
Lab13. AWS 보안-ISMS-P

서태호 강사

topasvga@naver.com



ISMS-P 정보보호 및 개인정보보호 관리체계 인증



AWS 사용시 · AWS 중급 과정

안전한 클라우드,
더 강한 보안, 더 큰 신뢰

ISMS-P란?

정보보호 및 개인정보보호 관리체계 인증으로
기업의 정보보호와 개인정보보호를 위한
체계적 관리체계를 갖추고 있음을 인증하는 제도입니다.

ISMS-P 인증 기준

- 1 관리체계 수립 및 운영 16개
- 2 보호대책 요구사항 64개
- 3 개인정보 처리단계 요구사항 21개

ISMS-P는 정보보호와 개인정보보호를
통합적으로 관리하는 인증입니다.

AWS 클라우드 환경에서의 ISMS-P 대응



주요 보안 통제 항목

- ✓ 접근통제
- ✓ 암호화
- ✓ 로그관리
- ✓ 백업 및 복구
- ✓ 사고대응
- ✓ 데이터 보호
- ✓ 네트워크 보안

AWS 중급 과정

ISMS-P 인증 기준을 기반으로
AWS 클라우드 환경에서의 정보보호 및 개인정보보호
실무 역량을 강화하는 과정입니다.

주요 학습 내용

- ✓ ISMS-P 인증 기준과 클라우드 보안 연계 이해
- ✓ AWS IAM을 통한 접근통제 및 권한관리
- ✓ VPC 네트워크 보안 및 보안그룹 구성
- ✓ 데이터 암호화 (KMS, S3, RDS)
- ✓ 로그 수집 및 모니터링 (CloudTrail, CloudWatch)
- ✓ 백업 및 재해복구 전략
- ✓ 사고대응 절차 및 보안 운영관리
- ✓ 개인정보 처리단계별 보호대책 실습

실무 중심의 클라우드 보안 교육으로
ISMS-P 인증 준비를 완벽하게!

ISMS-P 대응 7대 핵심 프로세스



목차

1. ISMS-P(정보보호 및 개인정보보호 관리체계 인증)
2. ISMS-P-정보 서비스 업무 절차
3. ISMS-P-안전한 접속 환경
4. ISMS-P-관리 콘솔
5. ISMS-P-계정 관리
6. ISMS-P-보안 그룹,네트워크
7. ISMS-P-EC2 체크
8. ISMS-P-DB 체크
9. ISMS-P-스토리지 체크
10. ISMS-P 주기적 점검 체크리스트

1. ISMS-P(정보보호 및 개인정보보호 관리체계 인증)

ISMS-P (정보보호 및 개인정보보호 관리체계 인증)

- ✓ ISMS-P는 “정보보호 및 개인정보보호 관리체계 인증(Information Security Management System – Personal Information Protection)”을 의미하는 한국의 인증 제도다.
- ✓ 내부 관리체계 구축 및 최소 2개월 운영 → 신청(공문·자료 제출, 예비점검) → 서면·현장 심사 및 결함 보완 → 인증위원회 심의 후 인증서 발급의 단계로 진행된다.
- ✓ 인증은 유효기간이 있으며, 주기적 사후심사·갱신심사를 통해 효력을 유지해야 한다.

ISMS-P (정보보호 및 개인정보보호 관리체계 인증)

- ISMS인증 의무대상자(정보통신망법 제47조제2항)
- 인증 의무 대상자는 '전기통신 사업법' 제 2조 제8호에 따른 전기통신 사업자의 전기통신 역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 아래의 표에서 기술한 의무 대상자 기준에 하나에 해당되는 기업과 기관을 말합니다.

구분	의무대상자 기준
ISP	「전기통신사업법」 제6조제1항에 따른 허가를 받은 자로서 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 자
IDC	정보통신망법 제46조에 따른 집적정보통신시설 사업자
다음의 조건 중 하나라도 해당하는 자	연간 매출액 또는 세입이 1,500억원 이상인 자 중에서 다음에 해당되는 경우 - 「의료법」 제3조의4에 따른 상급종합병원 - 직전연도 12월 31일 기준으로 재학생 수가 1만명 이상인 「고등교육법」 제2조에 따른 학교
	정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 자
	전년도 직전 3개월간 정보통신서비스 일일평균 이용자 수가 100만명 이상인 자

출처 : [정보보호 및 개인정보보호 관리체계 인증 의무 대상자 기준(Source:한국인터넷 진흥원)]

ISMS-P (정보보호 및 개인정보보호 관리체계 인증)

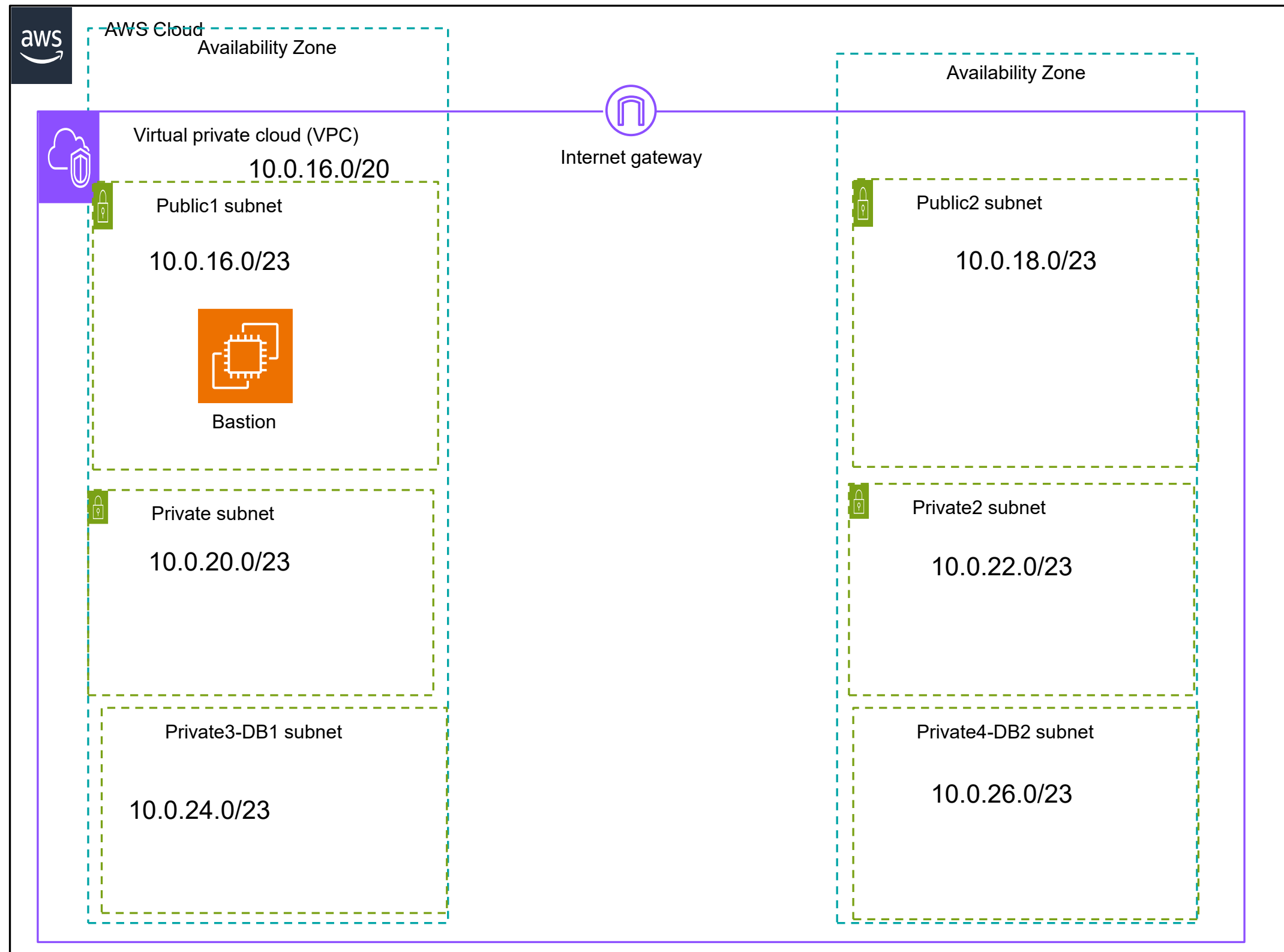
- 인증 분야

통합인증	인증 분야 (인증 기준 항목수)
1. 관리체계 수립 및 운영	1.1 관리체계 기반 마련(6) 1.2 위험관리(4) 1.3 관리체계 운영(3) 1.4 관리체계 점검 및 개선(3)
2. 보호 대책 요구 사항	2.1 정책,조직,자산관리(3) 2.2 인적보안(6) 2.3 외부자 보안(4) 2.4 물리보안(7) 2.5 인증 및 권한 관리(6) 2.6 접근 통제(7) 2.7 암호화 적용(2) 2.8 정보시스템 도입 및 개발 보안(6) 2.9 시스템 및 서비스 보안관리(9) 2.10 시스템 및 서비스 보안 관리(9) 2.11 사고 예방 및 대응(5) 2.12 재해복구(2)

2. ISMS-P-정보 서비스 업무 절차

ISMS-P-정보 서비스 업무 절차

- Bastion으로 통해 서버 접속한다.



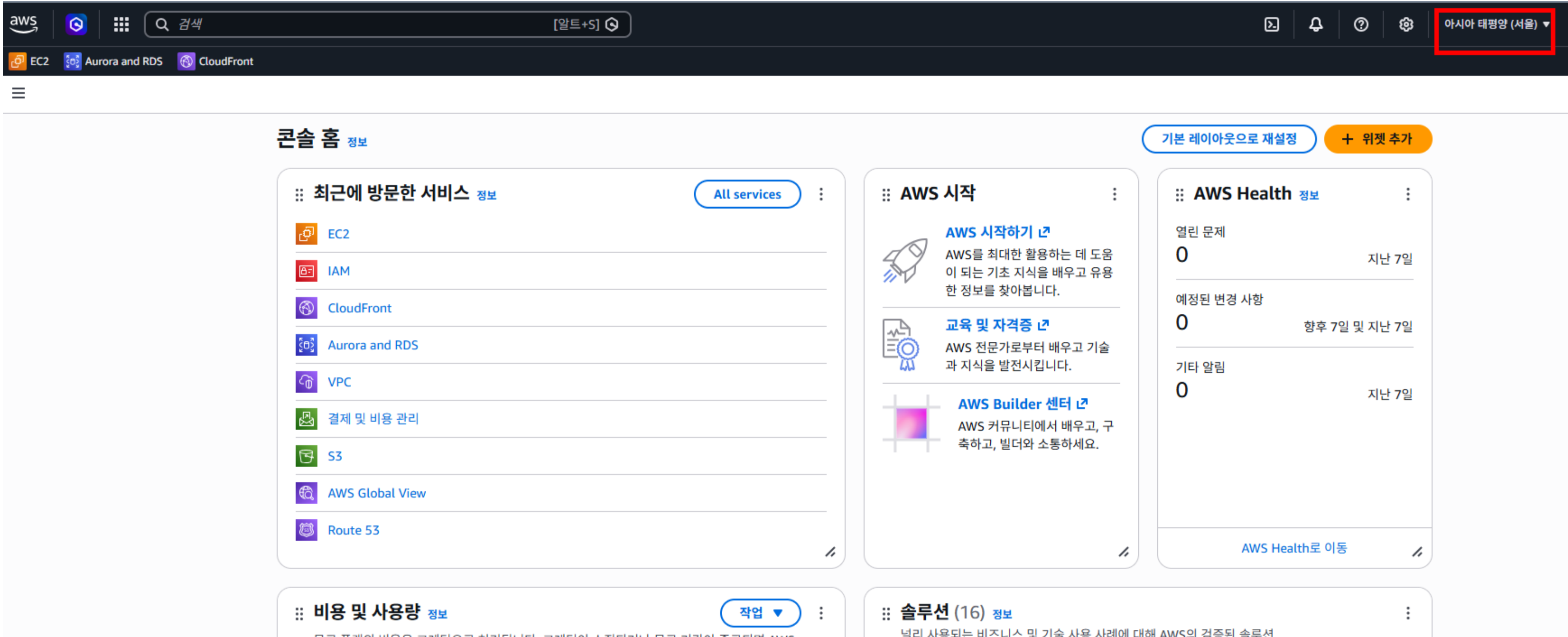
3. ISMS-P-안전한 접속 환경

ISMS-P-안전한 접속 환경

- <1> 국내에 리전을 보유하고 있어 데이터를 국내에 저장하는지 체크(필수)
- <2> 공인망에서 관리콘솔로 직접 접속하면 안 된다.
- <3> IPSEC VPN, SSL VPN , 전용선을 연결해 접속 체크(필수)
- <4> 관리자 및 특수 권한으로 접속할 경우 강화된 인증(2-Factor인증) 사용 체크(필수)
- <5> 재택, 원격 근무 시 클라이언트 체크 - 회사 자산 노트북, 백신, Windows방화벽 활성화 여부, 보안 솔루션 체크(필수)

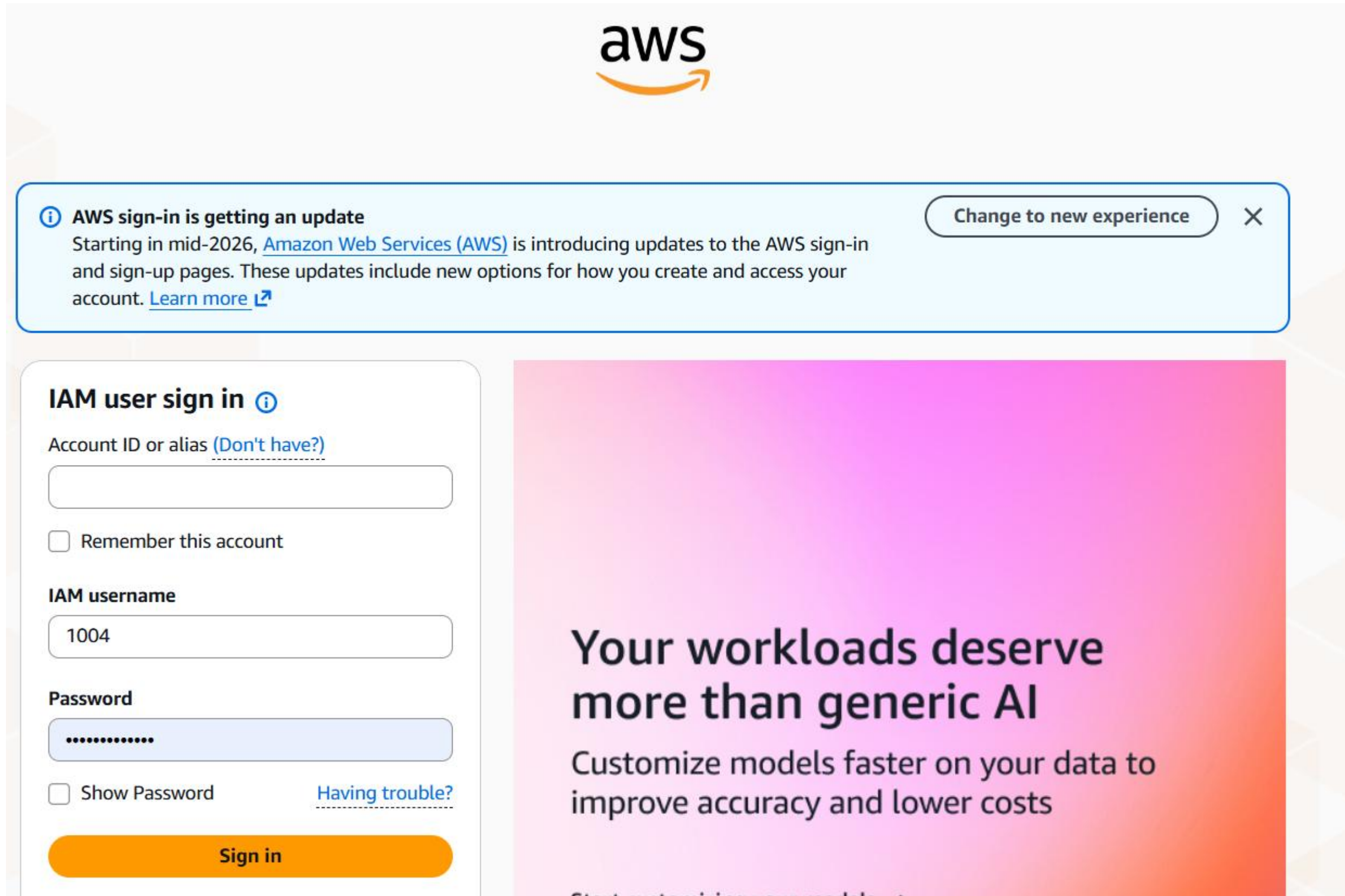
ISMS-P-안전한 접속 환경

- <1> 국내에 리전을 보유하고 있어 데이터를 국내에 저장하는지 체크(필수)



ISMS-P-안전한 접속 환경

- <2> 공인망에서 관리콘솔로 직접 접속하면 안 된다. (권고)



aws

AWS sign-in is getting an update
Starting in mid-2026, [Amazon Web Services \(AWS\)](#) is introducing updates to the AWS sign-in and sign-up pages. These updates include new options for how you create and access your account. [Learn more](#)

[Change to new experience](#) ✕

IAM user sign in ⓘ

Account ID or alias [\(Don't have?\)](#)

☐ Remember this account

IAM username

1004

Password

.....

☐ Show Password [Having trouble?](#)

Sign in

Your workloads deserve more than generic AI

Customize models faster on your data to improve accuracy and lower costs

ISMS-P-AWS IP제한

- {
- "Version": "2012-10-17",
- "Statement": [- {
- "Effect": "Deny",
- "Action": "*",
- "Resource": "*",
- "Condition": {
- "NotIpAddress": {
- "aws:SourceIp": ["203.0.113.100/32"]
- },
- "BoolIfExists": {
- "aws:ViaAWSService": "false"
- }
- }
- }
-]
- }

ISMS-P-AWS IP제한

- 적용 방법 (콘솔 기준)

1. **IAM 콘솔** → 사용자 또는 그룹 선택 - dev그룹
2. 권한 추가 → **인라인 정책 생성** 클릭
3. JSON 탭에서 위 정책 붙여넣기
4. IP 주소를 실제 허용할 IP/CIDR로 수정
5. 정책 검토 → 이름 입력 후 저장

1. **사용자 그룹 > 그룹 생성 > dev**

ISMS-P-AWS IP제한

2. 그룹 클릭 > 권한 > 권한 추가 > 인라인 정책 생성

Identity and Access Management(IAM)

Q IAM 검색

대시보드

▼ 액세스 관리

사용자 그룹

사용자

역할

정책

ID 제공업체

계정 설정

루트 액세스 관리

임시 위임 요청

▼ 보고서 액세스

Access Analyzer

리소스 분석

미사용 액세스

분석기 설정

자격 증명 보고서

조직 활동

서비스 제어 정책

리소스 제어 정책

dev 정보

삭제

편집

요약

사용자 그룹 이름

dev

생성 시간

April 06, 2026, 19:54 (UTC+09:00)

ARN

arn:aws:iam::697016550159:group/dev

사용자

권한

액세스 관리자

권한 정책 (1) 정보

최대 10개의 관리형 정책을 연결할 수 있습니다.

