

SK헬스 서비스 클라우드 전환 정보보안 컨설팅

보안요건 이행점검 보고서

2022.6.15

1조 헬썩해요

문서 이력

버전	주요내용	일자	작성자	검토자
Ver0.1.0	보고서 초안 작성	2022.06.09	고해준, 도규탁	백성광
Ver0.2.0	보고서 개요 작성 완료	2022.06.11	고해준, 도규탁	백성광
Ver1.0.0	보고서 최종 수정	2022.06.17	고해준, 도규탁	백성광

목차

I. 개요	4
1. 목적 및 배경	4
2. 점검 일정	4
3. 점검 인력	4
4. 점검 방법(수행 절차)	4
5. 점검 기준	5
6. 점검 대상	8
II. 점검결과	10
1. 점검결과 요약	10
2. 점검결과 상세	12
2.1 계정 권한 관리	12
2.2 식별 인증	16
2.3 접근 통제	19
2.4 암호화 적용	32
2.5 로깅 및 모니터링	35
2.6 보안관리	40

I. 개요

1. 목적 및 배경

SK헬스 서비스를 AWS 클라우드 환경에서 운영할 때 ISMS-P와 법률을 만족시키는 보안 요구사항 측면에서 클라우드 인프라를 점검한다. 보안요건정의서와 보안 아키텍처를 참고하여 보안 요구사항들이 충족·불충족한 지 식별하고 대책을 수립하는 데 그 목적이 있다.

2. 점검 일정

2022년 06월 08일부터 2022년 06월 16일까지 7일 간 수행하였다

분류	내용	2022년 6월								
		06.08	06.09	06.10	06.11	06.12	06.13	06.14	06.15	06.16
사전 준비	대상 범위 협의, 점검 방법 결정					휴일				
이행 점검	보안 요건 충족 여부 확인					휴일				
분석· 평가	결과 보고서 작성 및 리뷰					휴일				

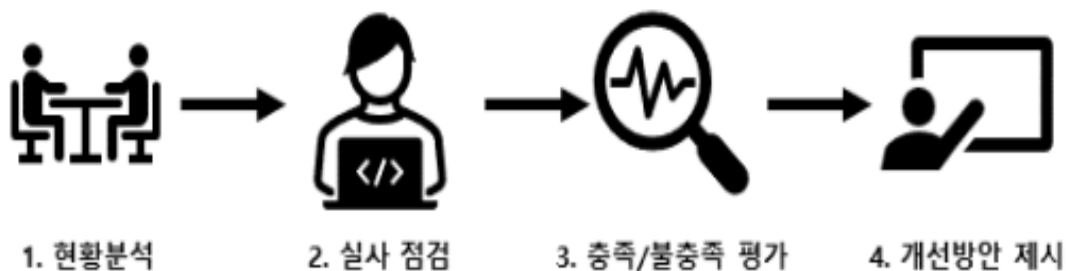
[표 1] 점검 일정

3. 점검 인력

이름	소속	파트	담당 업무
고해준	1 조 헬쓱해요	보안요건이행점검	보안요건이행점검 및 조치방안분석
도규탁	1 조 헬쓱해요	보안요건이행점검	보안요건이행점검 및 문서작성

[표 2] 점검 인력

4. 점검 방법(수행 절차)



[그림 1] 점검 절차

1) 현황분석

보안 요건 점검 대상들을 파악하고, AWS 클라우드에서 제공하는 보안 서비스(eg. WAF, Network Firewall, Cloud Watch 등)들에 대해 전반적으로 분석한다.

2) 실사 점검

SK헬스 서비스의 클라우드 인프라를 실사하여 보안 요건 항목들을 점검한다.

3) 충족/불충족 평가

SK헬스 서비스 클라우드 인프라를 점검한 것을 분석하여 보안 요구 항목 충족 여부를 판단한다.

4) 개선방안 제시

충족/불충족 평가를 통해 도출된 결과를 통해 불충족 항목에 대해 보안설정 가이드라인을 제공한다.

5. 점검 기준

법률과 ISMS-P 인증의 기술적 보호조치 항목을 분류하여 보안요건정의서를 작성하였다. 이를 기준으로 보안요건정의 항목들이 SK헬스 서비스의 클라우드 인프라에서 충족하는지 점검을 이행한다.

보안요건정의서에서 요구하는 항목들을 나타내고 있으며, 상세 현황은 다음과 같다.

보안코드	영역	세부영역	항목명
Sec101	계정·권한 관리	사용자 계정 관리	개인정보 및 중요정보에 대한 비인가 사용자 접근 권한 설정
Sec102		특수 계정 및 권한 관리	특수 계정의 권한 식별 및 관리
Sec103		계정 비밀번호 관리	사용자 및 관리자 계정 비밀번호 관리
Sec104		접근 권한 검토	사용자 계정의 접근 권한 이력 점검
Sec105		보안시스템 관리	예외 정책 사용자 권한 관리

Sec201	식별·인증	사용자 인증	사용자 접근에 대한 인증 수단 적용
Sec202		외부 접근 사용자 인증	외부 접근에 대한 사용자 인증
Sec203		사용자 식별	사용자 계정 식별자 할당
Sec301	접근 통제	네트워크 접근	네트워크 비인가 사용자 접근 통제
Sec302			네트워크 영역 분리 및 통제
Sec303			외부 네트워크 접근 통제
Sec304			무선 네트워크 접근 통제
Sec305		정보시스템 접근	정보시스템에 대한 접근수단 정의 및 접근 통제
Sec306			정보시스템 접근에 대한 사용자 인증 통제 적용
Sec307			정보시스템 접속 차단
Sec308			서비스에 따른 독립된 서버 운영
Sec309			정보시스템 관계없는 서비스 차단
Sec310		응용프로그램 접근	응용프로그램 접근 권한 제한
Sec311			응용프로그램 중요정보의 노출 최소화
Sec312			응용프로그램 세션 관리
Sec313			관리자 전용 응용프로그램 비인가자 접근 통제
Sec314		데이터베이스 접근	데이터베이스 접근 통제
Sec315		원격접근 통제	단말기 접근 통제
Sec316		인터넷 접속 통제	외부 인터넷 접속 통제
Sec317			망분리 적용 및 통제
Sec318		보안시스템 통제	보안시스템 비인가자 접근 통제
Sec401	암호화 적용	중요정보 암호화	개인정보 및 주요정보에 대한 암호화 적용
Sec402		암호키 관리	암호키 접근 권한 관리
Sec403		비밀번호 암호화	비밀번호 암호화 적용
Sec501	로깅 및 모니터링	로그 관리	로그 기록 보관 및 관리
Sec502			로그 기록 접근 권한 설정
Sec503			정보시스템 이상징후 인지를 위한 모니터링 절차 이행
Sec504			로그 시간 동기화
Sec505		개인정보보호	이상행위 발생 시 신속한 분석 및 점검
Sec506			개인정보처리시스템 법률 준수 검토 및 관리
Sec601	보안 관리	시험과 운영 환경 분리	시험 시스템과 운영시스템의 분리
Sec602		시험 데이터 보안	실제 운영 데이터의 사용 제한
Sec603		장애 관리	정보시스템의 장애 관리
Sec604		클라우드 보안	클라우드 서비스 보안 통제 정책 이행
Sec605			클라우드 서비스 관리자 권한 보호대책 적용

Sec606		공개서버 보안	공개서버 DMZ 설치 및 보안시스템 보호
Sec607		패치관리	공개 인터넷 접속을 통한 패치 제한
Sec608		악성코드 통제	악성코드 보호대책 이행
Sec609		취약점 점검 및 조치	최신 보안 취약점 분석 및 조치

[표 6] 보안요건정의서 항목 리스트

ISMS-P는 정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인터넷 진흥원 또는 인증기관이 증명하는 제도이다. ISMS-P항목 중 관리적·물리적 보호조치는 제외하고 기술적 보호조치 항목만을 대상으로 점검한다.

통합인증	보호조치 분류	점검 여부
ISMS-P 인증항목	관리적 보호조치 항목	N/A
	물리적 보호조치 항목	N/A
	기술적 보호조치 항목	Y

[표 3] ISMS-P 보호조치 분류 항목

통합인증	분야 (인증기준 개수)		기술적 보호조치 항목 개수
관리 체계 수립 및 운영(16)	1.1 관리체계 기반 마련(6)	1.3 관리체계 운영(3)	0개
	1.2 위험관리(4)	1.4 관리체계 점검 및 개선(3)	
보호대책 요구사항 (64)	2.1 정책, 조직, 자산 관리(3)	2.7 암호화 적용(2)	34개
	2.2 인적 보안(6)	2.8 정보시스템 도입 및 개발 보안(6)	
	2.3 외부자 보안(4)	2.9 시스템 및 서비스 운영관리(7)	
	2.4 물리 보안(7)	2.10 시스템 및 서비스 보안관리(9)	
	2.5 인증 및 권한 관리(6)	2.11 사고 예방 및 대응(5)	
	2.6 물리 통제(7)	2.12 재해복구(2)	
개인정보 처리 단계 별 요구사항 (22)	3.1 개인정보 수집 시 보호조치(7)	3.3 개인정보 제공 시 보호조치(3)	1개
	3.2 개인정보 보유 및 이용 시 보호조치(5)	3.4 개인정보 파기 시 보호조치(4)	
	3.5 정보주체 권리보호(3)		

[표 4] ISMS-P기준

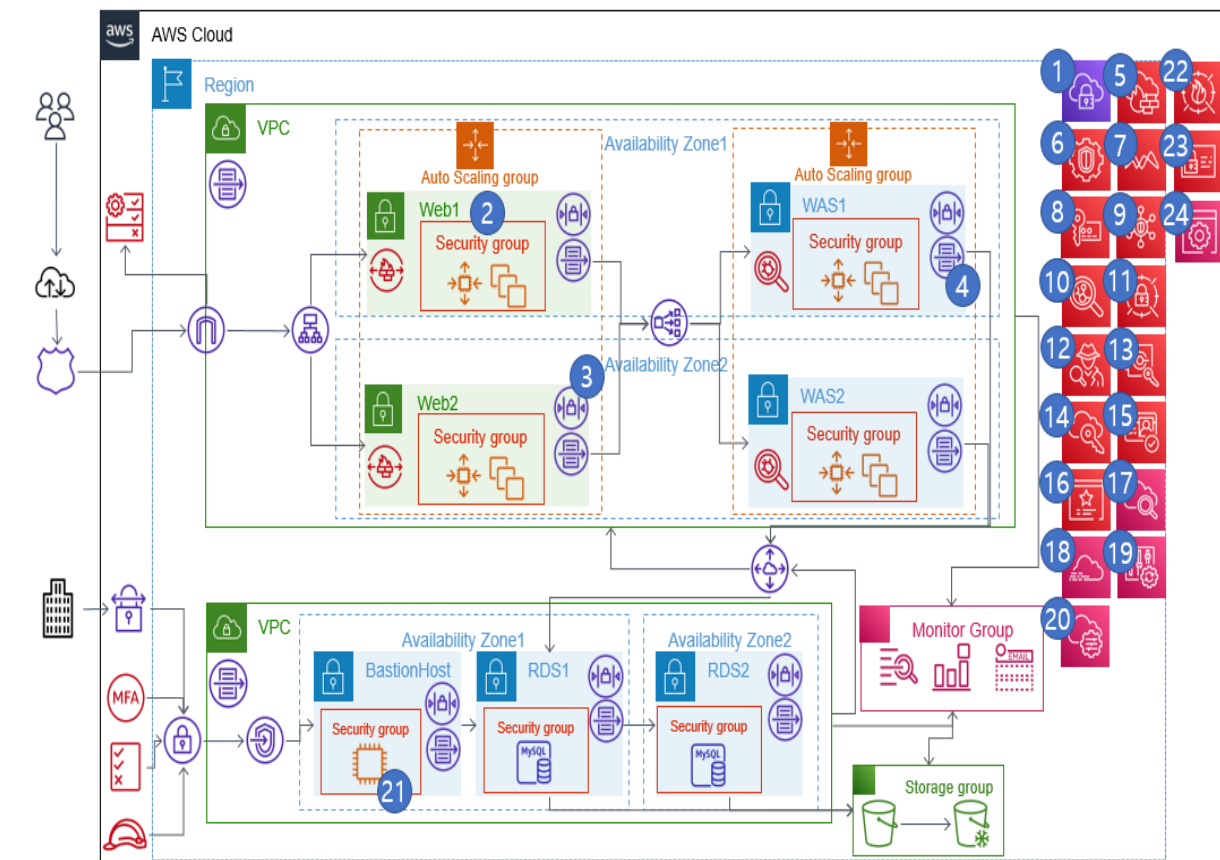
법	시행령	고시
---	-----	----

개인정보 보호법	개인정보 보호법 시행령	개인정보의 기술적·관리적 보호조치
		개인정보의 안정성 확보 조치
정보통신망법	정보통신망법 시행령	정보보호조치에 관한 지침
위치정보법	위치정보법 시행령	
클라우드컴퓨팅법		클라우드컴퓨팅서비스 정보보호에 관한 기준

※ SK헬스 서비스의 인프라 단계에서 개인정보 및 중요정보 보호를 위해 준수해야 할 법률
[표 5] 법률 분류 항목

6. 점검 대상

SK헬스 서비스 클라우드 인프라를 대상으로 보안요건 항목 리스트의 요구사항들을 점검한다. SK헬스 서비스의 클라우드 구성도와 AWS 보안 서비스는 다음과 같다. 운영체제, 어플리케이션, DBMS는 점검 대상에서 제외한다.



[그림 2] SK헬스 클라우드 보안 구성도

번호	이름	번호	이름
1	AWS VPN	13	AWS Single Sign-On
2	Security Group	14	AWS CloudHSM
3	Network Access Control List	15	Amazon Cognito
4	VPC Flow Log	16	AWS Certificate Manager
5	AWS Network Firewall	17	Amazon CloudWatch
6	Amazon GuardDuty	18	AWS CloudTrail
7	Amazon Macie	19	AWS Config
8	AWS Key Management Service	20	AWS Systems Manager
9	AWS Security Hub	21	Bastion Host
10	Amazon Inspector	22	AWS WAF
11	AWS Secrets Manager	23	AWS Identity and Access Management
12	Amazon Detective	24	AWS Management Console

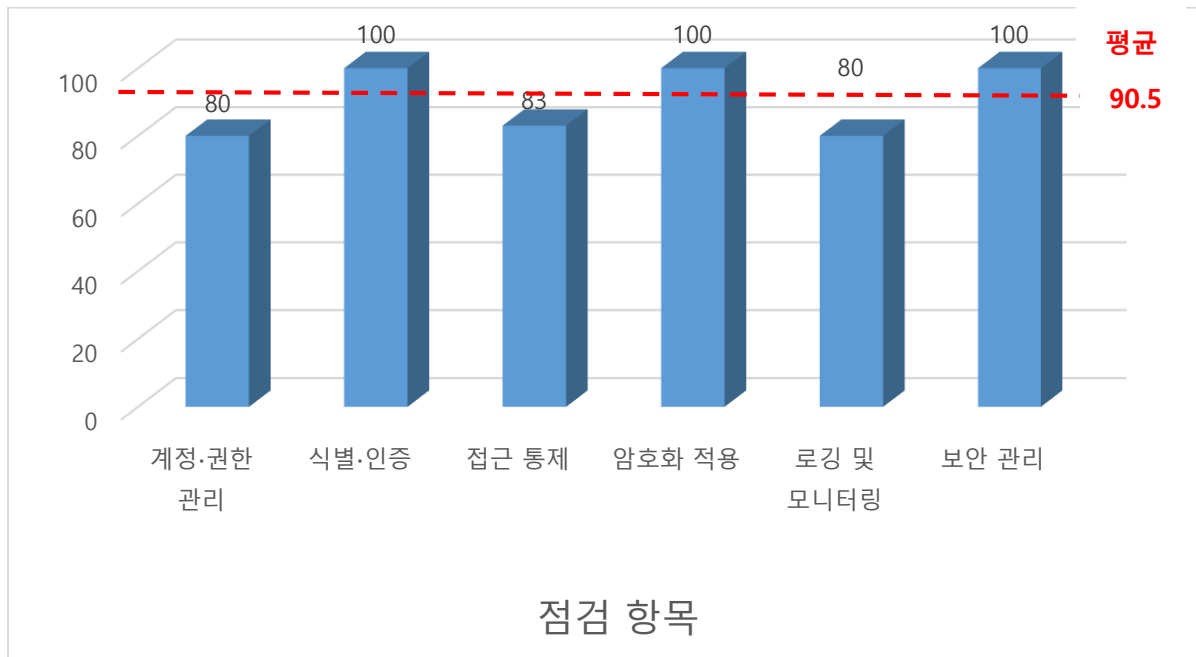
[표 8] AWS 보안 서비스

II. 점검결과

1. 점검결과 요약

점검 대상인 SK헬스의 클라우드 인프라가 ISMS- P의 기술적 보호조치 항목들과 법률들을 기준으로 정보보호 관점에서 안전하게 구성 되어있는지, 보안 요건 점검 항목 리스트를 살펴 해당 요구사항이 이행되었는지 점검한 결과이다.

