**2022.06.20**

**1조 핼쑥해요**

**클라우드 취약점 점검 및 조치 결과보고서**

**SK헬스 서비스 클라우드 전환 정보보안 컨설팅**

**문서 이력**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **버전** | **주요내용** | **일자** | **작성자** | **검토자** |
| Ver0.0.0 | 계획 수립 및 초안 작성 | 2022.06.07 | 김다빈  석우영 | 김백현 |
| Ver0.1.0 | 보고서 결과 작성 | 2022.06.09 | 김다빈  석우영 | 김백현 |
| Ver0.2.0 | 결과 분석 및 보고서 완성 | 2022.06.15 | 김다빈  석우영 | 김백현 |
| Ver1.0.0 | 최종 검토 | 2022.06.20 | 김다빈  석우영 | 김백현 |

목차

[**1.** **진단 개요** - 3 -](#_Toc106282271)

[**가.** **목적** - 3 -](#_Toc106282272)

[**나.** **진단 일정** - 3 -](#_Toc106282273)

[**다.** **진단 인력** - 3 -](#_Toc106282274)

[**라.** **진단 방법** - 3 -](#_Toc106282275)

[**2.** **진단 수행 절차** - 4 -](#_Toc106282276)

[**3.** **보안지수 및 등급** - 5 -](#_Toc106282277)

[**4.** **구성 현황 파악 및 진단 기준** - 7 -](#_Toc106282278)

[**가.** **구성 현황 파악** - 7 -](#_Toc106282279)

[**나.** **진단 기준** - 7 -](#_Toc106282280)

[**5.** **진단 대상** - 9 -](#_Toc106282281)

[**6.** **취약점 진단 및 조치** - 10 -](#_Toc106282282)

[**가.** **취약점 진단 결과** - 10 -](#_Toc106282283)

[**나.** **취약점 조치 결과** - 10 -](#_Toc106282284)

[**다.** **주요 개선 방안** - 12 -](#_Toc106282285)

[**7.** **세부항목 진단 결과 및 조치 가이드** - 13 -](#_Toc106282286)

[**가.** **계정관리** - 13 -](#_Toc106282287)

[**나.** **권한관리** - 30 -](#_Toc106282288)

[**다.** **데이터관리** - 40 -](#_Toc106282289)

[**라.** **가상 리소스 관리** - 44 -](#_Toc106282290)

[**마.** **감사/추적 관리** - 63 -](#_Toc106282291)

[**8.** **참조** - 75 -](#_Toc106282292)

# **진단 개요**

## **목적**

SK헬스에서 운영 중인 클라우드 서비스에 존재할 수 있는 위협 요소를 정확하게 분석하여 잠재된 보안 위협을 도출하고, 적절한 보안대책을 수립·적용하여 취약점을 제거하도록 조치한다. 이를 통해 클라우드 서비스의 보안 수준 향상 및 신뢰성을 확보하는데 그 목적이 있다.

## **진단 일정**

2022년 06월 07일부터 2022년 06월 14일까지 6일 간 수행하였다.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **분류** | **내용** | **2022년 6일** | | | | | | | |
| **06.07** | **06.08** | **06.09** | **06.10** | **06.11** | **06.12** | **06.13** | **06.14** |
| **사전준비** | 대상 범위 협의 |  |  |  |  | 휴일 | |  |  |
| **취약점 진단** | 진단 및 결과 리뷰 |  |  |  |  | 휴일 | |  |  |
| **분석 평가** | 결과 보고서 작성 및 리뷰 |  |  |  |  | 휴일 | |  |  |

[표 1] 진단 일정

## **진단 인력**

|  |  |  |  |
| --- | --- | --- | --- |
| **이름** | **소속** | **파트** | **담당업무** |
| 김다빈 | 1조 핼쑥해요 | 취약점 진단팀 | 취약점 진단 및 분석(총괄) |
| 석우영 | 1조 핼쑥해요 | 취약점 진단팀 | 취약점 진단 및 템플릿 작성 |

[표 2] 진단 인력

## **진단 방법**

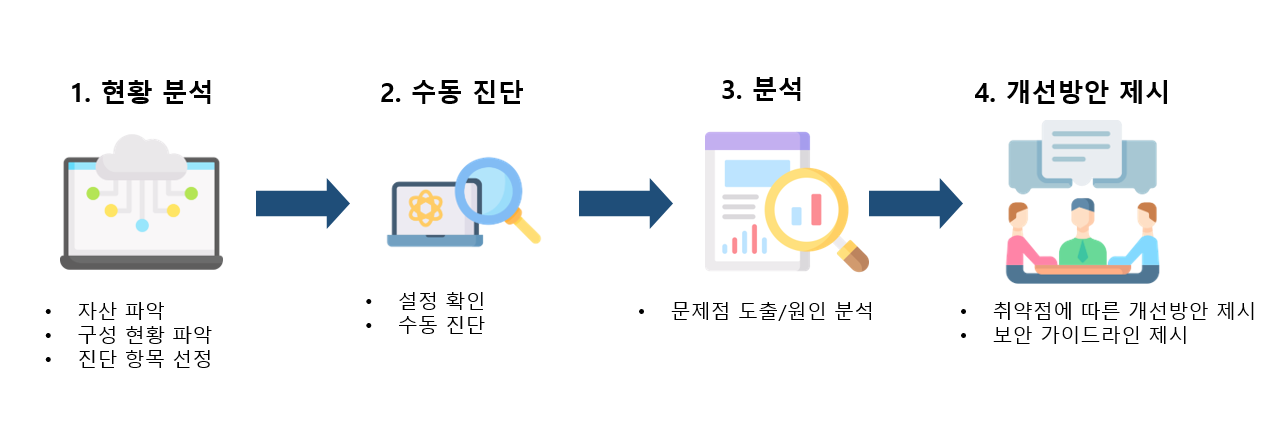
취약점 진단은 수동 진단, 실사 및 인터뷰를 통하여 실시하였다.