시뮬레이션

삭제

권한 추가

정책 연결

인라인 정책 생성

Q 검색

필터링 기준 유형

모든 유형

정책 이름

유형

연결된 엔터티

AdministratorAccess

AWS 관리형 - 직무

2

ISMS-P-AWS IP제한

- JSON

IAM > 사용자 그룹 > dev

Identity and Access Management(IAM)

Q IAM 검색

대시보드

▼ 액세스 관리

사용자 그룹

사용자

역할

정책

ID 제공업체

계정 설정

루트 액세스 관리

임시 위임 요청

▼ 보고서 액세스

Access Analyzer

리소스 분석

미사용 액세스

분석기 설정

자격 증명 보고서

조직 활동

서비스 제어 정책

리소스 제어 정책

권한 정책 (2) 정보

최대 10개의 관리형 정책을 연결할 수 있습니다.

Q 검색

필터링 기준 유형

모든 유형

☐

정책 이름 ↗

▲

유형

▼

연결된 엔터티

☐

+

AdministratorAccess

AWS 관리형 - 직무

2

☐

+

seo-ip-access

고객 인라인

0

seo-ip-access

1 {

2 "Version": "2012-10-17",

3 "Statement": [

4 {

5 "Effect": "Deny",

6 "Action": "*",

7 "Resource": "*",

8 "Condition": {

9 "NotIpAddress": {

10 "aws:SourceIp": [

11 "203.0.113.100/32"

12]

13 },

14 "BoolIfExists": {

15 "aws:ViaAWSService": "false"

16 }

17 }]

18 }

19]

20 }

ISMS-P-AWS IP제한

- JSON

7:15JSON

+ 새 문 추가

🛡️ 보안: 1

❌ 오류: 1

⚠️ 경고: 1

💡 추천: 0

정책 검증에 대해 자세히 알아보기

🔍 오류 검색

행 12, 열 6

Private IP Address: aws:SourceIp는 퍼블릭 IP 주소 범위에서만 작동합니다. 조건 키 aws: SourceIp의 값에는 프라이빗 IP 주소만 포함되어 있으며 원하는 효과를 제공하지 않습니다. 퍼블릭 IP 주소만 포함하도록 값을 업데이트하세요. [자세히 알아보기](#)

ISMS-P-AWS IP제한

- Seo-ip-access

☰

[IAM](#) > [사용자 그룹](#) > [dev](#) > 정책 생성

1단계

권한 지정

2단계

검토 및 생성

검토 및 생성

정보

권한을 검토하고 세부 정보 및 태그를 지정합니다.

정책 세부 정보

정책 이름

이 정책을 식별하는 의미 있는 이름을 입력합니다.

seo-ip-access

최대 128자입니다. 영문자 및 hyphen '-' 문자를 사용하세요.

이 정책에 정의된 권한

정보

이 정책 문서에 정의된 권한은 허용되거나 거부되는 작업을 지정합니다. IAM 자격 증명(사용자, 사용자 그룹 또는 역할)에 대한 권한을 정의하려면 여기에 정책을 연결합니다.

🔍

검색

허용(서비스 466개 중 466개)

서비스	▲	액세스 수준	▼	리소스		요청 조건
Access Analyzer		전체 액세스 권한		모든 리소스		aws:SourceIp IP Address 203.0.113.0/24,192.168.1.100/32
Account		전체 액세스 권한		모든 리소스		aws:SourceIp IP Address 203.0.113.0/24,192.168.1.100/32
Action Recommendations		전체 액세스 권한		모든 리소스		aws:SourceIp IP Address 203.0.113.0/24,192.168.1.100/32
Activate		전체 액세스 권한		모든 리소스		aws:SourceIp IP Address 203.0.113.0/24,192.168.1.100/32

ISMS-P-AWS IP제한

- 그룹에 계정 추가
 - 사용자 추가 > test111
 - Test111로 로그인 시도
- 콘솔 로그인
- <https://697016550159.signin.aws.amazon.com/console>

ISMS-P-AWS IP제한

- IAM 계정은 IP제한 적용 받는다.
- 로그인은 된다. 그러나 권한은 없다.

☰

EC2

<

대시보드

[AWS Global View](#)

이벤트

인스턴스

인스턴스

인스턴스 유형

시작 템플릿

스팟 요청

Savings Plans

예약 인스턴스

전용 호스트

용량 예약

Capacity Manager

이미지

AMI

AMI 카탈로그

Elastic Block Store

볼륨

스냅샷

수명 주기 관리자

네트워크 및 보안

보안 그룹

탄력적 IP

배치 그룹

리소스

아시아 태평양 (서울) 리전에서 다음 Amazon EC2 리소스를 사용하고 있음:

인스턴스(실행 중)	0	로드 밸런서	API 오류	배치 그룹	API 오류
보안 그룹	API 오류	볼륨	API 오류	스냅샷	API 오류
인스턴스	API 오류	전용 호스트	API 오류	키 페어	API 오류
탄력적 IP	API 오류	Auto Scaling 그룹	API 오류	Capacity Reservations	API 오류

인스턴스 시작

시작하려면 클라우드의 가상 서버인 Amazon EC2 인스턴스를 시작하십시오.

인스턴스 시작

서버 마이그레이션

참고: 인스턴스는 아시아 태평양 (서울) 리전에서 시작됩니다.

인스턴스 경고

CloudWatch에서 보기

User: arn:aws:iam::697016550159:user/test111 is not authorized to perform: cloudwatch:DescribeAlarms on resource: arn:aws:cloudwatch:ap-northeast-2:697016550159:alarm:* with an explicit deny in an identity-based policy

서비스 상태

AWS Health 대시보드

오류 발생

서비스 상태 정보를 검색하는 중에 오류가 발생했습니다.

영역

영역 이름	영역 ID
오류 발생	
서비스 상태 정보를 검색하는 중에 오류가 발생했습니다.	

추가 영역 활성화

EC2 비용

날짜 범위: 지난 6개월

리전: 글로벌

총 비용

로드할 수 없음

리전

로드할 수 없음

로드할 수 없음

Cost Explorer에서 비용 분석

EC2 프리 티어 정보

모든 AWS 리전에 대한 오퍼입니다.

0개의 EC2 프리 티어 오퍼 사용 중

월말 예측

User: arn:aws:iam::697016550159:user/test111 is not authorized to perform: freetier:GetFreeTierUsage on resource: arn:aws:freetier:us-east-1:697016550159:/GetFreeTierUsage with an explicit deny in an identity-based policy

프리 티어 초과

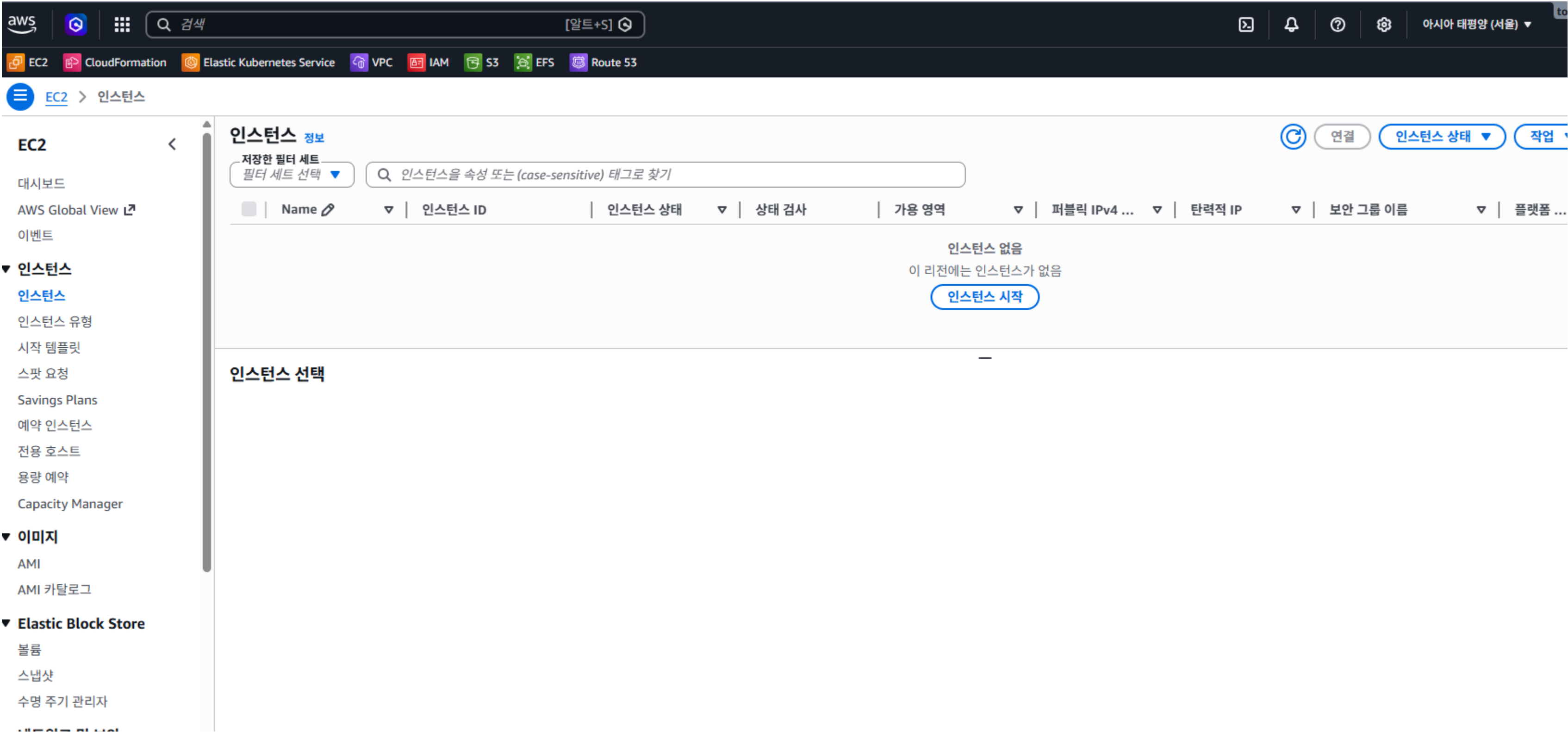
User: arn:aws:iam::697016550159:user/test111 is not authorized to perform: freetier:GetFreeTierUsage on resource: arn:aws:freetier:us-east-1:697016550159:/GetFreeTierUsage with an explicit deny in an identity-based policy

글로벌 EC2 리소스 보기

모든 AWS 프리 티어 오퍼 보기

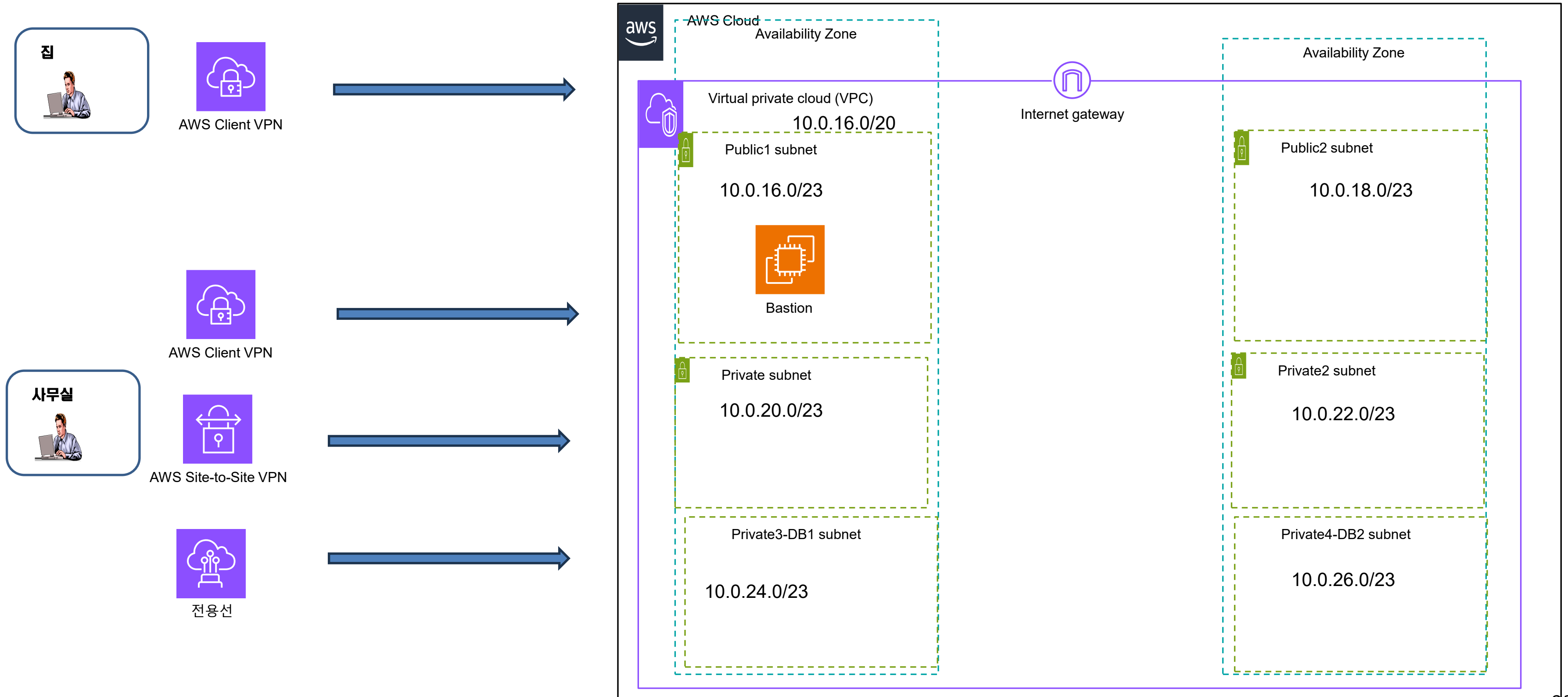
ISMS-P-AWS IP제한

- Root 계정은 IP 제한 되지 않는다.



ISMS-P-안전한 접속 환경

- <3> IPSEC VPN, SSL VPN , 전용선을 연결해 접속 체크



ISMS-P-안전한 접속 환경

- <4> 관리자 및 특수 권한으로 접속할 경우 강화된 인증(2-Factor인증) 사용 체크(필수)
- Root MFA 확인, IAM

IAM

대시보드

Identity and Access Management(IAM)

Q IAM 검색

대시보드

▼ 액세스 관리

역할

정책

IAM 사용자

IAM 사용자 그룹

ID 제공업체

계정 설정

루트 액세스 관리

임시 위임 요청

▼ 보고서 액세스

Access Analyzer

IAM 대시보드 정보

보안 권장 사항 0

✔ 루트 사용자에게 MFA 있음

루트 사용자에게 멀티 팩터 인증(MFA)을 적용하면 이 계정의 보안이 강화됩니다.

✔ 루트 사용자에게 활성 액세스 키가 없음

루트 사용자 대신 IAM 사용자에게 연결된 액세스 키를 사용하면 보안이 향상됩니다.

IAM 리소스

이 AWS 계정의 리소스

사용자 그룹	사용자	역할	정책	ID 제공업체
4	1	8	0	0

24

ISMS-P-안전한 접속 환경

- <4> 관리자 및 특수 권한으로 접속할 경우 강화된 인증(2-Factor인증) 사용 체크(필수)
- IAM 사용자 MFA 확인 , IAM

IAM > IAM 사용자

Identity and Access Management(IAM)

IAM 검색

대시보드

▼ 액세스 관리

역할

정책

IAM 사용자

IAM 사용자 그룹

ID 제공업체

계정 설정

루트 액세스 관리

임시 위임 요청

IAM 사용자 (1) 정보

IAM 사용자는 계정에서 AWS와 상호 작용하는 데 사용되는 장기 자격 증명을 가진 자격 증명입니다.

검색

☐	사용자 이름	경로	그룹	마지막 활동	MFA	암호 수명	콘솔 마지막 로그인
☐	10042	/	1	✓ 1시간 전	가상 (1)	✓ 3일	✓ 1시간 전

25

ISMS-P-안전한 접속 환경

- <5> 재택, 원격 근무 시 클라이언트 체크 - 회사 자산 노트북, 백신, Windows방화벽 활성화 여부, 보안 솔루션 체크(필수)





재택·원격 근무 시 클라이언트 체크

안전한 업무 환경을 위해 아래 항목을 반드시 확인해주세요.

 회사 자산 노트북 (업무용 장비 사용) ✓ 체크 완료  - 회사에서 지급한 업무용 노트북을 사용하고 있는지 확인합니다. - 개인 노트북이나 타인의 장비는 사용하지 않습니다.	 백신 (바이러스 백신) ✓ 체크 완료  - 백신 프로그램이 설치되어 있는지 확인합니다. - 최신 업데이트가 적용되어 있는지 확인합니다. - 실시간 보호 기능이 활성화되어 있는지 확인합니다.	 Windows 방화벽 (활성화 여부) ✓ 체크 완료  - Windows 방화벽이 활성화되어 있는지 확인합니다. - 비활성화되어 있다면 반드시 활성화합니다.	 보안 솔루션 (엔드포인트 보안 등) ✓ 체크 완료  - 회사에서 지정한 보안 솔루션이 설치되어 있는지 확인합니다. - 정상적으로 동작하고 있는지 확인합니다. (예: EDR, DLP, VPN 등)
--	---	--	--



꼭 기억하세요!

- 위 항목은 회사의 정보자산과 데이터를 보호하기 위한 필수 보안 수칙입니다.
- 체크 완료 후에만 원격 근무를 진행해 주세요.
- 문제가 있을 경우, 즉시 담당자에게 문의해 주세요.

함께 지켜요!
보안은 우리의 약속입니다.