항목 별 점검 결과 평균 이행률은 90.5%이고 식별·인증, 암호화 적용, 보안 관리 항목은 평균 이행률보다 높은 100%로 충족되었다. 반면 계정·권한 관리 80%, 접근 통제 83%, 로깅 및 모니터링 80%로 평균인 90.5%보다 이행률이 낮게 책정되었다.



[그림 2] 이행 점검 결과 그래프

점검 항목별로 구분하여 보안요건항목을 충족·불충족으로 나누어 점검하였다. 이행 점검 통계는 아래와 같다.

이행 점검 통계			
구분	점검 항목		
	전체	충족	불충족
계정·권한 관리	5	4	1
식별·인증	3	3	-
접근 통제	18	15	3
암호화 적용	3	3	-
로그 및 모니터링	5	4	1
보안 관리	9	9	-
통계	44	39	5

[표 9] 이행 점검 통계

2. 점검결과 상세

2.1 계정 권한 관리

사용자 계정 관리

점검 항목	Sec101		점검	충족
점검 기준	분류	사용자 계정 관리	결과	불충족
	항목명	개인정보 및 중요정보에 대한 비인가 사용자 접근 권한 설정		
	요구사항 내용	정보시스템과 개인정보 및 중요정보에 접근할 수 있는 사용자 계정 및 접근 권한 생성·등록·변경 시 직무 별 접근 권한 분류 체계에 따라 업무상 필요한 최소한의 권한만을 부여하고 있는가?		
점검 현황	현재 IAM에서 확인 가능한 사용자 계정 중 일부 계정(eg. SK101-003)은 일반계정임에도 불구하고 AdministratorAccess 권한이 부여되어 있다.			
보안요건 조치 방안	사용자 접근 권한 부여 방법 1. 접근 분류 체계에 따라 직무에 적합한 권한을 부여한다. 2. SK101-003에 대한 AdministratorAccess 권한을 제거하고 일반 사용자가 접근할 수 있는 범위를 설정한다. 3. IAM의 액세스 관리에서 알맞은 정책과 권한을 설정하고 직무에 맞는 계정을 선택한다.			

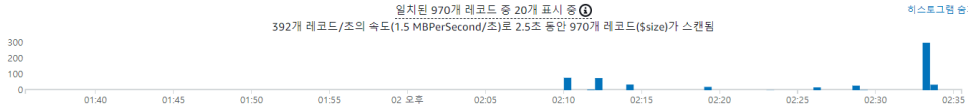
특수 계정 및 권한 관리

점검 항목	Sec102		점검 결과	충족																			
점검 기준	분류	특수 계정 및 권한 관리		불충족																			
	항목명	특수 계정의 권한 식별 및 관리																					
	요구사항 내용	특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도의 목록으로 관리하고 있는가?																					
점검 현황	IAM의 사용자 그룹으로 특수 목적을 위한 계정 분류 및 관리하고 있다.																						
	<div><div>IAM > 사용자 그룹</div><div><div>사용자 그룹 (3) 정보</div><div>사용자 그룹은 IAM 사용자의 할색선입니다. 그룹을 사용하여 사용자 할색선에 대한 권한을 지정할 수 있습니다.</div><div><div><div>Q 필터 속성 또는 그룹 이름을 기준으로 사용자 그룹을 필터링하고 Enter를 누릅니다.</div><div>< 1 ></div></div><table><thead><tr><th><input type="checkbox"/></th><th>그룹 이름</th><th>사용자</th><th>권한</th><th>생성 시간</th></tr></thead><tbody><tr><td><input type="checkbox"/></td><td>CostManagers</td><td>1</td><td>✔ 정의됨</td><td>10개월 전</td></tr><tr><td><input type="checkbox"/></td><td>sk-health</td><td>6</td><td>✔ 정의됨</td><td>2개월 전</td></tr><tr><td><input type="checkbox"/></td><td>skhealth_IT</td><td>1</td><td>✔ 정의됨</td><td>4일 전</td></tr></tbody></table></div></div></div>				<input type="checkbox"/>	그룹 이름	사용자	권한	생성 시간	<input type="checkbox"/>	CostManagers	1	✔ 정의됨	10개월 전	<input type="checkbox"/>	sk-health	6	✔ 정의됨	2개월 전	<input type="checkbox"/>	skhealth_IT	1	✔ 정의됨
<input type="checkbox"/>	그룹 이름	사용자	권한	생성 시간																			
<input type="checkbox"/>	CostManagers	1	✔ 정의됨	10개월 전																			
<input type="checkbox"/>	sk-health	6	✔ 정의됨	2개월 전																			
<input type="checkbox"/>	skhealth_IT	1	✔ 정의됨	4일 전																			
보안요건 조치 방안	공 란																						

계정 비밀번호 관리

점검 항목	Sec103		점검	충족
점검 기준	분류	계정 비밀번호 관리	결과	불충족
	항목명	사용자 및 관리자 계정 비밀번호 관리		
	요구사항 내용	사용자, 관리자 계정을 안전한 비밀번호를 설정하여 관리하고 있는가?		
점검 현황	IAM을 통해 비밀번호 정책을 수립하여 안전하게 관리하고 있다.			
	<div><div>▼ 비밀번호 정책</div><div>암호 정책은 IAM 사용자가 설정할 수 있는 암호의 유형을 정의하는 일련의 규칙입니다. 자세히 알아보기</div><div>비밀번호 정책</div><div>이 AWS 계정은 다음과 같은 기본 암호 정책을 사용합니다.</div><div><div><div><div>• 최소 암호 길이는 8자</div><div>• 대문자, 소문자, 숫자 및 !@#\$%^&*()_+ - = []{} ' 문자 유형 조합 중 최소 3개를 포함합니다.</div><div>• AWS 계정 이름 또는 이메일 주소와 동일할 수 없음</div></div></div><div><div>암호 정책 변경</div></div></div></div>			
점검 현황	<div>Cognito를 통해 사용자, 관리자 계정의 비밀번호 강도를 설정하여 관리하고 있다.</div> <div><div><div><div><div>사용자 풀 연동 자격 증명</div><div>SK-Health</div></div><div><div>일반 설정</div><div>사용자 및 그룹</div><div>속성</div><div>정책</div><div>MFA과확인</div><div>고급 보안</div><div>예시치 사용자 지향</div><div>태그</div><div>디바이스</div><div>앱 클라이언트</div><div>분석</div><div>앱 통합</div><div>앱 클라이언트 설정</div><div>도메인 이름</div><div>UI 사용자 지향</div><div>리소스 서버</div><div>연동</div><div>자격 증명 공급자</div><div>속성 매핑</div></div><div><div>최소 길이</div><div>8</div><div><div><div><div><input checked="" type="checkbox"/> 숫자 요구</div><div><input checked="" type="checkbox"/> 특수 문자 요구</div><div><input checked="" type="checkbox"/> 대문자 요구</div><div><input checked="" type="checkbox"/> 소문자 요구</div></div></div><div><div><input type="radio"/> 관리자만 사용자를 생성하도록 허용</div><div><input checked="" type="radio"/> 사용자가 가입할 수 있도록 허용</div></div></div><div><div>어떤 암호 강도를 요구하시겠습니까?</div><div>관리자만 사용자를 생성하도록 하거나 사용자의 직접 가입을 허용하도록 선택할 수 있습니다. 자세히 알아보기</div><div>사용자 가입을 허용하시겠습니까?</div><div>관리자가 설정한 임시 암호를 얼마 동안 사용하지 않으면 만료되도록 할지 선택할 수 있습니다. 여기에는 관리자가 생성한 계정이 포함됩니다.</div><div>관리자가 설정한 임시 암호를 얼마 동안 사용하지 않으면 만료되도록 할지 선택할 수 있습니다. 여기에는 관리자가 생성한 계정이 포함됩니다.</div><div><div>만료일까지 남은 일수</div><div>7</div></div><div><div>취소</div><div>변경 내용 저장</div></div></div></div></div></div></div>			
보안요건 조치 방안	공 란			

접근 권한 검토

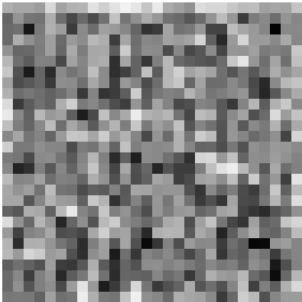
점검 항목		Sec104		점검 결과	충족										
점검 기준	분류	접근 권한 검토			불충족										
	항목명	사용자 계정의 접근 권한 이력 점검													
	요구사항 내용	정보시스템과 개인정보 및 중요정보에 대한 사용자 계정 및 접근 권한 생성·등록·부여·이용·변경·말소 등의 이력을 점검하고 있는가?													
점검 현황		CloudTrail을 통해 사용자 계정 접근 권한 변경 등 이력을 로그로 남겨 CloudWatch Log로 보내고 있다.													
		<div><div>로그</div><div>시각화</div><div>결과 내보내기 ▼</div><div>대시보드에 추가</div><div>🔍</div></div> <div><div>일치된 970개 레코드 중 20개 표시 중 ①</div><div>392개 레코드/초의 속도(1.5 MBPerSecond/초)로 2.5초 동안 970개 레코드(\$size)가 스캔됨</div><div>히스토그램 보기</div><div><table><thead><tr><th>@timestamp</th><th>@message</th></tr></thead><tbody><tr><td>1 2022-06-15T14:34:18.77...</td><td>{"eventVersion":"1.08","eventName":"2022-06-15T05:05:002","awsRegion":"us-east-1","eventID":"2b134dd6-8f38-4946-aaa4-41c013b5a319","eventType":"AwsCloudTrail...</td></tr><tr><td>2 2022-06-15T14:34:17.49...</td><td>{"eventVersion":"1.08","userIdentity":{"type":"AWSService","invokedBy":"cloudtrail.amazonaws.com"},"eventName":"2022-06-15T05:29:072","eventSource":"s3.amazo...</td></tr><tr><td>3 2022-06-15T14:34:17.49...</td><td>{"eventVersion":"1.08","userIdentity":{"type":"AWSService","invokedBy":"cloudtrail.amazonaws.com"},"eventName":"2022-06-15T05:31:332","eventSource":"s3.amazo...</td></tr><tr><td>4 2022-06-15T14:34:17.49...</td><td>{"eventVersion":"1.08","userIdentity":{"type":"AWSService","invokedBy":"cloudtrail.amazonaws.com"},"eventName":"2022-06-15T05:31:482","eventSource":"s3.amazo...</td></tr><tr><td>5 2022-06-15T14:34:17.49...</td><td>{"eventVersion":"1.08","userIdentity":{"type":"AWSService","invokedBy":"cloudtrail.amazonaws.com"},"eventName":"2022-06-15T05:32:012","eventSource":"s3.amazo...</td></tr></tbody></table></div></div>				@timestamp	@message	1 2022-06-15T14:34:18.77...	{"eventVersion":"1.08","eventName":"2022-06-15T05:05:002","awsRegion":"us-east-1","eventID":"2b134dd6-8f38-4946-aaa4-41c013b5a319","eventType":"AwsCloudTrail...	2 2022-06-15T14:34:17.49...	{"eventVersion":"1.08","userIdentity":{"type":"AWSService","invokedBy":"cloudtrail.amazonaws.com"},"eventName":"2022-06-15T05:29:072","eventSource":"s3.amazo...	3 2022-06-15T14:34:17.49...	{"eventVersion":"1.08","userIdentity":{"type":"AWSService","invokedBy":"cloudtrail.amazonaws.com"},"eventName":"2022-06-15T05:31:332","eventSource":"s3.amazo...	4 2022-06-15T14:34:17.49...	{"eventVersion":"1.08","userIdentity":{"type":"AWSService","invokedBy":"cloudtrail.amazonaws.com"},"eventName":"2022-06-15T05:31:482","eventSource":"s3.amazo...
@timestamp	@message														
1 2022-06-15T14:34:18.77...	{"eventVersion":"1.08","eventName":"2022-06-15T05:05:002","awsRegion":"us-east-1","eventID":"2b134dd6-8f38-4946-aaa4-41c013b5a319","eventType":"AwsCloudTrail...														
2 2022-06-15T14:34:17.49...	{"eventVersion":"1.08","userIdentity":{"type":"AWSService","invokedBy":"cloudtrail.amazonaws.com"},"eventName":"2022-06-15T05:29:072","eventSource":"s3.amazo...														
3 2022-06-15T14:34:17.49...	{"eventVersion":"1.08","userIdentity":{"type":"AWSService","invokedBy":"cloudtrail.amazonaws.com"},"eventName":"2022-06-15T05:31:332","eventSource":"s3.amazo...														
4 2022-06-15T14:34:17.49...	{"eventVersion":"1.08","userIdentity":{"type":"AWSService","invokedBy":"cloudtrail.amazonaws.com"},"eventName":"2022-06-15T05:31:482","eventSource":"s3.amazo...														
5 2022-06-15T14:34:17.49...	{"eventVersion":"1.08","userIdentity":{"type":"AWSService","invokedBy":"cloudtrail.amazonaws.com"},"eventName":"2022-06-15T05:32:012","eventSource":"s3.amazo...														
보안요건 조치 방안		공 란													

