항목
라우드 영향평가 체크리스트(IaaS) ver1
라우드 영향평가 체크리스트(IaaS) ver1
라우드 영향평가 체크리스트(IaaS) ver1

내용	배포일
- 중복 체크리스트/증적 사항 삭제	6/4/2021
- 체크리스트 구분 변경 - 체크리스트 항목 추가 (ACS, Well-known port 관련 사항) - 중복 체크리스트/증적 사항 삭제 - 인프라/네트워크 증적 관련 예시 추가	9/3/2021
- 데이터 변경, 사내 T/F관리 및 운영 관련 승인 담당자 추가 - 서비스별 접근/변경 이력 관리 항목 추가 - DB/서버 접근 통제 솔루션 관련 항목 삭제 (개인정보 영향평가 중복 사항) - ACL 접근 통제 항목 업데이트 - 웹페이지 보안 강화 항목 추가 - 내부 트래픽 로그 항목 추가 - 중복 점검 항목 삭제	7/29/2022

변경자
송기봉
송기봉
송기봉

[이행점검 담당자 정보]

이행점검 작성자 (성명/ 직함)
이행점검 작성자 소속 조직명
체크리스트 작성일
이행점검 승인 관리자 (성명/ 직함)

[시스템/서비스 정보]

시스템/서비스명
시스템/서비스 개요
외부 클라우드 서비스 종류
외부 클라우드 서비스명

[시스템/서비스 중요도 자체평가]

중요도 점수 (기밀성 점수+무결성 점수+가용성 점수)

기밀성	매우중요(3)	정보등급 자체평가(클라우드 영향평가 항목
	중요(2)	정보등급 자체평가(클라우드 영향평가 항목
	보통(1)	정보등급 자체평가(클라우드 영향평가 항목
무결성	매우중요(3)	시스템 내 데이터 변조 시 업무 또는 서비스 예) 다른 시스템으로 데이터를 전달하는 기능(
	중요(2)	시스템 내 데이터 변조 시 업무 또는 서비스 예) 다른 시스템으로부터 데이터를 전달받는 시
	보통(1)	시스템 내 데이터 변조 시 업무 또는 서비스
가용성	매우중요(3)	시스템 장애 또는 침해사고 발생 시 대체시
	중요(2)	시스템 장애 또는 침해사고 발생 시 대체시 예) Admin 시스템 (실제 서비스에는 이상이 없
	보통(1)	시스템 장애 또는 침해사고 발생 시 대체시 예) 고객 콜센터 시스템 장애 시, 홈페이지 채팅

[체크리스트 항목 작성 여부]

1. 정보등급 자체평가
2. 시스템 보안성 체크리스트
3. 클라우드 설계 보안성 체크르시트
4. 인프라 아키텍쳐
5. 데이터(서비스) 흐름도
6. IAM리스트
7. IP리스트(CIDR)
8. Security Group
9. Network ACL

예시) OOO / 선임, OOO / 선임
참고) EP상 정확한 부서명을 입력하세요.
예시) YYYY.MM.DD
예시) OOO / 팀장

예시) 사이버보안 서버
예시) IaaS, SaaS, PaaS 등
예시) GCP, AWS, Azure 등

8점

목) 항목 중 합계가 11점 이상인 경우
목) 항목 중 합계가 7점 이상인 경우
목) 항목 중 합계가 7점 미만인 경우
스에 장애를 유발하고, 타 시스템과 연동되어 타시스템에도 영향을 주는 시스템인 경우 이 있는 시스템
스에 장애를 유발하고 타 시스템과 연동되어 타 시스템에 영향을 받는 시스템인 경우 시스템
스에 장애를 유발하는 시스템인 경우
스템이 없어 서비스가 중단되는 경우
스템은 없지만 서비스는 일부 지속 되는 경우 었거나, 일부 영향이 있을 수 있음)
스템이 있어 업무 또는 서비스가 일부 지속되는 경우 팅 상담으로 일부 고객 서비스 진행 가능

예시) O / X (미작성 사유 작성)
예시) O / X (미작성 사유 작성)
예시) O / X (미작성 사유 작성)
예시) O / X (미작성 사유 작성)
예시) O / X (미작성 사유 작성)
예시) O / X (미작성 사유 작성)
예시) O / X (미작성 사유 작성)
예시) O / X (미작성 사유 작성)
예시) O / X (미작성 사유 작성)

[1. 정보등급 자체평가]

작성가이드

1. 사외 클라우드에 전송하여 활용하고자 하는 데이터를 식별한 후, 중요등급 평가 및 근거를 작성.

※ 개인정보인 경우 사내한 등급인 7점 이상으로 작성

정보등급 평가 항목별 기준

항목	내용	중요도
독점성	• 자사의 노력에 의해서 완성된 결과물(정보)로써 기업의 Know-how나 독점권을 확보하고 있으며 타사에서는 보유하고 있지 않은 정보	(1 2 3 4 5) 中 택 1
위험성	• 내·외부에 유출될 경우 경영차질, 법적소송, 기업 이미지 손상으로 이어질 수 있는 민감한 정보 (경영정보, 개발정보, 품질정보, 법적 보호 대상인 개인정보 등)	(1 2 3 4 5) 中 택 1
경제성	• 내·외부에 유출될 경우 직·간접적인 경제적 손실을 초래하거나 타사에 경제적 이익을 줄 수 있는 정보 (매출액, 점유율 하락, 판가 하락, 원가율 상승 등)	(1 2 3 4 5) 中 택 1
판정기준	• 기업의 생존과 직결된 정보로 특정 항목의 중요도가 특별히 높다고 판단될 경우 비밀로 관리	자체분류
	• 비밀(Confidential) 등급 : 유관부서 합의 후 클라우드 사용, 암호화 대상	합계 11점 이상
	• 사내한(Internal Use Only) 등급 : 유관부서 합의 후 클라우드 사용, 암호화 대상	합계 7점 이상
	• 일반 등급 : 외부 클라우드 사용 가능	합계 7점 미만

개인정보

기업비밀	개
비밀	
사내한	

비밀 분류 기준

(참고 : 특허청 영업비밀 등급 자가확인 서비스 https://www.tradesecret.or.kr/info/secret/home.do)

설명	저장 목적	독점성 (1~5점)	위험성 (1~5점)	경제성 (1~5점)
예) global repair data	data table(set)의 용도 기술	2	4	2
예) LDB 수집로그		3	2	1

분류 기준

개인정보	정의	개인정보 주요 내용
1등급	민감한 개인정보, 재경정보 또는 개인의 고유한 특성을 구별하기 위하여 부여된 식별정보 (이하 '고유식별정보'라 칭함)	법에서 정의한 1등급 정보 : 개인정보보호법에서 정한 고유식별정보(주민등록번호, 운전면허번호, 외국인 등록번호, 여권번호), 신용정보, 계좌번호, 신용카드번호, 바이오(지문/홍채/정맥)정보, 민감정보(종교, 노조, 정당, 장애, 질병(병력), 건강상태, 치료정보, 유전정보, 패스워드, 위치정보(GPS나 휴대폰에 의한 개인의 위치정보)
2등급	회사 외의 개인정보를 2가지 이상의 정보조합으로 개인을 특정할 수 있는 중요한 정보	이름, 개인용(ID, e-메일 계정, 주소, 전화번호, 핸드폰, PC Mac) 조합, ESN/IMEI, USIM No., 생년월일, 쿠키, 성별, 사진(이미지) 등
3등급	3가지 이상의 정보조합으로도 개인을 식별하거나 특정하기가 힘든 정보 및 개인정보로써 Risk가 적은 정보	이름, 학력, 고향, 종교, 취미, 전공, 성향, 생일, 기념일, 출신학교, 가족정보, 직업, 취미, 교육정보,병역기록, 회사정보(부서명, 사번, ID, 주소, 전화번호, 신용카드번호 등)