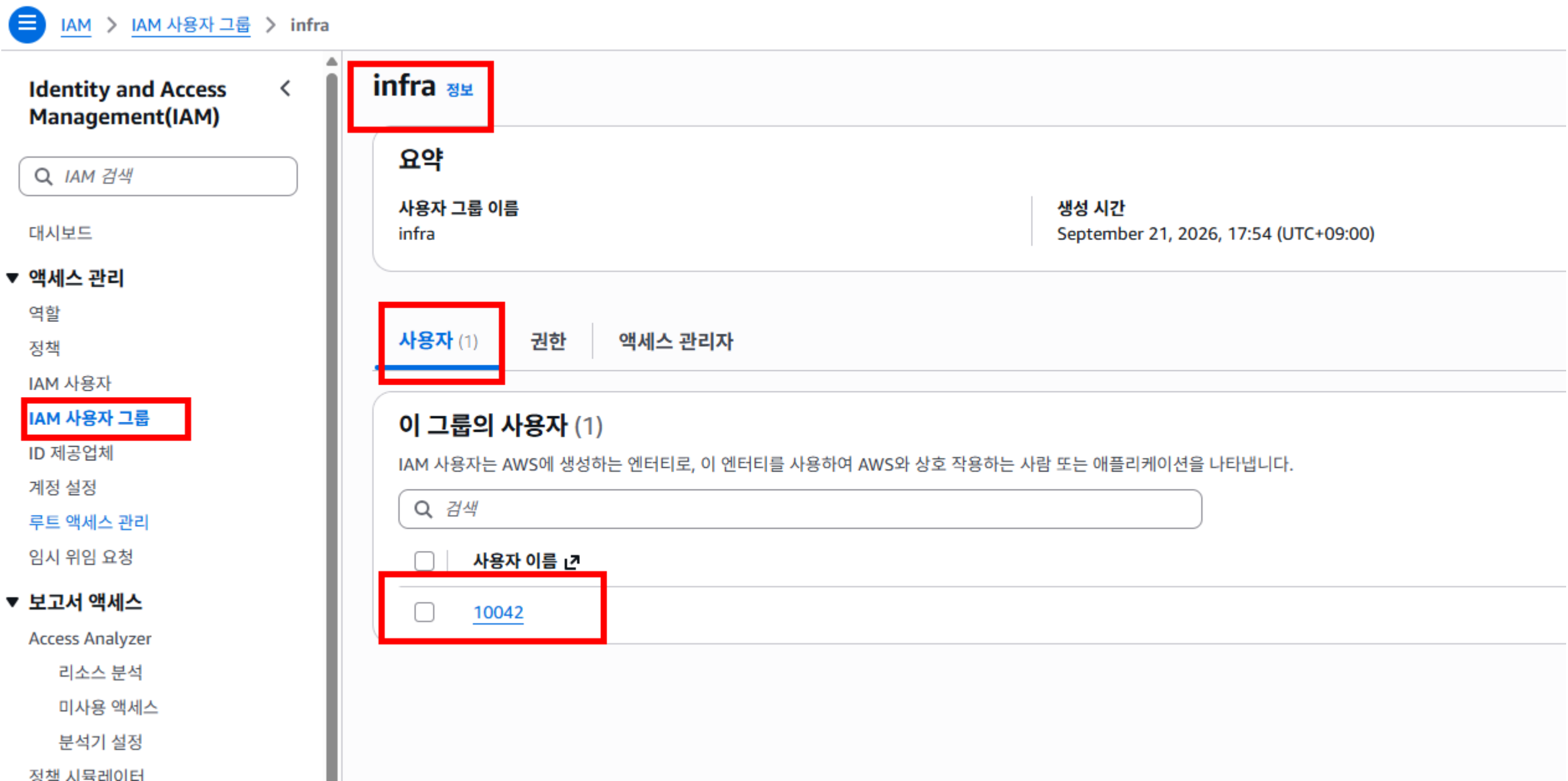
4. ISMS-P-관리 콘솔

ISMS-P-관리 콘솔

- <1> 관리자 계정 리스트 체크(필수)
- <2> 계정 관리 프로세스가 있는지 체크(필수)
- <3> 관리자 계정 로그인인 ID/Passwd 이외에 추가 2차 인증 사용 (필수)
- <4> 콘솔 로그인 기록과 검토를 하는지 체크 (필수)
- <5> Roo계정 사용하지 말아야 한다. Access/Secret Key/Pem키 체크
- <6> 관리 콘솔 로그인시 접근 할수 있는 IP 설정은 필수 이다.(필수)

ISMS-P-관리 콘솔

- <1> 관리자 계정 리스트 체크(필수)
- iam > IAM 사용자 그룹 > infra 에 있는 사용자 리스트 확인.
- 사용자이름 확인 , 퇴사와 휴직자 인지 확인



ISMS-P-관리 콘솔

- <2> 계정 관리 프로세스가 있는지 체크(필수)
- 계정 관리 프로세스 작성
- 시스템으로 계정 요청
- 분기별 계정 사용자 확인 – 결재 시스템을 이용해 확인

<2> 계정 관리 프로세스가 있는지 체크 (필수)

계정 생성부터 주기적인 확인까지, 체계적인 계정 관리 프로세스가 운영되고 있는지 확인합니다.



핵심 체크 포인트

- 계정 관리 프로세스 문서가 존재하는가?
- 시스템을 통한 계정 요청 절차가 마련되어 있는가?
- 분기별로 계정 사용자 확인을 하고, 결재 시스템을 통해 승인하는가?

체계적인 계정 관리로
보안을 강화합니다!

ISMS-P-관리 콘솔

- <3> 관리자 계정 로그인시 ID/Passwd 이외에 추가 2차 인증 사용 (필수)

IAM > IAM 사용자

Identity and Access Management(IAM)

Q IAM 검색

대시보드

▼ 액세스 관리

역할

정책

IAM 사용자

IAM 사용자 그룹

ID 제공업체

계정 설정

루트 액세스 관리

임시 위임 요청

IAM 사용자 (1) 정보

IAM 사용자는 계정에서 AWS와 상호 작용하는 데 사용되는 장기 자격 증명을 가진 자격 증명입니다.

Q 검색

☐	사용자 이름	경로	그룹	마지막 활동	MFA	암호 수명	콘솔 마지막 로그인
☐	10042	/	1	✔ 1시간 전	가상 (1)	✔ 3일	✔ 1시간 전

31

ISMS-P-관리 콘솔

- <4> 콘솔 로그인 기록과 검토를 하는지 체크 (필수)
- 1. AWS 콘솔 → CloudTrail 서비스 접속
- 2. 좌측 메뉴 "Event history" 클릭
- 3. 필터 설정: - Event name: "ConsoleLogin" 검색 - Event source: "signin.amazonaws.com" 선택 - 날짜 범위 지정
- 4. 로그인 기록 확인
- iam > 역할 >

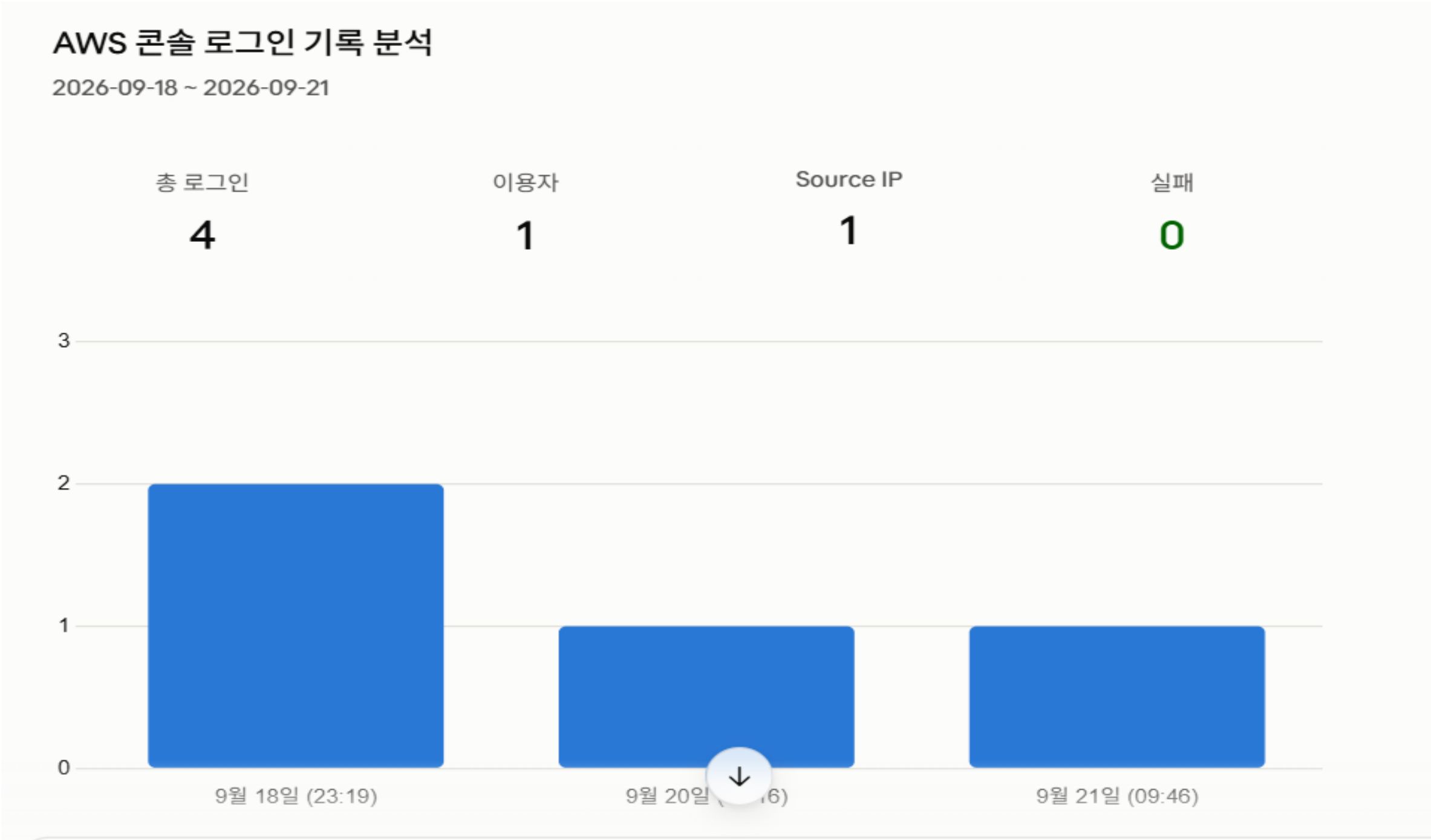
시스템으로 로그인 기록과 검토 승인 올려 이력을 남김

ISMS-P-관리 콘솔

- <4> 콘솔 로그인 기록과 검토를 하는지 체크 (필수)
- iam > 역할 > cloudtrail > 생성
- 1. AWS 콘솔 → CloudTrail 서비스 접속
- 2. 좌측 메뉴 "Event history" 클릭
- 3. 필터 설정: - Event name: "ConsoleLogin" 검색 - Event source: "signin.amazonaws.com" 선택 - 날짜 범위 지정
- 4. 로그인 기록 확인
- 5. 이벤트 다운로드 , .csv
- 6. AI통해 로그인 기록 검토

ISMS-P-관리 콘솔

- <4> 콘솔 로그인 기록과 검토를 하는지 체크 (필수)
- 6. AI통해 로그인 기록 검토



ISMS-P-관리 콘솔

- <5> Roo계정 사용하지 말아야 한다. Access/Secret Key/Pem키 체크
- Root 계정으로 로그인 , IAM에서 확인
- 루트 사용자에게 MFA 있음 , 루트 사용자에게 활성 액세스 키가 없음.

Identity and Access Management(IAM)

IAM 검색

대시보드

액세스 관리

역할

정책

IAM 사용자

IAM 사용자 그룹

ID 제공업체

계정 설정

루트 액세스 관리

임시 위임 요청

보고서 액세스

Access Analyzer

IAM 대시보드 정보

보안 권장 사항 0

✔ 루트 사용자에게 MFA 있음

루트 사용자에게 대해 멀티 팩터 인증(MFA)을 적용하면 이 계정의 보안이 강화됩니다.

✔ 루트 사용자에게 활성 액세스 키가 없음

루트 사용자 대신 IAM 사용자에게 연결된 액세스 키를 사용하면 보안이 향상됩니다.

IAM 리소스

이 AWS 계정의 리소스

사용자 그룹	사용자	역할	정책	ID 제공업체
4	1	9	0	0

새로운 기능

모두 보기

ISMS-P-관리 콘솔

- <6> 관리 콘솔 로그인시 접근 할수 있는 IP 설정은 필수 이다.(필수)
- 적용 방법 (콘솔 기준)
 1. IAM 콘솔 → 사용자 또는 그룹 선택 - dev그룹
 2. 권한 추가 → 인라인 정책 생성 클릭
 3. JSON 탭에서 위 정책 붙여넣기
 4. IP 주소를 실제 허용할 IP/CIDR로 수정
 5. 정책 검토 → 이름 입력 후 저장

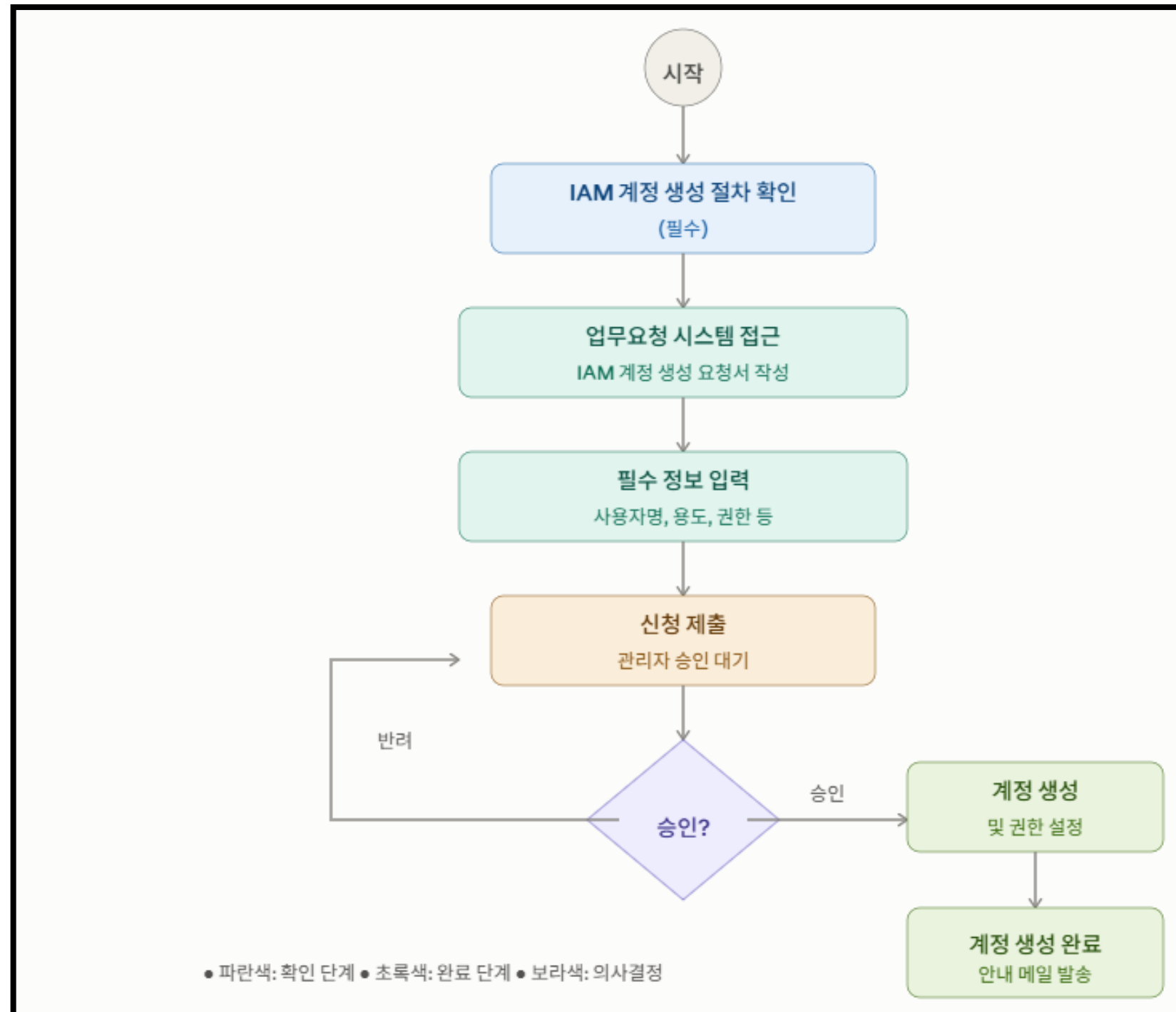
5. ISMS-P-계정 관리

ISMS-P-계정 관리

- <1> IAM계정 생성 절차 확인(필수)
- <2> 장기 미사용등 불필요한 AWS 계정이 있는지 점검 후 삭제 확인 (필수)
- <3> MFA는 필수로 설정 확인.(필수)
- <4> 그룹에 맞는 권한인지 확인. = 불필요한 Admin권한이 할당되어 있으면 회수하자.
- <5> 액세스 키는 발급 최소화 확인.(필수)

ISMS-P-계정 관리

- <1> IAM계정 생성 절차 확인(필수)
- 업무요청 시스템을 이용해 IAM계정 생성 요청함 – 별도 위키나 문서로 작성



ISMS-P-계정 관리

- <1> IAM계정 생성 절차 확인(필수)
- 업무요청 시스템을 이용해 IAM계정 생성 요청함 – 별도 위키나 문서로 작성

IAM 계정 생성 요청

신청자 정보

이름 *

홍길동

이메일 *

hong.gildong@company.com

부서 *

부서 선택하기

계정 정보

계정 사용자명 *

hong.gildong

영문 소문자, 숫자, 점(.)만 사용 가능

계정 용도 *

예: 클라우드 인프라 관리, CI/CD 파이프라인 구성 등

필요한 권한(Role) *

☐ Admin - 모든 권한

☐ Developer - 개발 권한

☐ Operator - 운영 권한

☐ Viewer - 조회 권한만

↓

ISMS-P-계정 관리

- <2> 장기 미사용등 불필요한 AWS 계정이 있는지 점검 후 삭제 확인 (필수)
- IAM 계정 점검
 - 1인 1계정 , 사용자 확인 가능 계정 필수, 공용 계정은 없어야 한다 , 장기 휴가자 계정이 있으면 삭제
 - 퇴사자 계정 삭제
 - 외부 계약 종료 업체 계정 삭제

IAM > IAM 사용자

Identity and Access Management(IAM)

Q IAM 검색

대시보드

▼ 액세스 관리

- 역할
- 정책
- IAM 사용자**
- IAM 사용자 그룹
- ID 제공업체
- 계정 설정
- 루트 액세스 관리
- 임시 위임 요청

▼ 보고서 액세스

- Access Analyzer
- 리소스 분석

IAM 사용자 (1) 정보

IAM 사용자는 계정에서 AWS와 상호 작용하는 데 사용되는 장기 자격 증명을 가진 자격 증명입니다.

Q 검색

☐	사용자 이름	경로	그룹	마지막 활동	MFA	암호 수명	콘솔 마지막 로그인	액세스
☐	10042	/	1	🟢 1시간 전	가상 (1)	🟢 3일	🟢 1시간 전	-

41

ISMS-P-계정 관리

- <2> 장기 미사용등 불필요한 AWS 계정이 있는지 점검 후 삭제 확인 (필수)
- 분기별 업무요청 시스템으로 점검 이력 남김



<2>

장기 미사용등 불필요한 AWS 계정이 있는지
점검 후 삭제 확인 (필수)

장기 미사용 계정, 불필요한 계정을 정기적으로 점검하여 보안 리스크를 줄이고, 사용자 관리를 철저히 합니다.