보안 시스템 관리

점검 항목	Sec105		점검	충족																	
점검 기준	분류	보안시스템 관리	결과	불충족																	
	항목명	예외 정책 사용자 권한 관리																			
	요구사항 내용	보안시스템의 예외 정책 등록에 대하여 절차에 따라 관리하고 있으며, 예외 정책 사용자에게 대하여 최소한의 권한으로 관리하고 있는가?																			
점검 현황	IAM에서 Network Firewall에 대한 정책을 생성하고 보안 시스템의 예외 정책 사용자에게 읽기 권한만 부여하여 관리하고 있다.																				
	<div><div>로그</div><div>시각화</div><div>결과 내보내기 ▼</div><div>대시보드에 추가</div><div>🔗</div></div> <div><div>일치된 970개 레코드 중 20개 표시 중 ④</div><div>392개 레코드/초의 속도(1.5 MBPerSecond/초)로 2.5초 동안 970개 레코드(\$size)가 스캔됨</div><div>히스토그램 숨기기</div><div><table><thead><tr><th>#</th><th>@timestamp</th><th>@message</th></tr></thead><tbody><tr><td>▶ 1</td><td>2022-06-15T14:34:18.77...</td><td>{ "eventVersion": "1.08", "eventTime": "2022-06-15T05:05:00Z", "awsRegion": "us-east-1", "eventID": "2b134dd6-8f38-4946-aaa4-41c013b56319", "eventType": "AwsCloudTrail...</td></tr><tr><td>▶ 2</td><td>2022-06-15T14:34:17.49...</td><td>{ "eventVersion": "1.08", "userIdentity": { "type": "AWSService", "invokedBy": "cloudtrail.amazonaws.com" }, "eventTime": "2022-06-15T05:29:07Z", "eventSource": "s3.amazo...</td></tr><tr><td>▶ 3</td><td>2022-06-15T14:34:17.49...</td><td>{ "eventVersion": "1.08", "userIdentity": { "type": "AWSService", "invokedBy": "cloudtrail.amazonaws.com" }, "eventTime": "2022-06-15T05:31:33Z", "eventSource": "s3.amazo...</td></tr><tr><td>▶ 4</td><td>2022-06-15T14:34:17.49...</td><td>{ "eventVersion": "1.08", "userIdentity": { "type": "AWSService", "invokedBy": "cloudtrail.amazonaws.com" }, "eventTime": "2022-06-15T05:31:48Z", "eventSource": "s3.amazo...</td></tr><tr><td>▶ 5</td><td>2022-06-15T14:34:17.49...</td><td>{ "eventVersion": "1.08", "userIdentity": { "type": "AWSService", "invokedBy": "cloudtrail.amazonaws.com" }, "eventTime": "2022-06-15T05:32:01Z", "eventSource": "s3.amazo...</td></tr></tbody></table></div></div>				#	@timestamp	@message	▶ 1	2022-06-15T14:34:18.77...	{ "eventVersion": "1.08", "eventTime": "2022-06-15T05:05:00Z", "awsRegion": "us-east-1", "eventID": "2b134dd6-8f38-4946-aaa4-41c013b56319", "eventType": "AwsCloudTrail...	▶ 2	2022-06-15T14:34:17.49...	{ "eventVersion": "1.08", "userIdentity": { "type": "AWSService", "invokedBy": "cloudtrail.amazonaws.com" }, "eventTime": "2022-06-15T05:29:07Z", "eventSource": "s3.amazo...	▶ 3	2022-06-15T14:34:17.49...	{ "eventVersion": "1.08", "userIdentity": { "type": "AWSService", "invokedBy": "cloudtrail.amazonaws.com" }, "eventTime": "2022-06-15T05:31:33Z", "eventSource": "s3.amazo...	▶ 4	2022-06-15T14:34:17.49...	{ "eventVersion": "1.08", "userIdentity": { "type": "AWSService", "invokedBy": "cloudtrail.amazonaws.com" }, "eventTime": "2022-06-15T05:31:48Z", "eventSource": "s3.amazo...	▶ 5	2022-06-15T14:34:17.49...
#	@timestamp	@message																			
▶ 1	2022-06-15T14:34:18.77...	{ "eventVersion": "1.08", "eventTime": "2022-06-15T05:05:00Z", "awsRegion": "us-east-1", "eventID": "2b134dd6-8f38-4946-aaa4-41c013b56319", "eventType": "AwsCloudTrail...																			
▶ 2	2022-06-15T14:34:17.49...	{ "eventVersion": "1.08", "userIdentity": { "type": "AWSService", "invokedBy": "cloudtrail.amazonaws.com" }, "eventTime": "2022-06-15T05:29:07Z", "eventSource": "s3.amazo...																			
▶ 3	2022-06-15T14:34:17.49...	{ "eventVersion": "1.08", "userIdentity": { "type": "AWSService", "invokedBy": "cloudtrail.amazonaws.com" }, "eventTime": "2022-06-15T05:31:33Z", "eventSource": "s3.amazo...																			
▶ 4	2022-06-15T14:34:17.49...	{ "eventVersion": "1.08", "userIdentity": { "type": "AWSService", "invokedBy": "cloudtrail.amazonaws.com" }, "eventTime": "2022-06-15T05:31:48Z", "eventSource": "s3.amazo...																			
▶ 5	2022-06-15T14:34:17.49...	{ "eventVersion": "1.08", "userIdentity": { "type": "AWSService", "invokedBy": "cloudtrail.amazonaws.com" }, "eventTime": "2022-06-15T05:32:01Z", "eventSource": "s3.amazo...																			
보안요건 조치 방안	공 란																				

2.2 식별 인증

사용자 인증

점검 항목	Sec201		점검 결과	충족
점검 기준	분류	사용자 인증		불충족
	항목명	사용자 접근에 대한 인증 수단 적용		
	요구사항 내용	정보시스템 및 개인정보처리시스템에 대한 접근 시 사용자 인증 수단(인증서, OTP등)을 사용하고 있는가?		
점검 현황	IAM의 MFA 추가 인증을 통해서 사용자 인증 수단을 추가적으로 사용하고 있다.			
	<div><div>가상 MFA 디바이스 설정</div><div><div>2. 가상 MFA 앱 및 디바이스의 카메라를 사용하여 QR 코드 스캔</div><div><div></div><div>또는 비밀 키를 입력할 수 있습니다. 비밀 키 표시</div></div><div><div>3. 아래에 2개의 연속된 MFA 코드 입력</div><div><div>MFA 코드 1</div><div>MFA 코드 2</div></div></div><div><div>취소</div><div>이전</div><div>MFA 할당</div></div></div></div>			
보안요건 조치 방안	공 란			

외부 사용자 인증

점검 항목	Sec202		점검	충족								
점검 기준	분류	사용자 인증	결과	불충족								
	항목명	외부 접근 사용자 인증										
	요구사항 내용	정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 법적 요구사항에 따라 안전한 인증 수단 또는 안전한 접속 수단을 적용하고 있는가?										
점검 현황	Client VPN 엔드포인트를 설정하여 외부에서 Bastion Host에 접근하기 위한 안전한 수단을 제공하고 있다.											
	<div>클라이언트 VPN 엔드포인트 (1/1) 정보<div><div><div><div><div><div></div></div></div><div><div>작업 ▼</div></div><div><div>클라이언트 구성 다운로드</div></div><div><div>클라이언트 VPN 엔드포인트 생성</div></div></div></div><div><div><div><div><div></div></div><div>클라이언트 VPN 엔드포인트 필터링</div></div><div><div>< 1 ></div><div><div></div></div></div></div></div></div></div>											
	<table><tr><th>Name ▼</th><th>클라이언트 VPN 엔드포인트 ID ▼</th><th>상태 ▼</th><th>클라이언트 CIDR ▼</th></tr><tr><td><div><div></div>SK-Health-Client-VPN</div></td><td>cvpn-endpoint-09a0d0498acb32cb0</td><td><div><div></div>Pending-associate</div></td><td>192.160.0.0/20</td></tr></table>				Name ▼	클라이언트 VPN 엔드포인트 ID ▼	상태 ▼	클라이언트 CIDR ▼	<div><div></div>SK-Health-Client-VPN</div>	cvpn-endpoint-09a0d0498acb32cb0	<div><div></div>Pending-associate</div>	192.160.0.0/20
Name ▼	클라이언트 VPN 엔드포인트 ID ▼	상태 ▼	클라이언트 CIDR ▼									
<div><div></div>SK-Health-Client-VPN</div>	cvpn-endpoint-09a0d0498acb32cb0	<div><div></div>Pending-associate</div>	192.160.0.0/20									
보안요건 조치 방안	공 란											

사용자 식별

점검 항목	Sec203		점검	충족																																							
점검 기준	분류	사용자 식별	결과	불충족																																							
	항목명	사용자 계정 식별자 할당																																									
	요구사항 내용	정보시스템 및 개인정보처리시스템에서 사용자 및 개인정보취급자를 유일하게 구분할 수 있는 식별자를 할당하고 있는가?																																									
점검 현황	Cognito를 통해서 사용자에게 대한 식별자를 할당해서 개인정보 취급자 및 사용자를 구분하고 있다.																																										
	<div>어떤 표준 속성을 필수 사항으로 지정하겠습니까?</div> <div>모든 표준 속성을 사용자 프로필에 사용할 수 있지만, 선택한 속성이 가입에 필요한 필수 속성으로 지정됩니다. 풀이 생성된 후에는 이러한 필수 사항을 변경할 수 없습니다. 별칭으로 사용할 속성을 선택하면 사용자가 해당 값 또는 사용자 이름을 이용해 로그인할 수 있습니다. 속성에 대해 자세히 알아보기.</div> <table><thead><tr><th>필수 사항</th><th>속성</th><th>필수 사항</th><th>속성</th></tr></thead><tbody><tr><td><input type="checkbox"/></td><td>address</td><td><input checked="" type="checkbox"/></td><td>nickname</td></tr><tr><td><input type="checkbox"/></td><td>birthdate</td><td><input type="checkbox"/></td><td>phone number</td></tr><tr><td><input checked="" type="checkbox"/></td><td>email</td><td><input type="checkbox"/></td><td>picture</td></tr><tr><td><input type="checkbox"/></td><td>family name</td><td><input type="checkbox"/></td><td>preferred username</td></tr><tr><td><input type="checkbox"/></td><td>gender</td><td><input type="checkbox"/></td><td>profile</td></tr><tr><td><input type="checkbox"/></td><td>given name</td><td><input type="checkbox"/></td><td>zoneinfo</td></tr><tr><td><input type="checkbox"/></td><td>locale</td><td><input type="checkbox"/></td><td>updated at</td></tr><tr><td><input type="checkbox"/></td><td>middle name</td><td><input type="checkbox"/></td><td>website</td></tr><tr><td><input checked="" type="checkbox"/></td><td>name</td><td></td><td></td></tr></tbody></table>				필수 사항	속성	필수 사항	속성	<input type="checkbox"/>	address	<input checked="" type="checkbox"/>	nickname	<input type="checkbox"/>	birthdate	<input type="checkbox"/>	phone number	<input checked="" type="checkbox"/>	email	<input type="checkbox"/>	picture	<input type="checkbox"/>	family name	<input type="checkbox"/>	preferred username	<input type="checkbox"/>	gender	<input type="checkbox"/>	profile	<input type="checkbox"/>	given name	<input type="checkbox"/>	zoneinfo	<input type="checkbox"/>	locale	<input type="checkbox"/>	updated at	<input type="checkbox"/>	middle name	<input type="checkbox"/>	website	<input checked="" type="checkbox"/>	name	
필수 사항	속성	필수 사항	속성																																								
<input type="checkbox"/>	address	<input checked="" type="checkbox"/>	nickname																																								
<input type="checkbox"/>	birthdate	<input type="checkbox"/>	phone number																																								
<input checked="" type="checkbox"/>	email	<input type="checkbox"/>	picture																																								
<input type="checkbox"/>	family name	<input type="checkbox"/>	preferred username																																								
<input type="checkbox"/>	gender	<input type="checkbox"/>	profile																																								
<input type="checkbox"/>	given name	<input type="checkbox"/>	zoneinfo																																								
<input type="checkbox"/>	locale	<input type="checkbox"/>	updated at																																								
<input type="checkbox"/>	middle name	<input type="checkbox"/>	website																																								
<input checked="" type="checkbox"/>	name																																										
보안요건 조치 방안	공 란																																										

2.3 접근 통제

네트워크 접근

점검 항목

Sec301

점검

충족

분류

네트워크 접근

결과

불충족

항목명

네트워크 비인가 사용자 접근 통제

점검 기준

요구사항 내용

네트워크에 접근할 수 있는 모든 경로를 식별하고 접근 통제 정책에 따라 내부 네트워크는 인가된 사용자만이 접근할 수 있도록 통제하고 있는가?

점검 현황

VPC의 NACL에서 SSH 접근에 대한 사용자를 제한하고 SSH의 인바운드 소스에는 개발자나 운영자 등 인가된 사용자의 IP 주소를 지정하고 있다.

인바운드 규칙 편집

인바운드 규칙은 VPC에 도달할 수 있는 수신 트래픽을 제어합니다.

규칙 번호 정보

유형 정보

프로토콜 정보

포트 범위 정보

소스 정보

허용/거부 정보

101

HTTP(80)

TCP(6)

80

0.0.0.0/0

허용

제거

102

HTTPS(443)

TCP(6)

443

0.0.0.0/0

허용

제거

103

SSH(22)

TCP(6)

22

허용

제거

104

사용자 지정 TCP

TCP(6)