|  |  |
| --- | --- |
| **구분** | **설명** |
| 수동 진단 | 취약점 진단 인력이 시스템에 직접 접근하여 점검을 수행  ※ 시스템운영자 등 고객사의 관리·감독 하에 수행 |
| 실사 및 인터뷰 | 점검 대상 시스템의 운영 화면(관리자 웹 페이지 등)을 실사하거나, 운영담당자를 대상으로 인터뷰를 실시하여 점검을 수행 |

[표 3] 진단 도구

# **진단 수행 절차**

취약점 분석 수행 절차는 아래 그림과 같이 “현황분석”, “수동 진단”, “분석”, “개선방안 제시”를 수행하여 최종 취약점 분석 보고서를 작성한다.



[그림 1] 취약점 분석 평가 수행 절차

**· 1. 현황 분석**

클라우드 인프라 구조를 파악하고 AWS 구성 현황을 분석한다. 이 후 취약점 분석 대상 항목을 선정하여 전반적인 보안 현황을 파악한다.

**· 2. 수동 진단**

SK쉴더스에서 제공한 ‘2021 클라우드 보안 가이드 - AWS’ 기준으로 클라우드 인프라 환경에 대한 보안 취약점을 진단한다.

**· 3. 분석**

진단 단계에서 식별된 취약점을 분석하여 문제점을 도출하고, 현재 취약점의 보안수준을 평가하여 미칠 수 있는 위험을 분석 평가한다.

**· 4. 개선방안 제시**

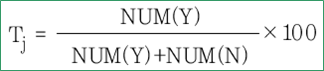
취약점 분석 평가를 통해 도출된 취약점에 대한 보안설정 가이드라인을 제공하고, 필요 시 적절한 보호대책을 제시한다.

# **보안지수 및 등급**

취약점 진단 결과에 대한 분석을 통해 발견된 취약점을 파악한 후 위험도 및 중요도, 업무 영향도 등을 평가 및 분석하여 보안지수를 산출한다.

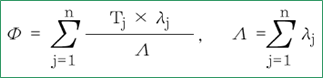
1. **항목별 평가점수 산정**

각 진단 항목별로 수행(양호) 또는 미수행(취약)을 평가하며, 진단 항목별 평가점수(Tj)는 다음과 같은 수식으로 산정한다.



1. **보안지수 산정**

진단 항목 별 위험도(λj)를 이용하여 해당 정보시스템의 평가점수를 합산한 후 누적 평가 점수를 통해 보안지수(Ф)를 산출한다.



※ 각 항목의 위험도는 과학기술정보통신부 KISA발간 ‘주요정보통신기반시설 기술적 취약점 분석·평가 방법 상세가이드라인(2017.12)’ 기준 및 클라우드 취약점 점검 가이드(2020.12)에 명시된 ’중요도‘에 따라 위험도를 1~3으로 적용한다.

1. **평가등급 기준**

보안지수에 따른 정보시스템의 평가 등급은 다음과 같이 적용한다.

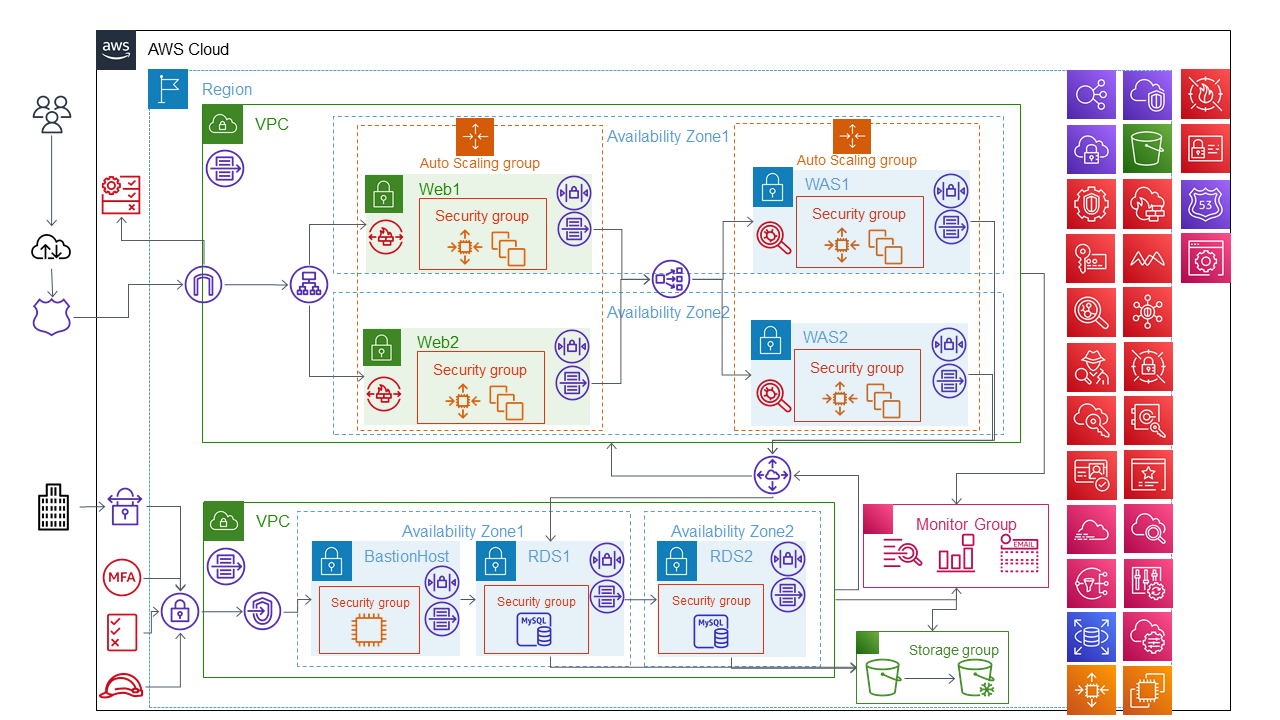
|  |  |  |
| --- | --- | --- |
| **수준** | **보안지수(%)** | **보안상태** |
| **우수** | 90 ≤ Ф ≤ 100 | 취약점 진단 평가 기준 대비 보안지수가 **90% 이상**으로 평가 |
| **양호** | 80 ≤ Ф < 90 | 취약점 진단 평가 기준 대비 보안지수가 **80% 이상, 90% 미만**으로 평가 |
| **보통** | 70 ≤ Ф <80 | 취약점 진단 평가 기준 대비 보안지수가 **70% 이상, 80% 미만**으로 평가 |
| **미흡** | 50 ≤ Ф <70 | 취약점 진단 평가 기준 대비 보안지수가 **50% 이상, 70% 미만**으로 평가 |
| **취약** | 0 ≤ Ф < 50 | 취약점 진단 평가 기준 대비 보안지수가 **50% 미만**으로 평가 |