1

계정 현황 점검



계정 ID	최종 로그인	상태
1234-5678-9012	2025-06-10	사용중
2345-6789-0123	2024-11-03	미사용
3456-7890-1234	2023-08-15	장기미사용
4567-8901-2345	2025-05-20	사용중

전체 AWS 계정 목록 확인

최종 로그인 일자 확인

장기 미사용 계정 식별
(예: 90일 이상 미사용)

2

불필요한 계정 삭제

aws

장기 미사용 계정

업무 종료 계정

테스트 계정

사용 목적 불분명 계정



삭제

불필요한 계정 식별 후 삭제 진행

연결된 리소스(EC2, S3 등) 정리

삭제 결과 확인 및 문서화

3

분기별 점검 이력 남김



업무요청 시스템

계정 점검 요청

점검 결과 등록

삭제 내역 확인

이력 저장

분기별
(3개월마다)

분기별로 계정 점검 요청 등록
(업무요청 시스템 이용)

점검 결과 및 삭제 이력 기록

✓

핵심 체크 포인트

장기 미사용 계정은 보안 위협의 원인이 될 수 있습니다.

불필요한 계정은 즉시 삭제하여 비용 절감 및 보안 강화가 가능합니다.

분기별 정기 점검과 이력 관리를 통해 체계적으로 관리합니다.

불필요한 계정은 삭제하고
보안은 더 안전하게!



42

ISMS-P-계정 관리

- <3> MFA는 필수로 설정 확인.(필수)

IAM > IAM 사용자

Identity and Access Management(IAM)

Q IAM 검색

대시보드

▼ 액세스 관리

역할

정책

IAM 사용자

IAM 사용자 그룹

ID 제공업체

계정 설정

루트 액세스 관리

임시 위임 요청

▼ 보고서 액세스

Access Analyzer

리소스 분석

IAM 사용자 (1) 정보

IAM 사용자는 계정에서 AWS와 상호 작용하는 데 사용되는 장기 자격 증명을 가진 자격 증명입니다.

Q 검색

☐	사용자 이름	경로	그룹	마지막 활동	MFA	암호 수명	콘솔 마지막
☐	10042	/	1	✓ 1시간 전	가상 (1)	✓ 3일	✓ 1시간 전

43

ISMS-P-계정 관리

- <3> MFA는 필수로 설정 확인.(필수)
- 사용자용 액세스키가 주기적으로 교체가 되는지 확인 (3개월,6개월)

IAM 사용자 (1) [정보](#)

사용자 삭제

사용자 생성

IAM 사용자는 계정에서 AWS와 상호 작용하는 데 사용되는 장기 자격 증명을 가진 자격 증명입니다.

Q 검색

☐	사용자 이름	경로	그룹	마지막 활동	MFA	암호 수명	콘솔 마지막 로그인	액세스 키 ID	활성 키 수명	마지막으로 사용한 액세스 키
☐	10042	/	1	✔ 2시간 전	가상 (1)	✔ 3일	✔ 2시간 전	-	-	-

ISMS-P-계정 관리

- <4> 그룹에 맞는 권한인지 확인. = 불필요한 Admin권한이 할당되어 있으면 회수하자.

Identity and Access Management(IAM)

Q IAM 검색

대시보드

▼ 액세스 관리

역할

정책

IAM 사용자

IAM 사용자 그룹

ID 제공업체

계정 설정

루트 액세스 관리

임시 위임 요청

▼ 보고서 액세스

Access Analyzer

리소스 분석

미사용 액세스

분석기 설정

정책 시뮬레이터

보안 인증 보고서

다중 계정 액세스

이 사용자 그룹에 연결된 정책입니다.

dev 정보

요약

사용자 그룹 이름

dev

생성 시간

September 21, 2026, 17:54 (UTC+09:00)

ARN

arn:aws:iam::350353785226:gr

사용자

권한

액세스 관리자

권한 정책 (1) 정보

최대 10개의 관리형 정책을 연결할 수 있습니다.

Q 검색

필터링 기준 유형

모든 유형

정책 이름

AmazonEC2FullAccess

유형

AWS 관리형

연결된 엔터티

1

45

ISMS-P-계정 관리

- <5> 액세스 키는 발급 최소화 확인.(필수)
- 1. 꼭 필요하지 않으면 발급하지 않는 것을 원칙으로 한다.
- 2. 팀에 1개만 발급한다. 관리자가 누구인지 확인하고 발급한다.

<5> 액세스 키는 발급 최소화 확인 (필수)

불필요한 액세스 키 발급을 줄여 보안을 강화하고, 계정 유출 위험을 최소화합니다.

1 꼭 필요하지 않으면 발급하지 않는 것을 원칙으로 한다.

확인 방법

- ✓ 사용 목적이 명확한지 확인
- ✓ 대체 인증 방식(역할, 임시 자격 증명 등) 사용 가능 여부 검토
- ✓ 정기적으로 불필요한 키가 발급되지 않았는지 점검

💡 액세스 키는 꼭 필요한 경우에만, 최소한으로 발급하세요!

2 팀에 1개만 발급한다.

관리자가 누구인지 확인하고 발급한다.

팀당 1개만 발급

확인 사항

- ✓ 팀의 액세스 키는 1개만 발급
- ✓ 관리자(책임자) 확인 후 발급
- ✓ 발급 이력 기록 및 관리
- ✓ 불필요한 추가 발급 금지

정확한 관리자 확인과 발급 이력 관리로 보안을 강화합니다.

핵심 체크 포인트

- 액세스 키는 꼭 필요한 경우에만 발급합니다.
- 팀에는 1개만 발급하고, 관리자(책임자)를 확인한 후 발급합니다.

작은 발급 하나가 큰 보안 차이를 만듭니다!

46

6. ISMS-P-보안 그룹,네트워크

ISMS-P-보안 그룹,네트워크

- <1> Security Group별 기본 정책 여부 확인 = 있다면 지침 존재 확인(필수)
- <2> Security Group에서 유입 트래픽이 Any로 허용되지 있는지 확인.(필수)
- <3> Outboud Traffic 제어하는지 확인
- <4> 사용자는 ELB를 통해 EC2에 접속 하는지 확인.
- <5> 개발용 AWS 계정과 서비스용 AWS 계정으로 분리 확인. (선택, 회사 정책)
- <6> 기본적으로 3 계층 네트워크로 구축 확인.
- <7> AWS 웹 콘솔로 접속하는 IP를 제한하여 접속하는지 확인.(필수)
- <8> Lambda구축시 VPC안에 구축 되어 있는지 확인(필수아님)
- <9> NACL 체크(필수)
- <10> 불필요한 ACM체크(필수)

ISMS-P-보안 그룹,네트워크

- <1> Security Group별 기본 정책 여부 확인 = 있다면 지침 존재 확인(필수)
- VPC > 보안 그룹 > 인바운드 규칙 편집

VPC

보안 그룹

VPC 대시보드

VPC로 필터링

AWS Global View

Virtual Private Cloud

VPC

서브넷

라우팅 테이블

인터넷 게이트웨이

송신 전용 인터넷 게이트웨이

캐리어 게이트웨이

DHCP 옵션 세트

탄력적 IP

관리형 접두사 목록

NAT 게이트웨이

피어링 연결

라우팅 서버

보안

네트워크 ACL

보안 그룹

PrivateLink 및 Lattice

시작하기

엔드포인트

보안 그룹 (1/6) 정보

속성 또는 태그로 보안 그룹 찾기

	Name	보안 그룹 ID	보안 그룹 이름	VPC ID	설명	소유
☐	-	sg-06b41b7dcdf045468	default	vpc-04c3d5c670d6b33cf	default VPC security group	350.
☐	-	sg-056587b08f2d28e25	launch-wizard-4	vpc-04c3d5c670d6b33cf	launch-wizard-4 created 2026-09-21T0...	350.
☐	-	sg-05ddb660c347e5c6d	launch-wizard-2	vpc-04c3d5c670d6b33cf	launch-wizard-2 created 2026-09-21T0...	350.
☐	-	sg-0a92320b59acbf01	launch-wizard-5	vpc-04c3d5c670d6b33cf	launch-wizard-5 created 2026-09-21T1...	350.
☐	-	sg-04d373b0baee074ba	launch-wizard-3	vpc-04c3d5c670d6b33cf	launch-wizard-3 created 2026-09-21T0...	350.
☒	-	sg-079b56eaf508d2d76	launch-wizard-1	vpc-04c3d5c670d6b33cf	launch-wizard-1 created 2026-09-20T0...	350.

sg-079b56eaf508d2d76 - launch-wizard-1

세부 정보

인바운드 규칙

아웃바운드 규칙

공유

VPC 연결

관련 리소스 - 신규

태그

인바운드 규칙 (2)

검색

	Name	보안 그룹 규칙 ID	IP 버전	유형	프로토콜	포트 범위	소스
☐	-	sgr-08aa5cd7616253ae6	IPv4	SSH	TCP	22	0.0.0.0/0
☐	-	sgr-0c33866b147acf7c7	IPv4	HTTP	TCP	80	0.0.0.0/0

ISMS-P-보안 그룹,네트워크

- <1> Security Group별 기본 정책 여부 확인 = 있다면 지침 존재 확인(필수)
- VPC > 보안 그룹 > 인바운드 규칙 편집
- 삭제
- 규칙 추가 > SSH , 내IP , 규칙 저장

인바운드 규칙 편집

정보

인바운드 규칙은 인스턴스에 도달하도록 허용된 수신 트래픽을 제어합니다.

인바운드 규칙

정보

보안 그룹 규칙 ID

sgr-08aa5cd7616253ae6

sgr-0c33866b147acf7c7

-

유형	정보	프로토콜	정보	포트 범위	정보	소스	정보	설명 - 선택 사항	정보
SSH		TCP		22		사용자 지정			삭제
							0.0.0.0/0		
HTTP		TCP		80		사용자 지정			삭제
							0.0.0.0/0		
SSH		TCP		22		내 IP			삭제

ISMS-P-보안 그룹,네트워크

- <2> Security Group에서 유입 트래픽이 Any로 허용되지 있는지 확인.(필수)
- Trusted Advisor로 점검

Trusted Advisor 권장 사항

모든 검사 새로 고침

모든 검사 다운로드

이 페이지를 사용하여 AWS 계정에 대한 검사 결과의 개요를 확인할 수 있습니다. 검사 이름 또는 검사 카테고리를 선택하면 Trusted Advisor가 찾아낸 권장 조치 또는 잠재적인 문제를 확인할 수 있습니다. 각 검사는 문제를 해결하는 방법에 대한 추가 정보를 제공합니다. 모든 검사 결과의 요약은 다운로드할 수도 있습니다. [자세히 알아보기](#)

검사 요약

2

조치 권고

정보

보안

2

0

조사 권고

정보

0

제외 항목이 있는 검사

정보

권장 조치

▶

✖

Amazon S3 버킷 권한

열기 액세스 권한이 있거나 인증된 AWS 사용자에게 액세스를 허용하는 Amazon Simple Storage Service(Amazon S3)의 버킷을 검사합니다.

버킷 3개 중 2개에 글로벌 액세스 권한을 부여하는 권한 속성이 있습니다.

최종 업데이트: 몇 초 전

↺

↓

▶

✖

보안 그룹 - 무제한 특정 포트

보안 그룹에서 특정 포트에 대한 무제한 액세스(0.0.0.0/0)를 허용하는 규칙을 확인합니다.

보안 그룹 규칙 19개 중 8개가 특정 포트에 대해 제한 없는 액세스 권한을 허용합니다.

최종 업데이트: 몇 초 전

↺

↓

ℹ

AWS Support 플랜을 업그레이드하여 모든 Trusted Advisor 검사 받기

전화 및 채팅 지원을 통해 클라우드 지원 엔지니어로부터 기술 지원을 받을 수 있습니다. 또한 AWS Support API를 사용하거나, AWS Identity and Access Management(IAM) 사용자가 AWS 계정에 대한 지원 사례를 생성하도록 허용하거나, 아키텍처 지원 및 사용 사례 지침을 받는 등의 작업을 수행할 수 있습니다. [자세히 알아보기](#)

업그레이드

51

ISMS-P-보안 그룹, 네트워크

- <3> Outboud Traffic 제어하는지 확인
- 일반적으로 Outboud Traffic은 제어하지 않는다.
- 제어가 가능하다면 수정한다.

VPC

>

보안 그룹

>

sg-0a92320b59acbfa01

VPC 대시보드

<

VPC로 필터링

▼

AWS Global View

▼ Virtual Private Cloud

VPC

서브넷

라우팅 테이블

인터넷 게이트웨이

송신 전용 인터넷 게이트웨이

캐리어 게이트웨이

DHCP 옵션 세트

탄력적 IP

관리형 접두사 목록

NAT 게이트웨이

피어링 연결

라우팅 서버

▼ 보안

네트워크 ACL

보안 그룹

▼ PrivateLink 및 Lattice

sg-0a92320b59acbfa01 - launch-wizard-5

세부 정보

보안 그룹 이름

launch-wizard-5

보안 그룹 ID

sg-0a92320b59acbfa01

설명

launch-wizard-5 created 2026-09-21T10:04:41.345Z

VPC ID

vpc-04c3d5c670d6b33cf

소유자

350353785226

인바운드 규칙 수

1 권한 항목

아웃바운드 규칙 수

1 권한 항목

인바운드 규칙

아웃바운드 규칙

공유

VPC 연결

관련 리소스 - 신규

태그

아웃바운드 규칙 (1)

태그 관리

검색

☐	Name	보안 그룹 규칙 ID	IP 버전	유형	프로토콜	포트 범위	대상
☐	-	sgr-003b6e7c89a943625	IPv4	모든 트래픽	전체	전체	0.0.0.0/0

ALTools

ISMS-P-보안 그룹,네트워크

- <4> 사용자는 ELB를 통해 EC2에 접속 하는지 확인.
- EC2 , 로드밸런서

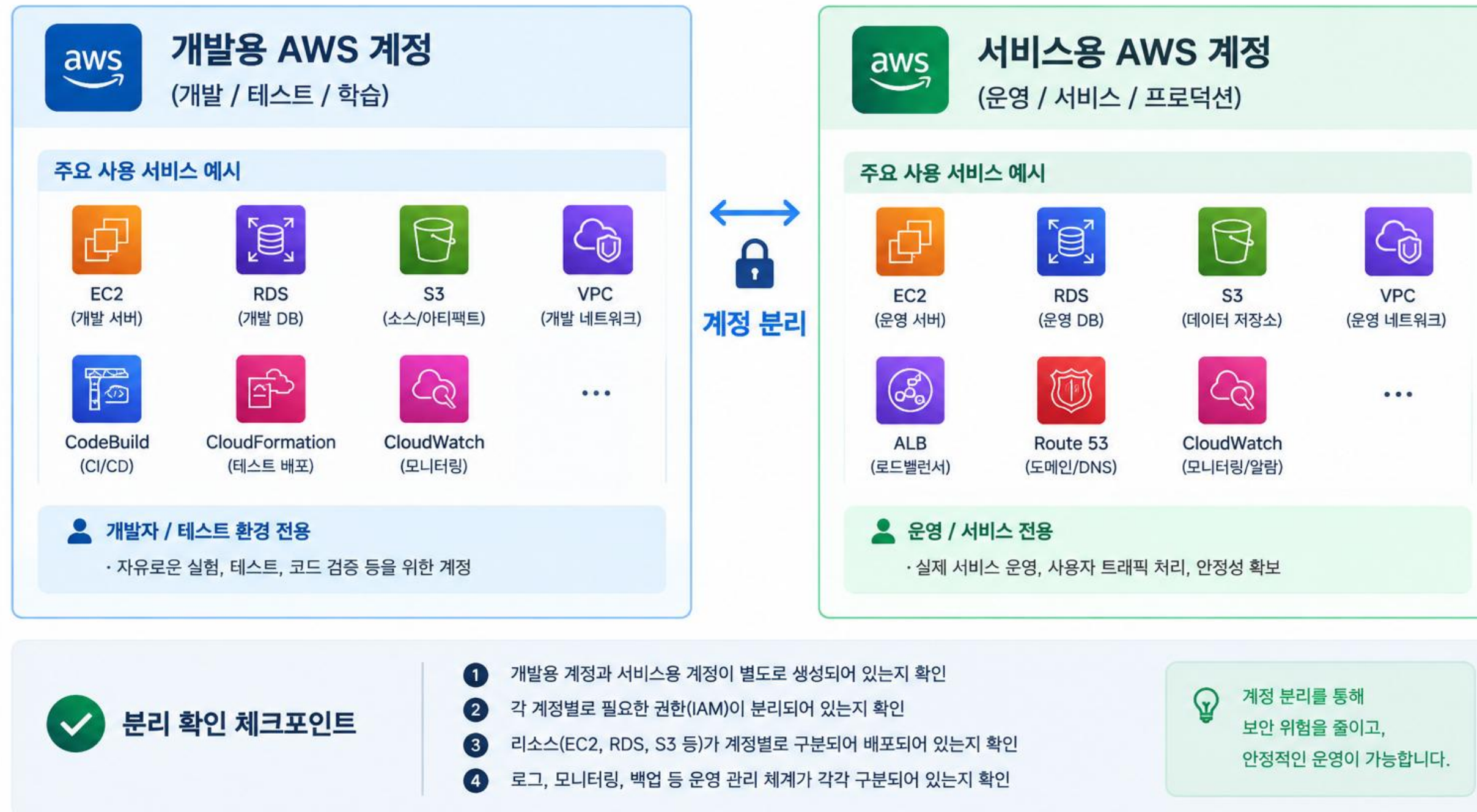


ISMS-P-보안 그룹, 네트워크

- <5> 개발용 AWS 계정과 서비스용 AWS 계정으로 분리 확인. (선택, 회사 정책)