합계	현업 검토의견	저장 데이터(or 로그)	저장 데이터 형태	값(예시)
8	배점 이유를 상세히 기술	Region Name	문자열	KR, US, COM, EU
		Parts Desc5	문자열	
6		locale	문자열	KR, US, COM, EU
		mcc	숫자	450

저장 데이터(or 로그) 설명
법인 위치한 지역
사용한 파츠 설명
국가코드
mcc

수집 시나리오(전송시점)(UX)	수집경로(From → To)	M/O
서비스수리기사가 수리시 GSFS(앱 또는 PC)에 입력	GSFS → GERP → EDW (LGE 전산시스템) -> Intellytics	M
서비스수리기사가 수리시 GSFS(앱 또는 PC)에 입력	GSFS → GERP → EDW (LGE 전산시스템) -> Intellytics	M
LDB Log 파일 추출 성공 후	RemoteCall -> Q-help Ser	M
LDB Log 파일 추출 성공 후	RemoteCall -> Q-help Ser	M

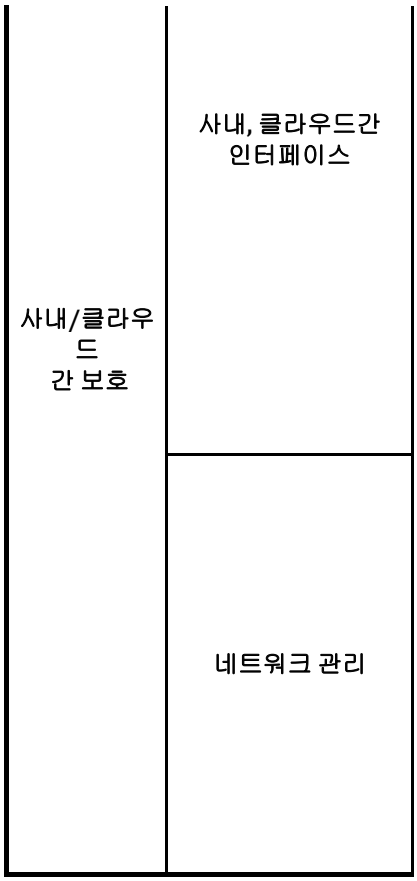
저장위치	저장방법	데이터 암호화
AWS S3	DB	N
AWS S3	DB	N
AWS RDS	DB	N
AWS RDS	DB	N

[2. 시스템 보안성 항목 검토서]

작성가이드
1. 평가내용/질문에 따른 적용 유/무 확
2. 답변(F)이 Yes인 경우 증적내용(I)를
3. 답변(F)이 No, N/A인 경우 사유를 비

구분	평가항목
계정 관리 및 Key 관리	MFA(다중인증) 적용
	계정 관리

	Key 관리
데이터 관리	데이터 정보 유출 방지
	데이터 흐름 관리
	데이터 보안
	데이터 파기


사내/클라우드
간 보호
사내, 클라우드간
인터페이스
네트워크 관리

확인 후 답변(F) 선택(Yes, No, N/A)
확인 후 비고(G)에 캡쳐하여 첨부
고(F)에 작성

평가내용	중요도
클라우드 생성 계정, 인프라 관리자 계정은 반드시 MFA를 적용한다.	매우 중요
역할 별 사용자 계정 분리 검토를 해야 한다.	매우 중요
클라우드 콘솔 이용 시 개인 업무메일을 이용하며, 1인 1계정을 생성한다.	매우 중요
사용자 및 관리자 계정 관리 방안을 수립해야 한다.	매우 중요
루트(root) 계정 사용자 엑세스 키는 삭제한다.	매우 중요
권한 할당 정책을 수립해야 한다.	매우 중요

공용계정(서비스/인프라 운영 계정 등)을 위한 계정은 반드시 사내 Alias 메일을 사용한다.	매우 중요
Key 관리 정책 및 기준 수립해야 한다	매우 중요
자원 접근 Key 변경에 대한 서비스 영향도 검토를 해야 한다.	매우 중요
데이터(DB)에 대한 부적절한 행위에 대해 통제 및 감사를 할 수 있어야 한다.	매우 중요
시스템 및 인프라 간 데이터의 이동, 복제 단위로 관리 되어야 하며 직·간접적인 모든 데이터 흐름을 포함하며 등록 및 변경 시 업무혁신담당 승인을 득해야 한다. (담당부서 : IT인프라팀)	매우 중요
자사 경영정보 및 1등급 정보의 저장영역은 자사 독립적(물리적 및 논리적)으로 제공해야 하며 타 부서간의 승인 없이 저장영역을 사용 및 재사용을 허용할 수 없다. ※ 경영정보 및 1등급 정보의 저장시에는 무조건 자사의 물리적으로 독립된 형태로 제공해야 합니다. 이 부분이 제공되지 않는 형태의 클라우드는 모든 항목에 평가를 PASS 하더라도 허용할 수 없습니다.	매우 중요
클라우드에 저장되는 데이터는 완전한 삭제를 위해 암호화하여 삭제하며, 이미 암호화되어 있는 경우에도 동일하게 진행한다.	매우 중요
사내 시스템과 외부 클라우드는 반드시 암호화 통신을 한다.	매우 중요

사내 I/F관리 및 운영은 클라우드 시스템 운영부서에서 하며 I/F의 신규, 변경, 삭제, 통제는 업무혁신담당의 승인을 득해야 한다. (담당부서 : IT인프라팀)	매우 중요
사내 I/F를 받은 외부 클라우드의 스토리지 및 DB는 암호화 되어야 한다.	매우 중요
사내망과 연동된 외부 클라우드의 IP 발급 및 네트워크 신규, 변경, 삭제는 업무혁신담당의 승인을 득해야 한다. (담당부서 : IT인프라팀)	매우 중요
전용선 및 IPsec-VPN 등 강화된 보안이 적용된 연결만 허용한다.	매우 중요

질문	답변
클라우드 계정에 MFA 정책을 강제화 하고 있는가?	
클라우드 생성 계정에 대한 권한 분리를 하고 있는가?	
클라우드 콘솔 접근 시 사내 업무메일 계정을 이용하여 계정을 생성하고 있으며, 적절하게 사용하고 있는가?	
클라우드 생성 계정에 대한 관리 대책이 존재하는가?	
루트(root) 계정 사용자 엑세스 키는 삭제하고, 관리자 계정을 생성하여 클라우드 리소스를 추가/수정을 하고 있는가? (AWS 미사용 시 N/A 처리 후 비고란에 사용하는 CSP 명시)	
클라우드 생성에 계정에 대한 그룹(Group) 별 권한 관리를 하는가?	

각 업무/부서 내 서비스 계정 생성시 Alias 메일을 이용하여 계정을 생성하였는가? 예) security@lge.com	
클라우드 구축 간 KEY에 대한 등록 및 관리를 수행하고 있으며, 관리는 정책에 따르고 있는가?	
클라우드에서 사용하는 키(Key)에 대한 사용 내역을 명확하게 파악하고 있는가?	
데이터(DB)에 대한 부적절한 행위에 대해서 통제할 수 있도록 감사로그를 기록하고 있는가?	
데이터 이동, 복제 간에 작업이 필요할 경우 작업을 승인 절차가 수립되어 있는가?	
자사 경영정보 및 1등급 정보의 저장영역은 논리적으로 독립된 공간을 제공받아 구성하고 있는가?	
클라우드에 저장되는 데이터의 파기는 완전삭제 되고 있는가?	
사내에서 연결되는 시스템과 대외로 서비스하는 클라우드는 암호화 통신을 하도록 하고 있는가?	

클라우드 시스템의 신규, 변경, 삭제 작업 내역을 기록하고 있으며, 작업을 승인 받고 있는가?	
중요한 데이터를 보관하고 있는 클라우드 스토리지/DB는 암호화를 적용하고 있는가?	
사내망과 연동된 외부 클라우드의 네트워크 신규/변경/삭제 작업 시에 승인을 받고 있는가?	
네트워크에 접근간IP-Sec-VPN 기술이 적용된 보안 연결을 사용하고 있는가?	

