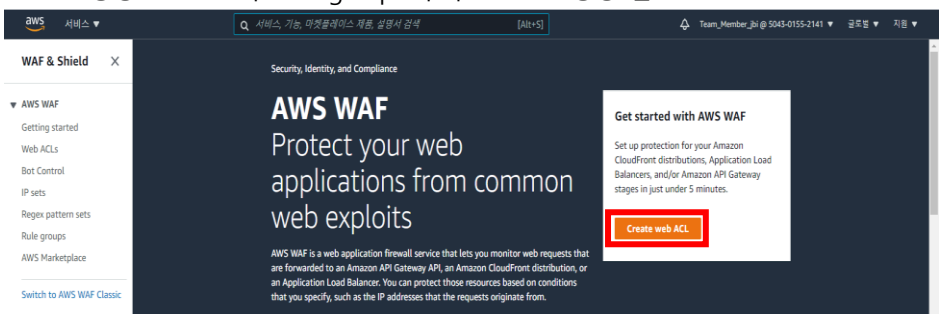
조항	항목번호	항목	일부내용
ISMS-P	2.6.1	네트워크 접근	네트워크에 대한 비인가 접근을 통제하기 위하여 IP 관리, 단말인증 등 관리절차를 수립·이행
ISMS-P	2.6.2	정보시스템 접근	정보시스템에 접근을 허용하는 사용자, 접근제한 방식...정의하고 통제
ISMS-P	2.10.1	보안시스템 운영	보안시스템 유형별로 관리자 지정, 최신 정책 업데이트, 룰셋 변경, 이벤트 모니터링 등의 운영절차를 수립·이행
ISMS-P	2.10.2	클라우드 보안	클라우드 서비스 이용 시 관리자 접근 및 보안 설정
ISMS-P	2.10.3	공개서버 보안	외부 네트워크에 공개되는 서버의 경우 내부 네트워크와 분리하고 취약점 점검, 접근통제, 인증, 정보수집·저장·공개 절차 보호대책을 수립·이행
ISMS-P	2.11.3	이상행위 분석 및 모니터링	내·외부에 의한 침해시도, 개인정보유출 시도, 부정행위 등을 신속하게 탐지·대응할 수 있도록 네트워크 및 데이터 흐름 등을 수집하여 분석하며, 모니터링 및 점검 결과에 따른 사후조치
CSAP	9.1.5	공개서버 보안	가상자원 및 서비스를 제공하기 위한 웹사이트 또는 공개서버를 제공하는 경우 기술적 보호대책을 수립
CSAP	9.2.1	악성코드 통제	악성코드로부터 이용자의 가상환경을 보호하기 위한 악성코드 탐지, 차단 등의 보안기술을 지원, 이상 징후 발견시 이용자 통지하고 사용 중지 및 격리 조치를 수행
CSAP	11.1.2	네트워크 모니터링 통제	DDoS, 비인가 접속 등으로 인한 서비스 중단 및 중요 정보 유출 등을 막기 위해 네트워크를 모니터링

				하고 통제, 내·외부에 의한 침해시도, 개인정보유출 시도, 부정행위 등을 탐지·대응
	CSAP	11.1.3	네트워크 정보보호 시스템 운영	클라우드컴퓨팅서비스와 관련된 내·외부 네트워크를 보호하기 위하여 정보보호시스템을 운영
	항목 준수를 위해 AWS 의 정보시스템에 접근하기 전 WAF 의 설정을 통해 웹 기반의 공격(ex. SQL Injection, XSS, CSRF 등)을 하거나 중요 정보를 보유한 제품에 접근시 제한된 IP 의 사용자만 허용하여 접근을 제한하며 Cloudwatch 를 통해 모니터링을 하며 공격시도를 탐지하고 이상징후 발견시 Amazon SNS 를 통해 이메일로 알림을 받을 수 있습니다.			

설정 방법

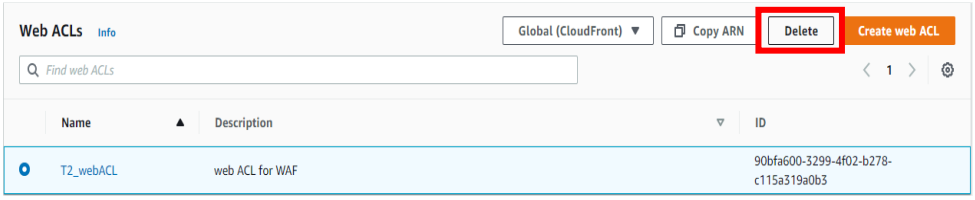
- WAF 생성 방법

Web ACLs 생성 → Rules와 Rule groups 추가 → WAF 생성 완료



- WAF 삭제 방법

Web ACLS 선택 → 삭제하려는 규칙을 사용하고 있는 웹 ACL 선택 -> 삭제 선택



※ 자세한 설명은

https://docs.aws.amazon.com/ko_kr/waf/latest/developerguide/getting-started.html 참고

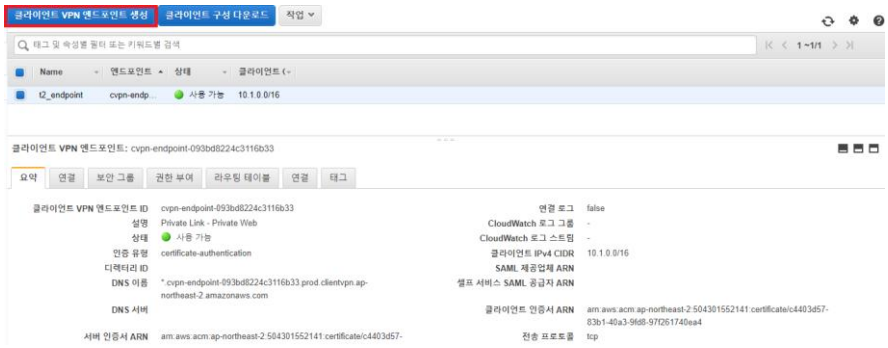
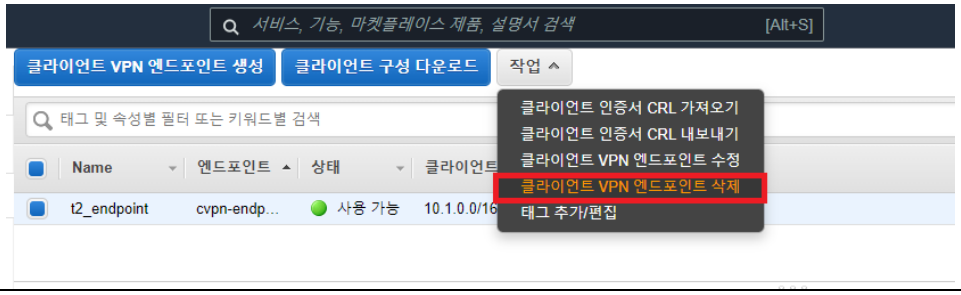
진단 기준	양호	웹 기반 공격대응에 대해 설정한 경우
	취약	웹 기반 공격대응에 대해 설정하지 않은 경우

적용 인증법

ISMS-P 2.6.1 네트워크 접근
ISMS-P 2.6.2 정보시스템 접근
ISMS-P 2.10.1 보안시스템 운영
ISMS-P 2.10.2 클라우드 보안
ISMS-P 2.10.3 공개서버 보안
ISMS-P 2.11.3 이상행위 분석 및 모니터링
CSAP 9.1.5 공개서버 보안
CSAP 9.2.1 악성코드 통제
CSAP 11.1.2 네트워크 모니터링 및 통제
CSAP 11.1.3 네트워크 정보보호시스템 운영

<table>
<tr><td>분류</td><td colspan="2">네트워크 보안</td><td>위험도</td><td>하</td></tr>
<tr><td>항목명</td><td colspan="4">VPN</td></tr>
<tr><td>항목
설명</td><td colspan="4">공식적으로 서비스에 이용되는 웹서버/WAS, 직원 전용으로 사용되는 웹서버/WAS에 대해 제한된 직원들만 엔드포인트를 통해 접근하여 관리 및 조회할 수 있도록 합니다.

- 구성 요소
• Client VPN 엔드포인트 - 클라이언트 VPN 세션을 활성화하고 관리하기 위해 생성하고 구성하는 리소스입니다. 여기에서 모든 클라이언트 VPN 세션이 종료됩니다.
• 대상 네트워크 - Client VPN 엔드포인트와 연결하는 네트워크입니다. VPC 의 서브넷이 대상 네트워크입니다. 서브넷을 Client VPN 엔드포인트와 연결하면 VPN 세션을 설정할 수 있습니다. 고가용성을 위해 여러 서브넷을 하나의 Client VPN 엔드포인트와 연결할 수 있습니다. 모든 서브넷이 동일한 VPC 에 위치해야 합니다. 각 서브넷이 서로 다른 가용 영역에 속해야 합니다.
• 라우팅 - 각 Client VPN 엔드포인트에는 사용 가능한 대상 네트워크 라우팅을 설명하는 라우팅 테이블이 있습니다. 라우팅 테이블의 각 라우팅은 특정 리소스 또는 네트워크에 대한 트래픽 경로를 지정합니다.
• 클라이언트 - VPN 세션을 설정하기 위해 Client VPN 엔드포인트에 연결하는 최종 사용자입니다. 최종 사용자는 OpenVPN 클라이언트를 다운로드하고 사용자가 생성한 VPN 구성 파일을 사용하여 VPN 세션을 설정해야 합니다.</td></tr>
<tr><td>세부
설명</td><td colspan="4"><table>
<tr><th>조항</th><th>항목번호</th><th>항목</th><th>일부내용</th></tr>
<tr><td>ISMS-P</td><td>2.6.1</td><td>네트워크 접근</td><td>네트워크에 대한 비인가 접근을 통제하기 위하여 IP관리,통제를 적용</td></tr>
<tr><td>ISMS-P</td><td>2.6.2</td><td>정보시스템 접근</td><td>서버, 네트워크 시스템... 접근제한 방식, 안전한 접근 수단등을 정의</td></tr>
<tr><td>ISMS-P</td><td>2.6.6</td><td>원격접근 통제</td><td>보호구역 이외 장소에서의 정보시스템 관리 및 개인정보 처리는 원칙적으로 금지, 불가피한 사유로 원격접근을 허용하는 경우 접근 허용범위 및 구간 암호화 등 보호대책 수립</td></tr>
<tr><td>ISMS-P</td><td>2.8.3</td><td>시험과 운영환경 분리</td><td>개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 분리</td></tr>
<tr><td>ISMS-P</td><td>2.8.5</td><td>소스 프로그램 관리</td><td>소스 프로그램은 인가된 사용자만이 접근할 수 있도록 관리</td></tr>
<tr><td>ISMS-P</td><td>2.10.1</td><td>보안시스템 운영</td><td>보안시스템 유형별로 관리자 지정, 최신 정책 업데이트, 룰셋 변경등의 운영절차를 수립·이행</td></tr>
<tr><td>ISMS-P</td><td>2.10.5</td><td>정보전송 보안</td><td>개인정보 및 중요정보를 전송할 경우 안전한 전송 정책을 수립</td></tr>
<tr><td>CSAP</td><td>9.2.3</td><td>데이터 이전</td><td>기존 정보시스템 환경에서 클라우드컴퓨팅서비스의 가상 환경으로 전환 시 안전하게 데이터를 이전하도록 암호화 등의 기술적인 조치방안을 제공</td></tr>
<tr><td>CSAP</td><td>11.1.1</td><td>네트워크 보안 정책 수립</td><td>클라우드컴퓨팅서비스와 관련된 내·외부 네트워크에 대해 보안시스템 유형별로 관리자 지정 운영절차를</td></tr>
</table></td></tr>
</table>