[표 4] 평가등급 기준

# **구성 현황 파악 및 진단 기준**

## **구성 현황 파악**

SK헬스의 인프라 구성을 파악하고 보안 요건 정의서와 STRM을 근거로 클라우드 보안 현황을 분석한다. SK헬스의 AWS 구성도는 다음과 같다.



[그림 2] SK헬스 AWS 구성도

## **진단 기준**

다음은 진단에 사용될 SK쉴더스 발간 ‘2021 클라우드 보안 가이드 – AWS’ 기준의 취약점 상세 체크리스트이다.

|  |  |  |  |
| --- | --- | --- | --- |
| **영역** | **항목 코드** | **항목명** | **중요도** |
| 계정관리 | 1.1 | 관리자 계정 최소화 관리 | **상** |
| 1.2 | IAM 사용자 계정 단일화 관리 | **상** |
| 1.3 | IAM 사용자 계정 식별 관리 | **중** |
| 1.4 | Key Pair 접근 관리 | **상** |
| 1.5 | Key Pair 보관 관리 | **상** |
| 1.6 | MFA (Multi-Factor Authentication) 설정 | **중** |
| 1.7 | 패스워드 정책 관리 | **중** |
| 권한 관리 | 2.1 | 인스턴스 보안 정책 관리 | **상** |
| 2.2 | RDS 보안 정책 관리 | **상** |
| 2.3 | S3 보안 정책 관리 | **상** |
| 2.4 | Access Key 정책 관리 | **중** |
| 2.5 | Admin Console 관리자 정책 관리 | **중** |
| 2.6 | IAM 사용자 및 그룹 정책 관리 | **중** |
| 데이터 관리 | 3.1 | 인스턴스 암호화 설정 | **중** |
| 3.2 | RDS 암호화 설정 | **중** |
| 3.3 | S3 암호화 설정 | **중** |
| 가상 리소스 관리 | 4.1 | 보안그룹 인/아웃바운드 ANY 설정 관리 | **중** |
| 4.2 | 보안그룹 인/아웃바운드 불필요 정책 관리 | **중** |
| 4.3 | ACL 네트워크 인/아웃바운드 트래픽 정책 관리 | **상** |
| 4.4 | 라우팅 테이블 정책 관리 | **중** |
| 4.5 | NAT 게이트웨이 연결 관리 | **중** |
| 4.6 | 인터넷 게이트웨이 연결 관리 | **하** |
| 4.7 | S3 버킷 접근 관리 | **중** |
| 4.8 | RDS 리소스 액세스 권한 관리 | **중** |
| 4.9 | RDS API 작업 권한 관리 | **중** |
| 4.10 | RDS 서브넷 가용 영역 관리 | **중** |
| 감사/추적관리 | 5.1 | AWS 사용자 계정 로깅 설정 | **하** |
| 5.2 | 가상 인스턴스 로깅 설정 | **하** |
| 5.3 | RDS 로깅 설정 | **하** |
| 5.4 | S3 버킷 로깅 설정 | **하** |

[표 5] AWS 보안 진단 체크리스트

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

|  |  |  |
| --- | --- | --- |
| **중요도** | **내용** | **위험도** |
| **상** | 관리자 계정 및 주요 정보 유출로 인한 치명적인 피해 발생 | 3 |
| **중** | 노출된 정보를 통해 서비스/시스템 관련 추가 정보 유출 발생 우려 | 2 |
| **하** | 타 취약점과 연계 가능한 잠재적인 위협 내재 | 1 |

[표 6] 위험도 분류

# **진단 대상**

AWS클라우드 환경에서 제공되는 서비스를 진단대상으로 선정하였으며, 상세 현황은 다음과 같다.

|  |  |  |
| --- | --- | --- |
| **구분** | **설명** | **수량** |
| AWS Identity and Access Management(IAM) | 리소스 제어 권한 관리 | 13 |
| Amazon EC2 | 가상 컴퓨팅 환경 | 6 |
| Amazon S3 | 인터넷용 스토리지 | 3 |
| Amazon RDS | 데이터베이스 관리 시스템 | 3 |
| Amazon VPC | 가상 네트워크 | 4 |
| AWS CloudTrail | 호출 기록 점검 및 모니터링 | 1 |
| **합계** | | **30** |

[표 7] 진단 대상

# **취약점 진단 및 조치**

## **취약점 진단 결과**

SK헬스의 클라우드 인프라에 대한 취약점 조치 전 예상 평균 보안지수는 다음 그래프와 같이 63%(점)으로 보안 수준이 '미흡'한 상태로 평가되었다.