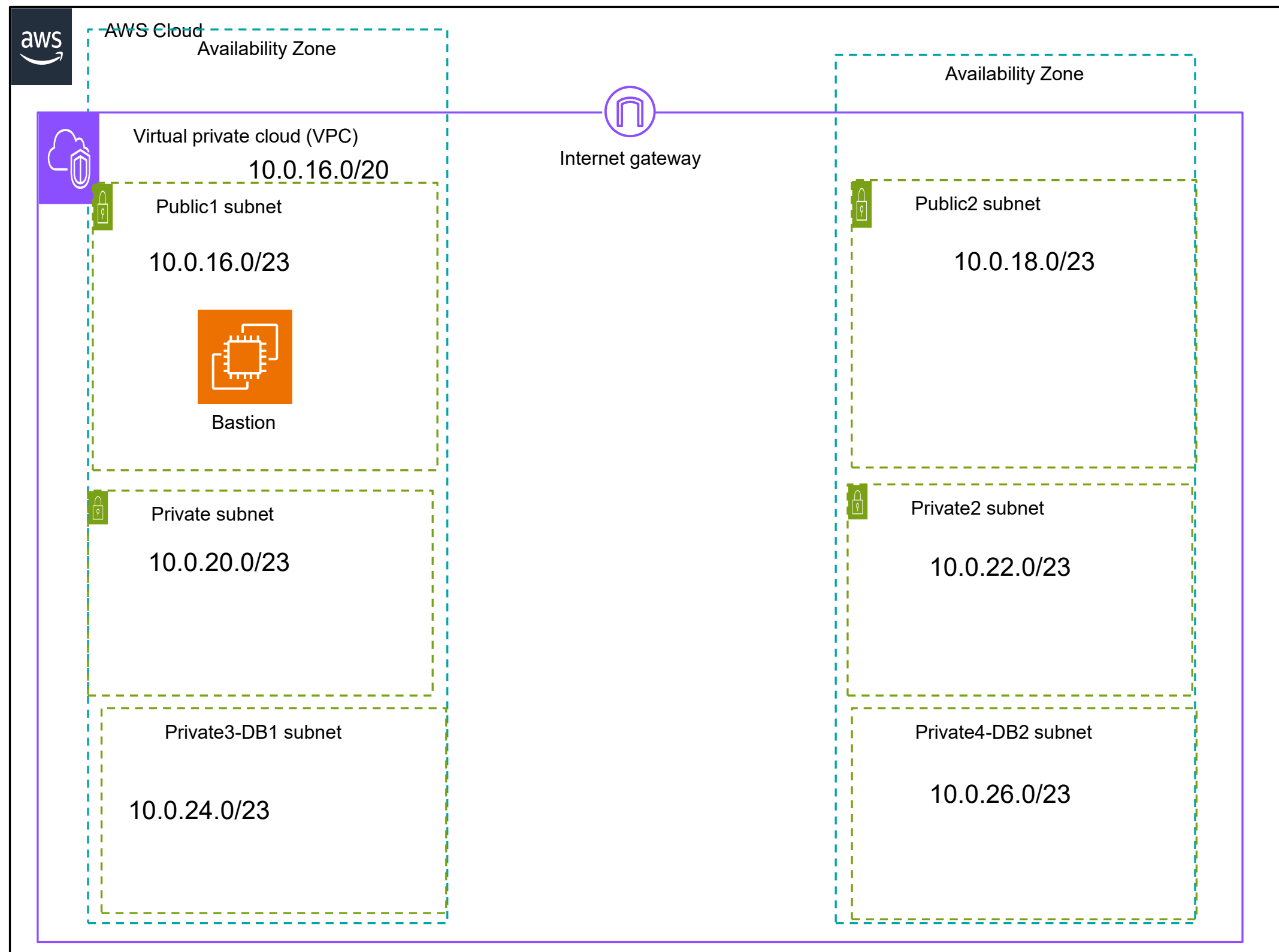
aws 개발용 AWS 계정과 서비스용 AWS 계정으로 분리 확인

개발 환경과 운영(서비스) 환경을 분리하여 보안 강화, 리스크 최소화, 관리 효율성을 높입니다.



ISMS-P-보안 그룹,네트워크

- <6> 기본적으로 3 계층 네트워크로 구축 확인.



ISMS-P-보안 그룹,네트워크

- <7> AWS 웹 콘솔로 접속하는 IP를 제한하여 접속하는지 확인.(필수)
- 적용 방법 (콘솔 기준)
 1. IAM 콘솔 → 사용자 또는 그룹 선택 - dev그룹
 2. 권한 추가 → 인라인 정책 생성 클릭
 3. JSON 탭에서 위 정책 붙여넣기
 4. IP 주소를 실제 허용할 IP/CIDR로 수정
 5. 정책 검토 → 이름 입력 후 저장
- 1. 사용자 그룹 > 그룹 생성 > dev

ISMS-P-보안 그룹, 네트워크

- <8> Lambda구축시 VPC안에 구축 되어 있는지 확인(필수아님)

Lambda함수 > 함수 생성

추가 설정

함수 아키텍처, 실행 역할, HTTP(S) 엔드포인트, 테넌트 격리 모드, VPC, 코드 서명, KMS 키 및 태그를 사용자 지정합니다.

일반 정보

ARM64 아키텍처
x86_64(기본값) 대신 ARM64를 사용하세요.

사용자 지정 실행 역할
기본 Lambda 권한이 있는 새 역할 대신 사용자 지정 실행 역할을 사용합니다(기본값).

네트워킹 정보

함수 URL
HTTP(S) 엔드포인트를 할당합니다.

테넌트 격리 모드
함수를 호출하는 각 테넌트에 대해 별도의 실행 환경을 보장합니다.

VPC
VPC에 연결하여 프라이빗 리소스에 안전하게 액세스하세요.

보안 및 거버넌스 정보

코드 서명
신뢰할 수 있는 코드만 배포해야 합니다.

AWS KMS를 사용한 암호화
자체 KMS 키를 사용하여 배포 패키지를 암호화합니다.

태그
레이블을 사용하여 함수를 구성하세요.

Settings marked with this icon cannot be added or removed after the function is created. All other settings can be changed later.

취소

함수 생성

계정의 VPC에 함수를 연결하면 VPC가 액세스를 제공하지 않는 한 인터넷에 액세스할 수 없습니다. 함수에 인터넷 액세스 권한을 부여하려면 퍼블릭 서브넷의 NAT 게이트웨이로 아웃바운드 트래픽을 라우팅합니다. 자세히 알아보기

VPC | 정보

액세스할 리소스의 VPC를 선택합니다.

vpc-04c3d5c670d6b33cf (172.31.0.0/16)

☐ 이중 스택 서브넷에 IPv6 트래픽 허용
IPv4 및 IPv6 CIDR 블록이 모두 있는 서브넷에 대한 아웃바운드 IPv6 트래픽을 허용할 수 있습니다.

서브넷

VPC 구성을 설정하는 데 사용할 Lambda의 VPC 서브넷을 선택합니다.

서브넷 선택

subnet-0d8cd037f31fcebae (172.31.48.0/20)
ap-northeast-2d

subnet-025918bc2baa20187 (172.31.0.0/20)
ap-northeast-2a

보안 그룹

VPC 구성에 사용할 보안 그룹을 선택합니다. 다음 표에는 선택한 보안 그룹의 인바운드 및 아웃바운드 규칙이 나와 있습니다.

보안 그룹 선택

sg-06b41b7dcdf045468 (default)
default VPC security group

▶ 보안 그룹 규칙 보기

ISMS-P-보안 그룹,네트워크

- <9> NACL 체크(필수)

VPC

네트워크 ACL

acl-0b0fb35282fd6f24c

AWS Global View

Virtual Private Cloud

VPC

서브넷

라우팅 테이블

인터넷 게이트웨이

송신 전용 인터넷 게이트웨이

캐리어 게이트웨이

DHCP 옵션 세트

탄력적 IP

관리형 접두사 목록

NAT 게이트웨이

피어링 연결

라우팅 서버

보안

네트워크 ACL

보안 그룹

PrivateLink 및 Lattice

시작하기

엔드포인트

acl-0b0fb35282fd6f24c

세부 정보

정보

네트워크 ACL ID

acl-0b0fb35282fd6f24c

연결 대상

4 서브넷

기본값

예

VPC ID

vpc-04c3d5c670d6b33cf

소유자

350353785226

인바운드 규칙

아웃바운드 규칙

서브넷 연결

태그

인바운드 규칙 (2)

Filter inbound rules

규칙 번호	유형	프로토콜	포트 범위	소스	허용/거부
100	모든 트래픽	모두	모두	0.0.0.0/0	Allow
*	모든 트래픽	모두	모두	0.0.0.0/0	Deny

ISMS-P-보안 그룹,네트워크

- <9> NACL 체크(필수)

VPC

네트워크 ACL

acl-0b0fb35282fd6f24c

AWS Global View

Virtual Private Cloud

VPC

서브넷

라우팅 테이블

인터넷 게이트웨이

송신 전용 인터넷 게이트웨이

캐리어 게이트웨이

DHCP 옵션 세트

탄력적 IP

관리형 접두사 목록

NAT 게이트웨이

피어링 연결

라우팅 서버

보안

네트워크 ACL

보안 그룹

PrivateLink 및 Lattice

시작하기

엔드포인트

엔드포인트 서비스

서비스 네트워크

acl-0b0fb35282fd6f24c

작업

세부 정보

정보

네트워크 ACL ID

acl-0b0fb35282fd6f24c

연결 대상

4 서브넷

기본값

예

VPC ID

vpc-04c3d5c670d6b33cf

소유자

350353785226

인바운드 규칙

아웃바운드 규칙

서브넷 연결

태그

아웃바운드 규칙 (2)

아웃바운드 규칙 편집

Filter outbound rules

규칙 번호	유형	프로토콜	포트 범위	대상	허용/거부
100	모든 트래픽	모두	모두	0.0.0.0/0	Allow
*	모든 트래픽	모두	모두	0.0.0.0/0	Deny

ISMS-P-보안 그룹,네트워크

- <10> 불필요한 ACM체크(필수)

acm

Amazon Q에게 질문하기

서비스

전체 16개 결과 보기

서비스 (16)
특징 (14)
블로그 게시물 (35)
설명서 (1,230)
지식 기사 (63)
마켓플레이스 (2,914)

 **Certificate Manager**
SSL/TLS 인증서 프로비저닝, 관리 및 배포

 **AWS Private Certificate Authority**
관리형 사설 인증 기관 서비스

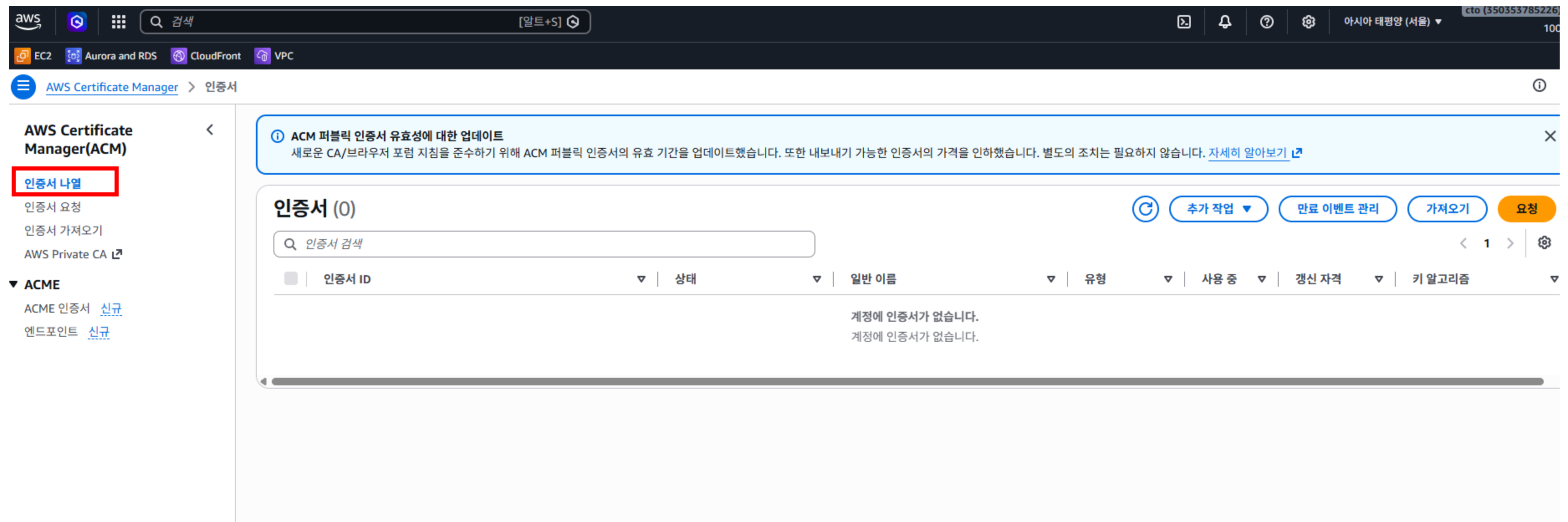
 **Secrets Manager**
수명 주기 동안 보안 암호를 손쉽게 교체, 관리 및 검색

특징

전체 14개 결과 보기

ISMS-P-보안 그룹,네트워크

- <10> 불필요한 ACM체크(필수)



7. ISMS-P-EC2 체크

ISMS-P-EC2 체크

- <1> 사전에 취약점 점검을 했는지?(필수)
- <2> EC2간 서버 간 통제 되는지 확인(필수)
- <3> EC2 로그를 저장하는가?(필수)
- <4> 장애 처리용으로 SSM 사용시 접근이력에 대한 검토가 있어야 한다(필수)

ISMS-P-EC2 체크

- <1> 사전에 취약점 점검을 했는지?(필수)
- 보안 점검을 한 결과가 있는지?
- Trusted Advisor를 통한 점검 결과

Trusted Advisor 권장 사항

모든 검사 새로 고침

모든 검사 다운로드

이 페이지를 사용하여 AWS 계정에 대한 검사 결과의 개요를 확인할 수 있습니다. 검사 이름 또는 검사 카테고리를 선택하면 Trusted Advisor가 찾아낸 권장 조치 또는 잠재적인 문제를 확인할 수 있습니다. 각 검사는 문제를 해결하는 방법에 대한 추가 정보를 제공합니다. 모든 검사 결과의 요약은 다운로드할 수도 있습니다. [자세히 알아보기](#)

검사 요약

2

조치 권고 정보

보안

0

조사 권고 정보

0

제외 항목이 있는 검사 정보

권장 조치

Amazon S3 버킷 권한

열기 액세스 권한이 있거나 인증된 AWS 사용자에게 액세스를 허용하는 Amazon Simple Storage Service(Amazon S3)의 버킷을 검사합니다.

버킷 3개 중 2개에 글로벌 액세스 권한을 부여하는 권한 속성이 있습니다.

최종 업데이트: 몇 초 전

보안 그룹 - 무제한 특정 포트

보안 그룹에서 특정 포트에 대한 무제한 액세스(0.0.0.0/0)를 허용하는 규칙을 확인합니다.

보안 그룹 규칙 19개 중 8개가 특정 포트에 대해 제한 없는 액세스 권한을 허용합니다.

최종 업데이트: 몇 초 전

AWS Support 플랜을 업그레이드하여 모든 Trusted Advisor 검사 받기

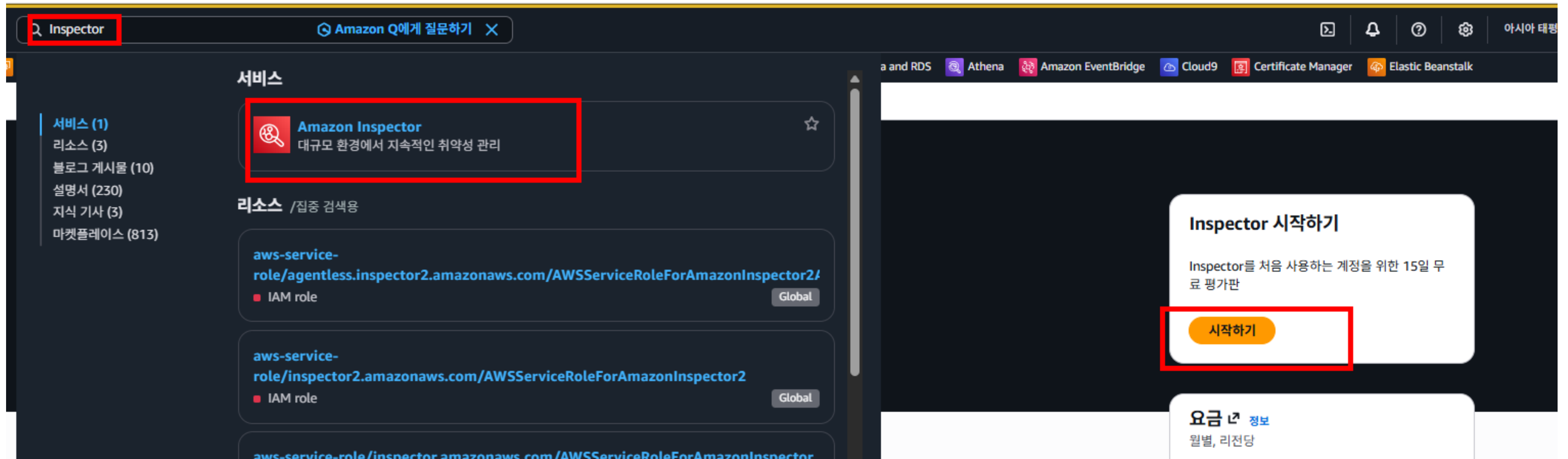
전화 및 채팅 지원을 통해 클라우드 지원 엔지니어로부터 기술 지원을 받을 수 있습니다. 또한 AWS Support API를 사용하거나, AWS Identity and Access Management(IAM) 사용자가 AWS 계정에 대한 지원 사례를 생성하도록 허용하거나, 아키텍처 지원 및 사용 사례 지침을 받는 등의 작업을 수행할 수 있습니다. [자세히 알아보기](#)

업그레이드

64

ISMS-P-EC2 체크

- <1> 사전에 취약점 점검을 했는지?(필수)
- EC2 생성, inspector를 통한 점검 결과



ISMS-P-EC2 체크

- <1> 사전에 취약점 점검을 했는지?(필수)
- 보안 점검을 한 결과가 있는지?

위임된 관리자

이 계정에는 조직의 Inspector를 관리하는 데 필요한 모든 권한이 부여됩니다. 이 계정에서는 Inspector가 활성화됩니다.

위임된 관리자 계정 ID

위임 정책

위임 정책을 업데이트하여 위임된 관리자에게 구성 정책을 관리할 권한을 부여합니다.

☒ 위임 정책을 업데이트해 주세요.

필수 정책 구문을 포함하여 위임 정책을 업데이트할 예정입니다. 아래에서 정책 구문을 검토할 수 있습니다.

☐ 정책을 수동으로 업데이트합니다.

아래 정책 구문을 복사하여 AWS Organizations의 위임 정책에 연결해야 합니다.

▼ 정책 구문

5"Sid": "SecurityServicesDelegatingOrgReadActions",

6"Effect": "Allow",

7"Principal": {

8"AWS": "arn:aws:iam::339713129945:root"

9},

10"Action": "organizations:ListRoots",

11"Resource": "*"

12},

13{

14"Sid": "SecurityServicesDelegatingNecessaryOrgManagementActions",

15"Effect": "Allow",

16"Principal": {

17"AWS": "arn:aws:iam::339713129945:root"

18},

19"Action": [

ISMS-P-EC2 체크

- <1> 사전에 취약점 점검을 했는지?(필수)
- 보안 점검을 한 결과가 있는지?

Inspector 소개

시작하기 위해 멤버 계정에 대한 Amazon EC2, Amazon ECR, AWS Lambda 스캔을 활성화합니다.

모든 계정 관리

알림

0 0 2 1 0

계정 커버리지

정보

아래에서 추가 Inspector 스캔 기능을 검토하고 구성합니다.