32768 - 65535

0.0.0.0/0

허용

제거

+

모든 트래픽

모두

모두

0.0.0.0/0

거부

새 규칙 추가

규칙 번호별 정렬

취소

변경 사항 미리 보기

변경 사항 저장

보안요건 조치 방안

공 란

점검 항목		Sec302		점검 결과	충족																																															
점검 기준	분류	네트워크 접근			불충족																																															
	항목명	네트워크 영역 분리 및 통제																																																		
	요구사항 내용	서비스, 사용자 그룹, 정보 자산의 중요도, 법적 요구사항에 따라 네트워크 영역을 물리적 또는 논리적으로 분리하고 통제하고 있는가?																																																		
점검 현황	VPC에서 서브넷 영역을 논리적으로 분리하여 네트워크 접근을 통제하고 있다.																																																			
	<div>서브넷 (7) 정보</div> <div>Q 서브넷 필터링</div> <table><tr><th><input type="checkbox"/></th><th>Name ▾</th><th>서브넷 ID ▾</th><th>상태 ▾</th><th>VPC ▾</th><th>IPv4 CIDR</th></tr><tr><td><input type="checkbox"/></td><td>Web-Subnet-1</td><td>subnet-00fbc2aba7e84e160</td><td>Available</td><td>vpc-06a0de8caccacc3a7 SK-Health-VPC</td><td>10.0.0.0/24</td></tr><tr><td><input type="checkbox"/></td><td>RDS-Subnet-2</td><td>subnet-04700254d49b046b0</td><td>Available</td><td>vpc-04b7276a409c46441 Bastion-RDS-VPC</td><td>10.1.4.0/24</td></tr><tr><td><input type="checkbox"/></td><td>Web-Subnet-2</td><td>subnet-09da92cc2d526d2be</td><td>Available</td><td>vpc-06a0de8caccacc3a7 SK-Health-VPC</td><td>10.0.2.0/24</td></tr><tr><td><input type="checkbox"/></td><td>WAS-Subnet-2</td><td>subnet-02005cb4c9b9c54bc</td><td>Available</td><td>vpc-06a0de8caccacc3a7 SK-Health-VPC</td><td>10.0.6.0/24</td></tr><tr><td><input type="checkbox"/></td><td>Bastion-Subnet</td><td>subnet-058c0cbca024d4a1f</td><td>Available</td><td>vpc-04b7276a409c46441 Bastion-RDS-VPC</td><td>10.1.0.0/24</td></tr><tr><td><input type="checkbox"/></td><td>RDS-Subnet-1</td><td>subnet-0c0951ca196d589c5</td><td>Available</td><td>vpc-04b7276a409c46441 Bastion-RDS-VPC</td><td>10.1.2.0/24</td></tr><tr><td><input type="checkbox"/></td><td>WAS-Subnet-1</td><td>subnet-0fe9f2d8b003801ae</td><td>Available</td><td>vpc-06a0de8caccacc3a7 SK-Health-VPC</td><td>10.0.4.0/24</td></tr></table>					<input type="checkbox"/>	Name ▾	서브넷 ID ▾	상태 ▾	VPC ▾	IPv4 CIDR	<input type="checkbox"/>	Web-Subnet-1	subnet-00fbc2aba7e84e160	Available	vpc-06a0de8caccacc3a7 SK-Health-VPC	10.0.0.0/24	<input type="checkbox"/>	RDS-Subnet-2	subnet-04700254d49b046b0	Available	vpc-04b7276a409c46441 Bastion-RDS-VPC	10.1.4.0/24	<input type="checkbox"/>	Web-Subnet-2	subnet-09da92cc2d526d2be	Available	vpc-06a0de8caccacc3a7 SK-Health-VPC	10.0.2.0/24	<input type="checkbox"/>	WAS-Subnet-2	subnet-02005cb4c9b9c54bc	Available	vpc-06a0de8caccacc3a7 SK-Health-VPC	10.0.6.0/24	<input type="checkbox"/>	Bastion-Subnet	subnet-058c0cbca024d4a1f	Available	vpc-04b7276a409c46441 Bastion-RDS-VPC	10.1.0.0/24	<input type="checkbox"/>	RDS-Subnet-1	subnet-0c0951ca196d589c5	Available	vpc-04b7276a409c46441 Bastion-RDS-VPC	10.1.2.0/24	<input type="checkbox"/>	WAS-Subnet-1	subnet-0fe9f2d8b003801ae	Available	vpc-06a0de8caccacc3a7 SK-Health-VPC
<input type="checkbox"/>	Name ▾	서브넷 ID ▾	상태 ▾	VPC ▾	IPv4 CIDR																																															
<input type="checkbox"/>	Web-Subnet-1	subnet-00fbc2aba7e84e160	Available	vpc-06a0de8caccacc3a7 SK-Health-VPC	10.0.0.0/24																																															
<input type="checkbox"/>	RDS-Subnet-2	subnet-04700254d49b046b0	Available	vpc-04b7276a409c46441 Bastion-RDS-VPC	10.1.4.0/24																																															
<input type="checkbox"/>	Web-Subnet-2	subnet-09da92cc2d526d2be	Available	vpc-06a0de8caccacc3a7 SK-Health-VPC	10.0.2.0/24																																															
<input type="checkbox"/>	WAS-Subnet-2	subnet-02005cb4c9b9c54bc	Available	vpc-06a0de8caccacc3a7 SK-Health-VPC	10.0.6.0/24																																															
<input type="checkbox"/>	Bastion-Subnet	subnet-058c0cbca024d4a1f	Available	vpc-04b7276a409c46441 Bastion-RDS-VPC	10.1.0.0/24																																															
<input type="checkbox"/>	RDS-Subnet-1	subnet-0c0951ca196d589c5	Available	vpc-04b7276a409c46441 Bastion-RDS-VPC	10.1.2.0/24																																															
<input type="checkbox"/>	WAS-Subnet-1	subnet-0fe9f2d8b003801ae	Available	vpc-06a0de8caccacc3a7 SK-Health-VPC	10.0.4.0/24																																															
보안요건 조치 방안		공 란																																																		

점검 항목	Sec303		점검	충족																																															
점검 기준	분류	네트워크 접근	결과	불충족																																															
	항목명	외부 네트워크 접근 통제																																																	
	요구사항 내용	데이터베이스 서버 등 중요 시스템이 외부와의 연결을 필요로 하지 않은 경우 사설 IP로 할당하여 외부 IP 접근 통제를 하고 있는가?																																																	
점검 현황	VPC를 통해 웹 서버, 데이터베이스 등에 A클래스 대역의 IP를 할당하여 외부 네트워크를 접근 통제를 하고 있다.																																																		
	<div>서브넷 (7) 정보</div> <div><div>Q 서브넷 필터링</div><table><thead><tr><th><input type="checkbox"/></th><th>Name</th><th>서브넷 ID</th><th>상태</th><th>VPC</th><th>IPv4 CIDR</th></tr></thead><tbody><tr><td><input type="checkbox"/></td><td>Web-Subnet-1</td><td>subnet-00fbc2aba7e84e160</td><td>Available</td><td>vpc-06a0de8caccacc3a7 SK-Health-VPC</td><td>10.0.0.0/24</td></tr><tr><td><input type="checkbox"/></td><td>RDS-Subnet-2</td><td>subnet-04700254d49b046b0</td><td>Available</td><td>vpc-04b7276a409c46441 Bastion-RDS-VPC</td><td>10.1.4.0/24</td></tr><tr><td><input type="checkbox"/></td><td>Web-Subnet-2</td><td>subnet-09da92cc2d526d2be</td><td>Available</td><td>vpc-06a0de8caccacc3a7 SK-Health-VPC</td><td>10.0.2.0/24</td></tr><tr><td><input type="checkbox"/></td><td>WAS-Subnet-2</td><td>subnet-02005cb4c9b9c54bc</td><td>Available</td><td>vpc-06a0de8caccacc3a7 SK-Health-VPC</td><td>10.0.6.0/24</td></tr><tr><td><input type="checkbox"/></td><td>Bastion-Subnet</td><td>subnet-058c0cbca024d4a1f</td><td>Available</td><td>vpc-04b7276a409c46441 Bastion-RDS-VPC</td><td>10.1.0.0/24</td></tr><tr><td><input type="checkbox"/></td><td>RDS-Subnet-1</td><td>subnet-0c0951ca196d589c5</td><td>Available</td><td>vpc-04b7276a409c46441 Bastion-RDS-VPC</td><td>10.1.2.0/24</td></tr><tr><td><input type="checkbox"/></td><td>WAS-Subnet-1</td><td>subnet-0fe9f2d8b003801ae</td><td>Available</td><td>vpc-06a0de8caccacc3a7 SK-Health-VPC</td><td>10.0.4.0/24</td></tr></tbody></table></div>				<input type="checkbox"/>	Name	서브넷 ID	상태	VPC	IPv4 CIDR	<input type="checkbox"/>	Web-Subnet-1	subnet-00fbc2aba7e84e160	Available	vpc-06a0de8caccacc3a7 SK-Health-VPC	10.0.0.0/24	<input type="checkbox"/>	RDS-Subnet-2	subnet-04700254d49b046b0	Available	vpc-04b7276a409c46441 Bastion-RDS-VPC	10.1.4.0/24	<input type="checkbox"/>	Web-Subnet-2	subnet-09da92cc2d526d2be	Available	vpc-06a0de8caccacc3a7 SK-Health-VPC	10.0.2.0/24	<input type="checkbox"/>	WAS-Subnet-2	subnet-02005cb4c9b9c54bc	Available	vpc-06a0de8caccacc3a7 SK-Health-VPC	10.0.6.0/24	<input type="checkbox"/>	Bastion-Subnet	subnet-058c0cbca024d4a1f	Available	vpc-04b7276a409c46441 Bastion-RDS-VPC	10.1.0.0/24	<input type="checkbox"/>	RDS-Subnet-1	subnet-0c0951ca196d589c5	Available	vpc-04b7276a409c46441 Bastion-RDS-VPC	10.1.2.0/24	<input type="checkbox"/>	WAS-Subnet-1	subnet-0fe9f2d8b003801ae	Available	vpc-06a0de8caccacc3a7 SK-Health-VPC
<input type="checkbox"/>	Name	서브넷 ID	상태	VPC	IPv4 CIDR																																														
<input type="checkbox"/>	Web-Subnet-1	subnet-00fbc2aba7e84e160	Available	vpc-06a0de8caccacc3a7 SK-Health-VPC	10.0.0.0/24																																														
<input type="checkbox"/>	RDS-Subnet-2	subnet-04700254d49b046b0	Available	vpc-04b7276a409c46441 Bastion-RDS-VPC	10.1.4.0/24																																														
<input type="checkbox"/>	Web-Subnet-2	subnet-09da92cc2d526d2be	Available	vpc-06a0de8caccacc3a7 SK-Health-VPC	10.0.2.0/24																																														
<input type="checkbox"/>	WAS-Subnet-2	subnet-02005cb4c9b9c54bc	Available	vpc-06a0de8caccacc3a7 SK-Health-VPC	10.0.6.0/24																																														
<input type="checkbox"/>	Bastion-Subnet	subnet-058c0cbca024d4a1f	Available	vpc-04b7276a409c46441 Bastion-RDS-VPC	10.1.0.0/24																																														
<input type="checkbox"/>	RDS-Subnet-1	subnet-0c0951ca196d589c5	Available	vpc-04b7276a409c46441 Bastion-RDS-VPC	10.1.2.0/24																																														
<input type="checkbox"/>	WAS-Subnet-1	subnet-0fe9f2d8b003801ae	Available	vpc-06a0de8caccacc3a7 SK-Health-VPC	10.0.4.0/24																																														
보안요건 조치 방안	공 란																																																		

점검 항목	Sec304		점검 결과	충족
점검 기준	분류	네트워크 접근		불충족
	항목명	무선 네트워크 접근 통제		
	요구사항 내용	무선 네트워크를 사용하는 경우 사용자 인증, 송수신 데이터 암호화 등 무선 네트워크 보호대책을 적용하고 통제하고 있는가?		
점검 현황	SK헬스 내부에서 무선 네트워크를 사용하고 있지 않으므로 해당 요건은 점검 사항에서 제외한다.			
보안요건 조치 방안	공 란			

정보시스템 접근

점검 항목	Sec305		점검	충족
점검 기준	분류	정보시스템 접근	결과	불충족
	항목명	정보시스템에 대한 접근 수단 정의 및 접근 통제		
	요구사항 내용	서버, 네트워크시스템, 보안시스템 등 정보시스템 별 운영체제(OS)에 접근이 허용되는 사용자, 접근 가능 위치, 접근 수단 등을 정의하여 통제하고 있는가?		
점검 현황	IAM를 통해 사용자 별 접근 가능한 서비스를 제한하고 있다.			
	<div><div>그룹에서 연결됨</div><div><div><div>▶</div><div> AmazonRDSFullAccess</div><div>sk-health 그룹의 AWS 관리형 정책</div><div>✕</div></div><div><div>▶</div><div> AmazonEC2FullAccess</div><div>sk-health 그룹의 AWS 관리형 정책</div><div>✕</div></div><div><div>▶</div><div> AmazonEC2ContainerRegistryFullAc...</div><div>sk-health 그룹의 AWS 관리형 정책</div><div>✕</div></div><div><div>▶</div><div> AmazonS3FullAccess</div><div>sk-health 그룹의 AWS 관리형 정책</div><div>✕</div></div><div><div>▶</div><div> AmazonVPCFullAccess</div><div>sk-health 그룹의 AWS 관리형 정책</div><div>✕</div></div><div><div>▶</div><div> AmazonEC2ContainerServiceforEC2...</div><div>sk-health 그룹의 AWS 관리형 정책</div><div>✕</div></div><div><div>▶</div><div> AmazonEC2ContainerServiceRole</div><div>sk-health 그룹의 AWS 관리형 정책</div><div>✕</div></div><div><div>▶</div><div> IAMUserSSHKeys</div><div>sk-health 그룹의 AWS 관리형 정책</div><div>✕</div></div></div></div>			
	VPC의 보안 그룹을 통해 EC2 인스턴스에 접근 가능한 위치와 수단을 정의하고 있다.			
<div><div>인바운드 규칙 편집</div><div><div>인바운드 규칙은 인스턴스에 도달하도록 허용될 수 있는 트래픽을 제어합니다.</div><div><div>인바운드 규칙</div><div><div>보안 그룹 규칙 ID</div><div>유형</div><div>프로토콜</div><div>포트 범위</div><div>소스</div><div>선택 - 선택 사항</div></div><div><div>sgr-0d5dde24526553347</div><div>HTTPS</div><div>TCP</div><div>443</div><div>사용자 ...</div><div>0.0.0.0/0 ✕</div><div>삭제</div></div><div><div>sgr-0d64bf524534c6cc0</div><div>SSH</div><div>TCP</div><div>22</div><div>사용자 ...</div><div>Q</div><div>삭제</div></div><div><div>sgr-0a2f401f17bc5670</div><div>HTTP</div><div>TCP</div><div>80</div><div>사용자 ...</div><div>0.0.0.0/0 ✕</div><div>삭제</div></div><div><div>규칙 추가</div></div></div><div><div>취소</div><div>변경 사항 미리 보기</div><div>규칙 저장</div></div></div></div>				
보안요건 조치 방안	공 란			

점검 항목	Sec306		점검 결과	충족
점검 기준	분류	정보시스템 접근		불충족
	항목명	정보시스템 접근에 대한 사용자 인증 통제 적용		
	요구사항 내용	정보시스템 및 개인정보처리시스템에 대한 접근 시 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전하게 식별하고 통제하고 있는가?		
점검 현황	IAM 기본 암호정책으로만 접근 제한을 하고 있음 1. 암호 최소 길이 2. 암호 만료 시 관리자 재설정 필요 3. 암호 재사용 제한 4. 사용자 자신의 암호 변경 허용 5. 암호 만료 활성화			
보안요건 조치 방안	IAM에서 지정된 횟수의 로그인 시도가 실패한 경우 계정에서 사용자를 통제하는 잠금 정책을 생성해서 불법 로그인 시도를 제한할 수 있다.			