AWS 서비스별 보안 수준 평가결과는 다음 그래프와 같이 VPC의 보안 수준이 ‘최우수’로 타 시스템보다 상대적으로 높은 보안수준을 유지하였고, AWS Identity and Access Management(IAM)의 보안지수가 53.8%, CloudTrail의 보안지수가 0%로 평균보다 낮게 평가되었다.

**평균**

**63**

[그림 1] 취약점 조치 전 AWS 서비스별 보안지수

## **취약점 조치 결과**

SK헬스의 클라우드 인프라에 대한 취약점 조치 후 예상 결과 평균 보안지수는 83.3%(점)으로 보안 수준이 ‘양호’한 상태로 평가되었다.

AWS 서비스별 보안 수준 평가결과는 다음 그래프와 같이 Amazon EC2 및 Amazon S3, Amazon RDS, AWS CloudTrail의 보안 수준이 ‘최우수’로 타 시스템보다 상대적으로 높은 보안수준을 유지하였고, AWS Identity and Access Management(IAM)의 보안지수가 69.2%로 가장 낮게 평가되었다.

**평균**

**83.3**

[그림 2] 취약점 조치 후 AWS 서비스별 보안지수

‘2021클라우드보안\_AWS’의 설정 방법에 따라 식별된 취약점을 조치하였다. 먼저, 가장 취약한 CloudTrail의 감사 로그를 S3에 별도로 보관했으며, IAM에서 사용자 계정에 태그를 추가하고 패스워드 정책을 보완하였다. 보안지수가 평균보다 높았던 EC2에서는 인스턴스 내에서 CloudWatch Agent를 설치하고, 인/아웃 바운드의 소스와 목적지를 ANY에서 변경해주었다. 마지막으로 RDS와 S3의 로그를 별도로 보관하기 위해 각각 데이터베이스 스트림과 서버 액세스 로깅을 활성화하였다.

AWS 시스템별 취약점 통계는 아래와 같다.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **구분** | **진단 항목** | | | |
| **전체** | **양호** | **조치 후 양호** | **취약** |
| AWS Identity and Management(IAM) | 13 | 7 | 2 | 4 |
| Amazon EC2 | 6 | 4 | 2 | - |
| Amazon S3 | 3 | 2 | 1 | - |
| Amazon RDS | 3 | 2 | 1 | - |
| Amazon VPC | 4 | 3 | - | 1 |
| AWS CloudTrail | 1 | - | 1 | - |
| **통계** | **30** | **18** | **7** | **5** |

[표 8] 시스템별 취약점 통계

다음 세부항목 진단 결과 및 조치 가이드에는 취약점을 조치한 항목만 조치 내용(가이드)과 조치 내용 설명이 있으며, 그 외 양호 혹은 취약한 항목은 점검 내용까지 존재한다.

## **주요 개선 방안**

주요 취약사항으로는 AWS Identity and Access Management(IAM)에서 권한 부여와 관리가 미흡하였으며, 인터넷 게이트웨이를 사용하는 과정이 취약점으로 판단되었다. 역할 및 그룹에 따라 필요한 권한만 부여하며 관리자가 지속적으로 IAM을 활용하여 권한에 대한 업데이트를 지속적으로 해야 한다.

1. **적절한 관리자 권한 부여**

각 서비스에 따른 관리자 권한이 사용 목적에 맞게 부여하도록 해야 한다. 특히 전체 권한으로 열어 둘 경우 서비스 정보들이 노출되어 정보의 유출을 예상할 수 있다. 특히 SK헬스 서비스는 신체 정보, 사생활 등 민감정보들을 포함하기 때문에 이 점을 유의하여 역할별로 리스트를 만들어 관리하여야 한다.

1. **사용자 역할에 따른 서비스 권한 부여**

Amazon EC2, Amazon RDS, Amazon S3 등 AWS 서비스의 IAM 사용 권한은 각 서비스 역할에 맞도록 설정해야 한다. 사전에 서비스 역할별 권한 정책을 정리하고 관리형 정책 권한 리스트를 작성하여 적절하게 사용해야 한다. SK헬스를 운영 시 총괄 관리, 데이터베이스 관리, 서버 관리, 네트워크 관리, 보안 관리 등 부여된 역할에 맞게 AWS 서비스의 권한을 부여하여야 한다.

1. **라우팅 테이블 대상 관리**

SK헬스 서비스는 인터넷을 활용하기 위해 라우팅 테이블에 인터넷 게이트웨이를 연결하며 대상이 ANY로 설정되어 있다. 그러나 망 분리를 활용하는 라우팅 테이블은 피어링을 통해 ANY가 아닌 지정된 대상이 연결되어 있다.

추후 라우팅 테이블을 인터넷 게이트웨이 연결 외 다른 목적으로 사용할 경우 0.0.0.0/0이 아닌 지정된 대상으로 정하여 취약점을 감소시키도록 노력하여야 한다.