				수립·이행하고 보안시스템별 정책적용 현황을 관리
	CSAP	11.1.3	네트워크 정보보호시스템 운영	클라우드컴퓨팅서비스와 관련된 내·외부 네트워크를 보호하기 위하여 정보보호시스템 운영
	CSAP	11.1.4	네트워크 암호화	클라우드 시스템에서 중요 정보가 이동하는 구간에 대해서는 암호화된 통신채널을 사용
	CSAP	11.1.5	네트워크 분리	클라우드컴퓨팅서비스 제공자의 관리 영역과 이용자의 서비스 영역, 이용자 간 서비스 영역의 네트워크 접근은 물리적 또는 논리적으로 분리
	CSAP	12.1.3	데이터 무결성	입·출력, 전송 또는 데이터 교환 및 저장소의 데이터에 대해 항상 데이터 무결성을 확인
	CSAP	13.1.2	인증 및 암호화 기능	클라우드 시스템 설계 시 중요정보의 입·출력 및 송수신 과정에서 무결성, 기밀성이 요구
	CSAP	13.1.4	접근권한 기능	클라우드 시스템 설계 시 업무의 목적 및 중요도에 따라 접근권한을 부여.
	CSAP	13.2.2	개발과 운영환경 분리	개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소하기 위해 원칙적으로 분리
	CSAP	13.2.4	소스 프로그램 보안	소스 프로그램에 대한 변경관리를 수행하고 인가된 사용자만이 소스 프로그램에 접근할 수 있도록 통제
	항목준수를 위해 중요 정보가 전송될 때 암호화된 통신채널을 사용하여 데이터 무결성과 기밀성을 보장하고 비인가 접근을 막기 위해 원칙적으로 분리하며 업무의 목적과 중요도에 따라 접근권한을 다르게 주는 식으로 하여 인가되지 않은 사용자의 접근을 제한하고 인가된 내부사용자만 접근 할 수 있게 통제합니다.			
설정 방법	**- VPN 생성 방법** 클라이언트 VPN 엔드포인트 → 클라이언트 VPN 엔드포인트 생성 선택 → 작업 → 클라이언트 VPN 엔드포인트 생성  **- VPN 삭제 방법** 클라이언트 VPN 엔드포인트 → 삭제할 클라이언트 VPN 엔드포인트 선택 → 작업 → 클라이언트 VPN 엔드포인트 삭제 선택  			

	※ 자세한 설명은 https://docs.aws.amazon.com/ko_kr/vpn/latest/clientvpn-admin/cvpn-getting-started.html 참고	
진단 기준	**양호**	VPN 엔드포인트를 설정한 경우
	취약	VPN 엔드포인트를 설정하지 않은 경우
적용 인증법	ISMS-P 2.6.1 네트워크 접근 ISMS-P 2.6.2 정보시스템 접근 ISMS-P 2.6.6 원격접근 통제 ISMS-P 2.8.3 시험과 운영 환경 분리 ISMS-P 2.8.5 소스 프로그램 관리 ISMS-P 2.10.1 보안시스템 운영 ISMS-P 2.10.5 정보전송 보안 CSAP 9.2.3 데이터 이전 CSAP 11.1.1 네트워크 보안 정책 수립 CSAP 11.1.3 네트워크 정보보호시스템 운영 CSAP 11.1.4 네트워크 암호화 CSAP 11.1.5 네트워크 분리 CSAP 12.1.1 데이터 분류 CSAP 12.1.3 데이터 무결성 CSAP 13.1.2 인증 및 암호화 기능 CSAP 13.1.4 접근권한 기능 CSAP 13.2.2 개발과 운영환경 분리 CSAP 13.2.4 소스 프로그램 보안	

분류	네트워크 보안	위험도	하
항목명	Internet Gateway		
항목 설명	Internet Gateway 는 EC2 인스턴스기반의 웹서버에 접근하려는 외부사용자가 인터넷을 통해 통신하여 접속할 수 있도록 합니다. Internet Gateway 에는 인터넷 Routing 가능 트래픽에 대한 VPC Routing 테이블에 대상을 제공하고, 퍼블릭 IPv4 주소가 할당된 인스턴스에 대해 NAT(네트워크 주소 변환)를 수행하는 두 가지 목적이 있습니다.		

세부 설명

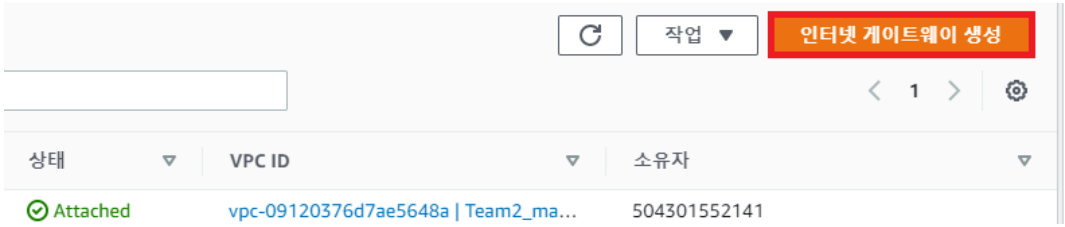
조항	항목번호	항목내용	일부내용
ISMS-P	2.6.2	정보시스템 접근	서버, 네트워크시스템 등 정보시스템에 접근을 허용하는 사용자, 접근제한 방식, 안전한 접근수단 등을 정의하여 통제하여야 한다.

항목 준수를 위해 Routing table에서 Internet Gateway를 설정하거나 미설정하는 식으로 해서 접근에 대해 허용/미허용 사용자를 통제합니다.

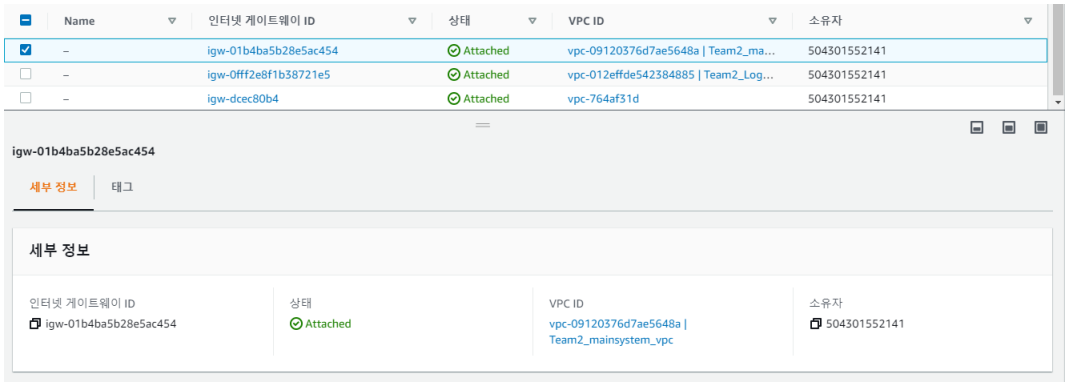
설정 방법

- **인터넷 게이트웨이 생성**

VPC 대시보드 → 인터넷 게이트웨이 → 인터넷 게이트웨이 생성 → 완료



- **인터넷 게이트웨이 예시**



※ 자세한 설명은

https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/VPC_Internet_Gateway.html 참고

진단 기준		
	양호	인터넷 게이트웨이를 생성한 경우
	취약	인터넷 게이트웨이를 생성하지 않은 경우
적용 인증법	ISMS-P 2.6.2 정보시스템 접근	

분류	네트워크 보안	위험도	중
항목명	Routing Tables		

항목 설명

외부인터넷에서 들어오는 네트워크 트래픽을 전달할 위치를 결정할 때 사용되는 규칙입니다. VPC 의 각 서브넷을 Routing Tables 에 연결해야 하며, Table 에서는 서브넷에 대한 Routing 을 제어하게 됩니다. 서브넷을 한 번에 하나의 Routing Table 에만 연결 할 수 있지만 여러 서브넷을 동일한 Routing Table 에 연결하는 것은 가능합니다.

- Routing 우선순위

- LPM(Longest Prefix Match)를 통해 트래픽과 일치하는 가장 구체적인 Routing 을 사용하여 트래픽의 Routing 방법을 결정합니다.

- LPM(Longest Prefix Match)

- CIDR 로 나뉘어진 네트워크로 패킷이 들어왔을 때 라우팅 테이블에서 알맞은 네트워크를 고르기 위해서 가장 긴 subnet mask 에 match 되는 네트워크를 선택합니다.

세부 설명

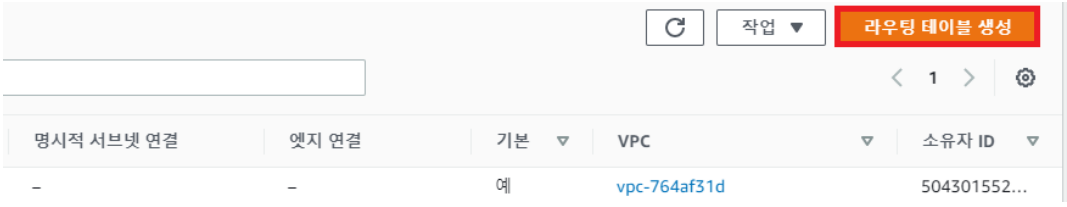
조항	항목번호	항목	일부내용
ISMS-P	2.6.2	정보시스템 접근	서버, 네트워크시스템 등 정보시스템에 접근을 허용하는 사용자, 접근제한 방식, 안전한 접근수단 등을 정의하여 통제하여 한다.

항목을 준수하기 위해 라우팅테이블 설정에서 Internet Gateway, NAT Gateway, instance, network interface 에 대해 설정하여 정보시스템에 접근을 허용하는 사용자, 접근제한을 하는식으로 통제가 가능합니다.