점검 항목	Sec307		점검 결과	충족
점검 기준	분류	정보시스템 접근		불충족
	항목명	정보시스템 접속 차단		
	요구사항 내용	정보시스템에 접속 후 일정시간 업무처리를 하지 않을 경우 자동으로 시스템 접속이 차단되도록 하고 있는가?		
점검 현황	Single Sign-On를 통해 사용자가 일정 시간 업무처리를 하지 않을 경우 로그인할 수 있는 시간을 설정하여 시스템이 차단되도록 하고 있다.			
	<div>일반 권한 세트 설정 편집</div> <div>권한 세트 설정</div> <div><div>권한 세트 이름</div><div>SK-Health-101-001-SSO</div><div>설명 – 선택 사항</div><div>이 권한 세트에 대하여 간단한 설명을 추가합니다.</div><div><div>SK-Health-101-001-SSO</div><div></div></div><div>권한 세트 설명은 700자 이하로 제한됩니다. 설명은 정규식 [\u0009\u000A\u000D\u0020-\u007E\u00A1-\u00FF]*과(와) 일치해야 합니다.</div><div><div>세션 기간</div><div>콘솔이 세션에서 사용자를 로그아웃할 때까지 사용자가 로그인할 수 있는 시간입니다. 자세히 알아보기</div><div><div>4시간</div><div></div></div></div><div><div>릴레이 상태 – 선택 사항</div><div>계정 내에서 사용자를 리디렉션하기 위해 연동 프로세스에 사용되는 값입니다. 자세히 알아보기</div><div><div>릴레이 상태 입력</div><div></div></div><div>릴레이 상태는 최대 320자까지 지원합니다. 릴레이 상태는 영숫자, 공백 및 특수 문자 & \$ @ # \ / % ? = ~ - _ ' " ! ; , . * + [] () 만 포함할 수 있습니다.</div><div><div>취소</div><div>변경 사항 저장</div></div></div></div>			
보안요건 조치 방안	공 란			

점검 항목	Sec308		점검 결과	충족																																															
점검 기준	분류	정보시스템 접근		불충족																																															
	항목명	서비스에 따른 독립된 서버 운영																																																	
	요구사항 내용	주요 서비스를 제공하는 정보시스템은 독립된 서버로 운영하고 있는가?																																																	
점검 현황	VPC를 통해 서브넷을 구분하여 WEB, WAS, DB를 독립적으로 서버를 구성하고 있다.																																																		
	<div>서브넷 (7) 정보</div> <div>Q 서브넷 필터링</div> <table><tr><th><input type="checkbox"/></th><th>Name</th><th>서브넷 ID</th><th>상태</th><th>VPC</th><th>IPv4 CIDR</th></tr><tr><td><input type="checkbox"/></td><td>Web-Subnet-1</td><td>subnet-00fbc2aba7e84e160</td><td>Available</td><td>vpc-06a0de8caccacc3a7 SK-...</td><td>10.0.0.0/24</td></tr><tr><td><input type="checkbox"/></td><td>RDS-Subnet-2</td><td>subnet-04700254d49b046b0</td><td>Available</td><td>vpc-04b7276a409c46441 Ba...</td><td>10.1.4.0/24</td></tr><tr><td><input type="checkbox"/></td><td>Web-Subnet-2</td><td>subnet-09da92cc2d526d2be</td><td>Available</td><td>vpc-06a0de8caccacc3a7 SK-...</td><td>10.0.2.0/24</td></tr><tr><td><input type="checkbox"/></td><td>WAS-Subnet-2</td><td>subnet-02005cb4c9b9c54bc</td><td>Available</td><td>vpc-06a0de8caccacc3a7 SK-...</td><td>10.0.6.0/24</td></tr><tr><td><input type="checkbox"/></td><td>Bastion-Subnet</td><td>subnet-058c0cbca024d4a1f</td><td>Available</td><td>vpc-04b7276a409c46441 Ba...</td><td>10.1.0.0/24</td></tr><tr><td><input type="checkbox"/></td><td>RDS-Subnet-1</td><td>subnet-0c0951ca196d589c5</td><td>Available</td><td>vpc-04b7276a409c46441 Ba...</td><td>10.1.2.0/24</td></tr><tr><td><input type="checkbox"/></td><td>WAS-Subnet-1</td><td>subnet-0fe9f2d8b003801ae</td><td>Available</td><td>vpc-06a0de8caccacc3a7 SK-...</td><td>10.0.4.0/24</td></tr></table>				<input type="checkbox"/>	Name	서브넷 ID	상태	VPC	IPv4 CIDR	<input type="checkbox"/>	Web-Subnet-1	subnet-00fbc2aba7e84e160	Available	vpc-06a0de8caccacc3a7 SK-...	10.0.0.0/24	<input type="checkbox"/>	RDS-Subnet-2	subnet-04700254d49b046b0	Available	vpc-04b7276a409c46441 Ba...	10.1.4.0/24	<input type="checkbox"/>	Web-Subnet-2	subnet-09da92cc2d526d2be	Available	vpc-06a0de8caccacc3a7 SK-...	10.0.2.0/24	<input type="checkbox"/>	WAS-Subnet-2	subnet-02005cb4c9b9c54bc	Available	vpc-06a0de8caccacc3a7 SK-...	10.0.6.0/24	<input type="checkbox"/>	Bastion-Subnet	subnet-058c0cbca024d4a1f	Available	vpc-04b7276a409c46441 Ba...	10.1.0.0/24	<input type="checkbox"/>	RDS-Subnet-1	subnet-0c0951ca196d589c5	Available	vpc-04b7276a409c46441 Ba...	10.1.2.0/24	<input type="checkbox"/>	WAS-Subnet-1	subnet-0fe9f2d8b003801ae	Available	vpc-06a0de8caccacc3a7 SK-...
<input type="checkbox"/>	Name	서브넷 ID	상태	VPC	IPv4 CIDR																																														
<input type="checkbox"/>	Web-Subnet-1	subnet-00fbc2aba7e84e160	Available	vpc-06a0de8caccacc3a7 SK-...	10.0.0.0/24																																														
<input type="checkbox"/>	RDS-Subnet-2	subnet-04700254d49b046b0	Available	vpc-04b7276a409c46441 Ba...	10.1.4.0/24																																														
<input type="checkbox"/>	Web-Subnet-2	subnet-09da92cc2d526d2be	Available	vpc-06a0de8caccacc3a7 SK-...	10.0.2.0/24																																														
<input type="checkbox"/>	WAS-Subnet-2	subnet-02005cb4c9b9c54bc	Available	vpc-06a0de8caccacc3a7 SK-...	10.0.6.0/24																																														
<input type="checkbox"/>	Bastion-Subnet	subnet-058c0cbca024d4a1f	Available	vpc-04b7276a409c46441 Ba...	10.1.0.0/24																																														
<input type="checkbox"/>	RDS-Subnet-1	subnet-0c0951ca196d589c5	Available	vpc-04b7276a409c46441 Ba...	10.1.2.0/24																																														
<input type="checkbox"/>	WAS-Subnet-1	subnet-0fe9f2d8b003801ae	Available	vpc-06a0de8caccacc3a7 SK-...	10.0.4.0/24																																														
보안요건 조치 방안	공 란																																																		

점검 항목	Sec309		점검 결과	충족																																		
점검 기준	분류	정보시스템 접근		불충족																																		
	항목명	정보시스템 관계없는 서비스 차단																																				
	요구사항 내용	정보시스템의 사용 목적과 관련이 없거나 침해 사고를 유발할 수 있는 서비스 또는 포트를 확인하여 차단하고 있는가?																																				
점검 현황	VPC NACL을 통해 WAS에 대한 인바운드 규칙(Flask, SSH, 동적 포트) 포트 범위를 오픈하고 나머지 허용되지 않는 포트를 차단한다.																																					
	<div>인바운드 규칙 편집 <small>정보</small> 인바운드 규칙은 VPC에 도달할 수 있는 수신 트래픽을 제어합니다.</div> <table><thead><tr><th>규칙 번호</th><th>유형</th><th>프로토콜</th><th>포트 범위</th><th>소스</th><th>허용/거부</th><th></th></tr></thead><tbody><tr><td>101</td><td>사용자 지정 TCP</td><td>TCP(S)</td><td>5000</td><td>10.0.0.0/22</td><td>허용</td><td>제거</td></tr><tr><td>102</td><td>SSH(22)</td><td>TCP(S)</td><td>22</td><td>10.0.0.0/22</td><td>허용</td><td>제거</td></tr><tr><td>103</td><td>사용자 지정 TCP</td><td>TCP(S)</td><td>32768 - 65535</td><td>10.0.0.0/22</td><td>허용</td><td>제거</td></tr><tr><td>*</td><td>모든 트래픽</td><td>모두</td><td>모두</td><td>0.0.0.0/0</td><td>거부</td><td></td></tr></tbody></table> <div>새 규칙 추가 규칙 번호별 정렬</div> <div>취소 변경 사항 미리 보기 변경 사항 저장</div>				규칙 번호	유형	프로토콜	포트 범위	소스	허용/거부		101	사용자 지정 TCP	TCP(S)	5000	10.0.0.0/22	허용	제거	102	SSH(22)	TCP(S)	22	10.0.0.0/22	허용	제거	103	사용자 지정 TCP	TCP(S)	32768 - 65535	10.0.0.0/22	허용	제거	*	모든 트래픽	모두	모두	0.0.0.0/0	거부
규칙 번호	유형	프로토콜	포트 범위	소스	허용/거부																																	
101	사용자 지정 TCP	TCP(S)	5000	10.0.0.0/22	허용	제거																																
102	SSH(22)	TCP(S)	22	10.0.0.0/22	허용	제거																																
103	사용자 지정 TCP	TCP(S)	32768 - 65535	10.0.0.0/22	허용	제거																																
*	모든 트래픽	모두	모두	0.0.0.0/0	거부																																	
보안요건 조치 방안	공 란																																					

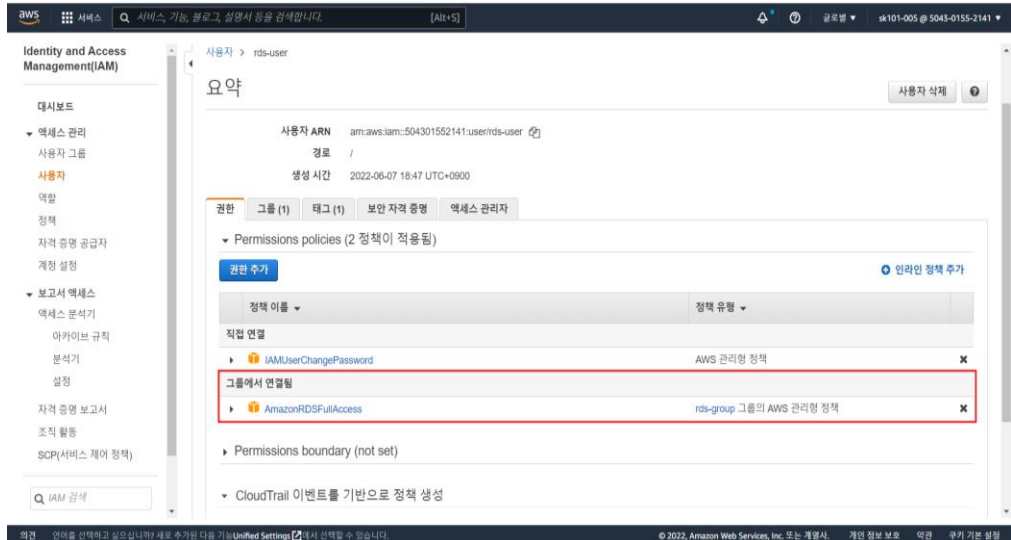
응용프로그램 접근

점검 항목	Sec310		점검 결과	충족
점검 기준	분류	응용프로그램 접근		불충족
	항목명	응용프로그램 접근 권한 제한		
	요구사항 내용	중요정보 접근을 통제하기 위하여 사용자의 업무에 따라 응용프로그램 접근 권한을 설정하고 있는가?		
점검 현황	SK헬스 서비스에 응용 프로그램의 영역은 점검 대상에서 제외한다.			
보안요건 조치 방안	공 란			

점검 항목	Sec311		점검 결과	충족
점검 기준	분류	응용프로그램 접근		불충족
	항목명	응용프로그램 중요정보의 노출 최소화		
	요구사항 내용	중요정보의 불필요한 노출(조회, 화면표시, 인쇄, 다운로드 등)을 최소화할 수 있도록 응용프로그램을 구현하고 있는가?		
점검 현황	SK헬스 서비스에 응용 프로그램의 영역은 점검 대상에서 제외한다.			
보안요건 조치 방안	공 란			

점검 항목	Sec312		점검	충족
점검 기준	분류	응용프로그램 접근	결과	불충족
	항목명	응용프로그램 세션 관리		
	요구사항 내용	일정 시간 동안 입력이 없는 세션은 자동 차단하고, 동일 사용자의 동시 세션 수를 제한하고 있는가?		
점검 현황	SK헬스 서비스에 응용 프로그램의 영역은 점검 대상에서 제외한다.			
보안요건 조치 방안	공 란			

데이터베이스 접근

점검 항목	Sec314		점검	충족
점검 기준	분류	데이터베이스 접근	결과	불충족
	항목명	데이터베이스 접근 통제		
	요구사항 내용	데이터베이스 내 정보에 접근이 필요한 응용프로그램, 정보시스템(서버) 및 사용자를 명확히 식별하고 접근 통제 정책에 따라 통제하고 있는가?		
점검 현황	<p>IAM에서 일반 사용자 계정에 RDS의 전체 접근 권한인 AmazonRDSFullAccess 권한을 부여하고 있다. 정보시스템, 응용프로그램을 별도로 식별하고 있지 않다.</p> 			
보안요건 조치 방안	<p>RDS 생성 시 퍼블릭 액세스 권한 설정해서 퍼블릭 IP주소를 할당하지 않고 VPC 내부의 인스턴스 및 응용프로그램만을 연결할 수 있게 한다. VPC 보안 그룹을 설정하여 데이터베이스 접근을 통제해야 한다.</p> <p>데이터베이스에 접근하는 사용자를 식별하여 IAM에서 접근 권한을 알맞게 부여한다.</p>			

원격접근 통제

점검 항목	Sec315		점검 결과	충족
점검 기준	분류	원격접근 통제		불충족
	항목명	단말기 접근 통제		
	요구사항 내용	내부 네트워크를 통하여 원격으로 정보시스템을 운영하는 경우 특정 단말에 한해서만 접근 통제 하고 있는가?		
점검 현황	현재 원격으로 정보시스템 운영 시 Client VPN 연결을 통해 단말에 대한 접근 통제는 불가능한 상태이다.			
보안요건 조치 방안	단말기에서 Amazon Workspaces에 접근 후 내부 업무용 시스템 접근하도록 아키텍처를 구성하여 특정 단말에 대해 접근 통제 한다.			

인터넷 접속 통제

점검 항목

Sec316

점검 결과

충족

점검 기준

분류

인터넷 접속 통제

항목명

외부 인터넷 접속 통제

요구사항 내용

주요 정보시스템(DB 서버 등)에서 불필요한 외부 인터넷 접속을 통제하고 있는가?

VPC의 보안 그룹을 이용해 WAS, RDS에 대한 인터넷(HTTP, HTTPS 등)에 대한 접속을 통제하고 있다.

인바운드 규칙 편집

정보

인바운드 규칙은 인스턴스에 도달하도록 허용된 수신 트래픽을 제어합니다.

인바운드 규칙

정보

보안 그룹 규칙 ID

유형 정보

프로토콜 정보

포트 범위 정보

소스 정보

설명 - 선택 사항 정보

sgr-0bb88a1fb96af23e3

MYSQL/Aurora

TCP

3306

사용자 ...

Q

삭제

10.1.0.0/24

X

규칙 추가

취소

변경 사항 미리 보기

규칙 저장

점검 현황

인바운드 규칙 편집

정보

인바운드 규칙은 인스턴스에 도달하도록 허용된 수신 트래픽을 제어합니다.

인바운드 규칙

정보

보안 그룹 규칙 ID

유형 정보

프로토콜 정보

포트 범위 정보

소스 정보

설명 - 선택 사항 정보

sgr-03184cd5a5b1d5fc6

사용자 지정 TCP

TCP

5000

사용자 ...

Q

삭제

10.0.0.0/22

X

sgr-06497c2bb9fb83a5c

SSH

TCP

22

사용자 ...