# **세부항목 진단 결과 및 조치 가이드**

## **계정관리**

**1) 관리자 계정 최소화 관리**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 계정관리 | **중요도** | **상** |
| **점검 날짜** | 2022년 6월 7일 | **결과** | **취약** |
| **점검 대상** | AWS Identity and Access Management (IAM) | | |
| **항목명** | 관리자 계정 최소화 관리 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | 모든 AWS 리소스는 AWS 계정의 소유이고, 리소스 생성 또는 액세스 권한은 권한 정책에 따라 결정됩니다. 계정 관리자는 IAM 자격 증명(즉 사용자, 그룹, 역할)에 권한 정책을 연결할 수 있으며 적절한 권한을 통한 서비스 관리가 이루어져야 합니다.  **1. AWS 관리형 정책**  서비스 내 FULL ACCESS 등과 같이 중요도가 높은 AWS 관리형 정책은 EC2 서비스 관리/운영자 및 관련 담당자 외에 다른 IAM 계정에 아래와 같은 권한 할당이 되지 않도록 해야 합니다. 그 중에서도 AWS Root 관리자 인 “Administratoraccess” 권한은 다수의 IAM 계정에 설정되지 않도록 관리 조치가 필요합니다.  **(\*) “Administratoraccess” 및 "Full Access" 권한이 부여된 다수의 계정이 존재할 경우 담당자 확인이 필요함** | | |
| **진단 기준** | **양호 기준**  관리자 권한이 사용 목적에 맞게 지정된 사용자가 부여되어 있을 경우  **취약 기준**  관리자 권한이 사용 목적에 맞지 않은 사용자에게 불필요하게 부여되어 있을 경우 | | |
| **점검 내용** | **가. IAM 그룹에 포함되지 않은 단일 사용자 권한 확인**  1) IAM 그룹에 포함되지 않은 단일 사용자 계정 전체 권한 확인    2) Root 계정 사용자 권한 확인    3) IAM 사용자 전체 권한 여부 확인 | | | |
| **조치**  **내용** | AdministratorAccess는 접근에 대한 모든 권한을 부여할 수 있기 때문에 해당 권한이 적용되면 범위 외의 서비스에도 접근이 가능하므로 취약하다.  따라서 AdministratorAccess권한을 최고관리자 및 관리자 역할을 부여받은 인원 외 타 인원은 전체 권한에 대해 접근이 불가능하도록 하여야 한다. | | |

**2) IAM 사용자 계정 단일화 관리**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 계정관리 | **중요도** | **상** |
| **점검 날짜** | 2022년 6월 7일 | **결과** | **양호** |
| **점검 대상** | AWS Identity and Access Management (IAM) | | |
| **항목명** | IAM 사용자 계정 단일화 관리 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | 모든 AWS 리소스는 AWS 계정의 소유이고, 리소스 생성 또는 액세스 권한은 권한 정책에 따라 결정됩니다. 계정 관리자는 IAM 자격 증명(즉 사용자, 그룹, 역할)에 권한 정책을 연결할 수 있으며 적절한 권한을 통한 서비스 관리가 이루어져야 합니다.  **1) 적절한 IAM 계정 사용**  AWS IAM 계정 생성 시 1인 1계정 발급을 원칙으로 하며, 1명의 담당자가 다수의 IAM 계정을 보유하는 것을 지양해야 합니다. Cloud 서비스 리소스 사용이 필요할 경우 내부 정책을 기준으로 목적에 맞게 권한이 부여되어야 합니다.  **※ Cloud 서비스 별 IAM 계정 생성 및 관리 금지** | | |
| **진단 기준** | **양호 기준**  단일 사용자가 다수의 IAM 계정을 사용하지 않을 경우  **취약 기준**  단일 사용자가 다수의 IAM 계정을 사용할 경우 | | |
| **점검 내용** | **가. 적절한 IAM 계정 사용**  1) AWS IAM 계정 1인 1계정 사용 확인  - 인터뷰를 통해 1인 1계정으로 사용자마다 ‘sk101-00X’ 사용 확인 | | | |

**3) IAM 사용자 계정 식별 관리**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 계정관리 | **중요도** | **중** |
| **점검 날짜** | 2022년 6월 7일 | **결과** | **양호**  **(조치)** |
| **점검 대상** | AWS Identity and Access Management (IAM) | | |
| **항목명** | 사용자 계정 식별 관리 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | IAM 사용자 계정에는 태그를 추가할 수 있으며, 해당 태그 설정은 사용자를 표현하는 정보 및 직책의 내용을 포함할 수 있습니다. 이러한 태그 사용은 IAM 사용자에 대한 액세스 구성, 추정 또는 제어가 가능합니다. | | |
| **진단 기준** | **양호 기준**  사용자 정보(이름, 이메일, 부서 등)가 IAM 사용자 태그에 설정되어 있을 경우  **취약 기준**  사용자 정보(이름, 이메일, 부서 등)가 IAM 사용자 태그에 설정되어 있지 않을 경우 | | |
| **점검 내용** | **가. IAM 사용자 정보 태그 확인**  1) AWS 주요 서비스 중 "IAM" 클릭    2) 사용자 계정 태그 확인 및 편집  - 현재 사용자 계정의 태그는 ‘name’ 하나만 존재하므로 정확한 식별 불가 | | |
| **조치 내용** | **가. IAM 사용자 정보 태그 변경**  1) IAM 사용자 태그 추가  - id, email 태그를 추가하여 IAM계정 식별이 가능하도록 저장    2) IAM 사용자 태그 확인 | | |
| **조치 내용 설명** | 사용자 정보 중 ‘이름’만 IAM 사용자 태그에 설정되어 있어 정확한 식별이 불가능 하다.  따라서 더 많은 사용자 정보를 IAM 사용자 태그에 추가하여 보다 정확한 식별이 가능하도록 설정해야 한다. | | |

**4) Key Pair 접근 관리**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 계정관리 | **중요도** | **상** |
| **점검 날짜** | 2022년 6월 7일 | **결과** | **양호** |
| **점검 대상** | Amazon EC2 | | |
| **항목명** | Key Pair 접근 관리 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | EC2는 키(Key)를 이용한 암호화 기법을 제공합니다. 해당 기법은 퍼블릭/프라이빗 키를 통해 각각 데이터의 암호화 및 해독을 하는 방식으로 여기에 사용되는 키를 ‘키페어’라고 하며, 해당 암호화 기법을 사용할 시 EC2의 보안성을 향상시킬 수 있으므로 EC2 인스턴스 생성 시 Key Pair 등록을 권장합니다.  또한, Amazon EC2에 사용되는 키는 ‘2048비트 SSH-2 RSA 키’이며, 키 페어는 리전 당 최대 5천 개까지 보유할 수 있습니다. | | |
| **진단 기준** | **양호 기준**  Key Pair(PEM)를 통해 EC2 인스턴스에 접근할 경우  **취약 기준**  Key Pair(PEM)가 아닌 일반 패스워드로 EC2 인스턴스에 접근할 경우 | | |
| **점검 내용** | **가. 키 페어 확인**  1) 키 페어 확인    **나. 인스턴스에 비밀번호 없이 접속**  1) 인스턴스에 key pair 등록 확인    2) key pair(.PEM)을 이용해 인스턴스 접속 | | |