설정 방법

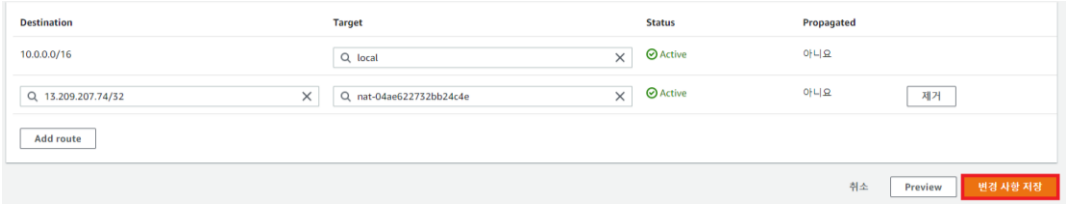
- 라우팅 테이블 생성

VPC 대시보드 → 라우팅 테이블 → 라우팅 테이블 생성 → 완료

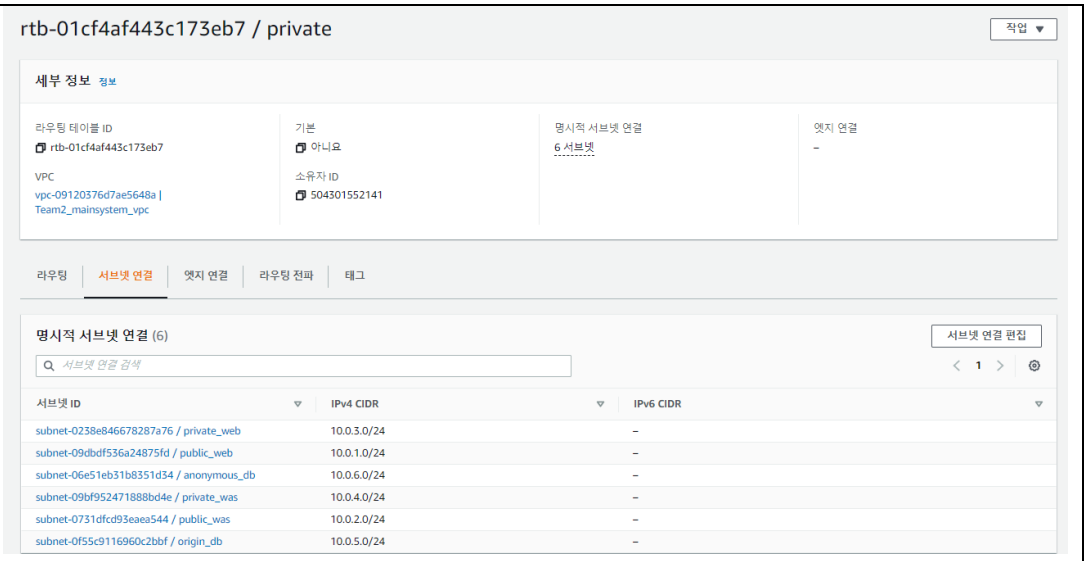


- 라우팅 테이블 설정

라우팅 테이블 → 라우팅 테이블 선택 → 라우팅 → 라우팅 편집 → 변경사항 저장 → 완료



- 라우팅 테이블 예시

<table>
<tr><td rowspan="3"></td><td colspan="2">


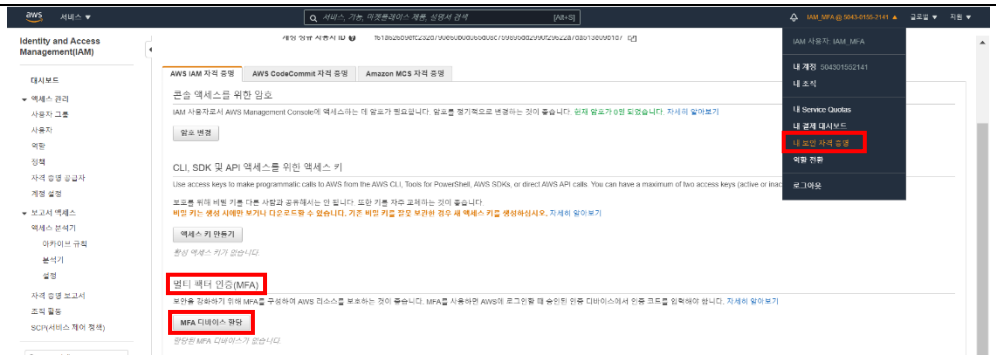
※ 자세한 설명은

https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/VPC_Route_Tables.html 참고
</td></tr>
<tr><td rowspan="2">진단 기준</td><td>양호</td><td>라우팅 테이블에서 편집을 한 경우</td></tr>
<tr><td>취약</td><td>라우팅 테이블에서 편집을 하지 않은 경우</td></tr>
<tr><td>적용 인증법</td><td colspan="2">ISMS-P 2.6.2 정보시스템 접근</td></tr>
</table>

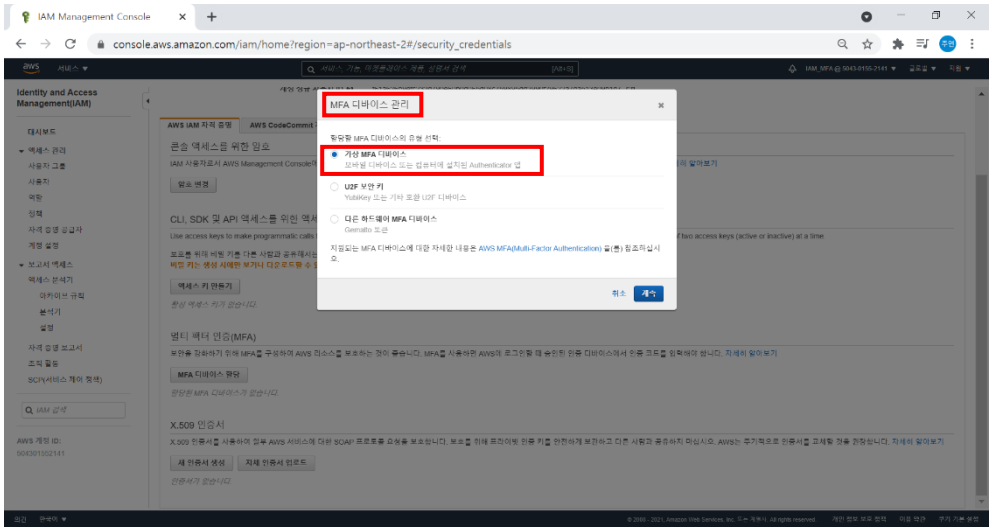
3. 계정 보안

<table>
<tr><td>분류</td><td colspan="3">계정 보안</td><td>위험도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="5">Multi-Factor Authentication</td></tr>
<tr><td>항목
설명</td><td colspan="5">AWS Multi-Factor Authentication(MFA)은 사용자 이름과 암호 외에 보안을 한층 더 강화할 수 있는 방법입니다. MFA는 사용자가 AWS 웹 사이트 또는 서비스에 액세스할 때 사용자의 정규 로그인 자격 증명 외에도 AWS가 지원되는 MFA 메커니즘의 고유 인증을 제출하라고 요청함으로써 보안을 더욱 강화합니다. 이러한 다중 요소를 통해 AWS 계정 설정 및 리소스에 대한 보안을 높일 수 있습니다.

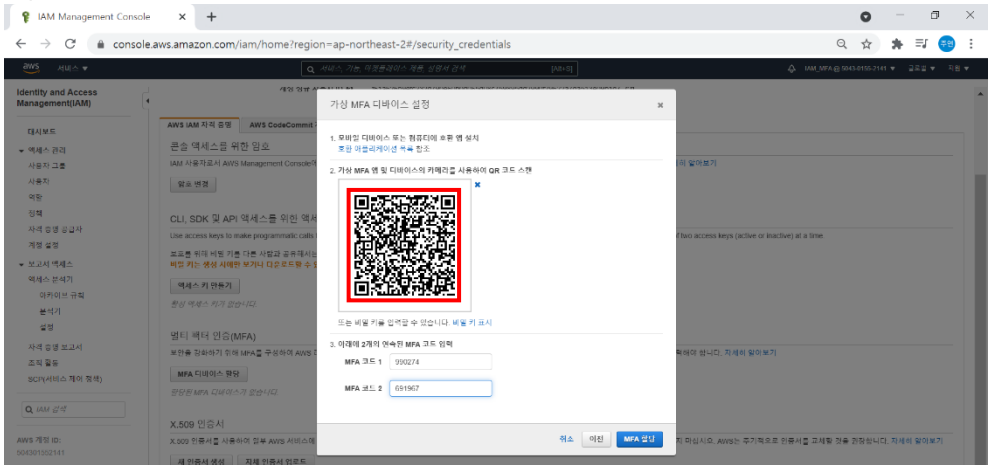
- 규칙 및 제한
• 한 사용자에게는 한 번에 하나의 MFA 디바이스만 할당할 수 있습니다. 사용자가 디바이스를 분실하거나 이유를 불문하고 교체할 필요가 있을 경우, 먼저 기존 디바이스를 비활성화해야 합니다. 그런 다음, 해당 사용자를 위한 새 디바이스를 추가할 수 있습니다.
• 스마트폰 또는 기타 디바이스를 가상 MFA 디바이스로 사용할 수 있습니다. 이를 위해서는 표준 기반 TOTP(시간 기반 일회용 암호) 알고리즘인 RFC 6238 과 호환되는 모바일 앱을 설치해야 합니다.
• 대부분의 가상 MFA 앱은 여러 개의 가상 디바이스 생성을 지원하므로 여러 개의 AWS 계정이나 사용자에게 동일한 앱을 사용할 수 있습니다. 그러나 MFA 디바이스는 사용자 1명당 단 1개만 활성화할 수 있습니다.</td></tr>
<tr><td rowspan="7">세부
내용</td><td>조항</td><td>항목번호</td><td>항목</td><td colspan="2">일부내용</td></tr>
<tr><td>ISMS-P</td><td>2.5.3</td><td rowspan="2">사용자 인증</td><td colspan="2" rowspan="2">정보시스템과 개인정보 및 중요정보에 대한 사용자의 접근은 안전한 인증절차와 필요에 따라 강화된 인증방식을 적용</td></tr>
<tr><td>CSAP</td><td>10.3.1</td></tr>
<tr><td>CSAP</td><td>10.3.3</td><td>강화된 인증 수단 제공</td><td colspan="2">이용자가 클라우드컴퓨팅서비스에 대해 다중 요소 인증 등 강화된 인증 수단을 요청하는 경우 이를 제공하기 위한 방안을 마련</td></tr>
<tr><td>CSAP</td><td>12.1.1</td><td>데이터 분류</td><td colspan="2">데이터 유형, 법적 요구사항, 민감도 및 중요도에 따라 데이터를 분류하고 관리</td></tr>
<tr><td>CSAP</td><td>13.1.2</td><td>인증 및 암호화 기능</td><td colspan="2">사용자 인증에 관한 보안요구사항을 반드시 고려하여야 하며 중요정보의 입·출력 및 송수신 과정에서 무결성,기밀성이 요구</td></tr>
<tr><td colspan="5">항목을 준수하기 위해 직원 전용으로 사용되는 웹서버/WAS와 개발 환경에 대해 AWS MFA를 활성화하면 제한된 직원들이 로그인할 때 사용자 이름과 암호뿐 아니라 AWS MFA 디바이스의 인증 응답을 입력하라는 메시지가 표시됩니다.</td></tr>
<tr><td>설정
방법</td><td colspan="5">IAM → 우측상단 계정 → 내 보안 자격 증명 → 멀티 팩터 인증 → MFA 디바이스 할당</td></tr>
</table>