체크리스트 담당자 작성
비고
(인프라)클라우드 인프라 운영파트에서 인프라를 운영하는 경우 답변을 Yes 로 작성

(인프라)클라우드 인프라 운영파트에서
인프라를 운영하는 경우 답변을 Yes 로 작성

(인프라)클라우드 인프라 운영파트에서
인프라를 운영하는 경우 답변을 Yes 로 작성

(인프라)클라우드 인프라 운영파트에서
인프라를 운영하는 경우 답변을 Yes 로 작성

(인프라)클라우드 인프라 운영파트에서
인프라를 운영하는 경우 답변을 Yes 로 작성

평가 기준
(취약점 설명) 사용자 이름과 암호 외에 보안을 강화할 수 있는 방법으로 MFA를 활성화 하면 계정 로그인 간 사용자 이름/암호 뿐만 아니라 MFA 디바이스 인증을 통해 계정보안을 향상해야함 **(양호)** 계정 및 IAM을 통한 사용자 계정 로그인시 MFA가 활성화 되어 있을 경우 **(취약)** 계정 및 IAM 사용자 계정 로그인 시 MFA가 비활성화되어 있을 경우 * MFA(Multi-Factor Authentication) * IAM(Identify And Management)
(취약점 설명) 해당 항목은 생성된 계정에 대한 권한 분리를 하고 있어, Root 계정과 일반 계정의 권한 분리를 통해 비인가된 행위를 막고 인가 사용자에 대한 지속적인 관리를 통해 보안성을 향상해야 함 **(양호)** IAM을 통해 최소한의 인원에게만 권한을 주고, 권한자에게는 과도한 권한이 없는 경우 **(취약)** IAM을 통해 불필요한 인원이 포함되어 있으며, 권한 분류가 적절하게 됮 ㅣ않을 경우
(취약점 설명) 클라우드 콘솔 접근 시 루트 계정이나 공용 계정으로 접근하지 않고, 접근자별로 사내 메일 계정명으로 생성하고 접근하여야 계정별로 권한 분리가 설정이 용이하고, 침해사고 발생시 분석이 용이함 **(양호)** 클라우드 콘솔 접근 계정 목록내 "업무 계정"목록을 구성하고 있고, 계정명(OOO@lge.com)을 업무 메일로 사용하여 사용자를 식별할 수 있는 경우 **(취약)** 클라우드 콘솔 접근 계정 목록 내 공용 계정 및 루트 계정을 사용하고 있는 경우
(취약점 설명) 해당 항목은 생성된 계정에 대한 권한 분리를 하고 있어, Root 계정과 일반 계정의 권한 분리를 통해 비인가된 행위를 막고 인가 사용자에 대한 지속적인 관리를 통해 보안성을 향상해야 함 **(양호)** 클라우드 생성 계정에 대해 적절하게 관리하고 있는 경우 **(취약)** 클라우드 생성 계정에 대한 관리 방안이 없는 경우
(취약점 설명) root 계정 정보 유출 시 외부 클라우드의 시스템에 영향이 크기때문에 관리자 권한을 갖는 계정을 생성하고 해당 계정으로 클라우드 리소스를 운영해야함 (양호) Root 계정의 사용자 엑세스 키를 삭제하고, 다른 계정에 관리자 권한을 부여하여 클라우드 리소스 추가/수정을 진행하는 경우 (취약) Root 계정을 통해서 클라우드 리소스 추가/수정을 진행하는 경우
(취약점 설명) 해당 항목은 생성된 계정에 대한 권한 분리를 하고 있으며, Group 별 권한 분리를 통해 권한에 대한 접근 제어로 보안성을 향상해야 함 **(양호)** 클라우드 생성 계정에 대한 Group 별 권한 분리를 하고 잇는 경우 **(취약)** 클라우드 생성 계정에 대한 Group별 권한 분리를 하지 않는 경우

(취약점 설명)
해당 항목은 생성된 계정에 대한 소유권이 개인에게 종속되어 있을 경우, 담당자의 휴가 및 퇴사, 업무 변경 등과 같은 상황에도 계정 관리가 가능하지 않음으로, Alias 메일을 기준으로 계정을 생성해야함

(양호) 업무/부서별 계정을 사내 Alias 메일로 가지고 있는 경우
(취약) 업무/부서별 관리 계정이 사내 Alias 메일을 하용하지 않는 경우

(취약점 설명)
클라우드의에서 사용하는 각종 Key에 대한 정의가 되어 있으며, Key에 대한 적절한 관리와 현황을 파악하고 있어, Key 노출 시 위험을 최소화 할 수 있어야 함

(양호) 클라우드에서 사용하는 Key관리를 정책이 있거나 Key관리를 적절하게 하고 있는 경우
(취약) 클라우드에서 사용하는 Key 관리를 하지 않는 경우

(취약점 설명)
클라우드의에서 사용하는 각종 Key에 대한 정의가 되어 있으며, Key에 대한 적절한 관리와 현황을 파악하고 있어, Key 노출 시 위험을 최소화 할 수 있어야 함

(양호) 클라우드에서 사용하는 Key가 현황을 적절하게 파악하고 있어, 임의의 키 번경에 따른 영향도에 대한 검토가 가능한 경우
(취약) 클라우드에서 사용하는 Key 현황을 적절하게 파악하지 않을 경우

(취약점 설명)
데이터에 대한 접근 통제와 접근자에 대한 감사로그를 기록하고 있으며, 데이터 유출과 같은 사고 발생간에 로그 분석이 용이하도록 구성할 수 있어야 함

(양호) 스토리지/DB에 대한 액세스 로그를 활성화하고 있는 경우
(취약) 스토리지/DB에 대한 로깅을 기록하지 않을 경우

(취약점 설명)
데이터 이동, 복제 간에 작업이 필요할 경우 승인 절차를 기록하고 있어, 결제 절차를 통해 승인된 작업만 수행할 수 있어야 함

(양호) 데이터 이동 간에 승인 절차를 구성하고 있으며, 승인된 작업만 수행할 경우
(취약) 데이터 이동 간에 승인 절차가 구성되지 않을 경우

(취약점 설명)
데이터에 대한 경영정보 및 1등급 정보의 저장영역에 대해서 독립된 형태의 데이터 공간 확보를 통해 데이터의 안전한 보관을 할 수 있어야 함

(양호) 데이터 저장공간 내 경영 정보 및 1등급 외 정보를 저장할 경우
(취약) 데이터 저장공간 내 경영 정보 및 1등급 저장 영역을 저장할 경우

(취약점 설명)
클라우드에 저장되는 데이터의 삭제는 복구가 가능하지 않도록 완전한 삭제를 통해 삭제되며, 이미 암호화 되어 있는 경우에도 동일하게 진행되어 안전한 데이터 파기가 가능해야 한다.