내 계정 (1) 정보

검색

계정 번호	계정 이름	상태	Amazon EC2 스캔	Amazon ECR 스캔	AWS Lambda 표준 스캔
	-	Activated	Activated	Activated	Activated

활성화

작업

☐ 모든 스캔

☒ Amazon EC2 스캔

☐ Amazon ECR 스캔

☐ AWS Lambda 표준 스캔

취소

제출

ISMS-P-EC2 체크

- <1> 사전에 취약점 점검을 했는지?(필수)
- 보안 점검을 한 결과가 있는지?

Inspector > 결과

Inspector

요약

취약성 데이터베이스 검색

Inventory

결과

SBOMs

CIS 스캔

Management

통합

신규

억제 규칙

설정

일반

계정 커버리지

리소스 커버리지

스캔 설정

업그레이드

사용량

새로운 소식

1개의 계정이 성공적으로 활성화되었습니다.

알림 0 0 3 1 0

결과 정보

결과 세부 정보를 보려면 행을 선택합니다.

모두 취약성별 가상 머신별 컨테이너 이미지별 컨테이너 리포지토리별 서버리스 함수별

결과 (2)

모든 결과는 심각도별로 순위가 정해집니다.

조사 결과 상태 Active

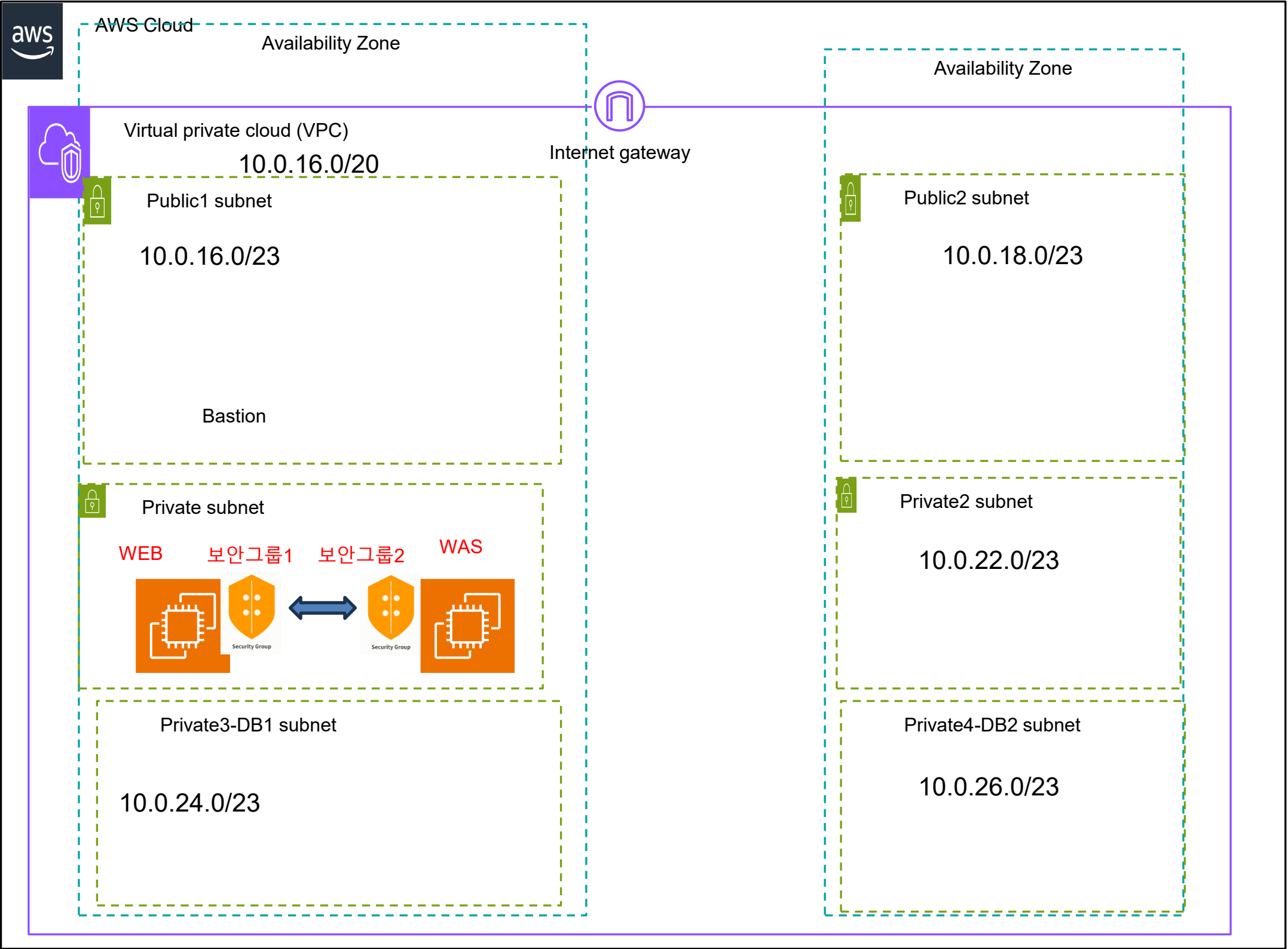
필터 기준

필터 추가

	제목	심각도	영향을 받는 리소스	계정	클라우...	리전	유형	수명	상태
	Port 22 is reachable from an Internet Gate	Medium	i-07f93bbdfb0bba741	339713129945	AWS	ap-northeast-2	Network Reachability	2 minutes	Active
	Port 80 is reachable from an Internet Gate	Low	i-07f93bbdfb0bba741	339713129945	AWS	ap-northeast-2	Network Reachability	2 minutes	Active

ISMS-P-EC2 체크

- <2> EC2간 서버 간 통제 되는지 확인(필수)
WEB서버와 WAS서버간 보안 그룹을 별도로 만들어 사용해야 한다.



ISMS-P-EC2 체크

- <2> EC2간 서버 간 통제 되는지 확인(필수)
WEB서버와 WAS서버간 보안 그룹을 별도로 만들어 사용해야 한다.

VPC

보안 그룹

VPC 대시보드

VPC로 필터링

AWS Global View

Virtual Private Cloud

- VPC
- 서브넷
- 라우팅 테이블
- 인터넷 게이트웨이
- 송신 전용 인터넷 게이트웨이
- 캐리어 게이트웨이
- DHCP 옵션 세트
- 탄력적 IP
- 관리형 접두사 목록
- NAT 게이트웨이
- 피어링 연결
- 라우팅 서버

보안

- 네트워크 ACL
- 보안 그룹

PrivateLink 및 Lattice

- 시작하기

보안 그룹 (2) 정보

속성 또는 태그로 보안 그룹 찾기

	Name	보안 그룹 ID	보안 그룹 이름	VPC ID	설명	소유자
☐	-	sg-060a1b51ac894ba47	default	vpc-00bb6414f662c7e92	default VPC security group	3397131299
☐	-	sg-082fdebefc867d109	launch-wizard-1	vpc-00bb6414f662c7e92	launch-wizard-1 created 2026-09-22T0...	3397131299

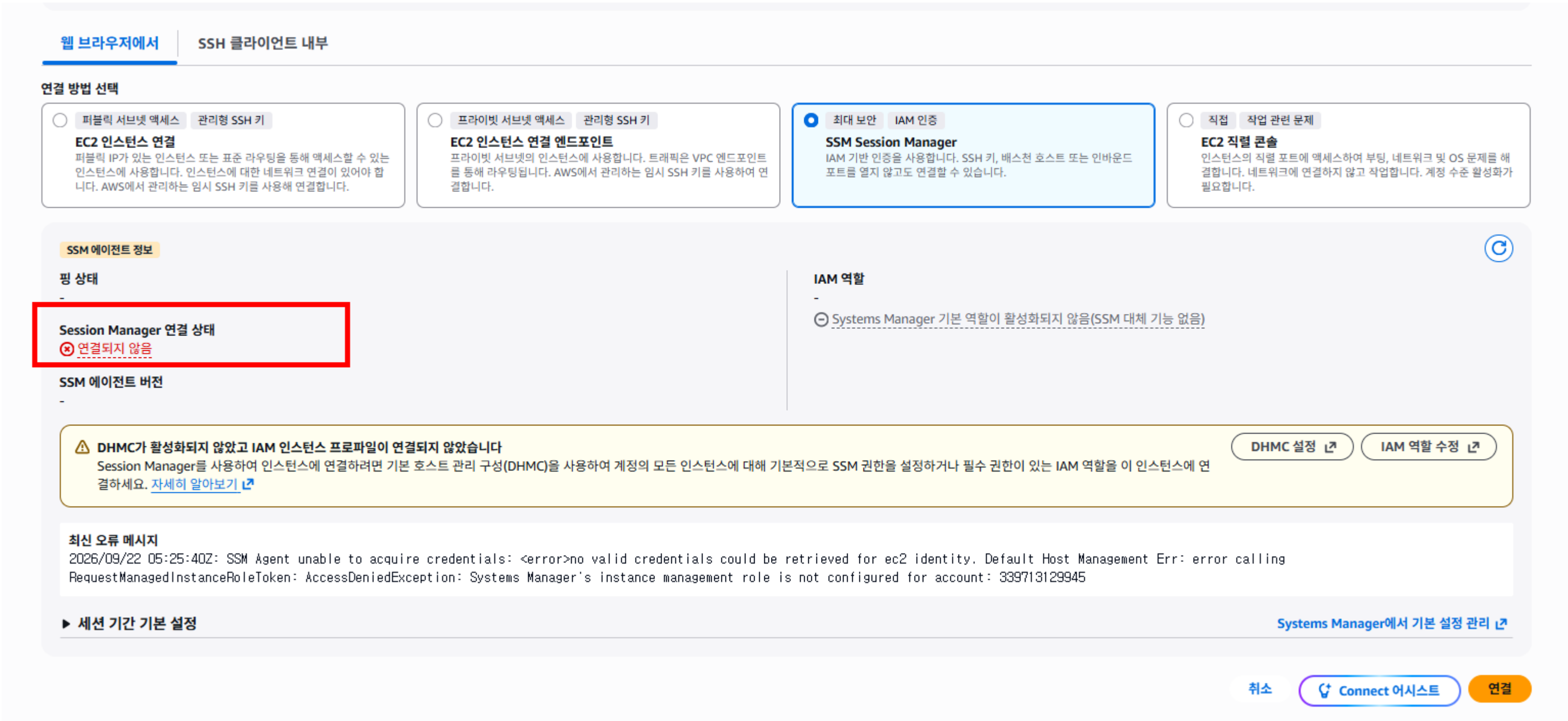
보안 그룹 선택

ISMS-P-EC2 체크

- <3> EC2 로그를 저장하는가?(필수)
- # 시스템 로그
 - /var/log/secure # 보안 관련
 - /var/log/messages # 일반 시스템 로그
 - /var/log/audit/ # 감시 로그
- # 웹 서버 로그 (Apache)
 - /var/log/httpd/access_log
 - /var/log/httpd/error_log
- # 웹 서버 로그 (Nginx)
 - /var/log/nginx/access.log
 - /var/log/nginx/error.log
- # 애플리케이션 로그
 - /var/log/myapp/application.log
 - /home/ec2-user/app/logs/
 - /opt/application/logs/
- # 커널 로그
 - /var/log/kernel
 - dmesg 명령어로도 확인 가능

ISMS-P-EC2 체크

- <4> 장애 처리용으로 SSM 사용시 접근이력에 대한 검토가 있어야 한다(필수)
- EC2 > 연결 > SSM Session Manaer 연결 상태 (연결되지 않음) – 사용하지 않으면 무관



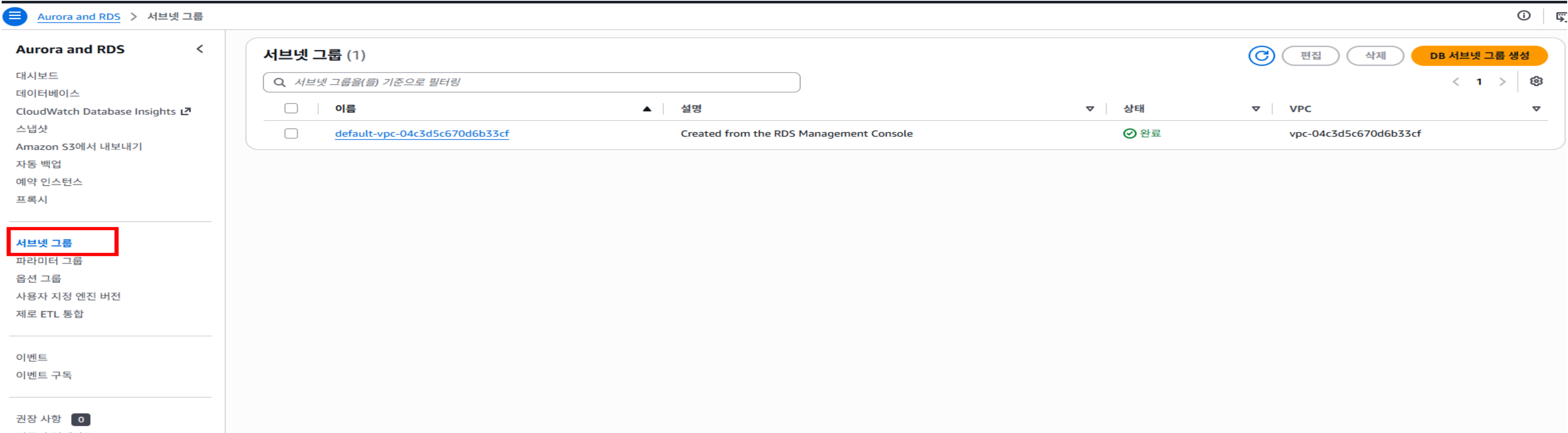
8. ISMS-P-DB 체크

ISMS-P-DB 체크

- <1> RDS서버의 DB Subnet그룹을 확인. DB Subnet만 포함되어 있는지 확인 (필수)
- <2> RDS서버의 VPC Security Group을 확인. 특정 Subnet에서만 접속되도록 설정
- <3> RDB 감사 로그를 남기도록 설정 확인.
- <4> AWS RDS 가 Public access는 허용되어 있지 않도록 되어 있는지 확인(필수)
- <5> AWS RDS 가 암호화 설정 적용되어 있는지 확인(필수)
- <6> DynamoDB는 VPC EndPoint를 사용 확인.
- <7> DB 생성/삭제 권한은 DB역할을 하는 인원만 가능 확인(필수)
- <8> DB접근 제어와 CRUD 쿼리를 제한하는지 체크(필수)
- <9> 개인정보 컬럼에 대한 암호화 적용 여부(필수)
- <10> 테이블 혹은 컬럼 명세서를 보유하고 있는지 여부(필수)

ISMS-P-DB 체크

- <1> RDS서버의 DB Subnet그룹을 확인. DB Subnet만 포함되어 있는지 확인 (필수)
- DB서버 보안을 위해 DB Subnet을 생성하고 DB를 생성한다.
- 고가용성을 위해 최소 2개 이상의 가용 영역에 걸친 서브넷이 필요하다. 이를 묶어 주는것.
- DB 서브넷 그룹을 만든 후 DB를 생성한다. Home-db-dbsg
- 데이터 베이스 생성 > 전체 구성



ISMS-P-DB 체크

- <2> RDS서버의 VPC Security Group을 확인. 특정 Subnet에서만 접속되도록 설정
- 데이터 베이스 생성 > 전체 구성 , 개발/테스트
- VPC > 보안 그룹

기존 VPC 보안 그룹

하나 이상의 옵션 선택

default X

인바운드 규칙 편집 정보

인바운드 규칙은 인스턴스에 도달하도록 허용된 수신 트래픽을 제어합니다.

인바운드 규칙 정보

보안 그룹 규칙 ID

sgr-0f899a0692808324d

-

유형 정보	프로토콜 정보	포트 범위 정보	소스 정보	설명 - 선택 사항 정보
모든 트래픽	전체	전체	사용자 지정	Q sg-060a1b51ac894ba47 X 삭제
사용자 지정 TCP	TCP	3306	사용자 지정	Q 10.0.2.0/23 X 10.0.2.0/23 X 삭제

규칙 추가

취소

변경 사항 미리 보기

규칙 저장

ISMS-P-DB 체크

- <3> RDB 감사 로그를 남기도록 설정 확인.

로그 내보내기

Amazon CloudWatch Logs로 게시할 로그 유형 선택

- ☒ 감사 로그
- ☒ 에러 로그
- ☒ 일반 로그
- ☒ iam-db-auth-error 로그
- ☒ instance 로그
- ☒ 느린 쿼리 로그

ISMS-P-DB 체크

- <4> AWS RDS 가 Public access는 허용되어 있지 않도록 되어 있는지 확인(필수)
- 퍼블릭 액세스 디폴트 값은 비허용이다.

퍼블릭 액세스 정보

- ☐ 예
RDS는 클러스터에 퍼블릭 IP 주소를 할당합니다. VPC 외부의 Amazon EC2 인스턴스 및 다른 리소스가 클러스터에 연결할 수 있습니다. VPC 내부의 리소스도 클러스터에 연결할 수 있습니다. 클러스터에 연결할 수 있는 리소스를 지정하는 VPC 보안 그룹을 하나 이상 선택합니다.
- ☒ 아니요
RDS는 클러스터에 퍼블릭 IP 주소를 할당하지 않습니다. VPC 내부의 Amazon EC2 인스턴스 및 다른 리소스만 클러스터에 연결할 수 있습니다. 클러스터에 연결할 수 있는 리소스를 지정하는 VPC 보안 그룹을 하나 이상 선택합니다.

ISMS-P-DB 체크

- <5> AWS RDS 가 암호화 설정 적용되어 있는지 확인(필수)
- 디폴트 값은 AWS관리형 KMS(SSE-KMS)사용

▼ 추가 구성

데이터베이스 옵션, 암호화 커짐, 백업 커짐, 역추적 커짐, 유지 관리, 삭제 방지 커짐.

초기 데이터베이스 이름

정보

데이터베이스 이름을 지정하지 않으면 Amazon RDS에서 데이터베이스를 생성하지 않습니다.

DB 클러스터 파라미터 그룹

정보

default.aurora-mysql8.0

DB 파라미터 그룹

정보

default.aurora-mysql8.0

장애 조치 우선 순위

기본 설정 없음

승격 티어 0 및 1의 리더 인스턴스는 라이더 인스턴스와 함께 자동 조정됩니다. 승격 티어 2~15의 인스턴스는 독립적으로 조정됩니다.

백업

백업 보존 기간

정보

자동 백업이 유지되는 일수(1~35)입니다.

7

일

백업 기간

정보

RDS에서 매일 자동 백업을 수행하는 시간 범위(UTC)입니다.

☐ 기간 선택

☒ 기본 설정 없음

백업 태그

정보

소스 데이터베이스의 태그를 자동 백업 및 스냅샷으로 각각 복사합니다.

☐ 자동 백업으로 태그 복사

☒ 스냅샷으로 태그 복사

이 설정은 일회성 설정입니다. 향후 태그를 수정하려면 수동 업데이트가 필요합니다.