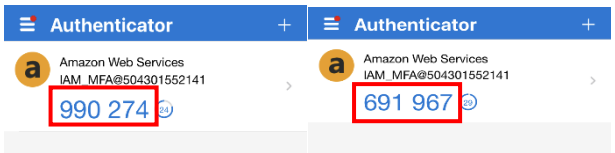
MFA 디바이스 관리 → 가상 MFA 디바이스 선택 → 계속

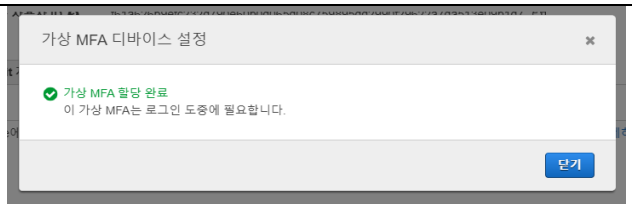


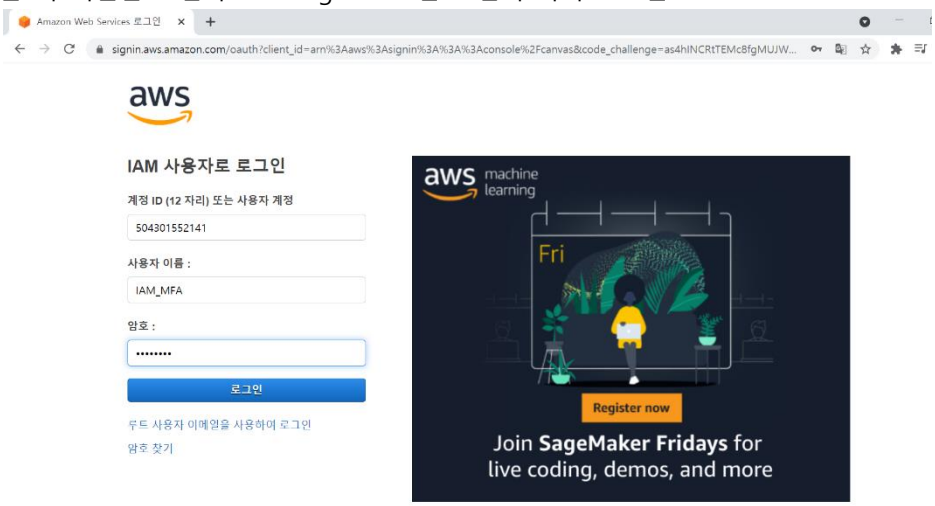
Google OTP 어플 설치 → '+' 버튼 → 바코드 스캔 → 나타난 QR코드를 어플에서 스캔

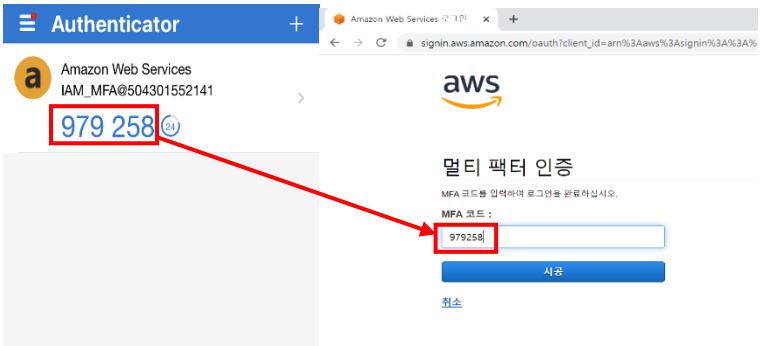


스캔 후 나타난 숫자 MFA 코드 1 입력 → 시간이 지난 후 재생성된 숫자 MFA 코드 2 입력



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


로그인 시 비밀번호 입력 → Google OTP 번호 입력 하여 로그인




</td></tr>
<tr><td rowspan="2">진단
기준</td><td>양호</td><td>AWS 계정 및 IAM 사용자 계정 로그인 시 MFA가 활성화되어 있을 경우</td></tr>
<tr><td>취약</td><td>AWS 계정 및 IAM 사용자 계정 로그인 시 MFA가 비활성화되어 있을 경우</td></tr>
<tr><td>적용
인증법</td><td colspan="2">ISMS-P 2.5.3 사용자 인증
CSAP 10.3.1 사용자 식별
CSAP 10.3.3 강화된 인증 수단 제공
CSAP 12.1.1 데이터 분류
CSAP 13.1.2 인증 및 암호화 기능</td></tr>
</table>

분류	계정 보안	위험도	하
항목명	IAM(자격 증명 기반 정책) 계정 보안		
항목 설명	- **기능** • AWS IAM(Identity and Access Management)은 AWS 리소스에 대한 접근 및 사용권한을 부여하여 관리하는 자격 증명 기반 정책 서비스입니다. 무분별한 IAM 계정 생성 및 유추하기 쉬운 계정명(test, user, adm, abcd 등) 사용 시 보안상 위험이 발생할 수 있으므로 계정 생성 시 사용자 식별 및 유추가 어려운 계정명을 사용해야 합니다.		

세부 설명

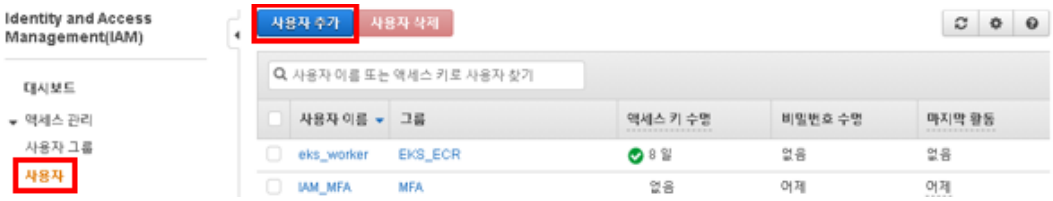
조항	항목번호	항목	일부내용
ISMS-P	2.2.1	주요 직무자 지정 및 관리	주요 직무자를 최소한으로 지정
ISMS-P	2.2.2	직무 분리	권한 오·남용 등으로 인한 잠재적인 피해 예방을 위하여
CSAP	2.1.3		
ISMS-P	2.5.1	사용자 계정 관리	개인정보 및 중요정보에 대한 비인가 접근을 통제하고 업무 목적에 따른 접근권한을 최소한으로 부여
CSAP	10.2.1		
ISMS-P	2.5.5	특수 계정 및 권한 관리	특수 목적을 위하여 사용하는 계정 및 권한은 최소한으로 부여
CSAP	10.2.2		
ISMS-P	2.5.6	접근권한 검토	개인정보 및 중요정보에 접근하는 사용자 계정의...주기적으로 검토
CSAP	10.2.3		
CSAP	9.2.4	가상 소프트웨어 보안	출처, 유통경로 및 제작자가 명확한 소프트웨어로 구성된 가상환경을 제공하여야 한다.
CSAP	10.1.1	접근통제 정책 수립	비인가자의 접근을 통제할 수 있도록 접근통제 영역 및 범위, 접근통제 규칙, 방법 등을 포함하여 접근통제 정책을 수립하여야 한다.
ISMS-P	2.5.2	사용자 식별	사용자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 한다.
CSAP	10.3.1		
ISMS-P	2.5.3	사용자 인증	사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제하여야 한다.
ISMS-P	2.10.2		
CSAP	10.3.2		
CSAP	10.3.3	강화된 인증 수단 제공	다중 요소 인증 등 강화된 인증 수단을 요청하는 경우 이를 제공하기 위한 방안을 마련하여야 한다.
ISMS-P	2.6.2	네트워크 정보보호시스템 운영	정보보호시스템(방화벽, IPS, IDS, VPN 등)을 운영하여야 한다.
CSAP	11.1.3		
ISMS-P	2.6.1	네트워크 분리	서비스 영역, 이용자 간 서비스 영역의 네트워크 접근은 물리적 또는 논리적으로 분리하여야 하고, 취약점 점검, 접근통제, 인증, 정보 수집·저장·공개 절차 등 강화된 보호대책을 수립·이행하여야 한다.
ISMS-P	2.10.3		
CSAP	11.1.5		
CSAP	12.1.4	데이터 보호	데이터에 대한 접근제어, 위·변조 방지 등 데이터 처리에 대한 보호 기능을 이용자에게 제공하여야 한다
CSAP	13.1.2	인증 및 암호화 기능	사용자 인증에 관한 보안요구사항을 반드시 고려하여야 하며 중요정보의 입·출력 및 송수신 과정

				에서 무결성, 기밀성이 요구될 경우 법적 요구사항을 고려하여야 한다.
	CSAP	13.1.4	인증 및 암호화 기능	업무의 목적 및 중요도에 따라 접근권한을 부여할 수 있도록 하여야 한다.
	ISMS-P	2.8.4	시험 데이터 보안	시험데이터 생성, 이용 및 관리, 파기, 기술적 보호조치에 관한 절차를 수립하여 이행하여야 한다.
	CSAP	13.2.3		
	ISMS-P	2.8.5	소스 프로그램 보안	소스 프로그램에 대한 변경관리를 수행하고 인가된 사용자만이 소스 프로그램에 접근할 수 있도록 통제절차를 수립하여 이행하여야 한다.
	CSAP	13.2.4		
	항목 준수를 위해 사용자를 추가하고 권한을 최소화하기 위해 콘솔에서 필요한 권한만 부여하고 유기적인 권한 부여를 위해 IAM 그룹을 만들어 관리합니다. 네트워크 및 리소스에 대해 인가 된 사용자만이 접근할 수 있도록 통제 절차를 수립하도록 합니다. 또한 필요에 따라 MFA 와 같은 추가 인증을 수행합니다.			