**5) Key Pair 보관 관리**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 계정관리 | **중요도** | **상** |
| **점검 날짜** | 2022년 6월 7일 | **결과** | **양호** |
| **점검 대상** | Amazon EC2 | | |
| **항목명** | Key Pair 보관 관리 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | EC2는 키(Key)를 이용한 암호화 기법을 제공합니다. 해당 기법은 퍼블릭/프라이빗 키를 통해 각각 데이터의 암호화 및 해독을 하는 방식으로 여기에 사용되는 키를 ‘키페어’ 라고 하며, 해당 암호화 기법을 사용할 시 EC2의 보안성을 향상시킬 수 있으므로 EC2 인스턴스 생성 시 Key Pair 등록을 권장합니다.  또한, Amazon EC2에 사용되는 키는 ‘2048비트 SSH-2 RSA 키’ 이며, 키 페어는 리전 당 최대 5천 개까지 보유할 수 있습니다.  **※ Key Pair는 타 사용자가 확인이 가능한 공개된 위치에 보관하게 될 경우 EC2 Instance에 무단으로 접근이 가능해지므로 비인가자가 쉽게 유추 및 접근이 불가능한 장소에 보관해야 합니다.** | | |
| **진단 기준** | **양호 기준**  Key Pair(PEM) File의 보관 위치가 쉽게 유추할 수 없는 공간에 보관되어 있을 경우  **취약 기준**  Key Pair(PEM) File의 보관 위치가 다수 접근이 가능한 공용공간(Public S3, EC2 “root(/)” 디렉토리 등)에 보관되어 있을 경우 | | |
| **점검 내용** | **가. S3 버킷 내 키 페어 관리하기**  1) 버킷 접근    3) 버킷에 Key Pair 업로드    4) 버킷에서 Key Pair 확인 | | |
| **조치 내용** | **가. 버킷 ACL 활성화**  1) 버킷 ACL을 활성화하여 다수 접근이 불가능한 공용 공간 확보 | | |

**6) MFA (Multi-Factor Authentication) 설정**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 계정관리 | **중요도** | **중** |
| **점검 날짜** | 2022년 6월 7일 | **결과** | **양호** |
| **점검 대상** | AWS Identity and Access Management (IAM) | | |
| **항목명** | MFA (Multi-Factor Authentication) 설정 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | AWS Multi-Factor Authentication(MFA)은 사용자 이름과 암호 외에 보안을 한층 더 강화할 수 있는 방법으로 MFA를 활성화하면 사용자가 AWS 웹 사이트에 로그인할 때 사용자 이름과 암호 뿐 아니라 AWS MFA 디바이스의 인증 응답을 입력하라는 메시지가 표시됩니다. 이러한 다중 요소를 통해 AWS 계정 설정 및 리소스에 대한 보안을 높일 수 있습니다.  **※ Key Pair는 타 사용자가 확인이 가능한 공개된 위치에 보관하게 될 경우 EC2 Instance에 무단으로 접근이 가능해지므로 비인가자가 쉽게 유추 및 접근이 불가능한 장소에 보관해야 합니다.** | | |
| **진단 기준** | **양호 기준**  AWS 계정 및 IAM 사용자 계정 로그인 시 MFA가 활성 되어 있을 경우  **취약 기준**  AWS 계정 및 IAM 사용자 계정 로그인 시 MFA가 비활성화 되어 있을 경우 | | |
| **점검**  **내용** | **가. MFA 인증 설정 및 확인**  1) IAM 메인 → 우측상단 계정 → 내 보안 자격 증명 → 멀티 팩터 인증  - 할당된 MFA 디바이스가 없음으로 보안에서 취약 | | |
| **조치 내용** | **가. MFA 인증 설정 및 확인**  1) IAM 메인 → 우측상단 계정 → 내 보안 자격 증명 → 멀티 팩터 인증 → MFA 디바이스 할당    2) MFA 디바이스 관리 → 가상 MFA 디바이스 선택    3) Google OTP 어플 설치 → ‘+’ 버튼 → 바코드 스캔 → 나타난 QR코드를 어플에서 스캔    4) 멀티 팩터 인증 | | |