(양호) 데이터 삭제시 완전한 삭제(Wiping) 하는 경우
(취약) 데이터 삭제시 완전한 삭제(Wiping)를 지원하지 않는 경우

(취약점 설명)
사내시스템 <> 대외 클라우드 간 서비스하는 통신 구간에 대해서는 전송구간 암호화를 전용하여 네트워크 상에 평문으로 노출되지 않아야 함

(양호) 전송 구간 암호화(HTTPS Only)가 적용되어 있을 경우
(취약) 전송 구간에 대한 암호화가 적용되지 않을 경우

(취약점 설명)
운영기 I/F 관리는 적절한 의사결정하에 신규, 변경, 삭제가 진행되도록 해야 하며 I/F 작업에 대한 결제 절차를 통해 승인된 작업만 수행할 수 있어야 함

(양호) 운영기 인프라의 신규, 변경, 삭제 작업 간에 결제 절차를 구성하여 승인된 작업만 수행할 경우
(취약) 운영기 인프라에 대한 승인 절차가 구성되지 않을 경우
(N/A) 운영기 시스템이 아닌 경우

(취약점 설명)
사내 I/F를 받은 외부 클라우드의 스토리지 및 DB의 중요도를 확인하여 암호화를 실시하여야 한다. 암호화를 통해 데이터 보호 대책을 적용할 수 있어야 함

(양호) 클라우드 스토리지/DB의 암호화 설정을 적용한 경우
(취약) 클라우드 스토리지/DB에 암호화 설정을 적용하지 않은 경우
(N/A) 암호화 적용 대상 시스템이 아닌 경우

(취약점 설명)
사내망과 연동된 외부 클라우드 IP 발급과 네트워크 신규/변경/삭제 작업이 필요할 경우 승인 절차를 기록하고 있어, 결제 절차를 통해 승인된 작업만 수행할 수 있어야 함

(양호) 네트워크 작업 간에 승인 절차를 구성하고 있으며, 승인된 작업만 수행할 경우
(취약) 네트워크 작업 간에 승인 절차가 구성되지 않을 경우

(취약점 설명)
네트워크 접근은 보안이 적용된 연결만 가능하도록 구성하고, 통신 구간에 대한 평문 노출이 가능하지 않도록 안전한 연결만을 제공해야 함

(양호) SSH, HTTPS, sFTP 등과 전송 구간 암호화 기술이 적용된 기술을 사용하거나, 별도의 전용 접근을 구성하여 인가된 사용자의 연결만 허용하는 경우
(취약) 보안 연결 기술을 적용하지 않았거나, 암호화 통신 이외의 평문 통신 기술 연결을 제공하는 경우

증적 내용
#CSP내 Group 구성 내역

#1. 데이터 파기 확인 확인서 혹은 그에 준하는 문서 (인증서, 감사리포트 등) ※ AWS, GCP, Azure 사용 시 별도 증적 필요 없음

#1. I/F 신규/변경/삭제에 대한 승인을 득한 기안 (품의, CSR, 메일 증적)
#1. 클라우드 인스턴스에서 스토리지/DB의 암호화 적용 화면 - 필수 : 스토리지 암호화 적용 화면 - 중요정보 : 오브젝트 암호화
#1. 네트워크 작업에 대해 승인을 득한 기안 (품의, CSR, 메일 증적)

[3. 클라우드 설계 보안성 항목 검토서]

작성가이드

1. 평가내용/질문에 따른 적용 유/무 확인 후 답변(H) 선택(Yes, No, N/A)
2. 답변(F)이 Yes인 경우 증적내용(K)를 확인 후 비고(I)에 캡쳐하여 첨부
3. 답변(F)이 No, N/A인 경우 사유를 비고(I)에 작성
※ GCP의 경우 Security Group, Netwokr ACL 사항은 방화벽으로 대체
※ 영향평가 이행점검 사전 품의 단계에서는 비고(G)에 "적용하겠음" 으로 작성

구분	항목	평가내용	중요도
	IP 할당 정책	생성되는 가상 네트워크에 임의 IP 할당을 방지 해야 한다.	중요
	네트워크 분리	사용 용도에 따른 가상 네트워크 망 분리를 해야 한다	매우 중요
		내,외부 하위 네트워크 (subnet) 분리를 해야 한다.	매우 중요
		inblound 및 outbound 트래픽 제어를 해야 한다	매우 중요
		IP 및 Port 기반 통제 구현을 해야 한다.	매우 중요

네트워크	**트래픽 제어**	네트워크 간 불필요한 연동을 최소화 해야 한다.	매우 중요
		외부 공격에 대한 대응 방안을 적용해야 한다.	매우 중요
			매우 중요
			매우 중요
			매우 중요
			매우 중요
		공인 IP 사용 및 외부 연동이 필요한 서버에 대한 보안	매우 중요

	트래픽 모니터링 및 추적 관리	가상 네트워크에서 발생하는 네트워크 트래픽 모니	중요
		클라우드 사업자 제공 서비스 사용 시 불필요한 외부	중요
서버(VM)	**Windows OS 보안**	윈도우 접근 보안 강화 방안을 마련 해야한다.	매우 중요
		윈도우 서버의 보안 강화 방안을 마련해야 한다.	매우 중요
	사용 이력 관리	운영자 및 사용자의 명령어 오남용에 대한 추적 관리	중요
	접근제어	서버(VM)에 대한 접근 제어를 검토 해야 한다.	매우 중요
	암호화	데이터 중요도에 따른 암호화 적합성을 확인해야 한	매우 중요

데이터베이스	**접근제어**	DB에 대한 접근 제어를 검토 해야 한다.	매우 중요
	데이터 관리	저장중인 데이터에 대한 접근 이력을 확인 해야 한다	매우 중요
스토리지	**암호화**	암호화 구현 방식 및 적합성 검토를 해야 한다.	매우 중요
	접근 제어	Object 스토리지의 외부 노출여부 검토를 해야 한다.	매우 중요
		Object Storage 권한 부여 현황 확인 해야한다.	매우 중요
	데이터 관리	저장중인 데이터에 대한 변경 이력 추적을 해야 한다	중요

		백업 주기 및 정책 수립해야 한다.	중요
인프라	**인벤토리 변경 증적 관리**	변경되는 자원에 대한 실시간 추적 관리 방안을 검토	매우 중요
		비 인가된 보안 설정 변경 모니터링 및 추적 관리를 ㅎ	매우 중요
	로그 및 자원 관리	인프라 자원 사용량 모니터링을 할 수 있어야 한다.	중요
		명시적 인프라 자원 관리를 해야 한다.	중요

질문	답변
임의 IP 할당을 하지 않도록 IP할당 정책을 통해 IP를 할당하고 있는가?	
운영, QA, PRD 등 환경에 따라 VPC를 분리 분리하고 있는가?	
Public 영역과 Private 영역의 IP 할당이 되도록 Network를 구성하고 있는가?	
In/Out bound 트래픽을 통제하고 있고, 트래픽 통제 이력에 대해 관리하고 있는가 - Security Group, NACL, VPC방화벽, VPC Service Controls 설정 여부	
사용하는 내/외부 트래픽에 대해서 IP와 Port 기반의 통제가 적용 되어 있는가?	

네트워크 내 불필요한 연동이 최소화 되어 있는가?	
Web Server 구성 시 SSRF(Server-side request forgery) 취약점 대응 하였는가? - WEB Backend Sever 인경우 WAF 적용 - WAF설정에 PUT Deny 설정 필수 - AWS EC2를 사용하는경우 IMDSv2 사용 - GCP 사용 시 "N/A"	
시스템 내 웹페이지를 제공하는 경우 HTTPS를 적용 하였는가? - 시스템 내 웹페이지를 제공하지 않는 경우 "N/A"	
Well-Known Port 사용 시 Port를 변경/제한하여 사용하는가?	
외부 및 타 시스템 연동 시 적절한 암호화 통신을 적용하여 통신을 하고 있는가? - 외부 및 타 시스템과 연동 사항이 없는 경우 N/A	
클라우드를 구성한 네트워크 내 WAF와 IPS 또는 웹 방화벽이 적용되어 있는가?	
외부 연동이 필요한 서버의 공인 IP 사용에 대한 명확한 Src/Dest 에대한 정의가 되어 있는가?	