설정 방법

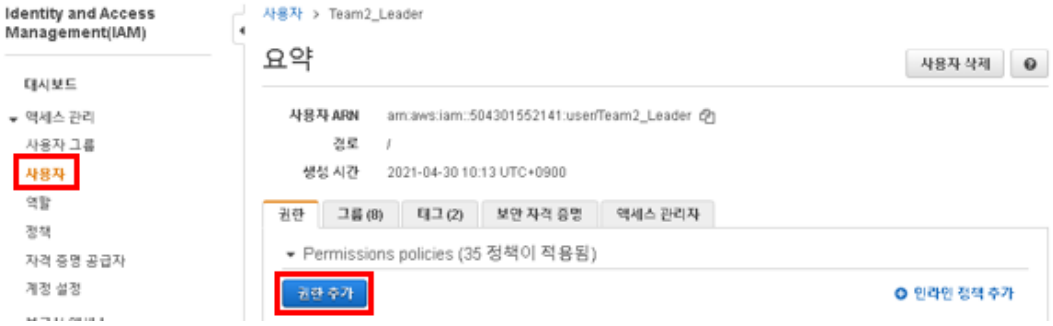
- IAM 사용자 생성

IAM → 사용자 → 사용자 추가 → 역할에 맞는 정책(권한) 추가



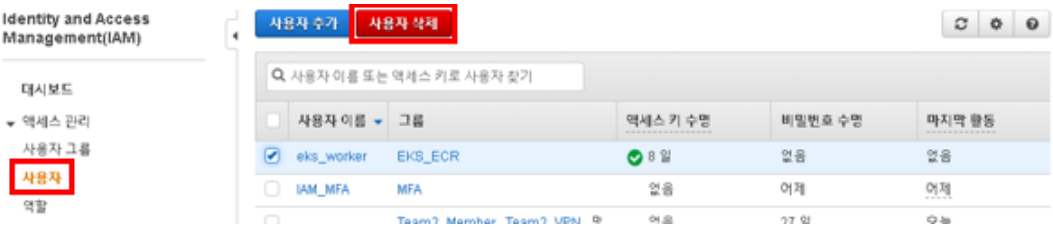
- 기존 생성 계정 권한 추가

IAM → 사용자 → 권한 변경하려는 사용자 선택 → 권한 추가



- IAM 사용자 삭제

IAM → 사용자 → 사용자 삭제

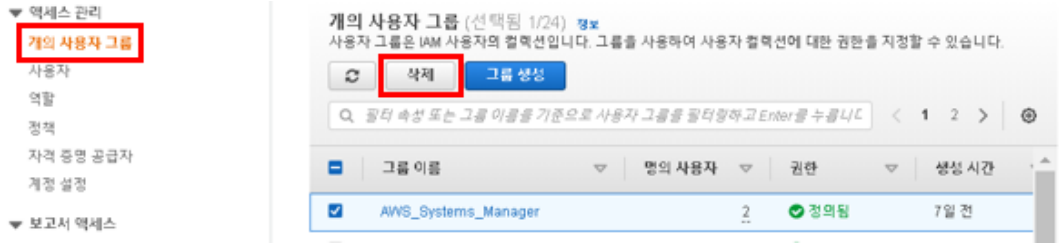


- IAM 그룹 생성

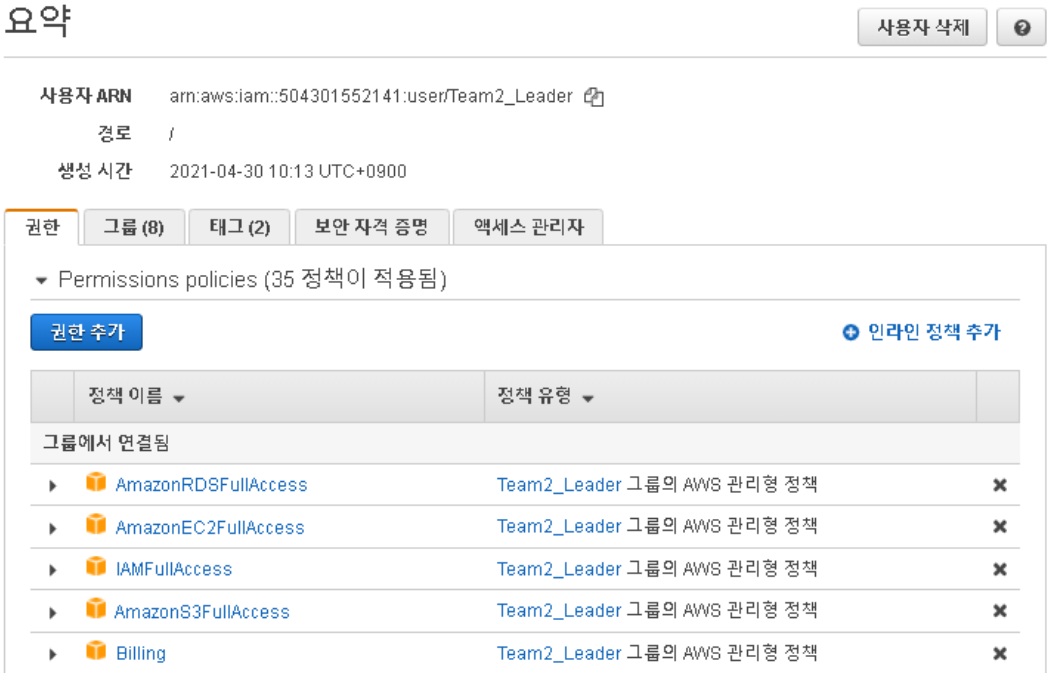
IAM → 그룹 → 새로운 그룹 생성 → 그룹 이름 설정 → IAM 계정 권한에 맞는 정책 연결 → 그룹 생성

- IAM 그룹 삭제

IAM → 그룹 → 삭제하려는 그룹 선택 → 삭제



- IAM 예시



※ 자세한 설명은

https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/vpc-network-acls.html 참고

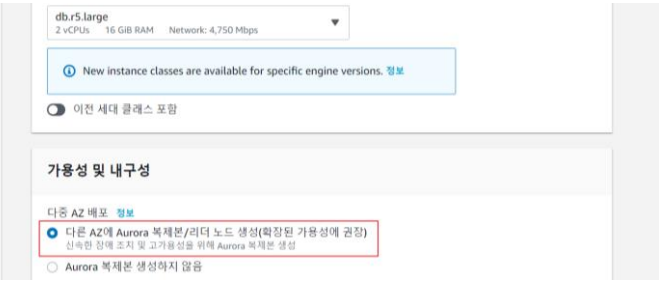
진단 기준	양호	1) IAM User Account 사용자를 식별할 수 있을 경우 2) 유추가 가능한 계정을 사용하지 않을 경우 3) IAM Group이 보유하고 있는 정책이 역할에 맞게 설정되어 있을 경우
	취약	1) IAM User Account 사용자를 식별할 수 없을 경우 2) 유추가 가능한 계정을 사용하고 있을 경우 3) IAM Group이 보유하고 있는 정책이 역할에 맞지 않게 설정되어 있을 경우
적용 인증법	ISMS-P 2.2.1 주요 직무자 지정 및 관리 ISMS-P 2.2.2 직무 분리 ISMS-P 2.5.1 사용자 계정 관리	

	ISMS-P 2.5.2 사용자 식별 ISMS-P 2.5.3 사용자 인증 ISMS-P 2.5.4 비밀번호 관리 ISMS-P 2.5.5 특수 계정 및 권한 관리 ISMS-P 2.5.6 접근권한 검토 ISMS-P 2.6.2 정보시스템 접근 ISMS-P 2.6.3 응용프로그램 접근 ISMS-P 2.6.4 데이터베이스 접근 ISMS-P 2.10.2 클라우드 보안 CSAP 2.1.3 직무 분리 CSAP 9.2.4 가상 소프트웨어 보안 CSAP 10.1.1 접근통제 정책 수립 CSAP 10.2.1 사용자 등록 및 권한부여 CSAP 10.2.2 관리자 및 특수 권한관리 CSAP 10.2.3 접근권한 검토 CSAP 10.3.1 사용자 식별 CSAP 10.3.2 사용자 인증 CSAP 10.3.3 강화된 인증 수단 제공 CSAP 11.1.3 네트워크 정보보호시스템 운영 CSAP 11.1.5 네트워크 분리 CSAP 12.1.4 데이터 보호 CSAP 13.1.2 인증 및 암호화 기능 CSAP 13.1.4 접근권한 기능 CSAP 13.2.3 시험 데이터 보안 CSAP 13.2.4 소스 프로그램 보안

4. RDS

<table>
<tr><td>분류</td><td colspan="2">RDS</td><td>위험도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="4">다중 AZ</td></tr>
<tr><td>항목
설명</td><td colspan="4">다중 AZ 배포는 RDS 데이터베이스(DB) 인스턴스를 위해 향상된 가용성 및 내구성을 제공합니다. DB 인스턴스를 프로비저닝하면 Amazon RDS는 자동으로 하나의 기본 DB 인스턴스를 생성하고 동시에 다른 가용 영역(AZ)의 예비 인스턴스에 데이터를 복제합니다.

인프라 장애가 발생하더라도 Amazon RDS가 예비 인스턴스(또는 Amazon Aurora의 경우 읽기 전용 복제본)로 자동 장애 조치를 수행하여 장애 조치 완료 후 데이터베이스 작업을 바로 재개할 수 있습니다. 장애 조치 후에도 DB 인스턴스의 엔드포인트는 그대로 유지되므로 관리자가 직접 개입할 필요 없이 애플리케이션에서 데이터베이스 작업을 재개할 수 있습니다.

MySQL, MariaDB, Oracle 및 PostgreSQL 엔진에 대한 다중 AZ 배포는 동기식 물리적 복제를 활용하여 예비 복제본의 데이터를 기본 복제본과 같은 최신 상태로 유지합니다.</td></tr>
<tr><td>세부
설명</td><td colspan="4"><table>
<tr><th>조항</th><th>항목번호</th><th>항목</th><th>일부내용</th></tr>
<tr><td>ISMS-P</td><td>2.9.3</td><td rowspan="2">백업 및 복구관리</td><td rowspan="2">정보시스템의 가용성과 데이터 무결성을 유지하기 위하여 백업 대상, 주기, 방법, 보관기간, 소산 등의 절차를 수립·이행하여야 한다</td></tr>
<tr><td>CSAP</td><td>6.2.2</td></tr>
<tr><td>ISMS-P</td><td>2.12.1</td><td>재해·재난 대비 안전 조치</td><td>복구 전략 및 대책, 비상시 복구 조직, 비상연락체계, 복구 절차 등 재해 복구체계를 구축하여야 한다.</td></tr>
</table>
항목을 준수하기 위해 적시에 복구가 가능하도록 하며 다중 AZ를 설정하여 장애 발생 시 자동 장애 조치를 수행하여 복구 체계를 구축할 수 있습니다.</td></tr>
<tr><td>설정
방법</td><td colspan="4">RDS → 데이터베이스 생성 → 가용성 및 내구성 → 다중 AZ 배포 → 다른 AZ에 Aurora 복제본/리더 노드 생성(확장된 가용성에 권장) 선택 → 완료
 

※ 다른 AZ에 Aurora 복제본/리더 노드 생성(확장된 가용성에 권장) 선택</td></tr>
<tr><td rowspan="2">진단
기준</td><td>양호</td><td colspan="3">다중 AZ 설정이 잘 되어있을 경우</td></tr>
<tr><td>취약</td><td colspan="3">다중 AZ 설정이 잘 되어있지 않을 경우</td></tr>
<tr><td>적용
인증법</td><td colspan="4">ISMS-P 2.9.3 백업 및 복구관리
ISMS-P 2.12.1 재해·재난 대비 안전 조치
CSAP 6.2.2. 이중화 및 백업</td></tr>
</table>

분류	RDS	위험도	중
항목명	스냅샷		

항목 설명

DB 스냅샷을 생성할 때는 백업할 DB 인스턴스를 구분한 다음 나중에 복구할 수 있도록 DB 스냅샷을 명명해야 합니다. 스냅샷을 생성하는 데 걸리는 시간은 데이터베이스 크기에 따라 다릅니다. 스냅샷에는 전체 스토리지 볼륨이 포함되기 때문에 임시 파일 같은 파일들의 크기가 스냅샷을 생성하는 데 걸리는 시간에 영향을 미치기도 합니다.

Amazon RDS는 개별 데이터베이스가 아닌 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 다중 AZ 배포에 대한 백업 시 기본 AZ에서는 I/O 작업이 중단되지 않습니다. 백업이 예비 복제본으로부터 수행되기 때문입니다. SQL Server의 경우, 다중 AZ 배포에 대한 백업 도중 I/O 작업이 일시적으로 중단됩니다.

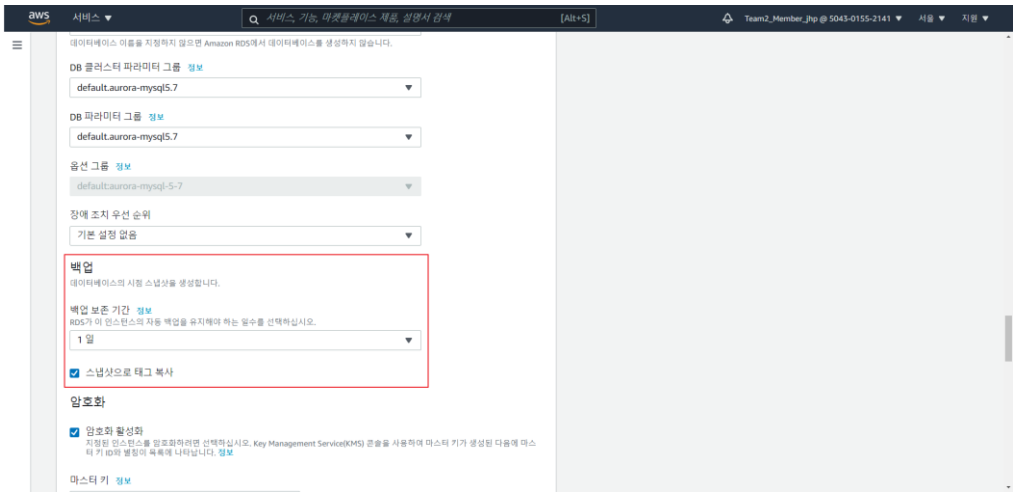
세부 설명

조항	항목번호	항목	일부내용
ISMS-P	2.9.3	백업 및 복구관리	정보시스템의 가용성과 데이터 무결성을 유지하기 위하여 백업 대상, 주기, 방법, 보관기간, 소산 등의 절차를 수립·이행하여야 한다
CASP	6.2.2		
CSAP	14.2.2	중요장비 이중화 및 백업체계 구축	클라우드컴퓨팅서비스를 제공하는 사업자는 네트워크 스위치, 스토리지 등 중요장비를 이중화하고 서비스의 가용성을 보장하기 위해 백업체계를 구축하여야 한다.