Q

삭제

10.0.0.0/22

X

규칙 추가

취소

변경 사항 미리 보기

규칙 저장

보안요건 조치 방안

공 란

점검 항목	Sec317		점검 결과	충족																										
점검 기준	분류	인터넷 접속 통제																												
	항목명	망 분리 적용 및 통제																												
	요구사항 내용	법령에 따라 인터넷 망 분리 의무가 부과된 경우 망 분리 대상자를 식별하여 안전한 방식으로 망 분리를 적용하여 접근 통제하는가?																												
점검 현황	2개의 VPC로 망 분리하여 피어링 연결 설정을 통해 각각의 VPC를 연결하여 접근 통제하고 있다.																													
	<div><div>VPC (2) 정보</div><div><div><div>Q VPC 필터링</div></div><div><table><tr><td><input type="checkbox"/></td><td>Name ▾</td><td>VPC ID ▾</td><td>상태 ▾</td><td>IPv4 CIDR ▾</td></tr><tr><td><input type="checkbox"/></td><td>SK-Health-VPC</td><td>vpc-06a0de8caccacc3a7</td><td>✔ Available</td><td>10.0.0.0/19</td></tr><tr><td><input type="checkbox"/></td><td>Bastion-RDS-VPC</td><td>vpc-04b7276a409c46441</td><td>✔ Available</td><td>10.1.0.0/20</td></tr></table></div></div></div> <div><div>피어링 연결 설정</div><div><div>이름 - 선택 사항</div><div>'Name' 키와 사용자가 지정하는 값을 포함하는 태그를 생성합니다.</div><div><div>SK-Health-Peering</div></div></div><div><div>피어링할 로컬 VPC 선택</div><div><div>VPC ID(요청자)</div><div><div>vpc-0fe616dc51f1c9c07 (Bastion-RDS-VPC)</div></div><div><div>vpc-0fe616dc51f1c9c07 (Bastion-RDS-VPC)용 VPC CIDR</div><table><tr><td>CIDR</td><td>상태</td><td>상태 사유</td></tr><tr><td>10.1.0.0/20</td><td>✔ Associated</td><td>-</td></tr></table></div></div></div><div><div>피어링할 다른 VPC 선택</div><div><div>계정</div><div><div><input checked="" type="radio"/> 내 계정</div><div><input type="radio"/> 다른 계정</div></div><div><div>리전</div><div><div><input checked="" type="radio"/> 현재 리전(ap-northeast-2)</div><div><input type="radio"/> 다른 리전</div></div></div></div><div><div>VPC ID(수락자)</div><div><div>vpc-0905137ab1c088d42 (SK-Health-VPC)</div></div><div><div>vpc-0905137ab1c088d42 (SK-Health-VPC)용 VPC CIDR</div><table><tr><td>CIDR</td><td>상태</td><td>상태 사유</td></tr><tr><td>10.0.0.0/19</td><td>✔ Associated</td><td>-</td></tr></table></div></div></div></div> <div>보안요건 조치 방안</div> <div>공 란</div>				<input type="checkbox"/>	Name ▾	VPC ID ▾	상태 ▾	IPv4 CIDR ▾	<input type="checkbox"/>	SK-Health-VPC	vpc-06a0de8caccacc3a7	✔ Available	10.0.0.0/19	<input type="checkbox"/>	Bastion-RDS-VPC	vpc-04b7276a409c46441	✔ Available	10.1.0.0/20	CIDR	상태	상태 사유	10.1.0.0/20	✔ Associated	-	CIDR	상태	상태 사유	10.0.0.0/19	✔ Associated
<input type="checkbox"/>	Name ▾	VPC ID ▾	상태 ▾	IPv4 CIDR ▾																										
<input type="checkbox"/>	SK-Health-VPC	vpc-06a0de8caccacc3a7	✔ Available	10.0.0.0/19																										
<input type="checkbox"/>	Bastion-RDS-VPC	vpc-04b7276a409c46441	✔ Available	10.1.0.0/20																										
CIDR	상태	상태 사유																												
10.1.0.0/20	✔ Associated	-																												
CIDR	상태	상태 사유																												
10.0.0.0/19	✔ Associated	-																												

보안시스템 통제

점검 항목	Sec318		점검	충족																											
점검 기준	분류	보안시스템 통제	결과	불충족																											
	항목명	보안시스템 비인가자 접근 통제																													
	요구사항 내용	보안시스템 관리자 등 접근이 허용된 인원수를 최소화하고 비인가자의 접근을 엄격하게 통제하고 있는가?																													
점검 현황	IAM을 통해 일부 사용자한테만 접근 권한을 부여하여 보안시스템에 접근 가능한 인원수를 최소화하고 있다.																														
점검 현황	<div>권한 그룹 (1) 태그 보안 자격 증명 액세스 관리자</div> <div>▼ Permissions policies (15 정책이 적용됨)</div> <div>권한 추가 인라인 정책 추가</div> <table><thead><tr><th>정책 이름 ▼</th><th>정책 유형 ▼</th><th></th></tr></thead><tbody><tr><td>직접 연결</td><td></td><td></td></tr><tr><td>▶ AmazonInspectorFullAccess</td><td>AWS 관리형 정책</td><td>✕</td></tr><tr><td>▶ AmazonGuardDutyFullAccess</td><td>AWS 관리형 정책</td><td>✕</td></tr><tr><td>▶ AWSCloudHSMFullAccess</td><td>AWS 관리형 정책</td><td>✕</td></tr><tr><td>▶ AmazonMacieFullAccess</td><td>AWS 관리형 정책</td><td>✕</td></tr><tr><td>▶ AmazonCognitoPowerUser</td><td>AWS 관리형 정책</td><td>✕</td></tr><tr><td>▶ AWSWAFFullAccess</td><td>AWS 관리형 정책</td><td>✕</td></tr><tr><td>▶ AWSCloudTrail_FullAccess</td><td>AWS 관리형 정책</td><td>✕</td></tr></tbody></table>				정책 이름 ▼	정책 유형 ▼		직접 연결			▶ AmazonInspectorFullAccess	AWS 관리형 정책	✕	▶ AmazonGuardDutyFullAccess	AWS 관리형 정책	✕	▶ AWSCloudHSMFullAccess	AWS 관리형 정책	✕	▶ AmazonMacieFullAccess	AWS 관리형 정책	✕	▶ AmazonCognitoPowerUser	AWS 관리형 정책	✕	▶ AWSWAFFullAccess	AWS 관리형 정책	✕	▶ AWSCloudTrail_FullAccess	AWS 관리형 정책	✕
	정책 이름 ▼	정책 유형 ▼																													
직접 연결																															
▶ AmazonInspectorFullAccess	AWS 관리형 정책	✕																													
▶ AmazonGuardDutyFullAccess	AWS 관리형 정책	✕																													
▶ AWSCloudHSMFullAccess	AWS 관리형 정책	✕																													
▶ AmazonMacieFullAccess	AWS 관리형 정책	✕																													
▶ AmazonCognitoPowerUser	AWS 관리형 정책	✕																													
▶ AWSWAFFullAccess	AWS 관리형 정책	✕																													
▶ AWSCloudTrail_FullAccess	AWS 관리형 정책	✕																													
보안요건 조치 방안	공 란																														

2.4 암호화 적용

중요정보 암호화

점검 항목	Sec401		점검	충족
점검 기준	분류	중요정보 암호화	결과	불충족
	항목명	개인정보 및 주요 정보에 대한 암호화 적용		
	요구사항 내용	암호 정책에 따라 개인정보 및 중요 정보의 저장 시 암호화를 수행하고 있는가?		
점검 현황	RDS를 생성할 때 암호화 활성화 기능을 통해 정보를 저장 시 암호화를 수행하고 있다. 암호화 <input checked="" type="checkbox"/> 암호화 활성화 지정한 인스턴스를 암호화하려면 이 옵션을 선택합니다. AWS Key Management Service 콘솔을 사용하여 마스터 키 ID와 별칭이 생성된 후 해당 항목이 목록에 표시됩니다. 정보 AWS KMS 키 정보 <div>(default) aws/rds</div>			
보안요건 조치 방안	공 란			

암호키 관리

점검 항목	Sec402		점검	충족
점검 기준	분류	암호키 관리	결과	불충족
	항목명	암호키 접근 권한 관리		
	요구사항 내용	암호키 사용에 관한 접근 권한을 최소화하고 있는가?		
점검 현황	KMS를 통해 암호키 사용 접근 권한을 설정하고 있다.			
	<div><div>키 관리자</div><div>KMS API를 통해 이 키를 관리할 수 있는 IAM 사용자 및 역할을 선택하십시오. 해당 사용자 또는 역할로 이 콘솔에서 이 키를 관리하려면 권한을 추가해야 할 수 있습니다. 자세히 알아보기</div><div><div><div><div>Q</div></div></div><div><div><</div><div>1</div><div>2</div><div>3</div><div>4</div><div>5</div><div>6</div><div>7</div><div>...</div><div>10</div><div>></div></div></div><div><div><div><div><div></div></div></div><div>이름</div><div></div></div><div><div><div><div></div></div></div><div>경로</div><div></div></div><div><div><div><div></div></div></div><div>유형</div><div></div></div></div><div><div><div><div><div></div></div></div><div>CostManager</div><div>/</div><div>User</div></div><div><div><div><div><div></div></div></div><div>sk101-001</div><div>/</div><div>User</div></div><div><div><div><div><div></div></div></div><div>sk101-002</div><div>/</div><div>User</div></div></div></div></div></div>			
보안요건 조치 방안	공 란			

비밀번호 암호화

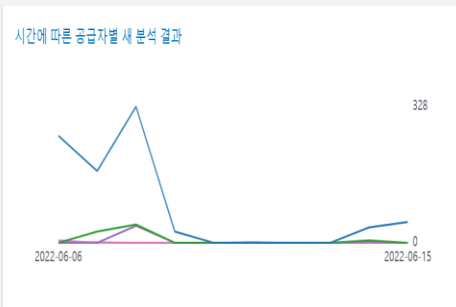
점검 항목	Sec403		점검	충족
점검 기준	분류	비밀번호 암호화	결과	불충족
	항목명	비밀번호 암호화 적용		
	요구사항 내용	개인정보처리시스템에 저장 시 암호화 적용을 하고 있는가?		
점검 현황	Secrets Manager를 통해 개인정보처리시스템에 저장 시 KMS 키를 사용하여 암호화하고 있다.			
	<div><div>새 보안 암호 저장</div><div><div>보안 암호 유형 정보</div><div><div><div><div><input checked="" type="radio"/> Amazon RDS 데이터베이스에 대한 자격 증명</div><div><input type="radio"/> Amazon DocumentDB 데이터베이스에 대한 자격 증명</div><div><input type="radio"/> Amazon Redshift 클러스터에 대한 자격 증명</div><div><input type="radio"/> 기타 데이터베이스에 대한 자격 증명</div><div><input type="radio"/> 다른 유형의 보안 암호 API 키, OAuth 토큰, 기타.</div></div></div><div><div>자격 증명 정보</div><div>사용자 이름</div><div>sk101-001</div><div>암호</div><div>*****</div><div><input type="checkbox"/> 암호 표시</div><div><div>암호화 키 정보</div><div>Secrets Manager가 생성하는 KMS 키 또는 사용자가 생성한 고객 관리형 KMS 키를 사용하여 암호화할 수 있습니다.</div><div><div>aws/secretsmanager</div><div>새 키 추가</div><div></div></div></div><div><div>데이터베이스 정보</div><div><div>Q 인스턴스 검색</div><div>< 1 ></div></div><div><div>DB 인스턴스</div><div>DB 엔진</div><div>상태</div><div>생성 날짜</div></div><div><div><input checked="" type="radio"/> sk-health-db</div><div>mysql</div><div>modifying</div><div>2022. 6. 6.</div></div></div><div><div>취소</div><div>다음</div></div></div></div></div></div>			
보안요건 조치 방안	공 란			

2.5 로깅 및 모니터링

로그 관리

점검 항목	Sec501		점검	충족
점검 기준	분류	로그 관리	결과	불충족
	항목명	로그 기록 보관 및 관리		
	요구사항 내용	서버, 응용프로그램, 보안시스템, 네트워크시스템 등 정보시스템에 대한 로그를 보관 및 관리를 하고 있는가?		
점검 현황	VPC Flow log를 사용하여 네트워크 시스템에 대해서 S3에 로그를 기록 관리하고 있다. CloudWatch에서 로그 그룹을 설정해서 관리하고 있다.			
	<div><div>플로우 로그 (1/1) 정보</div><div><div>Q 플로우 로그 필터링</div><div><div><div><div><input checked="" type="checkbox"/></div><div>Name</div><div>▼</div></div><div><div><input checked="" type="checkbox"/></div><div>VPC-Log</div></div><div><div>플로우 로그 ID</div><div>▼</div></div><div><div>fl-0479685edc5c5e353</div></div><div><div>필터</div><div>▼</div></div><div><div>ALL</div></div><div><div>대상 유형</div><div>▼</div></div><div><div>s3</div></div><div><div>대상 이름</div><div>▼</div></div><div><div>sk-health-flowlogs</div><div>🔗</div></div></div></div></div></div> <div><div>CloudWatch > Log groups</div><div><div>로그 그룹 (3)</div><div>기본적으로 최대 10,000개의 로그 그룹만 로드합니다.</div><div><div>Q 로그 그룹 필터링 또는 접두사 검색 시도</div><div><input type="checkbox"/> 정확히 일치</div></div><div><div><div><input type="checkbox"/></div><div>로그 그룹</div><div>▲</div><div>보존</div></div><div><div><input type="checkbox"/></div><div>/aws/rds/instance/sk-health-db/error</div><div>만기 없음</div></div><div><div><input type="checkbox"/></div><div>RDSOSMetrics</div><div>1개월</div></div><div><div><input type="checkbox"/></div><div>SK-Health-Test</div><div>만기 없음</div></div></div></div></div>			
보안요건 조치 방안	공 란			

점검 항목	Sec502		점검 결과	충족
점검 기준	분류	로그 관리		불충족
	항목명	로그 기록 접근 권한 설정		
	요구사항 내용	정보시스템의 로그 기록에 대한 접근 권한은 최소화하여 부여하고 있는가?		
점검 현황	IAM 통해 계정에 S3와 CloudTrail에 대한 접근 권한을 부여하고 있다			
	<div><div>정책 이름 ▼</div><div>정책 유형 ▼</div></div>			
	직접 연결			
	<div><div>▶  AmazonS3FullAccess</div><div>AWS 관리형 정책</div><div>X</div></div>			
보안요건 조치 방안	<div><div>▶  AWSCloudTrail_FullAccess</div><div>AWS 관리형 정책</div><div>X</div></div>			
	공 란			

점검 항목	Sec503		점검 결과	충족								
점검 기준	분류	로그 관리		불충족								
	항목명	정보시스템 이상징후 인지를 위한 모니터링										
	요구사항 내용	정보시스템 관련 오류, 오·남용(비인가 접속, 과다조회 등), 부정행위 등 이상징후를 인지할 수 있도록 로그 검토 주기, 대상, 방법 등을 포함한 로그 검토 및 모니터링 하고 있는가?										
점검 현황	Security Hub를 통해 정보시스템에 이상징후를 인지하고 대상 별로 모니터링하고 있다. <div><div>인사이트</div><div><div>시간에 따른 공급자별 새 분석 결과</div><div>시간에 따른 심각도별 새 분석 결과</div><div>2022-06-08 @ 09:00:00</div><table><tr><td>Critical</td><td>16</td></tr><tr><td>High</td><td>89</td></tr><tr><td>Medium</td><td>166</td></tr><tr><td>Low</td><td>142</td></tr></table><div>분석 결과가 가장 많은 S3 버킷</div><div>분석 결과가 가장 많은 EC2 인스턴스</div></div></div>				Critical	16	High	89	Medium	166	Low	142
Critical	16											
High	89											
Medium	166											
Low	142											
보안요건 조치 방안	공 란											

점검 항목	Sec504		점검 결과	충족
점검 기준	분류	로그 관리		불충족
	항목명	로그 시간 동기화		
	요구사항 내용	로그 및 접속 기록의 정확성을 보장하고 신뢰성 있는 로그 분석을 위하여 각 정보시스템의 시간을 표준시간으로 동기화하고 있는가?		
점검 현황	CloudWatch를 통해 정확한 로그를 분석하기 위하여 Local time zone을 설정하여 표준시간으로 동기화 하고 있다.			
	<div><div><div>Absolute</div><div>Relative</div></div><div><div>Local time zone ▲</div><div>Local time zone</div><div>UTC</div></div><div><div>Minutes</div><div>5</div><div>10</div><div>15</div><div>30</div><div>45</div></div><div><div>Hours</div><div>1</div><div>2</div><div>3</div><div>6</div><div>8</div><div>12</div></div><div><div>Days</div><div>1</div><div>2</div><div>3</div><div>4</div><div>5</div><div>6</div></div><div><div>Weeks</div><div>1</div><div>2</div><div>3</div><div>4</div></div><div><div>180</div><div>Minutes ▼</div></div><div><div>Cancel</div><div>Apply</div></div></div>			
보안요건 조치 방안	공 란			