네트워크에서 발생하는 트래픽에 대한 Log 설정 및 모니터링을 하고 있는가?	
클라우드 제공 서비스 이용 시 불필요한 외부 연계에 대한 검토를 수행하였는가?	
윈도우 서버의 원격 접근을 위한 RDP 사용 및 보안 강화 방안이 있는가? - 윈도우OS 미사용 시 "N/A	
윈도우 서버에 대해 백신을 설치 하였는가? - 윈도우OS 미사용 시 "N/A	
클라우드 서버(VM) 운영상 요청하는 명령어에 대한 기록을 기록하고 있는가?	
서버(VM)에 대한 접근 제어(IP기반 접근제어, 권한기반 접근제어) 를 하고 있는가?	
DBMS에서 데이터 중요도에 대해 검토하였으며, 이에 따라 데이터 암호화를 하고 있는가? "정보등급 자체평가" 내 비밀/사내한 혹은 개인정보 저장 시 데이터 암호화 필수	

DB 서버에 대한 접근 제어(IP기반 접근제어, 권한기반 접근제어) 를 하고 있는가?	
데이터 베이스에 대한 Query 요청 이력을 관리하고 있는가?	
안전한 데이터 보관을 위해 Object Storage에 대한 암호화를 적용하고 있는가? "정보등급 자체평가" 내 비밀/사내한 혹은 개인정보 저장 시 데이터 암호화 필요	
Object Storage에 Public Access가 미설정 되어 있는가?	
Object Storage에 대한 접근 제어와 각종 Method(View/Edit)에 대한 요청 권한 분류가 되어 있는가?	
스토리지에 대한 데이터의 변경 이력을 남기고 있으며, 이력관리에 대한 방안이 존재하는가?	

스토리지에 대한 백업/복구에 대한 절차가 존재하는가?	
인프라 자원에 대한 생성/변경/삭제에 대해 추적이 가능하도록 구성되어 있는가?	
클라우드에 구축된 보안 설정에 대한 설정 변경 모니터링 및 증적을 기록하고 있는가?	
인프라 자원에 대한 사용량 모니터링을 수행하고 있는가?	
인프라 관리를 위한 각 서버(인스턴스)에 대한 네이밍에 대한 기준이 있으며, 이에 따라 Tagging을 하고 있는가?	

체크리스트 담당자 작성
비고
(인프라)클라우드 인프라 운영파트에서 인프라를 운영하는 경우 답변을 Yes 로 작성
(인프라)클라우드 인프라 운영파트에서 인프라를 운영하는 경우 답변을 Yes 로 작성
(인프라)클라우드 인프라 운영파트에서 인프라를 운영하는 경우 답변을 Yes 로 작성
(인프라)클라우드 인프라 운영파트에서 인프라를 운영하는 경우 답변을 Yes 로 작성
(인프라)클라우드 인프라 운영파트에서 인프라를 운영하는 경우 답변을 Yes 로 작성

증적 내용 필수

증적 내용 필수 (인프라)클라우드 인프라 운영파트에서 인프라를 운영하는 경우 답변을 Yes 로 작성 및 증적 미필요
(인프라)클라우드 인프라 운영파트에서 인프라를 운영하는 경우 답변을 Yes 로 작성
증적 내용 필수 (인프라)클라우드 인프라 운영파트에서 인프라를 운영하는 경우 답변을 Yes 로 작성 및 증적 미필요
증적 내용 필수

증적 내용 필수
증적 내용 필수
증적 내용 필수 (인프라)클라우드 인프라 운영파트에서 인프라를 운영하는 경우 답변을 Yes 로 작성 및 증적 미필요
증적 내용 필수

증적 내용 필수 (인프라)클라우드 인프라 운영파트에서 인프라를 운영하는 경우 답변을 Yes 로 작성 및 증적 미필요
증적 내용 필수 (인프라)클라우드 인프라 운영파트에서 인프라를 운영하는 경우 답변을 Yes 로 작성 및 증적 미필요
증적 내용 필수 (인프라)클라우드 인프라 운영파트에서 인프라를 운영하는 경우 답변을 Yes 로 작성 및 증적 미필요
증적 내용 필수 (인프라)클라우드 인프라 운영파트에서 인프라를 운영하는 경우 답변을 Yes 로 작성 및 증적 미필요
증적 내용 필수 (인프라)클라우드 인프라 운영파트에서 인프라를 운영하는 경우 답변을 Yes 로 작성 및 증적 미필요

평가 기준
(취약점 설명) 클라우드 내 구축되는 시스템은 임의로 IP를 할당하지 않고, IP 할당 정책을 통해 IP를 할당하고 있어, IP 관리를 통해 네트워크 보안을 향상해야함 **(양호)** IP 할당 기준 및 할당을 하고 있음 **(취약)** IP 할당 기준이 없음
(취약점 설명) 클라우드에서 사용하는 네트워크 구성을 각 환경(운영, QA, Prod) 별로 분리하여 운영하고 있어, 네트워크에 환경에 대한 혼용이 없어야 함 (GCP의 경우 별도의 VPC운영) **(양호)** ACL를 통해 네트워크에 대한 환경 분리를 하고 있으며, 해당 리소스들이 배치되어 있음 **(취약)** ACL를 통해 각 영역이 환경별로 구성되어 있지 않음
(취약점 설명) 클라우드에서 사용하는 리소스는 ACL을 통해 접근 제어를 해야하며, 접근 제어는 Public 영역과, Private에 대한 영역 분리 및 리소스 배치를 하여 각각의 리소스를 보호할 수 있어야 함 (GCP의 경우 VPC내 방화벽 설정) **(양호)** ACL를 통해 Public/Private 환경 분리를 하고 있으며, 해당 리소스들이 배치되어 있음 **(취약)** Network ACL을 통해 Public/Private 환경 분리를 하고 있지 않으며,
(취약점 설명) 클라우드에서 사용하는 리소스는 In/Out bound에 대한 기준이 있어야 하며, 기준 별로 접근 제어를 수행해야 네트워크에 대한 안정성을 확보할 수 있음 **(양호)** ACL 서비스를 적용하고 있고, 트래픽 통제 이력을 관리하고 있는 경우 **(취약)** ACL 서비스를 적용하지 않거나, 적용하였지만 트래픽 통제 이력에
(취약점 설명) 클라우드 네트워크에서 ACL과 같은 접근 제어를 통해 IP/Port에 대한 접근제어를 구축하고 있어야 함 **(양호)** ACL서비스를 통해 필요한 IP, Port만 허용되어 있는 경우 **(취약)** ACL서비스를 통해 불필요한 IP, Port가 허용 되어 있는 경우

(취약점 설명)
클라우드에서 사용하는 리소스에 대한 NACL을 통해 네트워크 접근제어를 해야 하며 네트워크에 대한 불필요한 연동이 없도록 검토하고 설계해야 함 (GCP의 경우 VPC내 방화벽 설정)

(양호) NACL 적용 내역과 설계도를 통해 NACL 적용에 대한 검토서가 존재하는 경우
(취약) NACL 구성에 대한 검토가 이루어지지 않은 경우

(취약점 설명)
SSRF취약점에 대응할 수 있는 방안이 작용되어 있음.

(양호) EC2를 통해 Web Backend Server 구현 시 WAF적용이 되어 있는 경우
(취약) EC2를 통해 Web Backend Server 구현 시 WAF적용이 되어 있지 않는

(취약점 설명)
시스템 내 웹페이지를 제공하는 경우 HTTPS가 적용 되어 있음.