항목을 준수하기 위해 스냅샷을 생성하여 적시에 복구가 가능하도록 합니다. Auto Scaling 기능을 통해 서비스의 가용성을 확보하며 CloudWatch를 통해 장애 발생시 즉각 대응하도록 조치합니다.

설정 방법

RDS → 데이터베이스 생성 → 추가 구성 → 백업 설정 → 완료



※ 백업 보존 기간 선택 후 스냅샷으로 태그 복사

진단 기준

양호	스냅샷 설정이 잘 되어있을 경우
취약	스냅샷 설정이 잘 되어있지 않을 경우

적용 인증법

ISMS-P 2.9.3 백업 및 복구관리
CSAP 6.2.2 이중화 및 백업
CSAP 14.2.2 중요장비 이중화 및 백업체계 구축

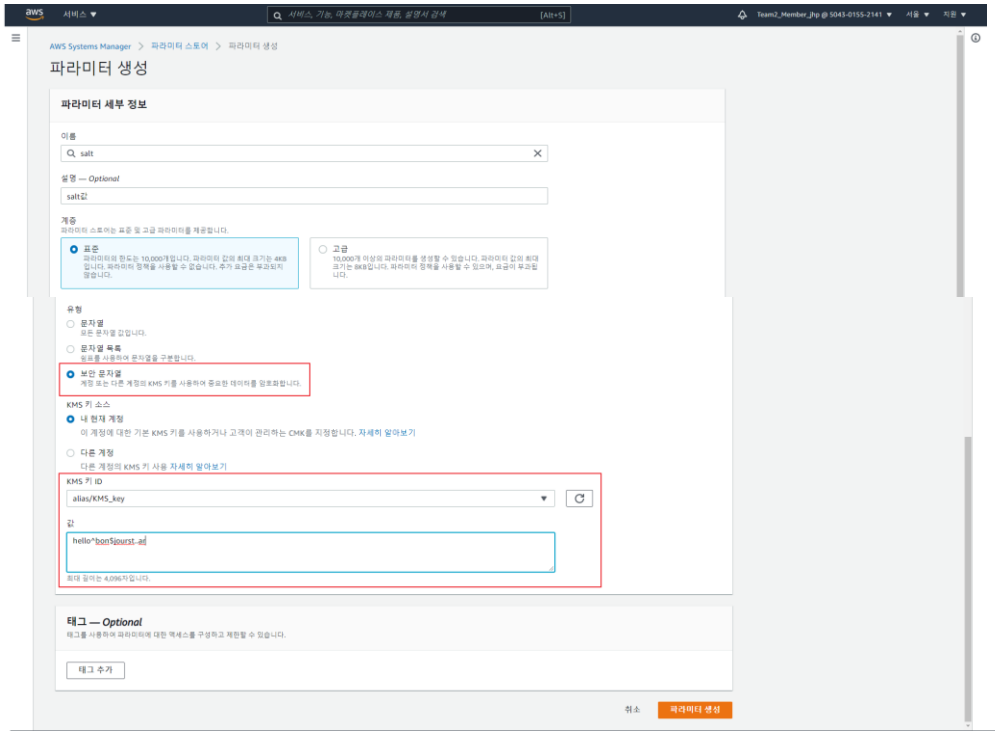
<table>
<tr><td>분류</td><td colspan="3">RDS</td><td>위험도</td><td>상</td></tr>
<tr><td>항목명</td><td colspan="5">파라미터 스토어</td></tr>
<tr><td>항목
설명</td><td colspan="5">회원ID를 가명처리할 때, Salt값을 이용합니다. Salt값을 파라미터 스토어에서 보안문자열을 사용하여 저장합니다. 보안문자열을 이용하면 파라미터 스토어에서 AWS Key Management Service(KMS) Customer Master Key(CMK)를 사용하여 파라미터 값을 암호화합니다. 또한, Salt값에 대한 권한이 있는 IAM 계정만 접근하도록 합니다.

파라미터 스토어는 AWS Systems Manager 의 기능으로 구성 데이터 관리 및 암호 관리를 위한 안전한 계층적 스토리지를 제공합니다. 암호, 데이터베이스 문자열, Amazon Machine Image (AMI) ID와 라이선스 코드를 파라미터 값으로 사용합니다. 값을 일반 텍스트 또는 암호화된 데이터로 저장할 수 있습니다. 파라미터 및 파라미터 정책 모두에 대해 변경 알림을 구성하고 자동화된 작업을 호출할 수 있습니다.

안전하고 확장 가능한 호스팅 방식 암호 관리 서비스를 사용합니다(관리할 서버가 없음). 데이터를 코드와 격리하여 보안 태세를 개선합니다.
파라미터 저장소는 AWS Secrets Manager 와 통합되어 파라미터 스토어 파라미터에 대한 참조를 이미 지원하는 다른 AWS 서비스를 사용하는 경우 암호 관리자 암호를 검색할 수 있습니다.

파라미터 스토어 파라미터는 텍스트 블록, 이름 목록, 암호, 암호 등과 같이 파라미터 스토어에 저장되는 모든 데이터입니다. AMI ID, 라이센스 키 등이 있습니다. 스크립트, 명령 및 SSM 문서에서 이 데이터를 중앙에서 안전하게 참조할 수 있습니다.

승인된 사용자만 파라미터 값에 액세스할 수 있도록 하면서 비밀번호 및 구성 데이터를 일반 관리 작업에서 분리합니다. 콘솔 또는 프로그래밍 방식의 도구를 사용하여 AWS 서비스에 걸쳐, 그리고 사용자 지정 솔루션으로부터 파라미터에 액세스합니다.</td></tr>
<tr><td rowspan="8">세부
설명</td><td>조항</td><td>항목번호</td><td>항목</td><td colspan="2">일부내용</td></tr>
<tr><td>ISMS-P</td><td>2.7.1</td><td rowspan="2">암호정책 적용</td><td colspan="2" rowspan="2">개인정보 및 주요정보 보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호 강도, 암호 사용 정책을 수립하고 개인정보 및 주요정보의 저장·전송·전달 시 암호화를 적용하여야 한다</td></tr>
<tr><td>CSAP</td><td>12.2.1</td></tr>
<tr><td>ISMS-P</td><td>2.7.2</td><td rowspan="2">암호키 관리</td><td colspan="2" rowspan="2">암호키의 안전한 생성·이용·보관·배포·파기를 위한 관리 절차를 수립·이행</td></tr>
<tr><td>CASP</td><td>12.2.2</td></tr>
<tr><td>ISMS-P</td><td>2.10.2</td><td>클라우드 보안</td><td colspan="2">클라우드 서비스 이용 시 (중략) 중요정보와 개인정보가 유·노출되지 않도록 관리자 접근 및 보안 설정 등에 대한 보호대책을 수립·이행하여야 한다</td></tr>
<tr><td>CSAP</td><td>13.1.2</td><td>인증 및 암호화 기능</td><td colspan="2">클라우드 시스템 설계 시 사용자 인증에 관한 보안요구사항을 반드시 고려하여야 하며 중요정보의 입·출력 및 송수신 과정에서 무결성, 기밀성이 요구될 경우 법적 요구사항을 고려하여야 한다.</td></tr>
<tr><td colspan="5">항목을 준수하기 위해 Salt값을 파라미터 스토어에서 보안문자열을 사용하여 저장하며 KMS의 CMK를 사용하여 파라미터값을 암호화합니다. 그리고 지정된 IAM 계정만 접근하도록 합니다.</td></tr>
</table>

<table>
<tr>
<td>설정
방법</td>
<td>
AWS Systems Manager → 파라미터 스토어 → 보안 문자열 선택 → KMS 키 소스 선택(CMK 지정) → 값(Salt값) 입력 → 파라미터 생성


<table>
<tr><td>Salt값</td><td>hello^bon$jourst..ar</td></tr>
<tr><td>KMS 키</td><td>Alias/KMS_key</td></tr>
</table>
</td>
</tr>
<tr>
<td rowspan="2">진단
기준</td>
<td>양호</td>
<td>파라미터 생성이 잘 되었을 경우</td>
</tr>
<tr>
<td>취약</td>
<td>파라미터 생성이 잘 되어있지 않을 경우</td>
</tr>
<tr>
<td>적용
인증법</td>
<td colspan="2">ISMS-P 2.7.1 암호정책 적용
ISMS-P 2.7.2 암호키 관리
ISMS-P 2.10.2 클라우드 보안
CSAP 12.2.1 암호 정책 수립
CSAP12.2.2 암호키 관리
CSAP 13.1.2 인증 및 암호화 기능</td>
</tr>
</table>

분류	RDS	위험도	중
항목명	프라이빗 엑세스		
항목 설명	원본DB는 개인정보가 저장되어 있기 때문에 외부에서 RDS 접근을 불가능하도록 프라이빗으로 설정합니다.		

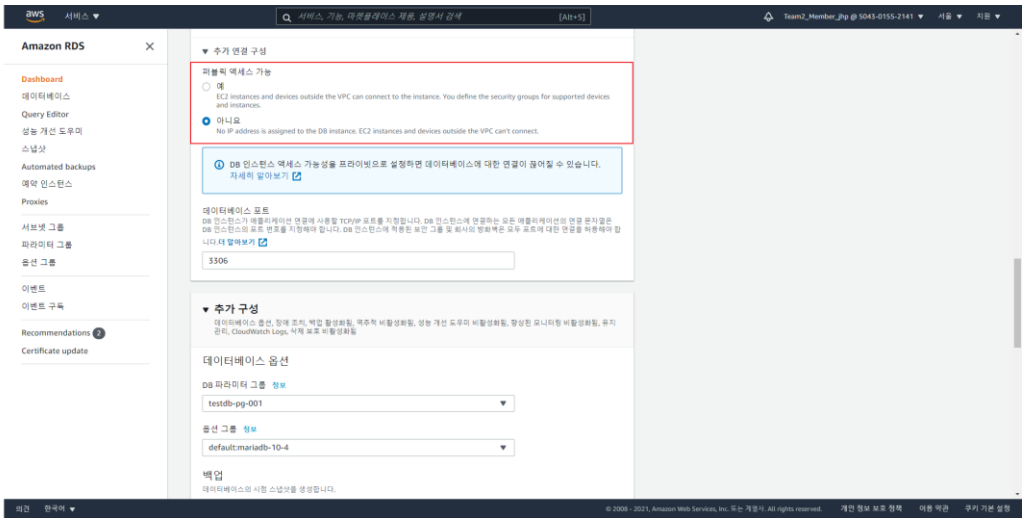
세부 설명

조항	항목번호	항목	일부내용
ISMS-P	2.6.1	네트워크 접근	네트워크에 대한 비인가 접근을 통제하기 위하여 IP고나리, 단말인증 등 관리절차를 수립·이행하고, 업무목적 및 중요도에 따라 네트워크 분리(DMZ, 서버팜, DB존, 개발존 등)와 접근통제를 적용하여야 한다.
ISMS-P	2.6.4	데이터베이스 접근	테이블 목록 등 데이터베이스 내에서 저장·관리되고 있는 정보를 식별하고, 정보의 중요도와 응용프로그램 및 사용자 유형 등에 따른 접근통제 정책을 수립·이행하여야 한다.
CSAP	12.1.1	데이터 분류	데이터 유형, 법적 요구사항, 민감도 및 중요도에 따라 데이터를 분류하고 관리하여야 한다.
CSAP	12.1.4	데이터 보호	데이터에 대한 접근제어, 위·변조 방지 등 데이터 처리에 대한 보호 기능을 이용자에게 제공하여야 한다.