**7) AWS 계정 패스워드 정책 관리**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 계정관리 | **중요도** | **중** |
| **점검 날짜** | 2022년 6월 7일 | **결과** | **양호**  **(조치)** |
| **점검 대상** | AWS Identity and Access Management (IAM) | | |
| **항목명** | AWS 계정 패스워드 정책 관리 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | AWS Root Account 계정 및 IAM 사용자 계정의 암호 설정 시 일반적으로 유추하기 쉬운 암호를 설정하는 경우 비인가 된 사용자가 해당 계정을 획득하여 접근 가능성이 존재합니다.   |  | | --- | | **<패스워드 설정 기준>** | | 1) 패스워드는 아래의 4가지 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성  \* 영문 대문자(26개), 영문 소문자(26개), 숫자(10개), 특수문자(32개) |  |  | | --- | | **<패스워드는 비인가자에 의한 추측이 어렵도록 다음의 사항을 반영하여 설계해야 함>** | | 1) Null 패스워드 사용 금지  2) 문자 또는 숫자만으로 구성 금지  3) 사용자 ID와 동일한 패스워드 금지  4) 연속적인 문자 및 숫자 사용 금지  5) 주기성 패스워드 사용 금지  6) 전화번호, 생일, 계정 명, hostname과 같이 추측하기 쉬운 패스워드 사용 금지 |  |  | | --- | | 1) 패스워드 최소 길이  패스워드 추측 공격을 피하기 위하여 패스워드 최소 길이가 설정되어 있는지 점검함  패스워드 최소 길이가 설정되어 있지 않거나 짧게 설정되어 있을 경우 취약한 패스워드를 사용함으로 인해 악의적인 사용자가 패스워드를 쉽게 유추할 수 있음  2) 패스워드 최대 사용기간  패스워드가 임의의 경로를 통해 유출되었을 때, 임의로 접속한 사용자가 언제든 다시  접속할 수 있는 환경을 방지하기 위해 패스워드 날짜 제한을 점검함  3) 패스워드 최소 사용기간  패스워드가 임의의 경로를 통해 유출되었을 때, 임의로 접속한 사용자가 언제든 다시  접속할 수 있는 환경을 방지하기 위해 패스워드 날짜 제한을 점검함  4) 이전 패스워드 기억  이전에 사용하였던 패스워드를 기억하여 패스워드 변경 시 기존에 사용하였던 패스워드 재사용 금지  - 패스워드 길이는 8자 이상 설정하는 것을 권고  - 패스워드 최대 사용 기간을 60일 이하로 설정할 것을 권고  - 패스워드 최소 사용 기간을 1일 이상으로 설정할 것을 권고 | | | |
| **진단 기준** | **양호 기준**  Admin Console 및 IAM 계정의 패스워드가 복잡성 기준을 준수하였을 경우  **취약 기준**  Admin Console 및 IAM 계정의 패스워드가 복잡성 기준을 준수하지 않을 경우 | | |
| **점검 내용** | **가. IAM 계정 비밀번호 정책 확인**  1) 계정 설정 확인 | | |
| **조치**  **내용** | **가. 암호 정책 설정**  1) 복잡성 기준을 준수하는 암호 정책을 설정 | | |
| **조치 내용 설명** | IAM 계정에 패스워드 복잡성 기준을 준수하고 있지 않아 보안이 취약하다.  IAM 계정의 암호 정책을 다음과 같이 변경한다. 1개 이상의 라틴 알파벳 소문자(a-Z)필수, 1개 이상의 숫자 필수, 영어, 숫자를 제외한 문자 1개 이상 필수, 암호 재사용 제한을 정책으로 설정하여 복잡성 기준을 준수할 수 있도록 조치해야 한다. | | |

## **권한관리**

**1) 인스턴스 보안 정책 관리**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 권한관리 | **중요도** | **상** |
| **점검 날짜** | 2022년 6월 7일 | **결과** | **취약** |
| **점검 대상** | AWS Identity and Access Management (IAM) | | |
| **항목명** | 인스턴스 보안 정책 관리 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | 모든 AWS 리소스는 AWS 계정의 소유이고, 리소스 생성 또는 액세스 권한은 권한 정책에 따라 결정됩니다. 계정 관리자는 IAM 자격 증명(즉, 사용자, 그룹, 역할)에 권한 정책을 연결할 수 있으며 적절한 권한을 통한 서비스 관리가 이루어져야 합니다.  **1) 인스턴스 관리형 정책**  - 인스턴스 관리형 정책은 AWS에서 생성 및 관리하는 정책으로 여러 가지 직무 및 일반 사용 사례에서 권한을 제공할 목적으로 설계된 정책입니다.  ※ 인스턴스 서비스 내 FULL ACCESS 등과 같이 중요도가 높은 AWS 관리형 정책은 EC2 서비스 관리/운영자 및 관련 담당자 외에 다른 IAM 계정에 아래와 같은 권한 할당이 되지 않도록 해야 ㅕ합니다.  **2) 인스턴스 역할별 권한 관리 (예시)**   |  |  | | --- | --- | | **역할** | **관리형 정책명** | | AWS Root 관리자 | \* ALL FULL ACCESS \*, AdministratorAccess | | Infra 운영/관리자 및 담당자 | Amazon EC2 / ECR / ECS \*FullAccess\* | | Application 운영/관리자 및 담당자 | Amazon EC2 / ECR / ECS \*ReadOnlyAccess\* /  \*Poweruser\* / \*Role\* / CloudWatchActionsEC2Access | | 개발 관리자 및 담당자 | Amazon EC2 / ECR / ECS \*ReadOnlyAccess\* /  \*Poweruser\* / \*Role\* / CloudWatchActionsEC2Access | | 재무 / 비용 관리자 및 담당자 | Amazon EC2 / ECR / ECS 중요도 “하” Access |   **3) IAM 관리형 정책 권한 관리 List (예시)**   |  |  |  |  | | --- | --- | --- | --- | | **역할** | **계정 관리**  **(그룹 및 계정명)** | **AWS 관리형 정책** | **취약**  **유/무** | | AWS Root 관리자 | Ex) EC2\_Admin  (admin\_accout) | Ex) EC2\_Admin  (AmazonEC2FullAcces) | N/A | | Infra 운영/관리자 및 담당자 |  |  | N/A | | Application 운영/관리자 및 담당자 |  |  | N/A | | 개발 관리자 및 담당자 |  |  | N/A | | 재무 / 비용 관리자 및 담당자 |  |  | N/A | | | |
| **진단 기준** | **양호 기준**  인스턴스 서비스 IAM 사용 권한이 각각 서비스 역할에 맞게 설정되어 있을 경우  **취약 기준**  인스턴스 서비스 IAM 사용 권한이 각각 서비스 역할에 맞지 않게 설정되어 있을 경우 | | |
| **점검 내용** | **가. IAM 관리자/운영자 권한 설정**  1) 그룹에서 연결한 권한이 서비스 역할에 맞게 설정되어 있는지 확인 | | |
| **조치 내용 설명** | 시스템 운영 시 관리적 측면에서 역할에 맞게 IAM 관리형 정책 권한 List를 생성하여 권한 관리를 해야 한다. | | |