(양호) HTTPS가 적용 되어 있는 경우
(취약) HTTPS가 적용 되어 있지 않은 경우

(취약점 설명)
외부에서 예상 가능한 Well-Known Port port 사용 시 변경하여 사용 필요(ex, ssh)
Well-known Port 를 특정 IP만 허용 필요 (외부오픈 지양) (ex. Icmp)

(양호) Well-Known Port port를 변경하여 사용
(취약) Well-Known Port port를 그대로 사용

(취약점 설명)
다른 시스템 <> 클라우드 간 서비스하는 통신 구간에 대해서는 전송구간 암호화를 전용하여 네트워크 상에 평문으로 노출되지 않아야 함

(양호) 전송 구간 암호화(TLS1.2이상, HTTPS, sFTP)가 적용되어 있거나 IP 접근 제어가 적용되어 있을 경우
(취약) 전송 구간에 대한 암호화가 적용되지 않거나 IP 접근제어가 없는 경우

(취약점 설명)
클라우드에서 구성한 네트워크 구성도 내 WAF와 IPS와 같은 방화벽이 배치 되어 있어 이를 통해 네트워크에 대한 보호조치를 적용해야 함

(양호) 네트워크 설계도 내 "ACL" 적용과 같은 규칙이 존재하거나, 클라우드에서 제공되는 보안 기능(WAF, CloudTrail)을 적용한 내역이 있을 경우
(취약) 리소스에 대한 보안 적용을 하지 않은 경우

(취약점 설명)
클라우드에서 사용하는 리소스가 공인IP를 사용하는 경우, 명확한 Src/Dest에 대한 정의가 되어 있으며, 이를 통해 대외에 존재하는 리소스에 대한 보호 조치가 적용되어야 함

(양호) 공인 IP를 가지는 리소스에 대한 Src/Dest에 대해 정의가 되거나 공인IP로 구성이 되지 않은 경우
(취약) 공인 IP를 가지면서 Src/Dest에 대한 정의 명확하지 않은 경우

(취약점 설명)
클라우드에서 발생하는 트래픽에 대한 모니터링을 위해 트래픽에 대한 로그를 남기고 검토하여 리소스를 관리하여야 서비스에 대한 무중단 서비스가 가능할 수 있어야 함

(양호) 네트워크 트래픽에 대한 모니터링을 하는 경우
(취약) 네트워크 트래픽에 대한 모니터링을 하지 않는 경우

(취약점 설명)
클라우드의 제공 서비스를 이용하여 서비스를 제공할 경우, 불필요한 외부 시스템 연동과 같은 작업이 이루어지지 않아야 하며, 이를 사전에 검토하여야 함

(양호) 클라우드 제공 서비스 사용 시 불필요한 외부 연계에 대해서 검토를 진행한 경우
(취약) 클라우드 제공 서비스 사용 시 불필요한 외부 연계가 존재하거나 외부 연계에 대한 검토를 진행하지 않은 경우

(취약점 설명)
클라우드에서 윈도우 OS로 구축 간에 RDP 서비스를 활용하여 원격 서버 접근을 할 경우 무분별한 접근을 방지 하기 위해 인가된 사용자에게만 접근할 수 있도록 구성해야 함

(양호) RDP 서비스 접근 간 IP 접근과 같은 접근 제어가 존재하는 경우
(취약) RDP 통해 인가되지 않은 사용자가 접근을 시도할 수 있는 경우
(N/A) OS에서 RDP를 통해 원격 접근 제어를 사용하지 않는 경우

(취약점 설명)
클라우드에서 윈도우 OS로 구축 간에 보안 강화를 위해 백신을 설치해야 함

(양호) 원도우 OS 서버에 백신을 설치 한 경우
(취약) 윈도우 OS 서버에 백신을 설치 하지 않은 경우
(**N/A)** 윈도우 OS 서버를 사용하지 않는 경우

해외 : SEP 백신 홈페이지(https://v3.lge.com)를 통해 다운로드
국내 : SEP 설치 파일의 경우 IT인프라팀(ssora.lee@lge.com) 문의

(취약점 설명)
클라우드 서버에서 운영상 요청하는 명령어에 대한 기록을 통해 오남용 명령어에 대한 로깅을 하고 있어, 침해 사고 발생 간 악성 행위 분석이 용이함

(양호) 클라우드 서버에서 요청하는 명령어를 로깅하고 있는 경우
(취약) 클라우드 서버에서 요청하는 명령어를 로깅하지 않는 경우

(취약점 설명)
클라우드에서 사용하는 서버(VM)에 대한 접근 제어를 위해 인가된 사용자만 접근을 하도록 구현해야 함

(양호) 서버(VM)를 사용하며 인가된 사용자만 접근이 가능하도록 구성한 경우
(취약) 서버(VM)를 사용하며 별도의 접근제어가 없는 경우
(N/A) 서버(VM)를 사용하지 않을 경우

(취약점 설명)
스토리지 및 DB의 중요도를 확인하여 암호화를 실시하여야 한다.
암호화를 통해 데이터 보호 대책을 적용할 수 있어야 함

(양호) 클라우드 DB의 암호화 설정을 적용한 경우
(취약) 클라우드 DB에 암호화 설정을 적용하지 않은 경우
(N/A) 암호화 적용 대상 시스템이 아닌 경우

(취약점 설명)
클라우드에서 사용하는 DB에 대한 접근 제어를 위해 인가된 사용자만 접근을 하도록 구현해야 함

(양호) DB 서비스를 사용하며 인가된 사용자만 접근이 가능하도록 구성한 경우
(취약) DB 서비스를 사용하며 별도의 접근제어가 없는 경우
(N/A) DB 서비스를 사용하지 않을 경우

(취약점 설명)
클라우드에서 데이터 베이스에 대한 적절한 권한 분리를 하고 있어, Root 계정과 운영 계정을 분리를 통해 과도한 권한 부여를 제한해야 하며, DB Query 요청에 대한 이력 관리를 통해 데이터 베이스에 보안에 대한 보안성을 향상할 수 있어야 함

(양호) 데이터 베이스에 대한 변경 이력을 로깅 하고 있는 경우
(취약) 데이터 베이스에 대한 변경 이력을 로깅 하지 않을 경우
(N/A) 데이터 베이스를 사용하지 않는 경우
AWS RDS Audit Log 설정 :
https://aws.amazon.com/ko/blogs/database/configuring-an-audit-log-to-capture-database-activities-for-amazon-rds-for-mysql-and-amazon-aurora-with-mysql-compatibility/
DynamoDB API CloudTrail 설정 :
https://docs.aws.amazon.com/ko_kr/amazondynamodb/latest/developerguide/logging-using-cloudtrail.html
Cloud SQL Audit Log 설정 : https://cloud.google.com/sql/docs/audit-logging

(취약점 설명)
스토리지에 저장되는 데이터의 안전한 보관을 위해 스토리지에 대한 암호화 적용이 되어 있어, 스토리지 내 데이터가 유출 시에 암호화 된 데이터가 노출될 수 있어 스토리지 암호화를 적용하여 보안성을 향상할 수 있어야 함

(양호) 스토리지 암호화 설정을 적용한 경우
(취약) 스토리지 암호화 설정을 적용하지 않은 경우
(N/A) 암호화 적용 대상 시스템이 아닌 경우

(취약점 설명)
클라우드에서 Object Storage를 Public Access 설정으로 사용하고 있을 경우 외부에서 접속이 가능하여 데이터 유출 가능성이 있음

(양호) Object Storage에 대한 Public Access 설정 적용되어 있지 않은 경우
(취약) Object Storage에 대한Public Access 설정 적용되어 있는 경우
(N/A) Object Storage를사용하지 않는 경우

(취약점 설명)
클라우드에서 Object Storage를 사용하고 있을 경우, 접근 제한에 대한 적용이 되어 있어야 스토리지에 대한 보안성을 향상할 수 있음

(양호) Object Storage에 대한 접근 권한 적용되어 있는 경우
(취약) Object Storage에 대한 접근 권한 적용되어 있지 않은 경우
(N/A) Object Storage를사용하지 않는 경우

(취약점 설명)
클라우드에서 Object Storage에 대한 변경 이력 관리를 통해 데이터 베이스에 보안에 대한 보안성을 향상할 수 있어야 함

(양호) Object Storage에 대한 데이터 변경에 대한 이력 관리를 하는 경우
(취약) Object Storage에 대한 데이터 변경에 대한 이력 관리를 하고 있지 않는 경우
(N/A) Object Storage를 사용하지 않는 경우

(취약점 설명)
클라우드에서 발생하는 트래픽에 대한 모니터링을 위해 트래픽에 대한 로그를 남기고 검토하여 리소스를 관리하여야 서비스에 대한 무중단 서비스가 가능할 수 있어야 함