암호화

정보

암호화 키

정보

☐ AWS 소유 KMS 키(SSE-RDS)

☒ AWS 관리형 KMS 키(SSE-KMS)

☐ 고객 관리형 KMS 키(SSE-KMS)

AWS KMS 키

정보

arn:aws:kms:ap-northeast-2:339713129945:key/16e526a7-3de9-428-8426-c60148b07c2f

ISMS-P-DB 체크

- <6> DynamoDB는 VPC EndPoint를 사용 확인.
- AWS DynamoDB를 **VPC Endpoint**를 통해 사용하려면 **DynamoDB용 Gateway Endpoint**를 VPC에 생성하면 됩니다.
- **VPC → Endpoints** , **Create endpoint** , **home-dy-ep**
- Services에서 **com.amazonaws.ap-northeast-2.dynamodb** 선택 , **Type: Gateway**
- 사용할 **VPC** 선택
- **Route tables**에서 **EC2가 사용하는 Private Subnet의 라우팅 테이블** 선택
- Policy는 필요에 따라 설정
 - Full Access
 - Custom
- **라우팅 테이블**에 다음과 같은 경로가 자동으로 추가됩니다.
pl-xxxxxxx (DynamoDB) vpce-xxxxxxx
따라서 Private Subnet의 EC2에서 인터넷/NAT Gateway를 거치지 않고 DynamoDB에 접근할 수 있습니다.

ISMS-P-DB 체크

- <6> DynamoDB는 VPC EndPoint를 사용 확인.

엔드포인트 설정

이름을 지정하고 엔드포인트 유형을 선택합니다.

이름 태그 - 선택 사항
키가 'Name'이고 지정된 값을 사용하여 태그를 만듭니다. 태그는 엔드포인트를 찾고 관리하는 데 도움이 됩니다.

home-dy-ep

유형 정보
카테고리 선택

☒ **AWS 서비스**
인터페이스 엔드포인트 또는 게이트웨이 엔드포인트를 사용하여 Amazon에서 제공하는 서비스에 연결

☐ **PrivateLink Ready 파트너 서비스**
인터페이스 엔드포인트를 사용하여 AWS Service Ready 지정이 있는 SaaS 서비스에 연결합니다. AWS PrivateLink를 사용합니다.

☐ **AWS Marketplace 서비스**
인터페이스 엔드포인트를 사용하여

☐ **EC2 인스턴스 연결 엔드포인트**
프라이빗 서브넷의 리소스에 연결할 수 있는 탄력적 네트워크 인터페이스

☐ **리소스**
리소스 엔드포인트를 사용하여 Amazon Relational Database Services(RDS)와 같은 리소스에 연결합니다. AWS PrivateLink를 사용합니다.

☐ **서비스 네트워크**
서비스 네트워크 엔드포인트를 사용하여 PrivateLink를 사용합니다.

☐ **NLB 및 GWLB를 사용하는 엔드포인트 서비스**
나와 공유된 서비스를 서비스 이름으로 찾아보세요. 인터페이스 엔드포인트를 사용하여 Network Load Balancer(NLB) 서비스에 연결하거나 Gateway Load Balancer 엔드포인트를 사용하여 Gateway Load Balancer(GWLB) 서비스에 연결합니다.

☐ **터널**
터널 엔드포인트를 사용하여 네트워크 세그먼트에 연결합니다. GENEVE 캡슐화가 필요합니다. AWS PrivateLink를 사용합니다.

서비스 리전

☐ **리전 간 엔드포인트 활성화** 정보
리전 간 지원 서비스에 연결합니다.

ISMS-P-DB 체크

- <6> DynamoDB는 VPC EndPoint를 사용 확인.

서비스 (1/2)

Q 검색

서비스 이름 = com.amazonaws.ap-northeast-2.dynamodb X

필터 지우기

< 1 > ⚙

서비스 이름	소유자	유형
☐ com.amazonaws.ap-northeast-2.dynamodb	amazon	Interface
☒ com.amazonaws.ap-northeast-2.dynamodb	amazon	Gateway

네트워크 설정

엔드포인트를 생성할 VPC를 선택

VPC

리소스에 액세스할 동일한 AWS 리전의 VPC에 VPC 엔드포인트를 생성합니다.

vpc-00bb6414f662c7e92

▶ 추가 설정

라우팅 테이블 (1) 정보

Q 검색

< 1 > ⚙

이름	라우팅 테이블 ID	기본	연결된 ID
☐ -	rtb-0cb0b400d23feda5d	예	4 서브넷

ISMS-P-DB 체크

- <7> DB 생성/삭제 권한은 DB역할을 하는 인원만 가능 확인(필수)
- IAM > IAM 사용자 그룹 > 그룹의 권한 확인

IAM > IAM 사용자 그룹 > dev

Identity and Access Management(IAM)

Q IAM 검색

대시보드

▼ 액세스 관리

- 역할
- 정책
- IAM 사용자
- IAM 사용자 그룹**
- ID 제공업체
- 계정 설정
- 루트 액세스 관리
- 임시 위임 요청

▼ 보고서 액세스

- Access Analyzer
 - 리소스 분석
 - 미사용 액세스
 - 분석기 설정
- 정책 시뮬레이터
- 보안 인증 보고서

▼ 다중 계정 액세스

- 계정 액세스 관리자

이 사용자 그룹에 연결된 정책입니다.

dev 정보

요약

사용자 그룹 이름

dev

생성 시간

September 21, 2026, 17:54 (UTC+09:00)

ARN

arn:aws:iam::3503537

사용자

권한

액세스 관리자

권한 정책 (2) 정보

최대 10개의 관리형 정책을 연결할 수 있습니다.

Q 검색

필터링 기준 유형

모든 유형

☐	정책 이름 ↗	▲	유형	▼	연결된 엔터티
☐	AmazonEC2FullAccess		AWS 관리형		1
☐	AmazonRDSFullAccess		AWS 관리형		1

83

ISMS-P-DB 체크

- <7> DB 생성/삭제 권한은 DB역할을 하는 인원만 가능 확인(필수)
- IAM > IAM 사용자 그룹 > 그룹의 권한 확인

4. 감사 점검은 이렇게 표로 만들면 좋습니다

사용자/역할	담당 업무	DB 생성	DB 삭제	DB 수정	결과
db-admin	DB 담당자	O	O	O	적정
developer	개발자	X	X	X	적정
ec2-admin	서버 담당자	X	X	X	적정
readonly	조회 담당	X	X	X	적정
admin	전체 관리자	O*	O*	O*	별도 관리

ISMS-P-DB 체크

- <8> DB접근 제어와 CRUD 쿼리를 제한하는지 체크(필수)
- RDS라면 **Security Group → Inbound rules**를 확인
- TCP 3306 Source: 10.0.10.0/24

ISMS-P-DB 체크

- <8> DB접근 제어와 CRUD 쿼리를 제한하는지 체크(필수)
- **MySQL/MariaDB 확인**
- DB에 접속해서:
 - SELECT user, host
 - FROM mysql.user;
- GRANT SELECT, INSERT, UPDATE
- ON mydb.*
- TO 'appuser'@'%'

ISMS-P-DB 체크

- <8> DB접근 제어와 CRUD 쿼리를 제한하는지 체크(필수)
- 삭제 권한 확인
- SHOW GRANTS FOR 'appuser'@'%';
- 전체 권한 확인
- SHOW GRANTS FOR 'appuser'@'%';
- **증적 자료**는 RDS Security Group, DB 사용자 목록, SHOW GRANTS 또는 권한 조회 결과를 캡처해 두면 좋습니다.

ISMS-P-DB 체크

- <9> 개인정보 컬럼에 대한 암호화 적용 여부(필수)
- **증적자료**로는 RDS 암호화 설정 화면 + KMS Key 설정 + 개인정보 컬럼 목록 + 암호화 적용된 데이터 또는 애플리케이션 암호화 코드를 확보하면 좋습니다.

ISMS-P-DB 체크

- <10> 테이블 혹은 컬럼 명세서를 보유하고 있는지 여부(필수)
- **증적자료**로는 RDS 암호화 설정 화면 + KMS Key 설정 + 개인정보 컬럼 목록 + 암호화 적용된 데이터 또는 애플리케이션 암호화 코드를 확보하면 좋습니다.

9. ISMS-P-스토리지 체크

ISMS-P-스토리지 체크

- <1> S3 스토리지가 Public에 노출되어 있는지 확인(필수)
- <2> Server access log가 남도록 서버 액세스 로깅 설정 확인
- <3> 스토리지 암호화 설정 적용 확인(필수)
- <4> S3 스토리지 접속 권한이 최소화되어 있는지 확인(필수)
- <5> S3 스토리지 접속 IP가 최소화되어 있는지 확인(필수)
- <6> CloudTail 로그를 별도의 S3에 저장 확인
- <7> S3에 저장된 로그에 대한 검토와 검토결과 보고 이력 확인(필수)
- <8> S3 스토리지 생성시, 생성 요청자 Tag로 남기기,팀이름 담당자명
- <9> 버전 관리 활성화 여부 확인(필수)
- <10> (정리)비공인 AWS ISMS-P체크 리스트

ISMS-P-스토리지 체크

- <1> S3 스토리지가 Public에 노출되어 있는지 확인(필수)

Amazon S3

<

bed-seo1 정보

버킷

범용 버킷

디렉터리 버킷

테이블 버킷

벡터 버킷

파일

파일 시스템

액세스 관리 및 보안

액세스 지점

FSx용 액세스 포인트

Access Grants

IAM Access Analyzer

스토리지 관리 및 인사이트

Storage Lens

배치 작업

계정 및 조직 설정

S3용 AWS Marketplace

객체

메타데이터

속성

권한

지표

관리

파일 시스템

액세스 지점

권한 개요

액세스 찾기

액세스 조사 결과는 IAM 외부 액세스 분석기에서 제공합니다. [IAM 분석기 조사 결과가 작동하는 방식](#)에 대해 자세히 알아보세요.

[us-west-2에 대한 분석기 보기](#)

퍼블릭 액세스 차단(버킷 설정)

퍼블릭 액세스는 ACL(액세스 제어 목록), 버킷 정책, 액세스 지점 정책 또는 모두를 통해 버킷 및 객체에 부여됩니다. 모든 S3 버킷 및 객체에 대한 퍼블릭 액세스가 차단되었는지 확인하려면 [모든 퍼블릭 액세스 차단]을 활성화합니다. 이 설정은 이 버킷 및 해당 객체에 대한 퍼블릭 액세스 차단]을 활성화하도록 권장하지만, 이 설정을 적용하기 전에 퍼블릭 액세스가 없어도 애플리케이션이 올바르게 작동하는지 확인합니다. 버킷 또는 내부 객체에 어느 정도 수준의 퍼블릭 액세스가 필요한 경우 특정 스토리지 사용 사례에 맞게 아래 개별 링크를 참조하십시오.

모든 퍼블릭 액세스 차단

✓ 활성화

▶ 이 버킷의 개별 퍼블릭 액세스 차단 설정

버킷 정책

JSON으로 작성된 버킷 정책은 버킷에 저장된 객체에 대한 액세스 권한을 제공합니다. 버킷 정책은 다른 계정이 소유한 객체에는 적용되지 않습니다. [자세히 알아보기](#)

이 버킷에 대해 퍼블릭 액세스 차단 설정이 활성화되어 있기 때문에 퍼블릭 액세스가 차단됩니다.

활성화된 설정을 확인하려면 이 버킷의 퍼블릭 액세스 차단 설정을 확인하세요. [Amazon S3 퍼블릭 액세스 차단 사용](#)에 대해 자세히 알아보기

ISMS-P-스토리지 체크

- <2> Server access log가 남도록 서버 액세스 로깅 설정 확인
- S3 > 속성 , 서버 액세스 로깅은 디폴트 비활성화됨 , 편집 > 활성화로 변경

Amazon S3 > 버킷 > bed-seo1

Amazon S3

버킷

- 범용 버킷
- 디렉터리 버킷
- 테이블 버킷
- 벡터 버킷

파일

- 파일 시스템

액세스 관리 및 보안

- 액세스 지점
- FSx용 액세스 포인트
- Access Grants
- IAM Access Analyzer

스토리지 관리 및 인사이트

- Storage Lens
- 배치 작업

계정 및 조직 설정

S3용 AWS Marketplace

구성 생성

CloudWatch에 로그 전달 (0)

여러 대상으로의 로그 배포를 구성합니다.

리소스 찾기

< 1 >

대상	유형	로그 유형	배포 ID
로그 배포가 구성되지 않았습니다.			

로그 배포 추가

서버 액세스 로깅

버킷 액세스 요청을 기록합니다. [CloudWatch](#)를 사용하여 서버 액세스 로깅의 상태를 확인하세요. [자세히 알아보기](#)

서버 액세스 로깅
비활성됨

편집

AWS CloudTrail 데이터 이벤트

AWS CloudTrail 콘솔에서 Amazon S3 버킷 개체 수준 작업에 대한 CloudTrail 데이터 이벤트를 보고 구성할 수 있습니다.

AWS CloudTrail

ISMS-P-스토리지 체크

- <2> Server access log가 남도록 서버 액세스 로깅 설정 확인
- S3 > 속성, 서버 액세스 로깅은 디폴트 비활성화됨 , 편집 > 활성화로 변경
- 대상 S3 버킷이 있어야 한다.

서버 액세스 로깅 편집 정보

서버 액세스 로깅

버킷에 대한 액세스 요청을 기록합니다. [자세히 알아보기](#)

서버 액세스 로깅

☐ 비활성화

☒ 활성화

⚠ 버킷 정책이 업데이트됨

서버 액세스 로깅을 활성화하면 S3 콘솔이 S3 로그 전송 그룹에 대한 액세스 권한을 포함하도록 버킷 정책을 자동으로 업데이트합니다.

대상

리전 미국 서부(오레곤) us-west-2에 대상 버킷을 지정합니다. 특정 접두사로 로그를 저장하려면 접두사 이름 뒤에 슬래시(/)를 포함해야 합니다. 그렇지 않으면 접두사가 로그 파일 이름에 추가됩니다.

s3://bucket-name/prefix

S3 찾아보기

예시: s3://<bucket>/<optional prefix with path>

대상 리전

-

대상 버킷 이름

-

대상 접두사

-

94

ISMS-P-스토리지 체크

- <3> 스토리지 암호화 설정 적용 확인(필수)
- 기본 암호화

기본 암호화

서버 측 암호화는 이 버킷에 저장된 새 객체에 자동으로 적용됩니다.

암호화 유형 [정보](#)

Amazon S3 관리형 키(SSE-S3)를 사용한 서버 측 암호화

버킷 키

KMS 암호화가 이 버킷의 새 객체를 암호화하는 데 사용되는 경우 버킷 키는 AWS KMS에 대한 호출을 줄여 암호화 비용을 줄입니다. [자세히 알아보기](#)

활성화된

차단된 암호화 유형 [정보](#)

고객 제공 키를 사용한 서버 측 암호화(SSE-C)

지능형 계층화 아카이브 구성 (0)

지능형 계층화 스토리지 클래스에 저장된 객체를 활성화하여 아카이브 액세스 계층이나 딥 아카이브 액세스 계층으로 하향됩니다. 이들 액세스 계층은 장기간 거의 액세스되지 않는 객체에 최적화

🔍 지능형 계층화 아카이브 구성 찾기

이름	상태	범위	아카이브 액세스 계층으로
----	----	----	---------------

아카이브 구성 없음

ISMS-P-스토리지 체크

- <4> S3 스토리지 접속 권한이 최소화되어 있는지 확인(필수)
- IAM 사용자/역할의 S3 권한 확인
- `aws iam list-attached-user-policies --user-name 사용자명`
- `aws iam list-user-policies --user-name 사용자명`
- 역할(Role)은:
- `aws iam list-attached-role-policies --role-name 역할명`
- `aws iam list-role-policies --role-name 역할명`
- 정책 내용 확인:
- `aws iam get-policy-version #`
- `--policy-arn 정책ARN #`
- `--version-id v1`

ISMS-P-스토리지 체크

- <4> S3 스토리지 접속 권한이 최소화되어 있는지 확인(필수)

점검 포인트

점검 항목	확인 기준
s3:*	가능하면 사용하지 않음
Action: "*"	S3 전체 권한이면 최소권한 위반 가능
Resource: "*"	필요한 버킷/객체로 제한
s3:GetObject	읽기만 필요한 계정에 적합
s3:PutObject	업로드가 필요한 경우에만
s3:DeleteObject	삭제가 필요한 담당자에게만
s3:ListBucket	버킷 목록 조회가 필요한 경우에만

ISMS-P-스토리지 체크

- <5> S3 스토리지 접속 IP가 최소화되어 있는지 확인(필수)
- AWS S3에서 스토리지 접속 IP가 최소화되어 있는지 확인하려면, 핵심은 **Bucket Policy**에서 **aws:SourceIp** 조건으로 허용 IP를 제한하고 있는지 확인하는 것입니다.
- 1. AWS 콘솔에서 확인
- S3 → 해당 버킷 → 권한 → 버킷 정책으로 이동합니다.
- 다음과 같은 정책이 있는지 확인합니다.

ISMS-P-스토리지 체크

- <5> S3 스토리지 접속 IP가 최소화되어 있는지 확인(필수)

- {
- "Effect": "Allow",
- "Principal": "*",
- "Action": "s3:*",
- "Resource": [- "arn:aws:s3::my-bucket",
- "arn:aws:s3::my-bucket/*"
-],
- "Condition": {
- "IpAddress": {
- "aws:SourceIp": [- "203.0.113.10/32",
- "203.0.113.20/32"
-]
- }
- }
- }
- }

ISMS-P-스토리지 체크

- <6> CloudTrail 로그를 별도의 S3에 저장 확인
- CloudTrail 로 확인 가능한것
- 1. 모든 API 작업 로그 기록 확인
- 2. 시스템 사용 이력을 확인
- 3. 로그를 S3에 저장하여 추후 감사
- 순서
- 1. CloudTrail 생성
- 2. S3 생성 : test6-bucket-kr
- 3. CloudTrail Event history 확인
- 4. S3에서 CloudTrail log 확인

ISMS-P-스토리지 체크

- <7> S3에 저장된 로그에 대한 검토와 검토결과 보고 이력 확인(필수)
- S3에서 Cloud Trail log 확인
- 검토 결과를 시스템으로 등록하여 이력 확인 되도록 증거를 남김



S3에 저장된 로그에 대한 검토와 검토결과 보고 이력 확인(필수)

S3에서 CloudTrail log 확인



로그는
보안의 시작입니다.

1 전체 흐름

S3에 저장된 CloudTrail 로그를 확인하고, 주요 이벤트를 검토한 후 검토결과를 보고합니다.