점검 항목	Sec505		점검 결과	충족																																																					
점검 기준	분류	로그 관리		불충족																																																					
	항목명	이상 행위 발생 시 신속한 분석 및 점검																																																							
	요구사항 내용	내·외부에 의한 침해 시도, 개인정보 유출 시도, 부정행위 등 이상행위를 탐지할 수 있도록 주요 정보시스템, 응용프로그램, 네트워크, 보안시스템 등에서 발생한 네트워크 트래픽, 데이터 흐름, 이벤트 로그 등을 수집하여 분석 및 모니터링하고 있는가?																																																							
점검 현황	Detective를 통해 정보시스템에 접속하는 네트워크 트래픽, IP등 로그를 수집하고 모니터링하고 있다.																																																								
	<div><div>로컬 포트</div><div><div>범위: 06. 14. 06:00 - 06. 15. 06:00</div></div></div> <div><div>원격 포트</div><div><div>범위: 06. 14. 06:00 - 06. 15. 06:00</div></div></div> <div>활동 표시 중: 2022. 06. 14. 06:00 UTC - 2022. 06. 15. 06:00 UTC <div>편집</div></div> <div><div>Q 필터</div><div>< 1 2 3 4</div><table><tr><td><input type="checkbox"/></td><td>IP 주소 ▾</td><td>로컬 포트 ▾</td><td>원격 포트 ▾</td><td>인바운드 트래픽 ▾</td><td>아웃바운드 트래픽 ▾</td><td>프로토콜 ▾</td><td>방향성 ▾</td><td>수락 및 거부</td></tr><tr><td><input type="checkbox"/></td><td>103.178.236.132</td><td>22</td><td>-</td><td>80 B</td><td>44 B</td><td>TCP</td><td>인바운드</td><td>수락</td></tr><tr><td><input type="checkbox"/></td><td>103.203.57.11</td><td>22</td><td>-</td><td>120 B</td><td>300 B</td><td>TCP</td><td>인바운드</td><td>수락</td></tr><tr><td><input type="checkbox"/></td><td>103.203.57.14</td><td>443</td><td>-</td><td>40 B</td><td>40 B</td><td>TCP</td><td>인바운드</td><td>수락</td></tr><tr><td><input type="checkbox"/></td><td>103.203.57.21</td><td>22</td><td>-</td><td>80 B</td><td>44 B</td><td>TCP</td><td>인바운드</td><td>수락</td></tr><tr><td><input type="checkbox"/></td><td>104.206.128.30</td><td>443</td><td>-</td><td>44 B</td><td>40 B</td><td>TCP</td><td>인바운드</td><td>수락</td></tr></table></div>				<input type="checkbox"/>	IP 주소 ▾	로컬 포트 ▾	원격 포트 ▾	인바운드 트래픽 ▾	아웃바운드 트래픽 ▾	프로토콜 ▾	방향성 ▾	수락 및 거부	<input type="checkbox"/>	103.178.236.132	22	-	80 B	44 B	TCP	인바운드	수락	<input type="checkbox"/>	103.203.57.11	22	-	120 B	300 B	TCP	인바운드	수락	<input type="checkbox"/>	103.203.57.14	443	-	40 B	40 B	TCP	인바운드	수락	<input type="checkbox"/>	103.203.57.21	22	-	80 B	44 B	TCP	인바운드	수락	<input type="checkbox"/>	104.206.128.30	443	-	44 B	40 B	TCP	인바운드
<input type="checkbox"/>	IP 주소 ▾	로컬 포트 ▾	원격 포트 ▾	인바운드 트래픽 ▾	아웃바운드 트래픽 ▾	프로토콜 ▾	방향성 ▾	수락 및 거부																																																	
<input type="checkbox"/>	103.178.236.132	22	-	80 B	44 B	TCP	인바운드	수락																																																	
<input type="checkbox"/>	103.203.57.11	22	-	120 B	300 B	TCP	인바운드	수락																																																	
<input type="checkbox"/>	103.203.57.14	443	-	40 B	40 B	TCP	인바운드	수락																																																	
<input type="checkbox"/>	103.203.57.21	22	-	80 B	44 B	TCP	인바운드	수락																																																	
<input type="checkbox"/>	104.206.128.30	443	-	44 B	40 B	TCP	인바운드	수락																																																	
보안요건 조치 방안	공 란																																																								

점검 항목	Sec506		점검 결과	충족
점검 기준	분류	개인정보보호		불충족
	항목명	개인정보처리시스템 법률 준수 검토 및 관리		
	요구사항 내용	개인정보처리시스템에 대한 접속 기록은 법적 요구사항을 준수할 수 있도록 관리하고 있는가?		
점검 현황	현재 CloudTrail을 통해 개인정보처리 시스템의 접속 기록을 남기고 있다. 1. 계정 식별자 (개인정보 취급자 ID) 2. 접속 일시(접속한 시간 또는 업무 수행 시간) 3. 접속지 정보(접속 IP) 4. 처리 정보 주체 정보(이용자 ID, 및 개인정보) 5. 수행업무(조회, 변경, 입력, 삭제 등) 개인정보처리 시스템에 대한 접속 기록을 별도의 저장장치를 통해 백업하고 있지는 않음.			
보안요건 조치 방안	기록 백업 방법 순서 1. S3 에서 버전 관리를 사용해서 활성화시킨다. 2. SDK 를 사용하여 기존의 S3 버킷에서 다른 버킷으로 복사한다. 3. Amazon Glacier 를 사용하여 백업한다. 4. 자체 백업되는 프로덕션 서버로 백업한다.			

2.6 보안관리

시험과 운영 환경 분리

점검 항목	Sec601		점검 결과	충족
점검 기준	분류	시험과 운영 환경 분리		불충족
	항목명	시험 시스템과 운영시스템의 분리		
	요구사항 내용	정보시스템의 개발 및 시험 시스템을 운영시스템과 분리하고 있는가?		
점검 현황	현재 SK헬스 클라우드 인프라는 운영시스템으로만 구성되어 있어 점검 항목에서 제외한다.			
보안요건 조치 방안	공 란			

시험 데이터 보안

점검 항목	Sec602		점검 결과	충족
점검 기준	분류	시험 데이터 보안		불충족
	항목명	실제 운영 데이터의 사용 제한		
	요구사항 내용	정보시스템의 개발 및 시험 과정에서 실제 운영 데이터의 사용을 제한하고 있는가?		
점검 현황	현재 SK헬스 클라우드 인프라는 운영시스템으로만 구성되어 있어 점검 항목에서 제외한다.			
보안요건 조치 방안	공 란			

장애 관리

점검 항목	Sec603		점검 결과	충족																																																	
점검 기준	분류	장애 관리		불충족																																																	
	항목명	정보시스템의 장애 관리																																																			
	요구사항 내용	정보시스템의 장애를 인지하고 탐지 및 관리를 하고 있는가?																																																			
점검 현황	GuardDuty를 통해 정보시스템의 이상행위를 탐지하고 있다.																																																				
	<div><div>GuardDuty > 결과</div><div>표시 102 / 102 12 39 51</div><div><div>결과 정보</div><div><div>결과 표시 안 함</div><div>정보</div><div>저장된 규칙</div><div>저장된 규칙 없음</div></div></div><div><div>현재</div><div>필터 추가</div></div><table><thead><tr><th><input type="checkbox"/></th><th>찾기 유형</th><th>리소스</th><th>최근 발견 ...</th><th>개수</th></tr></thead><tbody><tr><td><input type="checkbox"/></td><td>▲ {생물} UnauthorizedAccess:S3/MaliciousIPCaller.Custom</td><td>S3 Bucket: bucketName</td><td>12시간 전</td><td>1</td></tr><tr><td><input type="checkbox"/></td><td>■ {생물} Discovery:Kubernetes/SuccessfulAnonymousAccess</td><td>EKSCluster: GeneratedFindingEKSClusterName</td><td>12시간 전</td><td>1</td></tr><tr><td><input type="checkbox"/></td><td>○ {생물} PolicyIAMUser/RootCredentialUsage</td><td>GeneratedFindingUserName: GeneratedFindingAccessKeyId</td><td>12시간 전</td><td>1</td></tr><tr><td><input type="checkbox"/></td><td>▲ {생물} Exfiltration:S3/MaliciousIPCaller</td><td>S3 Bucket: bucketName</td><td>12시간 전</td><td>1</td></tr><tr><td><input type="checkbox"/></td><td>▲ {생물} Trojan:EC2/DriveBySourceTraffic:DNS</td><td>Instance: i-99999999</td><td>12시간 전</td><td>1</td></tr><tr><td><input type="checkbox"/></td><td>■ {생물} CredentialAccess:IAMUser/AnomalousBehavior</td><td>GeneratedFindingUserName: GeneratedFindingAccessKeyId</td><td>12시간 전</td><td>1</td></tr><tr><td><input type="checkbox"/></td><td>▲ {생물} CredentialAccess:Kubernetes/MaliciousIPCaller.Custom</td><td>EKSCluster: GeneratedFindingEKSClusterName</td><td>12시간 전</td><td>1</td></tr><tr><td><input type="checkbox"/></td><td>■ {생물} Recon:EC2/Portscan</td><td>Instance: i-99999999</td><td>12시간 전</td><td>1</td></tr><tr><td><input type="checkbox"/></td><td>▲ {생물} PolicyS3/BucketAnonymousAccessGranted</td><td>GeneratedFindingUserName: GeneratedFindingAccessKeyId</td><td>12시간 전</td><td>1</td></tr></tbody></table></div>				<input type="checkbox"/>	찾기 유형	리소스	최근 발견 ...	개수	<input type="checkbox"/>	▲ {생물} UnauthorizedAccess:S3/MaliciousIPCaller.Custom	S3 Bucket: bucketName	12시간 전	1	<input type="checkbox"/>	■ {생물} Discovery:Kubernetes/SuccessfulAnonymousAccess	EKSCluster: GeneratedFindingEKSClusterName	12시간 전	1	<input type="checkbox"/>	○ {생물} PolicyIAMUser/RootCredentialUsage	GeneratedFindingUserName: GeneratedFindingAccessKeyId	12시간 전	1	<input type="checkbox"/>	▲ {생물} Exfiltration:S3/MaliciousIPCaller	S3 Bucket: bucketName	12시간 전	1	<input type="checkbox"/>	▲ {생물} Trojan:EC2/DriveBySourceTraffic:DNS	Instance: i-99999999	12시간 전	1	<input type="checkbox"/>	■ {생물} CredentialAccess:IAMUser/AnomalousBehavior	GeneratedFindingUserName: GeneratedFindingAccessKeyId	12시간 전	1	<input type="checkbox"/>	▲ {생물} CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	EKSCluster: GeneratedFindingEKSClusterName	12시간 전	1	<input type="checkbox"/>	■ {생물} Recon:EC2/Portscan	Instance: i-99999999	12시간 전	1	<input type="checkbox"/>	▲ {생물} PolicyS3/BucketAnonymousAccessGranted	GeneratedFindingUserName: GeneratedFindingAccessKeyId	12시간 전
<input type="checkbox"/>	찾기 유형	리소스	최근 발견 ...	개수																																																	
<input type="checkbox"/>	▲ {생물} UnauthorizedAccess:S3/MaliciousIPCaller.Custom	S3 Bucket: bucketName	12시간 전	1																																																	
<input type="checkbox"/>	■ {생물} Discovery:Kubernetes/SuccessfulAnonymousAccess	EKSCluster: GeneratedFindingEKSClusterName	12시간 전	1																																																	
<input type="checkbox"/>	○ {생물} PolicyIAMUser/RootCredentialUsage	GeneratedFindingUserName: GeneratedFindingAccessKeyId	12시간 전	1																																																	
<input type="checkbox"/>	▲ {생물} Exfiltration:S3/MaliciousIPCaller	S3 Bucket: bucketName	12시간 전	1																																																	
<input type="checkbox"/>	▲ {생물} Trojan:EC2/DriveBySourceTraffic:DNS	Instance: i-99999999	12시간 전	1																																																	
<input type="checkbox"/>	■ {생물} CredentialAccess:IAMUser/AnomalousBehavior	GeneratedFindingUserName: GeneratedFindingAccessKeyId	12시간 전	1																																																	
<input type="checkbox"/>	▲ {생물} CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	EKSCluster: GeneratedFindingEKSClusterName	12시간 전	1																																																	
<input type="checkbox"/>	■ {생물} Recon:EC2/Portscan	Instance: i-99999999	12시간 전	1																																																	
<input type="checkbox"/>	▲ {생물} PolicyS3/BucketAnonymousAccessGranted	GeneratedFindingUserName: GeneratedFindingAccessKeyId	12시간 전	1																																																	
보안요건 조치 방안	공 란																																																				

클라우드 보안

점검 항목	Sec604		점검 결과	충족
점검 기준	분류	클라우드 보안		불충족
	항목명	클라우드 서비스 보안 통제 정책 이행		
	요구사항 내용	클라우드 서비스 이용 시 비인가 접근, 설정 오류 등을 방지할 수 있도록 보안 구성 및 설정 기준, 보안설정 변경 및 승인 절차, 안전한 접속방법, 권한 체계 등 보안 통제 정책을 이행하고 있는가?		
점검 현황	접근 통제와 계정·권한 관리 항목에서 요구사항을 충족하고 있다.			
보안요건 조치 방안	공 란			

점검 항목	Sec605		점검 결과	충족
점검 기준	분류	클라우드 보안		불충족
	항목명	클라우드 서비스 관리자 권한 보호대책 적용		
	요구사항 내용	클라우드 서비스 관리자 권한은 역할에 따라 최소화하여 부여하고 관리자 권한에 대한 비인가된 접근, 권한 오남용 등을 방지할 수 있도록 강화된 인증, 암호화, 접근 통제, 감사 기록 등 보호대책을 적용하고 있는가?		
점검 현황	계정·권한 관리, 식별·인증, 암호화 로깅 모니터링에서 요구사항을 충족하고 있다.			
보안요건 조치 방안	공 란			