(양호) 클라우드에 적절한 주기에 따라 백업을 하고 있으며, 복구 방안이 있는 경우
(취약) 클라우드에 백업/복구 방안 수립되지 않는 경우

(취약점 설명)
클라우드 인프라는 설정 변경에 따른 영향도가 클 수 있으므로 인프라 변경 행위에 대한 변경이록을 기록해야 함

(양호) 클라우드에서 변경하는 변경이력 로깅을 하고 있을 경우
(취약) 클라우드에서 변경하는 변경이력 로깅을 하고 있지 않은 경우

(취약점 설명)
클라우드에서 사용하는 각종 인프라 설정은 편리한 UI로 제공 됨에 따라 변경에 따른 영향력이 예측할 수 없는 경우가 있음에 따라, 설정 변경이력에 대해서 기록할 수 있어야 함

(양호) 클라우드의 보안 설정 변경에 대해 모니터링이 가능하도록 변경이력을 기록하는 경우
(취약) 클라우드에서 보안 설정 변경에 대해서 기록하지 않는 경우

(취약점 설명)
클라우드에서 자원에 대한 모니터링을 하고 있어 무중단 서비스가 가능할 수 있어야 함

(양호) 클라우드 리소스 모니터링을 하는 경웅
(취약) 클라우드 리소스 모니터링을 하지 않는 경우

(취약점 설명)
클라우드에서 인프라에 대한 네이밍 기준이 있어, 이에 따라 네밍을 통해 적절한 인스턴스 관리와 그룹 설정이 할 수 있어야 함

(양호) 클라우드 인스턴스에 대한 네이밍 규칙 및 규칙에 따라 네이밍을 하는 경우
(취약) 클라우드 인스턴스에 대한 네이밍 규칙이 없고, 무분별하게 생성한 경우

증적 내용

#1. 암호화 통신 설정화면 캡쳐

#1. 클라우드 네트워크 트래픽 기록 화면 캡쳐
#1. 클라우드 인스턴스에서 스토리지/DB의 암호화 적용 화면

#1. CSP별 DB서비스 Audit Log 설정 증적 AWS - DynamoDB : Cloud Trail Log - RDS/Aurora : Audit Log 설정 증적 GCP - Cloud SQL : Audit Log 설정 증적
#1. 클라우드 인스턴스에서 스토리지 암호화(Encrytion) 적용 화면
#1. Object Storage 외부 접근 설정 내역
#1. Object Storage 에 변경 이력 로깅 화면 - AWS : CloudTrail 설정 내역 증적 - GCP : Audit Log 설정 증적

#1. 클라우드 스토리지 백업 정책 #2. 클라우드 스토리지 백업 설정 화면
#1. 클라우드 변경이력 기록 화면 - AWS : CloudTrail 설정 내역 증적 - GCP : Audit Log 설정 증적
#1. 클라우드 리소스 모니터링화면 증적
#1. 클라우드 인스턴스 네이밍(Tagging) 룰

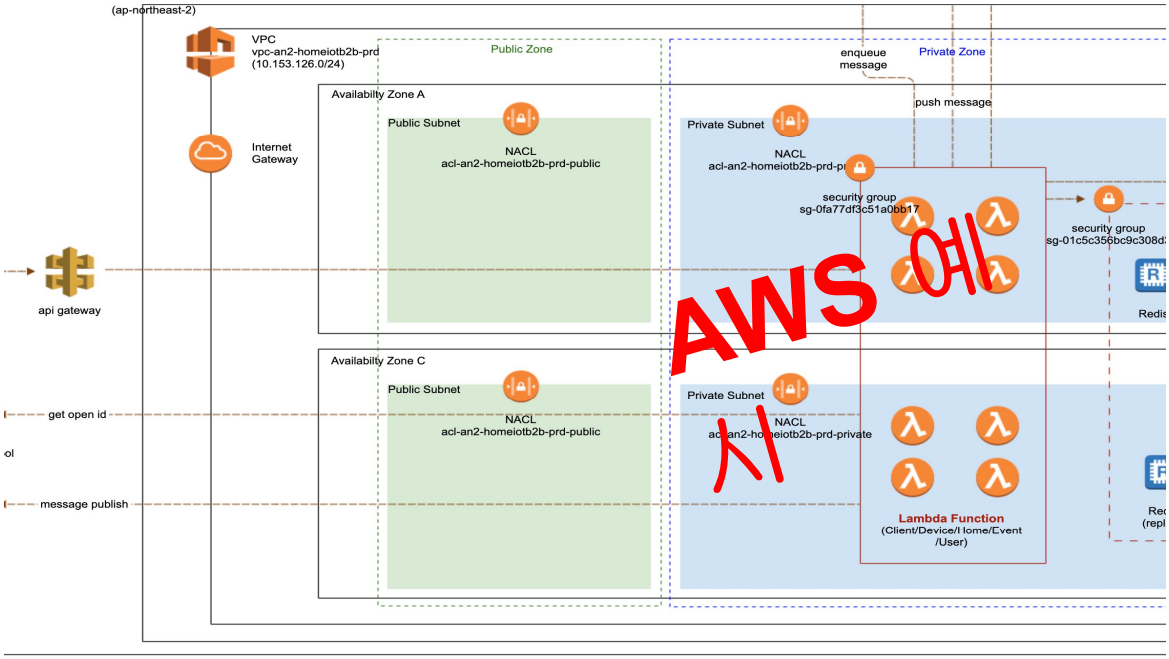
[4. 인프라 아키텍쳐]

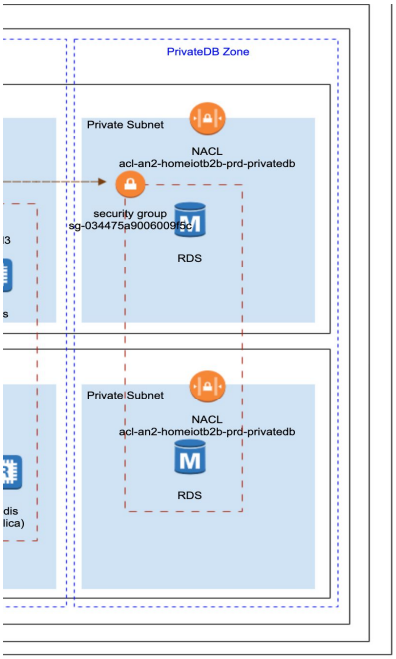
작성가이드

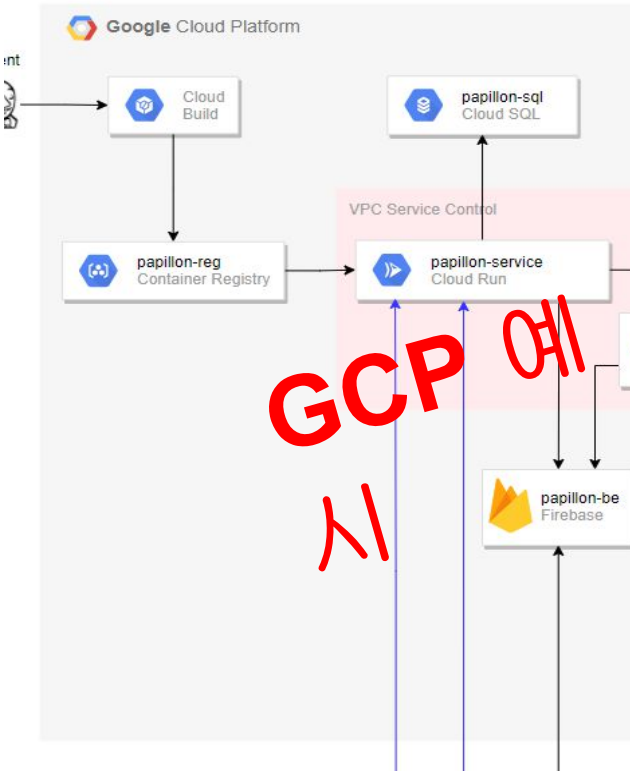
1. 외부 클라우드 서비스 종류가 IaaS, PaaS인 경우 작성

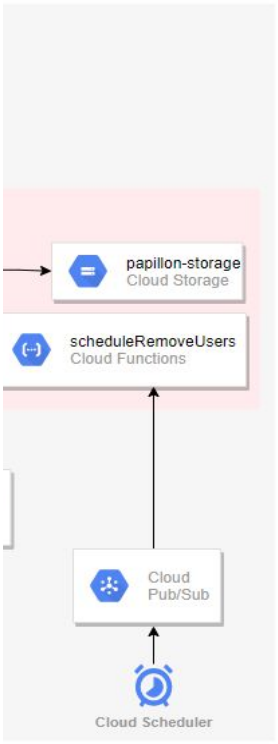
2. 네트워크 보안 설정 사항 표시 (Host Name 작성)