S3
(CloudTrail 로그 저장)



CloudTrail
(API 호출 로그 수집)



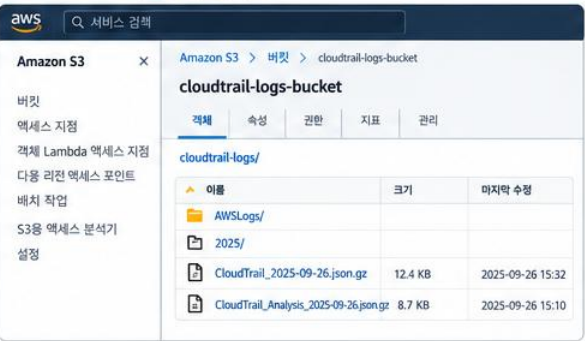
로그 검토
(이상 활동, 권한 사용 등)



검토결과 보고
(이력 확인 및 기록)

2 S3에서 CloudTrail 로그 확인

AWS Management Console에서 S3 버킷에 저장된 CloudTrail 로그 파일을 확인합니다.



3 CloudTrail 로그 확인 방법

1 S3 콘솔에서 CloudTrail 로그 버킷 선택
(예: cloudtrail-logs-bucket)

2 로그 파일 확인
(점두사: AWSLogs/계정번호/CloudTrail/연도/월/일/)

3 로그 파일 다운로드 또는 Athena를 통한 조회
(대용량 로그는 Athena 권장)

4 로그 분석 시 주요 이벤트 필터링
(예: ReadOnly, ConsoleLogin, DeleteObject 등)

TIP

Athena를 사용하면 S3에 저장된 로그를 직접 쿼리하여 빠르게 분석할 수 있습니다.

4 로그 검토 예시

CloudTrail 로그에서 주요 이벤트를 확인하고, 이상 징후가 있는지 검토합니다.

CloudTrail 이벤트 로그 예시

시간	이벤트 이름	사용자	리소스	결과
2025-09-26 10:12:34	ConsoleLogin	john@company.com	-	Success
2025-09-26 11:03:21	GetObject	app-role	arn:aws:s3::my-bucket	Success
2025-09-26 12:44:10	PutObject	user123	arn:aws:s3::my-bucket/test/	Success
2025-09-26 14:22:17	DeleteObject	unknown-user	arn:aws:s3::my-bucket/prod/	Success
2025-09-26 15:05:33	AssumeRole	admin	arn:aws:iam::123456789012:role/	Success
2025-09-26 16:18:45	CreateUser	admin	arn:aws:iam::123456789012:user/	Success

검토 포인트

비정상적인 사용자(예: unknown-user)의 접근 여부

대량 삭제/수정 등 이상 징후

정책 변경, 권한 부여 등 보안 관련 이벤트

5 검토결과 보고 이력 확인

검토한 결과를 문서로 기록하고, 보고 이력을 관리합니다.

로그 검토 결과 보고서 (예시)

검토 기간	2025-09-26 00:00 ~ 2025-09-26 23:59
검토 대상	S3 (CloudTrail 로그)
검토자	홍길동 (보안담당자)
검토 결과	특이사항 없음 정상적인 접근 및 이벤트만 확인됨
조치 사항	- 없음
보고 일시	2025-09-26 17:30

검토결과 보고 이력 확인 방법

1 보안 관련 시스템 또는 문서함에서 보고서 조회

2 보고 이력(작성자, 일시, 내용) 확인

3 필요 시 재검토 및 후속 조치

6 핵심 체크리스트 및 요약

✓ S3에 저장된 CloudTrail 로그 파일 확인 완료

✓ 주요 이벤트(로그인, 접근, 권한변경, 삭제 등) 검토 완료

✓ 이상 징후 여부 확인 및 검토결과 도출

✓ 검토결과 보고서 작성 및 이력 확인 완료

기대 효과

보안 위험 조기 탐지 및 대응

감사 및 컴플라이언스 대응 (ISMS-P 등)

데이터 접근 이력의 투명성 확보

AWS 계정 및 리소스 보호 강화

aws

로그를 확인하는 습관이
더 안전한 클라우드를 만듭니다.



101

ISMS-P-스토리지 체크

- <8> S3 스토리지 생성시, 생성 요청자 Tag로 남기기,팀이름 담당자명

S3 스토리지 생성 시, 생성 요청자 Tag로 남기기
(팀이름 / 담당자명)

목적

S3 버킷 생성 시 생성 요청자 정보를 Tag로 남겨 관리하면,

- ✓ 누가 생성했는지 쉽게 확인할 수 있습니다.
- ✓ 비용, 보안, 운영 관리 시 책임 소재를 명확히 할 수 있습니다.
- ✓ 자원 관리를 체계적으로 할 수 있습니다.

Tag 추가
팀이름 : AI팀
담당자명 : 김철수

1 S3 버킷 생성 화면 접속

AWS 콘솔에서 S3 서비스를 선택하고 버킷 만들기(Create bucket) 버튼을 클릭합니다.

2 Tag 섹션에서 태그 추가

버킷 생성 설정 중 '태그' 섹션에서 다음 형식으로 태그를 추가합니다.

태그

태그를 사용하면 비용을 추적하고 리소스를 식별하고 관리할 수 있습니다.

키	값
팀이름	AI팀
담당자명	김철수

태그 추가

3 버킷 생성 완료

생성이 완료되면, 설정한 Tag가 정상적으로 적용되었는지 확인합니다.

✓ 버킷이 생성되었습니다.
버킷의 이름: my-team-bucket-001

버킷 속성

키	값
팀이름	AI팀
담당자명	김철수

4 생성된 S3 버킷 확인

버킷 목록에서도 태그 정보를 확인할 수 있습니다.

버킷 (1)

버킷 이름 접두사로 검색

이름	리전	태그
my-team-bucket-001	ap-northeast-2	팀이름 : AI팀 담당자명 : 김철수

태그 예시

Amazon S3

키 (Tag Key)	값 (Tag Value)
팀이름	AI팀
담당자명	김철수

추가 팁

- 태그 키/값은 조직의 표준에 맞게 통일하세요.
(예: 팀이름, 담당자명, 생성일, 용도 등)
- 태그는 생성 시점에 추가하는 것이 가장 좋습니다.
- 기존 버킷에도 태그를 추가할 수 있습니다.
(버킷 > 관리 > 태그 편집)

기대 효과

- ✓ 생성 요청자 식별로 책임소재 명확화
- ✓ 비용 및 운영 관리 효율성 향상
- ✓ 보안 및 접근 제어 강화
- ✓ 자원 관리의 가시성 확보

작은 Tag 하나가, 큰 차이를 만듭니다. | AWS에서 더 안전하고 체계적인 자원 관리를 시작하세요!

102

ISMS-P-스토리지 체크

- <9> 버전 관리 활성화 여부 확인(필수)
- 디폴트 비활성화
- 활성화로 변경 필요

버킷 버전 관리

버전 관리는 객체의 여러 버전을 동일한 버킷에서 관리하기 위한 수단입니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 [자세히 알아보기](#) 

버킷 버전 관리

☐ 비활성화

☒ 활성화

10. ISMS-P 주기적 점검 체크리스트

ISMS-P 주기적 점검 체크리스트

AWS 클라우드 환경 기준 · 점검 주기 / 방법 / 증적 자료 정리

안전한 접속 환경 · 관리 콘솔 · 계정 관리 · 보안 그룹/네트워크 · EC2 · DB · 스토리지

점검 주기별 요약

주기는 권장값이며, 조직의 정보보호 정책·지침에 명시한 주기가 우선합니다

주기	주요 점검 항목	활용 도구	대표 증적
월	콘솔 로그인 기록 검토, Root 사용 여부, MFA 설정, SG Any 허용, ACM 만료, EC2 로그·SSM 이력, OS 패치, RDS Public 액세스, S3 퍼블릭 노출, CloudTrail 로그 검토	CloudTrail, IAM 자격 증명 보고서, Trusted Advisor, Inspector, Security Hub	검토 보고서 + 결재 이력
분기	관리자·IAM 계정 현황(퇴사·휴직·계약종료), 권한 적정성, 액세스 키 발급 현황, 접속 IP 제한, VPN 접속, NACL, 취약점 점검, DB 권한·CRUD, S3 권한·IP·로깅·태그	IAM, VPC, Inspector, RDS/MySQL 권한 조회, S3 버킷 정책	계정·권한 검토 결재, 점검 결과표
3~6개월	IAM 액세스 키 교체	IAM > 보안 자격 증명	키 생성일·교체 이력
반기	국내 리전 저장, SG 정책·지침, 아웃바운드 제어, 3계층 네트워크, ELB 경유, Lambda VPC, 서버 간 통제, DB 서브넷 그룹·암호화·엔드포인트, 개인정보 컬럼 암호화, 명세서, S3 암호화·버전 관리	VPC, ELB, Lambda, RDS, KMS, DynamoDB, S3	구성 캡처, 명세서, 지침 문서
연	개발/운영 계정 분리, 점검 체크리스트·지침 전면 개정	AWS Organizations	개정 이력, 계정 구조도
수시	계정 생성·삭제, 네트워크·DB 구조 변경 시 즉시 점검	업무요청 시스템	요청·승인 이력

① 안전한 접속 환경 · 관리 콘솔

관리자 접속 경로와 콘솔 계정 보호 상태를 주기적으로 확인

No	점검 항목	주기	점검 방법 (AWS 경로 / 도구)	구분	관련 기준	증적 자료
1	국내 리전 데이터 저장	반기	리전별 사용 리소스 확인(서울 ap-northeast-2), 필요 시 SCP로 리전 제한	필수	2.10.2	리전별 리소스 현황 캡처
2	관리 콘솔 접속 IP 제한	분기	IAM 그룹 인라인 정책(aws:SourceIp Deny) 적용 여부, 허용 IP 목록 최신화	필수	2.6.2	정책 JSON, 허용 IP 목록
3	VPN·전용선 경유 접속	분기	Client VPN / Site-to-Site VPN / Direct Connect 연결 상태 및 접속 로그	필수	2.6.6	VPN 설정·접속 로그
4	관리자·특수권한 2차 인증(MFA)	월	IAM 사용자 목록 MFA 열, 자격 증명 보고서(CSV) 확인	필수	2.5.3	자격 증명 보고서
5	원격근무 단말 보안	분기	회사 자산 여부, 백신·Windows 방화벽·보안 솔루션 적용 확인	필수	2.10.6	단말 점검표
6	관리자 계정 목록 검토	분기	IAM 사용자 그룹(infra 등) 사용자 ↔ 인사 현황 대조(퇴사·휴직)	필수	2.5.6	검토 결재 이력
7	콘솔 로그인 기록 검토	월	CloudTrail Event history: ConsoleLogin / signin.amazonaws.com → CSV 다운로드·분석	필수	2.9.5	검토 보고서, 결재 이력
8	Root 계정 미사용	월	IAM 대시보드: 루트 MFA 설정, 활성 액세스 키 없음, Root 로그인 이벤트 유무	필수	2.5.5	IAM 보안 권장사항 캡처

② 계정 관리 (IAM)

1인 1계정 · 최소 권한 · 키 최소화 원칙 유지 여부 점검

No	점검 항목	주기	점검 방법 (AWS 경로 / 도구)	구분	관련 기준	증적 자료
1	IAM 계정 생성 절차 준수	분기	업무요청 시스템 요청 이력 ↔ 실제 IAM 계정 대조, 절차 문서(위키) 최신화	필수	2.5.1	요청·승인 이력, 절차 문서
2	불필요 계정 정리	분기	자격 증명 보고서의 마지막 사용일 확인, 퇴사자·장기 휴가자·계약종료 업체·공용 계정 삭제	필수	2.5.1	분기 점검 결재 이력
3	전 사용자 MFA 설정	월	IAM > 사용자 > MFA 열 확인, 미설정자 조치	필수	2.5.3	자격 증명 보고서
4	액세스 키 주기적 교체	3~6개월	IAM > 보안 자격 증명 > 액세스 키 생성일·마지막 사용일	필수	2.5.4	키 교체 이력
5	그룹별 권한 적정성	분기	그룹 정책 확인, 불필요한 AdministratorAccess 회수, IAM Access Analyzer 미사용 권한	권고	2.5.6	권한 검토 결과
6	액세스 키 발급 최소화	분기	필요 시에만 발급, 팀당 1개·관리자 지정 여부 확인	필수	2.5.1	키 발급 대장

③ 보안 그룹 · 네트워크

콘솔 접속 IP 제한은 ① 관리 콘솔 항목에서 함께 점검

No	점검 항목	주기	점검 방법 (AWS 경로 / 도구)	구분	관련 기준	증적 자료
1	SG 기본 정책·지침 존재	반기	VPC > 보안 그룹 인바운드 규칙 ↔ 보안 지침 대조	필수	2.6.1	지침 문서, 규칙 캡처
2	인바운드 Any(0.0.0.0/0) 허용	월	Trusted Advisor 무제한 접근 SG 점검, Security Hub 결과	필수	2.6.1	점검 결과 캡처
3	아웃바운드 트래픽 제어	반기	SG 아웃바운드 규칙 검토, 가능 시 필요한 대상만 허용	권고	2.6.7	규칙 캡처
4	ELB 경유 EC2 접속	반기	EC2 퍼블릭 IP 부여 여부, 로드밸런서 대상 그룹 구성	권고	2.6.1	ELB 구성 캡처
5	개발/서비스 계정 분리	연	AWS Organizations 계정 구조 확인(회사 정책)	선택	2.8.3	계정 구조도
6	3계층 네트워크 구성	반기	Public / Private / DB 서브넷 및 라우팅 테이블 확인	권고	2.6.1	네트워크 구성도
7	Lambda VPC 내 구축	반기	Lambda > 구성 > VPC 연결 여부	선택	2.10.2	구성 캡처
8	NACL 규칙 점검	분기	VPC > 네트워크 ACL 인바운드·아웃바운드 규칙	필수	2.6.1	NACL 규칙 캡처
9	불필요 ACM 인증서	월	ACM 인증서 사용 여부·만료일 확인, 미사용 삭제	필수	2.7.2	인증서 목록

④ EC2

취약점 · 서버 간 통제 · 로그 · 원격 접근 이력

No	점검 항목	주기	점검 방법 (AWS 경로 / 도구)	구분	관련 기준	증적 자료
1	사전·정기 취약점 점검	분기	Amazon Inspector 스캔 결과, Trusted Advisor 보안 항목, 조치 결과 확인	필수	2.11.2	점검 결과·조치 보고서
2	OS 보안 패치 적용	월	SSM Patch Manager 준수 현황 또는 패치 이력	필수	2.10.8	패치 적용 현황
3	서버 간 접근 통제	반기	WEB/WAS 보안 그룹 분리, 소스를 SG ID로 지정했는지 확인	필수	2.6.1	SG 규칙 캡처
4	EC2 로그 저장·보관	월	/var/log/secure, messages, audit, 웹·애플리케이션 로그 수집(CloudWatch Logs) 및 보존 기간	필수	2.9.4	로그 수집 설정, 보존 정책
5	SSM 세션 접근 이력 검토	월	Session Manager 세션 기록(S3/CloudWatch), CloudTrail StartSession 이벤트 (미사용 시 해당 없음)	필수	2.9.5	접근 이력 검토 결과

⑤ 데이터베이스 (RDS · DynamoDB)

네트워크 격리 · 암호화 · 권한 · 개인정보 보호

No	점검 항목	주기	점검 방법 (AWS 경로 / 도구)	구분	관련 기준	증적 자료
1	DB 서브넷 그룹 구성	반기	RDS > 서브넷 그룹에 DB 전용 서브넷(2개 AZ 이상)만 포함	필수	2.6.4	서브넷 그룹 캡처
2	RDS 보안 그룹 접근 제한	분기	인바운드 TCP 3306 소스가 특정 서브넷(예: 10.0.10.0/24)인지 확인	권고	2.6.4	SG 규칙 캡처
3	DB 감사 로그	월	파라미터/옵션 그룹 감사 로그 활성화, CloudWatch Logs 게시	권고	2.9.4	로그 설정·검토 결과
4	Public 액세스 비허용	월	RDS > 연결 및 보안 > 퍼블릭 액세스 “아니요”	필수	2.6.4	설정 캡처
5	RDS 암호화 적용	반기	RDS > 구성 > 암호화 활성화, KMS 키 확인	필수	2.7.1	암호화·KMS 설정 캡처
6	DynamoDB VPC 엔드포인트	반기	VPC > 엔드포인트(Gateway), 라우팅 테이블 pl- 경로	권고	2.6.1	엔드포인트 구성
7	DB 생성/삭제 권한 제한	분기	IAM 그룹 정책의 RDS 생성·삭제 권한 보유자 확인	필수	2.5.5	권한 목록
8	DB 접근제어·CRUD 제한	분기	SELECT user, host FROM mysql.user; SHOW GRANTS 로 권한 확인	필수	2.6.4	계정·권한 조회 결과
9	개인정보 컬럼 암호화	반기	개인정보 컬럼 목록, 암호화 데이터 또는 애플리케이션 암호화 코드	필수	2.7.1	컬럼 목록, 암호화 증빙
10	테이블·컬럼 명세서 보유	반기	명세서 최신화 여부(스키마 변경 시 즉시 반영)	필수	2.1.3	테이블·컬럼 명세서

⑥ 스토리지 (S3)

노출 · 암호화 · 권한 · 로그 · 버전 관리

No	점검 항목	주기	점검 방법 (AWS 경로 / 도구)	구분	관련 기준	증적 자료
1	S3 퍼블릭 노출 여부	월	버킷별 “퍼블릭 액세스 차단” 설정, IAM Access Analyzer for S3	필수	2.10.2	설정·분석 결과 캡처
2	서버 액세스 로깅	분기	S3 > 속성 > 서버 액세스 로깅 활성화(기본 비활성), 대상 버킷 지정	권고	2.9.4	로깅 설정 캡처
3	기본 암호화	반기	S3 > 속성 > 기본 암호화(SSE-S3 / SSE-KMS)	필수	2.7.1	암호화 설정 캡처
4	접근 권한 최소화	분기	aws iam list-attached-user-policies / list-role-policies, get-policy-version	필수	2.5.6	정책 조회 결과
5	접속 IP 최소화	분기	버킷 정책의 aws:SourceIp 조건으로 허용 IP 제한 여부	필수	2.6.1	버킷 정책 JSON
6	CloudTrail 로그 별도 S3 저장	월	CloudTrail 추적 활성화 및 전용 로그 버킷 저장 확인	권고	2.9.4	추적 설정 캡처
7	저장 로그 검토·보고	월	S3의 CloudTrail 로그 검토 후 결과를 시스템에 등록	필수	2.9.5	검토 보고·결재 이력
8	생성자 태그 관리	분기	버킷 태그(팀명·담당자) 누락 여부, Tag Editor 조회	권고	2.1.3	태그 현황
9	버전 관리 활성화	반기	S3 > 속성 > 버전 관리 활성화(기본 비활성)	필수	2.9.3	설정 캡처

연간 점검 캘린더 (예시)

● 점검 수행 월 — 분기 점검은 3·6·9·12월, 반기 점검은 6·12월 기준

[illegible]