공개서버 보안

점검 항목	Sec606		점검	충족									
점검 기준	분류	공개서버 보안	결과	불충족									
	항목명	공개서버 DMZ 설치 및 보안시스템 보호											
	요구사항 내용	공개서버는 내부 네트워크와 분리된 DMZ(Demilitarized Zone)영역에 설치하고 침입차단시스템 등 보안시스템을 통해 보호하고 있는가?											
점검 현황	VPC의 라우팅 테이블에 Web-Subnet을 연결하여 퍼블릭 서브넷으로 설정하고 Network Firewall에 연결하여 보호하고 있다.												
	rtb-09543b3b04e3b7728 / SK-Health-RT												
	세부 정보 라우팅 서브넷 연결 엣지 연결 라우팅 전파 태그												
	명시적 서브넷 연결 (2)												
	<div>서브넷 연결 검색</div>												
	<table><thead><tr><th>서브넷 ID</th><th>▼</th><th>IPv4 CIDR</th></tr></thead><tbody><tr><td>subnet-00fbc2aba7e84e160</td><td>Web-Subnet-1</td><td>10.0.0.0/24</td></tr><tr><td>subnet-09da92cc2d526d2be</td><td>Web-Subnet-2</td><td>10.0.2.0/24</td></tr></tbody></table>				서브넷 ID	▼	IPv4 CIDR	subnet-00fbc2aba7e84e160	Web-Subnet-1	10.0.0.0/24	subnet-09da92cc2d526d2be	Web-Subnet-2	10.0.2.0/24
서브넷 ID	▼	IPv4 CIDR											
subnet-00fbc2aba7e84e160	Web-Subnet-1	10.0.0.0/24											
subnet-09da92cc2d526d2be	Web-Subnet-2	10.0.2.0/24											
	<div>방화벽 서브넷</div> <div>여러 가용 영역에서 영역당 하나의 서브넷으로 방화벽을 배포할 수 있습니다. 각 서브넷에는 하나 이상의 가용 IP 주소가 있어야 합니다.</div> <div>가용 영역</div> <div><div>ap-northeast-2a</div><div>ap-northeast-2b</div></div> <div>서브넷</div> <div><div>Web-Subnet-1</div><div>Web-Subnet-2</div></div>												
보안요건 조치 방안	공 란												

패치관리

점검 항목	Sec607		점검 결과	충족
점검 기준	분류	패치관리		불충족
	항목명	공개 인터넷 접속을 통한 패치 제한		
	요구사항 내용	주요 서버, 네트워크시스템, 보안시스템 등의 경우 공개 인터넷 접속을 통한 패치를 제한하고 있는가?		
점검 현황	VPC의 보안 그룹을 통해 WAS의 인바운드 규칙에서 HTTP 포트를 막아 인터넷 접속 패치를 제한하고 있다.			
	<div>sg-043ef07aa1e8f54f5 - WAS-SG</div> <div>세부 정보 인바운드 규칙 아웃바운드 규칙 태그</div> <div>인바운드 규칙 (2) 🔄 태그 관리 인바운드 규칙 편집</div> <div><input type="text" value="Q 보안 그룹 규칙 필터"/></div> <div><div><div><input type="checkbox"/></div><div>Name ▾</div></div><div><div><input type="checkbox"/></div><div>sg-03184cd5a5b1d5fc6</div></div><div><div><input type="checkbox"/></div><div>sg-06497c2bb9fb83a5c</div></div></div> <div><div>보안 그룹 규칙 ID ▾</div><div>IP 버전 ▾</div><div>유형 ▾</div><div>프로토콜 ▾</div><div>포트 범위 ▾</div><div>소스 ▾</div></div> <div><div>-</div><div>IPv4</div><div>사용자 지정 TCP</div><div>TCP</div><div>5000</div><div>10.0.0.0/22</div></div> <div><div>-</div><div>IPv4</div><div>SSH</div><div>TCP</div><div>22</div><div>10.0.0.0/22</div></div> <div><div><</div><div>></div><div>1</div><div>🔍</div></div>			
보안요건 조치 방안	공 란			

악성코드 통제

점검 항목	Sec608		점검	충족																				
점검 기준	분류	악성코드 통제	결과	불충족																				
	항목명	악성코드 보호대책 이행																						
	요구사항 내용	바이러스, 웜, 트로이목마, 랜섬웨어 등의 악성코드로부터 정보시스템 및 업무용 단말기 등을 보호하기 위하여 보호대책을 이행하고 있는가?																						
점검 현황	WAF를 통해 Rule을 설정하여 다양한 악성코드 등 공격으로부터 보호대책을 이행하고 있다.																							
	<div><div>Free rule groups</div><table><thead><tr><th>Name</th><th>Capacity</th><th>Action</th></tr></thead><tbody><tr><td><div>Admin protection</div><div>Contains rules that allow you to block external access to exposed admin pages. This may be useful if you are running third-party software or would like to reduce the risk of a malicious actor gaining administrative access to your application.</div></td><td>100</td><td><div><div><div><div></div></div>Add to web ACL</div><div>Edit</div></div></td></tr><tr><td><div>Amazon IP reputation list</div><div>This group contains rules that are based on Amazon threat intelligence. This is useful if you would like to block sources associated with bots or other threats.</div></td><td>25</td><td><div><div><div><div></div></div>Add to web ACL</div><div>Edit</div></div></td></tr><tr><td><div>Anonymous IP list</div><div>This group contains rules that allow you to block requests from services that allow obfuscation of viewer identity. This can include request originating from VPN, proxies, Tor nodes, and hosting providers (including AWS). This is useful if you want to filter out viewers that may be trying to hide their identity from your application.</div></td><td>50</td><td><div><div><div><div></div></div>Add to web ACL</div><div>Edit</div></div></td></tr><tr><td><div>Core rule set</div><div>Contains rules that are generally applicable to web applications. This provides protection against exploitation of a wide range of vulnerabilities, including those described in OWASP publications.</div></td><td>700</td><td><div><div><div><div></div></div>Add to web ACL</div><div>Edit</div></div></td></tr><tr><td><div>Known bad inputs</div><div>Contains rules that allow you to block request patterns that are known to be invalid and are associated with exploitation or discovery of vulnerabilities. This can help reduce the risk of a malicious actor discovering a vulnerable application.</div></td><td>200</td><td><div><div><div><div></div></div>Add to web ACL</div><div>Edit</div></div></td></tr><tr><td><div>Linux operating system</div><div>Contains rules that block request patterns associated with exploitation of vulnerabilities specific to Linux, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which the attacker should not have had access.</div></td><td>200</td><td><div><div><div><div></div></div>Add to web ACL</div><div>Edit</div></div></td></tr></tbody></table></div>				Name	Capacity	Action	<div>Admin protection</div> <div>Contains rules that allow you to block external access to exposed admin pages. This may be useful if you are running third-party software or would like to reduce the risk of a malicious actor gaining administrative access to your application.</div>	100	<div><div><div><div></div></div>Add to web ACL</div><div>Edit</div></div>	<div>Amazon IP reputation list</div> <div>This group contains rules that are based on Amazon threat intelligence. This is useful if you would like to block sources associated with bots or other threats.</div>	25	<div><div><div><div></div></div>Add to web ACL</div><div>Edit</div></div>	<div>Anonymous IP list</div> <div>This group contains rules that allow you to block requests from services that allow obfuscation of viewer identity. This can include request originating from VPN, proxies, Tor nodes, and hosting providers (including AWS). This is useful if you want to filter out viewers that may be trying to hide their identity from your application.</div>	50	<div><div><div><div></div></div>Add to web ACL</div><div>Edit</div></div>	<div>Core rule set</div> <div>Contains rules that are generally applicable to web applications. This provides protection against exploitation of a wide range of vulnerabilities, including those described in OWASP publications.</div>	700	<div><div><div><div></div></div>Add to web ACL</div><div>Edit</div></div>	<div>Known bad inputs</div> <div>Contains rules that allow you to block request patterns that are known to be invalid and are associated with exploitation or discovery of vulnerabilities. This can help reduce the risk of a malicious actor discovering a vulnerable application.</div>	200	<div><div><div><div></div></div>Add to web ACL</div><div>Edit</div></div>	<div>Linux operating system</div> <div>Contains rules that block request patterns associated with exploitation of vulnerabilities specific to Linux, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which the attacker should not have had access.</div>	200
Name	Capacity	Action																						
<div>Admin protection</div> <div>Contains rules that allow you to block external access to exposed admin pages. This may be useful if you are running third-party software or would like to reduce the risk of a malicious actor gaining administrative access to your application.</div>	100	<div><div><div><div></div></div>Add to web ACL</div><div>Edit</div></div>																						
<div>Amazon IP reputation list</div> <div>This group contains rules that are based on Amazon threat intelligence. This is useful if you would like to block sources associated with bots or other threats.</div>	25	<div><div><div><div></div></div>Add to web ACL</div><div>Edit</div></div>																						
<div>Anonymous IP list</div> <div>This group contains rules that allow you to block requests from services that allow obfuscation of viewer identity. This can include request originating from VPN, proxies, Tor nodes, and hosting providers (including AWS). This is useful if you want to filter out viewers that may be trying to hide their identity from your application.</div>	50	<div><div><div><div></div></div>Add to web ACL</div><div>Edit</div></div>																						
<div>Core rule set</div> <div>Contains rules that are generally applicable to web applications. This provides protection against exploitation of a wide range of vulnerabilities, including those described in OWASP publications.</div>	700	<div><div><div><div></div></div>Add to web ACL</div><div>Edit</div></div>																						
<div>Known bad inputs</div> <div>Contains rules that allow you to block request patterns that are known to be invalid and are associated with exploitation or discovery of vulnerabilities. This can help reduce the risk of a malicious actor discovering a vulnerable application.</div>	200	<div><div><div><div></div></div>Add to web ACL</div><div>Edit</div></div>																						
<div>Linux operating system</div> <div>Contains rules that block request patterns associated with exploitation of vulnerabilities specific to Linux, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which the attacker should not have had access.</div>	200	<div><div><div><div></div></div>Add to web ACL</div><div>Edit</div></div>																						
보안요건 조치 방안	공 란																							

취약점 점검

점검 항목	Sec609		점검 결과	충족																																																																									
점검 기준	분류	취약점 점검 및 조치		불충족																																																																									
	항목명	최신 보안 취약점 분석 및 조치																																																																											
	요구사항 내용	최신 보안 취약점이 정보시스템에 미치는 영향을 분석하여 조치하고 있는가?																																																																											
점검 현황	Security Hub를 통해 정보시스템에 미치는 보안 취약점을 심각도 별로 분류한다. Inspector를 통해 정보시스템에 미치는 보안 취약점 분석하고 있다.																																																																												
	<div><div><div><div>분석 결과</div><div>보안 문제나 실례한 보안 감사가 분석 결과로 표시됩니다.</div><div><div>Q</div><div>위요율로 상태</div><div>알지알</div><div>NEW</div><div>X</div></div><div><div>위요율로 상태</div><div>알지알</div><div>NOTIFIED</div><div>X</div></div><div><div>레코드로 상태</div><div>알지알</div><div>ACTIVE</div><div>X</div></div><div>필터 추가</div></div><div><div><</div><div>1</div><div>></div></div><table><thead><tr><th><input type="checkbox"/></th><th>심각도</th><th>위요율로 상태</th><th>레코드로 상태</th><th>리전</th><th>Account ID</th><th>회사</th><th>제품</th><th>제목</th><th>리소스</th><th>규정 준수 상태</th><th>업데이트 시간</th></tr></thead><tbody><tr><td><input type="checkbox"/></td><td>MEDIUM</td><td>NEW</td><td>ACTIVE</td><td>ap-northeast-2</td><td>504301552141</td><td>AWS</td><td>Security Hub</td><td>EC2.6 VPC flow logging should be enabled in all VPCs</td><td>EC2 VPC vpc-04b7276a409e46441</td><td>FAILED</td><td>35분 전</td></tr><tr><td><input type="checkbox"/></td><td>MEDIUM</td><td>NEW</td><td>ACTIVE</td><td>ap-northeast-2</td><td>504301552141</td><td>AWS</td><td>Security Hub</td><td>EC2.22 Unused EC2 security groups should be removed</td><td>EC2 보안 그룹 RDS-SG</td><td>FAILED</td><td>35분 전</td></tr></tbody></table></div><div><div>Finding overview</div><table><tr><td>AWS account ID</td><td>504301552141</td></tr><tr><td>Type</td><td>Network Reachability</td></tr><tr><td>Open port range</td><td>[22, 22]</td></tr><tr><td>Severity</td><td>Medium</td></tr><tr><td>Updated at</td><td>June 15, 2022 7:22 AM (UTC+09:00)</td></tr><tr><td>Created at</td><td>June 15, 2022 7:22 AM (UTC+09:00)</td></tr></table><div><div>Resource affected</div><table><tr><td>Resource ID</td><td>i-099bc7df685086f22</td><td></td></tr><tr><td>Type</td><td>AWS EC2 Instance</td><td></td></tr><tr><td>EC2 instance type</td><td>t2.micro</td><td></td></tr><tr><td>Platform</td><td>--</td><td></td></tr><tr><td>VPC ID</td><td>vpc-06a0de8caccacc3a7</td><td></td></tr><tr><td>Subnet ID</td><td>subnet-00fbc2aba7e84e160</td><td></td></tr><tr><td>AMI</td><td>ami-058165de3b7202099</td><td></td></tr><tr><td>Launched at</td><td>June 14, 2022 2:34 PM (UTC+09:00)</td><td></td></tr></table><div><div>Tags</div><table><tr><td>Name</td><td>web</td></tr></table><div><div>Open Network Paths</div><div>1. Internet Gateway > Network Acl > Security Group > Network Interface > Instance</div></div></div></div></div></div>				<input type="checkbox"/>	심각도	위요율로 상태	레코드로 상태	리전	Account ID	회사	제품	제목	리소스	규정 준수 상태	업데이트 시간	<input type="checkbox"/>	MEDIUM	NEW	ACTIVE	ap-northeast-2	504301552141	AWS	Security Hub	EC2.6 VPC flow logging should be enabled in all VPCs	EC2 VPC vpc-04b7276a409e46441	FAILED	35분 전	<input type="checkbox"/>	MEDIUM	NEW	ACTIVE	ap-northeast-2	504301552141	AWS	Security Hub	EC2.22 Unused EC2 security groups should be removed	EC2 보안 그룹 RDS-SG	FAILED	35분 전	AWS account ID	504301552141	Type	Network Reachability	Open port range	[22, 22]	Severity	Medium	Updated at	June 15, 2022 7:22 AM (UTC+09:00)	Created at	June 15, 2022 7:22 AM (UTC+09:00)	Resource ID	i-099bc7df685086f22		Type	AWS EC2 Instance		EC2 instance type	t2.micro		Platform	--		VPC ID	vpc-06a0de8caccacc3a7		Subnet ID	subnet-00fbc2aba7e84e160		AMI	ami-058165de3b7202099		Launched at	June 14, 2022 2:34 PM (UTC+09:00)		Name
<input type="checkbox"/>	심각도	위요율로 상태	레코드로 상태	리전	Account ID	회사	제품	제목	리소스	규정 준수 상태	업데이트 시간																																																																		
<input type="checkbox"/>	MEDIUM	NEW	ACTIVE	ap-northeast-2	504301552141	AWS	Security Hub	EC2.6 VPC flow logging should be enabled in all VPCs	EC2 VPC vpc-04b7276a409e46441	FAILED	35분 전																																																																		
<input type="checkbox"/>	MEDIUM	NEW	ACTIVE	ap-northeast-2	504301552141	AWS	Security Hub	EC2.22 Unused EC2 security groups should be removed	EC2 보안 그룹 RDS-SG	FAILED	35분 전																																																																		
AWS account ID	504301552141																																																																												
Type	Network Reachability																																																																												
Open port range	[22, 22]																																																																												
Severity	Medium																																																																												
Updated at	June 15, 2022 7:22 AM (UTC+09:00)																																																																												
Created at	June 15, 2022 7:22 AM (UTC+09:00)																																																																												
Resource ID	i-099bc7df685086f22																																																																												
Type	AWS EC2 Instance																																																																												
EC2 instance type	t2.micro																																																																												
Platform	--																																																																												
VPC ID	vpc-06a0de8caccacc3a7																																																																												
Subnet ID	subnet-00fbc2aba7e84e160																																																																												
AMI	ami-058165de3b7202099																																																																												
Launched at	June 14, 2022 2:34 PM (UTC+09:00)																																																																												
Name	web																																																																												
보안요건 조치 방안	공 란																																																																												