- AWS : Security Group, Network ACL, VPC 범위 표시
- GCP : VPC, VPC Service Control 범위 표시




PrivateDB Zone
Private Subnet
NACL
acl-an2-homeiotb2b-prd-privatedb
security group
RDS
Private Subnet
NACL
acl-an2-homeiotb2b-prd-privatedb
RDS


Google Cloud Platform
Cloud Build
papillon-sql
Cloud SQL
VPC Service Control
papillon-reg
Container Registry
papillon-service
Cloud Run
papillon-be
Firebase
GCP 예시


papillon-storage
Cloud Storage
scheduleRemoveUsers
Cloud Functions
Cloud
Pub/Sub
Cloud Scheduler

[5. 데이터(서비스) 흐름도]

작성가이드

1. 외부 클라우드 서비스 종류가 IaaS, PaaS인 경우 작성

2. 추가작성 없이 인프라 아키텍쳐 내에서 데이터의 이동경로를 화살표로 표시

***데이터 종류 표시**

[6. IAM리스트]
작성가이드
1. 외부 클라우드 서비스에서 제공하는 IAM 리스트 캡쳐
2. MFA 적용 필수 확인, 미사용 계정 삭제 필요
*****

밀번호 수명	마지막 활동	MFA
7 일	4 일	가상
5 일	오늘	가상
7 일	4 일	가상
5 일	오늘	가상

[7. IP리스트(CIDR)]

[8. Security Group]

작성가이드

1. 외부 클라우드 서비스 종류가 IaaS인 경우 작성

2. 외부 클라우드 서비스에서 제공하는 Security Group 리스트 캡쳐

3. 네트워크 보안 설정 상세 항목 캡쳐

- AWS : Security Group 상세 항목 캡쳐

- GCP : 미작성

sg-0c78d1b5d50a5c714 - scg-an2-img-signing-dev-was

Details

Security group name	Security group ID	Description
scg-an2-img-signing-dev-was	sg-0c78d1b5d50a5c714	ssh

Owner	Inbound rules count	Outbound rul
525245832464	10 Permission entries	7 Permission

Inbound rules | Outbound rules | Tags

Inbound rules (10)

Type	Protocol	Port range	Source
Custom TCP	TCP	8001	0.0.0.0/0
SSH	TCP	22	sg-06bbbc43e6cf15b8e / scg-an2-img-signing-dev-bastion
Custom TCP	TCP	1095	10.182.53.0/24
Custom TCP	TCP	1095	sg-0c78d1b5d50a5c714 / scg-an2-img-signing-dev-was
Custom TCP	TCP	1414	10.181.2.55/32
Custom TCP	TCP	7411	0.0.0.0/0
Custom TCP	TCP	9004	10.158.5.36/32
Custom TCP	TCP	9004	10.158.5.7
Custom TCP	TCP	1097	10.1
Custom TCP	TCP	1097	sg- 8d a5c714 / scg-an2-img-signing-dev-was

AWS SIG

Inbound rules | Outbound rules | Tags

Outbound rules (7)

Type	Protocol	Port range	Destination
All TCP	TCP	0 - 65535	10.182.53.0/24
Custom TCP	TCP	44441 - 44443	10.185.246.59/32
SMTP	TCP	25	156.147.51.104/32
Custom TCP	TCP	1414	10.181.2.55/32
Custom TCP	TCP	10051	10.185.248.250/32
Custom TCP	TCP	9004	10.158.5.37/32
Custom TCP	TCP	9004	10.158.5.36/32

VPC ID

vpc-07f86ddbfc6d0ad7f

es count

entries

	Description - optional
	Custom SSHD Port, from LGE Internal Network
	ssh was connection
	Java RMI Object Port, from DEV VPC
	Java RMI Object Port, from DEV WAS
	DB Interface Port, from DEV MQ
	Apache HTTP Port, from LGE Internal Network
	HSM Connection Port, from HSM VS #1
	HSM Connection Port, from HSM VS #2
	Java RMI Registry Port, from DEV VPC
	Java RMI Registry Port, from DEV WAS

	Description - optional
	–
	SSO Server (DEV)
2	SMTP Server (OPER), lgekrhqsy01.lge.com
	DB Interface Port, from DEV MQ
2	CMS Monitoring
	HSM Connection port
	HSM Connection port

[9. Network ACL]

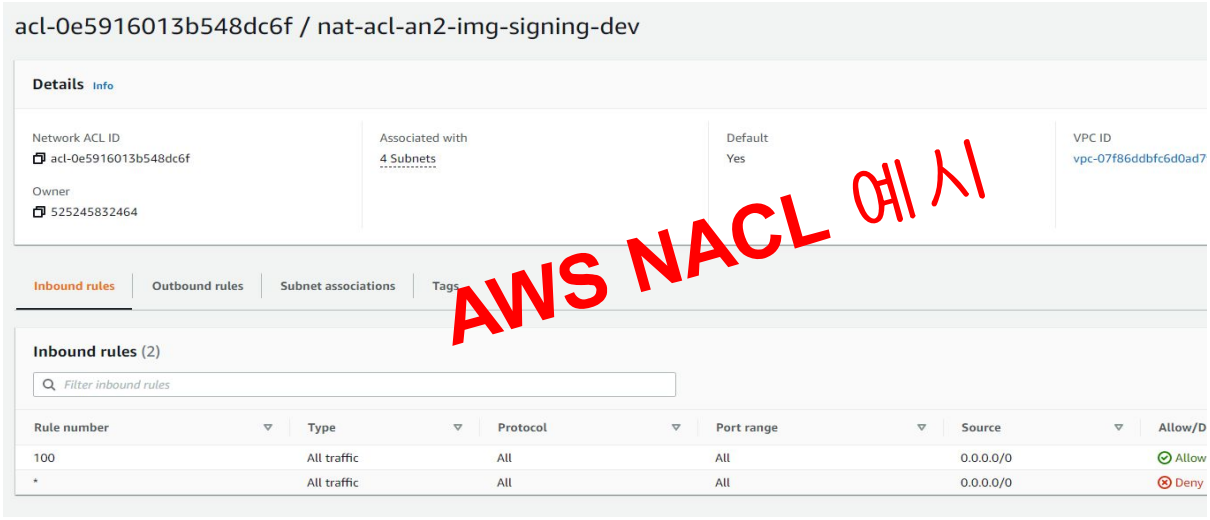
작성가이드

1. 외부 클라우드 서비스 종류가 IaaS인 경우 작성

2. 외부 클라우드 서비스에서 제공하는네트워크 보안 설정 상세 항목 캡쳐

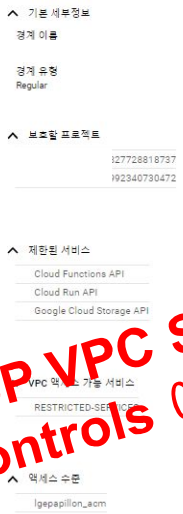
- AWS : Network ACL 상세 항목 캡쳐

- GCP : 방화벽, GCP VPC Service Controls 상세 항목 캡쳐



	이름	유형	대상	필터	프로토콜/포트	작업	우
☐	default-allow-internal	수신	전체 적용	IP 범위: 10.[illegible]/9	tcp:0-65535 udp:0-65535	허용	

GCP 방화벽 예시



GCP VPC Service Controls 예시

우선순위	네트워크 ↑	로그
65534	default	사용 안함