항목을 준수하기 위해 퍼블릭 액세스 가능을 '아니요'로 설정하여 프라이빗 액세스로 설정하여 외부에서 접근할 수 없도록 합니다. 법적 요구사항에 따라 중요 데이터를 별도로 관리히며 데이터에 대한 접근제어를 수행하여 데이터가 보호되도록 조치합니다.

설정 방법

RDS → 데이터베이스 생성 → 퍼블릭 엑세스 가능 '아니요'로 선택 → 완료



진단 기준		
	양호	프라이빗 엑세스로 설정되었을 경우
	취약	프라이빗 엑세스로 설정되어있지 않을 경우

적용 인증법

ISMS-P 2.6.1 네트워크 접근
ISMS-P 2.6.4 데이터베이스 접근
CSAP 12.1.1 데이터 분류
CSAP 12.1.4 데이터 보호

5. 데이터 보안

분류	데이터 보안	위험도	상
항목명	가명처리		

항목 설명

개인정보란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보를 말합니다. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함합니다.

가명처리는 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가정보가 없이는 특정 개인을 알아 볼 수 없도록 처리하는 것을 의미합니다. 가명처리 시 가명정보 자체만으로 특정 개인을 알아볼 수 있는 자와 추가정보 또는 다른 정보의 결합가능성을 고려할 필요가 있습니다.

가명정보는 개인정보처리자의 정당한 처리 범위 내에서 통계작성, 과학적 연구, 공익적 기록보존 등의 목적으로 정보주체의 동의 없이 처리할 수 있습니다.

- **통계작성** : 통계란 특정 집단이나 대상 등에 관하여 작성한 수량적인 정보를 의미 – 시장조사와 같은 상업적 목적의 통계 처리도 포함합니다.
- **과학적 연구** : 과학적 연구는 기술의 개발과 실증, 기초연구, 응용연구 및 민간 투자 연구 등 과학적 방법을 적용하는 연구를 의미합니다.
- **공익적 기록보존** : 공공의 이익을 위하여 지속적으로 열람할 가치가 있는 정보를 기록하여 보존하는 것을 의미합니다.

가명정보처리자는 가명정보의 활용목적 달성에 필요한 수준을 고려하여 가명처리 수준 정의를 하여야 합니다.

< 가명처리 수준 정의표 >

순번	테이블명	컬럼명	식별	처리수준
1	회원정보	회원번호	가명식별자	회원번호 + SALT 를 SHA256 암호화 후 기존 회원번호 삭제
2	회원정보	이름	식별정보	삭제
3	회원정보	ID	식별정보	삭제
4	회원정보	Password	식별정보	삭제
5	회원정보	생년월일	식별정보	삭제
6	회원정보	성별	식별정보	삭제

7	회원정보	우편번호	식별가능정보	앞에서 부터 3자리를 남긴 후 일반화
8	회원정보	핸드폰번호	식별정보	삭제
9	회원정보	이메일	식별정보	삭제
10	회원정보	신장	식별가능정보	상단 코딩 처리 (200cm 이상의 경우 → 200)
11	회원정보	체중	식별가능정보	상단 코딩 처리 (200kg 이상의 경우 → 200)
12	회원정보	보험여부	식별가능정보 (민감정보)	해부화 (Y = [1, 12, 3, 14, 5, 16, 7, 18, 9], N = [11, 2, 13, 4, 15, 6, 17, 8, 19])
13	건강정보	건강정보번호	-	삭제
14	건강정보	혈압	식별가능정보	-
15	건강정보	걸음수	식별가능정보	-
16	건강정보	심박수	식별가능정보	-
17	건강정보	혈당	식별가능정보	-
18	건강정보	체온	식별가능정보	-
19	건강정보	측정 날짜	식별가능정보	-
20	결제정보	결제정보번호	-	삭제
21	결제정보	카드사	식별가능정보	삭제
22	결제정보	카드번호	식별정보	삭제

23	결제정보	카드CVC번호	식별정보	삭제
24	결제정보	은행명	식별가능정보	삭제
25	결제정보	계좌번호	식별정보	삭제
26	결제정보	결제금액	식별가능정보	앞에서부터 2자리를 남긴 후 자릿수만큼 0을 입력 (156400 → 150000)
27	결제정보	결제날짜	식별가능정보	일반화 (YYYYMM)

가명처리는 AWS Lambda를 활용합니다. 원본DB에서 데이터가 가명처리되어 가명DB로 저장될 때 Lambda를 이용하여 가명처리합니다.
Lambda는 서버를 프로비저닝하거나 관리하지 않고도 코드를 실행할 수 있는 컴퓨팅 서비스입니다. Lambda는 고가용성 컴퓨팅 인프라에서 코드를 실행하고 서버 및 운영 체제 유지 관리, 용량 프로비저닝 및 자동 확장, 코드 모니터링 및 로깅을 비롯한 모든 컴퓨팅 리소스 관리를 수행합니다. Lambda를 사용하면 거의 모든 유형의 애플리케이션 또는 백엔드 서비스에 대한 코드를 실행할 수 있습니다.
코드를 Lambda 함수로 구성합니다. Lambda는 필요할 때만 함수를 실행하고 하루에 몇 개의 요청에서 초당 수천 개까지 자동으로 확장합니다.
Lambda를 사용하면 사용자는 자신의 코드에 대해서만 책임을 갖습니다. Lambda는 메모리, CPU, 네트워크 및 기타 리소스의 균형을 제공하는 컴퓨팅 플릿을 관리하여 코드를 실행합니다. Lambda에서는 이러한 리소스를 관리하므로 컴퓨팅 인스턴스에 로그인하거나 제공된 런타임에 운영 체제를 사용자 지정할 수 없습니다. Lambda는 사용자를 대신하여 용량 관리, 모니터링 및 Lambda 함수 로깅을 비롯한 운영 및 관리 활동을 수행합니다.

가명처리 시 가명처리 로그 기록을 남깁니다. 또한, 가명DB 접속 로그를 기록합니다.

< 가명처리 로그 기록 >

데이터베이스 설계서			
테이블 ID	RECORD_TB	**테이블유형**	일반테이블
테이블명	가명처리 로그 기록	**DB분류**	비식별화 DB

설명	가명처리 시 날짜와 메시지 기록

번호	물리명	논리명	타입	KEY	널 유무	초기값	비고
1	RECORD_ID	기록 ID	INT	PK	N		AUTO INCREMENT
2	RECORD_DATE	기록 날짜	VARCHAR(8)		N		
3	RECORD_MSG	기록 메시지	VARCHAR(20)		N		

특이사항 (형식 예시)

RECORD_ID : 1, 2, 3, 4, … (Auto Increment 사용)

RECORD_DATE : YYYYMMDD

RECORD_MSG : '비식별화 처리 성공'으로 입력됨

< 가명DB 접속 로그 기록 >

데이터베이스 설계서			
테이블 ID	ACC_RECORD_TB	**테이블유형**	일반테이블

테이블명	시스템 접속 로그 기록	DB분류	비식별화 DB
설명	시스템 접속 후 발생하는 로그를 기록		

번호	물리명	논리명	타입	KEY	널 유무	초기값	비고
1	ACC_RECORD_ID	접속 기록ID	INT	PK	N		AUTO INCREMENT
2	ACC_ID	접속 계정	VARCHAR(30)		N		
3	ACC_DATE	접속 일시	VARCHAR(50)		N		
4	ACC_PLACE	접속지 정보	VARCHAR(30)		N		
5	ACC_TARGET	정보 주체 정보	VARCHAR(10)		N		
6	ACC_WORK	수행 업무	VARCHAR(30)		N		

특이사항 (형식 예시)

ACC_RECORD_ID : 1, 2, 3, 4, ... (Auto Increment 사용)

ACC_DATE : YYYYMMDDTT:MM:SS

<table>
<tr><td></td><td colspan="4">ACC_TARGET : 처리한 정보 주체 정보를 뜻함</td></tr>
<tr><td rowspan="13">세부
설명</td><td>조항</td><td>항목번호</td><td>항목</td><td>일부내용</td></tr>
<tr><td>ISMS-P</td><td>2.5.2</td><td>사용자 식별</td><td>사용자 계정은 사용자별로 유일하게 구분할 수 있도록 식별자를 할당하고 추측 가능한 식별자 사용을 제한</td></tr>
<tr><td>ISMS-P</td><td>2.8.1</td><td>보안 요구사항 정의</td><td>정보시스템의 도입·개발·변경 시 정보보호 및 개인정보보호 관련 법적 요구사항, 최신 보안취약점, 안전한 코딩방법 등 보안 요구사항을 정의하고 적용하여야 한다.</td></tr>
<tr><td>ISMS-P</td><td>2.8.5</td><td>소스 프로그램 관리</td><td>소스 프로그램은 인가된 사용자만이 접근할 수 있도록 관리하고, 운영환경에 보관하지 않는 것을 원칙적으로 하여야 한다.</td></tr>
<tr><td>ISMS-P</td><td>2.9.4</td><td>로그 및 접속기록 관리</td><td>정보시스템에 대한 사용자 접속기록, 시스템로그, 권한부여 내역 등의 로그 유형, 보존기간, 보존방법 등을 정하고 위·변조, 도난, 분실 되지 않도록 안전하게 보존·관리하여야 한다.</td></tr>
<tr><td>ISMS-P</td><td>2.9.5</td><td>로그 및 접속기록 점검</td><td>접근 및 사용에 대한 로그 검토기준을 수립하여 주기적으로 점검하며, 문제 발생 시 사후조치를 적시에 수행하여야 한다.</td></tr>
<tr><td>ISMS-P</td><td>3.2.1</td><td>개인정보 현황관리</td><td>수집·보유하는 개인정보의 항목, 보유량, 처리 목적 및 방법, 보유기간 등 현황을 정기적으로 관리</td></tr>
<tr><td>ISMS-P</td><td>3.2.3</td><td>개인정보 표시제한 및 이용 시 보호조치</td><td>개인정보의 조회 및 출력시 용도를 특정하고 용도에 따라 출력 항목 최소화, 개인정보, 표시제한, 출력물 보호조치 등을 수행하여야 한다. 또한 빅데이터 분석, 테스트 등 데이터 처리 과정에서 개인정보가 과도하게 이용되지 않도록 업무상 반드시 필요하지 않은 개인정보는 삭제하거나 또는 식별할 수 없도록 조치하여야 한다.</td></tr>
<tr><td>ISMS-P</td><td>2.7.1</td><td rowspan="2">암호 정책 수립</td><td rowspan="2">클라우드컴퓨팅서비스에 저장 또는 전송 중인 데이터를 보호하기 위해 암호화 대상, 암호 강도(복잡도), 키관리, 암호 사용에 대한 정책을 마련하여야 한다. 또한 정책에는 개인정보 저장 및 전송 시 암호화 적용 등 암호화 관련 법적 요구사항을 반드시 반영하여야 한다.</td></tr>
<tr><td>CSAP</td><td>12.2.1</td></tr>
<tr><td>ISMS-P</td><td>13.2.3</td><td rowspan="2">시험 데이터 보안</td><td rowspan="2">시스템 시험 과정에서 운영데이터 유출을 예방하기 위해 시험데이터 생성, 이용 및 관리, 파기, 기술적 보호조치에 관한 절차를 수립하여 이행하여야 한다.</td></tr>
<tr><td>CSAP</td><td>2.8.4</td></tr>
<tr><td colspan="4">항목을 준수하기위해 AWS Lambda를 사용하여 가명처리 하드코딩을 하며, Lambda는 지정된 IAM계정으로만 접근할 수 있도록 하며 가명처리 로그 기록과 시스템 접속 로그 기록 테이블을 생성합니다. 또한, 3년이상 안전하게 보관하도록 합니다. 또한 회원번호를 식별자로 합니다.</td></tr>
<tr><td>설정
방법</td><td colspan="4">사전 준비 → 가명처리(가명처리 수준정의 및 처리) → 적정성 검토 및 추가 가명처리 → 활용 및 사후관리

- 가명처리 과정</td></tr>
</table>

1. 원본 데이터베이스 RDS 에서 테이블 내용 읽어옴
2. Select 쿼리문을 통해 회원 ID 추출
3. 파라미터 스토어에서 Salt 값 추출
4. [회원 ID + Salt] 를 SHA 256 암호화
5. 컬럼 각각 비식별화 처리
6. 가명처리 데이터베이스 테이블에 데이터 삽입
   a. if [회원 ID + Salt] 를 SHA 256 암호화한 값이 가명처리 디비의 테이블에 있으면
      → 가명처리 디비에 있는 그 회원의 데이터를 업데이트 (삭제 후 신규 값 삽입)
   b. 없으면
      → 신규 값 삽입

- **의사코드**

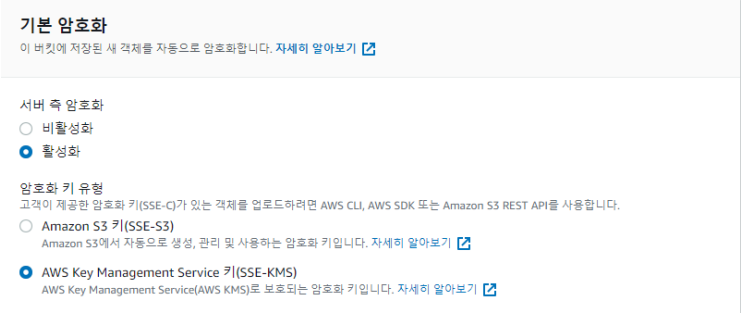
```
import random
from Cryptodome.Hash import SHA256


def top_coding(x):
        if x >= 200 :
                x의 첫번째 자리의 수는 기존 값 그대로 둠
                x의 두번째, 세번째자리의 값을 0으로 변경
                (ex. 223 → 200)
        return x

def post_code_generalization(x):
        x를 리스트화( list(x) )
        앞에서부터 3자리는 그대로 남긴 후, 뒤의 4번째, 5번째자리의 값은 제거
       (list[ : 2 ] 슬라이싱 이용)
       x를 문자열화
       return x

def pay_date_generalization(x):
        x를 리스트화( list(x) )
        앞에서부터 6자리는 그대로 남긴 후, 뒤의 7번째, 8번째자리의 값은 제거
       (list[ : 5 ] 슬라이싱 이용)
       x를 문자열화
       return x

def price_rounding(x):
        x를 리스트화( list(x) )
        x의 길이 계산
        앞에서부터 2자리는 그대로 남긴 후, 뒤의 나머지 값을 자릿수만큼 0으로 변
경
```

```
            x를 문자열화
            return x

원본 데이터 RDS에 있는 데이터 테이블 불러오기()

if 불러온 테이블 값이 NULL이 아니면 :
        회원 ID 컬럼 값 추출. (Select 쿼리문 이용)
        Parameter Store를 이용해 SALT 추출.

         # 암호화된 회원ID = (회원ID + SALT)를 SHA256으로 암호화 처리
         암호화된 회원 ID = SHA256.new(SALT)
         암호화된 회원 ID.update(회원ID.encode('utf-8'))
         암호화된 회원 ID.hexdigest()

        # 식별자 삭제 처리
        회원 ID, 이름, ID, Password, 생년월일, 성별, 핸드폰번호, 이메일,
        건강정보번호, 결제정보번호, 카드사, 카드번호, 카드CVC번호, 은행명, 계좌번호
        컬럼 삭제
        (ex. Drop(columns = ['이름'] 이용)

        # 앞에서 부터 3자리를 남긴 후 일반화
        우편번호 = post_code_generalization(우편번호)

        # 상단 코딩 처리
         신장 = top_coding(신장)
         체중 = top_coding(체중)

        # 해부화 (보험 여부를 특정 구간 값으로 변환)
         y_list = [1, 12, 3, 14, 5, 16, 7, 18, 9]
         n_list = [11, 2, 13, 4, 15, 6, 17, 8, 19]
         for i in 보험 여부 컬럼 데이터 길이 :
                if 보험 여부(i) == 'Y' :
                        보험 여부(i) = random.choice(y_list)
                else :
                        보험 여부(i) = random.choice(n_list)

        # 앞에서 부터 2자리를 남긴 후 자릿수만큼 0을 입력
        결제금액 = price_rounding(결제금액)

        # 앞에서 부터 6자리를 남긴 후 일반화
        결제날짜 = pay_date_generalization(결제날짜)
```

		가명처리한 데이터를 가명처리 RDS에 삽입 (삽입시 회원 ID는 암호화된 회원 ID로 삽입) (Insert 쿼리문 사용) 완료되었습니다 성공 메시지 출력 **else :** 테이블을 불러오지 못했습니다 오류 메시지 출력 RDS에 있는 테이블 다시 불러오기()
진단 기준	양호	가명처리가 잘 되었을 경우
	취약	가명처리가 잘 되어있지 않을 경우
적용 인증법	ISMS-P 3.2.1 개인정보 현황관리 ISMS-P 3.2.3 개인정보 표시제한 및 이용 시 보호조치 ISMS-P 2.8.1 보안 요구사항 정의 ISMS-P 2.8.5 소스 프로그램 관리 ISMS-P 2.9.4 로그 및 접속기록 관리 ISMS-P 2.9.5 로그 및 접속기록 점검 ISMS-P 2.9.6 시간 동기화 ISMS-P 2.5.2 사용자 식별 개인정보 보호법 제28조의2 제1항 개인정보 보호법 제28조의4 개인정보 보호법 제28조의5 CSAP 12.2.1 암호 정책 수립 CSAP 13.2.3 시험 데이터 보안	

<table>
<tr><td>분류</td><td colspan="3">데이터 보안</td><td>위험도</td><td>상</td></tr>
<tr><td>항목명</td><td colspan="5">KMS</td></tr>
<tr><td>항목
설명</td><td colspan="5">사내시스템에서 사용될 DB 와 모니터링에 쓰일 로그를 저장하는용도로 사용될 S3 standard 와 S3 glaicer 에 대해서 암호화 되도록하는 설정이며 Amazon S3 관리형 키(SSE-S3) 또는 AWS KMS 관리형 키(SSE-KMS)로 서버 측 암호화를 사용하여 객체를 암호화합니다.

- 이점
• 완전관리형 - 사용자가 키 사용 권한을 정의함으로써 암호화된 데이터의 액세스를 제어하는 반면 AWS KMS 는 권한을 시행하고 키의 내구성과 물리적 보안을 처리합니다.
• 중앙 집중식 키 관리 - AWS KMS 는 통합된 AWS 서비스 및 자체 애플리케이션에 걸쳐 일관적으로 키를 관리하고 정책을 정의하는 단일 제어 지점을 제공합니다. AWS Management Console 에서 또는 AWS SDK 나 CLI 를 사용하여 키에 대한 권한을 손쉽게 생성하고, 가져오고, 교체하고, 삭제하며, 관리할 수 있습니다.
• 애플리케이션의 데이터 암호화 – AWS KMS 는 AWS Encryption SDK 와 통합되어 KMS 보호 데이터 암호화 키를 사용하여 애플리케이션 내 로컬 암호화를 지원합니다. 단순한 API 를 사용함으로써 어디에서 실행하든 자체 애플리케이션에 암호화 및 키 관리를 빌드할 수도 있습니다.
• 데이터 디지털 서명 - AWS KMS 를 사용하면 비대칭 키 페어로 디지털 서명 작업을 수행하여 데이터의 무결성을 확보할 수 있습니다. 디지털 서명된 데이터의 수신자는 AWS 계정의 보유 여부와 관계없이 서명을 확인할 수 있습니다.</td></tr>
<tr><td rowspan="6">세부
설명</td><td>조항</td><td>항목번호</td><td>항목</td><td colspan="2">일부내용</td></tr>
<tr><td>ISMS-P</td><td>2.5.1</td><td>사용자 계정 관리</td><td colspan="2">접근권한을 최소한으로 부여</td></tr>
<tr><td>ISMS-P</td><td>2.7.1</td><td>암호정책 적용</td><td colspan="2">법적 요구사항을 반영한 암호화 대상,사용 적책을 수립하고 전송시 암호화를 적용</td></tr>
<tr><td>ISMS-P</td><td>2.7.2</td><td rowspan="2">암호키 관리</td><td colspan="2" rowspan="2">암호키의 안전한 생성,보관을 위한 관리절차 수립</td></tr>
<tr><td>CSAP</td><td>12.2.2</td></tr>
<tr><td>CSAP</td><td>13.1.2</td><td>인증 및 암호화 기능</td><td colspan="2">클라우드 시스템 설계 시 사용자 인증에 관한 보안요구사항을 반드시 고려하여야 하며 중요정보의 입·출력 및 송수신 과정에서 무결성, 기밀성이 요구될 경우 법적 요구사항을 고려하여야 한다.</td></tr>
<tr><td colspan="5">항목을 준수하기 위해 S3 버킷에 대해 암호화를 했으며 AES-256 이나 AWS-KMS 를 이용하여 자동으로 암호화를 진행할 수 있습니다. 중요정보의 입출력 시 SSL/TLS 의 통신방법을 통해 무결성과 기밀성을 유지합니다.</td></tr>
<tr><td>설정
방법</td><td colspan="5">- S3 암호화설정 방법</td></tr>
</table>

<table>
<tr><td></td><td colspan="2">S3 대시보드 → 버킷 → 버킷 만들기 → 기본 암호화 → SSE - S3/SSE – KMS 선택 → 완료
 

※ 자세한 설명은
https://docs.aws.amazon.com/ko_kr/kms/latest/developerguide/overview.html 참고</td></tr>
<tr><td rowspan="2">진단 기준</td><td>양호</td><td>S3설정시 KMS를 설정한 경우</td></tr>
<tr><td>취약</td><td>S3설정시 KMS를 설정하지 않은 경우</td></tr>
<tr><td>적용 인증법</td><td colspan="2">ISMS-P 2.5.1 사용자 계정 관리
ISMS-P 2.7.1 암호정책 적용
ISMS-P 2.7.2 암호키 관리
CSAP 12.2.2 암호키 관리
CSAP 13.1.2 인증 및 암호화 기능</td></tr>
</table>