**2) RDS 보안 정책 관리**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 권한관리 | **중요도** | **중** |
| **점검 날짜** | 2022년 6월 7일 | **결과** | **취약** |
| **점검 대상** | AWS Identity and Access Management (IAM) | | |
| **항목명** | RDS 보안 정책 관리 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | 모든 AWS 리소스는 AWS 계정의 소유이고, 리소스 생성 또는 액세스 권한은 권한 정책에 따라 결정됩니다. 계정 관리자는 IAM 자격 증명(즉, 사용자, 그룹, 역할)에 권한 정책을 연결할 수 있으며 적절한 권한을 통한 서비스 관리가 이루어져야 합니다.  **1) RDS 관리형 정책**  - RDS 관리형 정책은 AWS에서 생성 및 관리하는 정책으로 여러 가지 직무 및 일반 사용 사례에서 권한을 제공할 목적으로 설계된 정책입니다.  ※ RDS 서비스 내 “AmazonRDSFullAccess” 등과 같이 중요도가 높은 AWS 관리형 정책은 RDS 서비스 관리/운영자 및 관련 담당자 외에 다른 IAM 계정에 아래와 같은 권한 할당이 되지 않도록 해야합니다.  **2) RDS 역할별 권한 관리 (예시)**   |  |  | | --- | --- | | 역할 | 관리형 정책명 | | AWS Root 관리자 | \* ALL FULL ACCESS \*, AdministratorAccess | | Infra 운영/관리자 및 담당자 | Amazon RDS \*FullAccess\* | | Application 운영/관리자 및 담당자 | Amazon RDS / AmazonRDSDataFullAccess /  \*ReadOnlyAccess\* / \*Role\* / 중요도 “하” Access | | 개발 관리자 및 담당자 | Amazon RDS / AmazonRDSDataFullAccess /  \*ReadOnlyAccess\* / \*Role\* / 중요도 “하” Access | | 재무 / 비용 관리자 및 담당자 | Amazon RDS 중요도 “하” Access |   **3) IAM 관리형 정책 권한 관리 List (예시)**   |  |  |  |  | | --- | --- | --- | --- | | 역할 | **계정 관리**  (그룹 및 계정명) | **AWS 관리형 정책** | **취약**  **유/무** | | AWS Root 관리자 | Ex) RDS\_Admin  (admin\_accout) | Ex) RDS\_Admin  (AmazonRDSFullAccess) | N/A | | Infra 운영/관리자 및 담당자 |  |  | N/A | | Application 운영/관리자 및 담당자 |  |  | N/A | | 개발 관리자 및 담당자 |  |  | N/A | | 재무 / 비용 관리자 및 담당자 |  |  | N/A | | | |
| **진단 기준** | **양호 기준**  RDS 서비스 IAM 사용 권한이 각각 서비스 역할에 맞게 설정되어 있을 경우  **취약 기준**  RDS 서비스 IAM 사용 권한이 각각 서비스 역할에 맞지 않게 설정되어 있을 경우 | | |
| **점검 내용** | **가. RDS 관리자/운영자 권한 설정**  1) RDS 서비스 IAM 사용 권한이 역할에 맞게 설정되어 있는지 확인 | | |
| **조치 내용 설명** | 시스템 운영 시 관리적 측면에서 역할에 맞게 IAM 관리형 정책 권한 List를 생성하여 권한 관리를 해야 한다. | | |

**3) S3 보안 정책 관리**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 권한관리 | **중요도** | **상** |
| **점검 날짜** | 2022년 6월 7일 | **결과** | **취약** |
| **점검 대상** | AWS Identity and Access Management (IAM) | | |
| **항목명** | S3 보안 정책 관리 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | 모든 AWS 리소스는 AWS 계정의 소유이고, 리소스 생성 또는 액세스 권한은 권한 정책에 따라 결정됩니다. 계정 관리자는 IAM 자격 증명(즉, 사용자, 그룹, 역할)에 권한 정책을 연결할 수 있으며 적절한 권한을 통한 서비스 관리가 이루어져야 합니다.  **1) AWS 관리형 정책 (S3)**  - AWS 관리형 정책은 AWS에서 생성 및 관리하는 정책으로 여러 가지 직무 및 일반 사용 사례에서 권한을 제공할 목적으로 설계된 정책입니다.  ※ S3 서비스 내 FULL ACCESS 등과 같이 중요도가 높은 AWS 관리형 정책은 S3 서비스 관리/운영자 및 관련 담당자 외에 다른 IAM 계정에 아래와 같은 권한 할당이 되지 않도록 해야 합니다.  **2) RDS 역할별 권한 관리 (예시)**   |  |  | | --- | --- | | 역할 | 관리형 정책명 | | AWS Root 관리자 | \* ALL FULL ACCESS \*, AdministratorAccess | | Infra 운영/관리자 및 담당자 | AmazonS3FullAccess | | Application 운영/관리자 및 담당자 | Amazon S3 / AmazonDMSRedshiftS3Role /  AmazonS3ReadOnlyAccess | | 개발 관리자 및 담당자 | Amazon S3 / AmazonDMSRedshiftS3Role /  AmazonS3ReadOnlyAccess | | 재무 / 비용 관리자 및 담당자 | Amazon S3 / AmazonS3ReadOnlyAccess /  QuickSightAccessForS3StorageManagement  AnalyticsReadOnly |   **3) IAM 관리형 정책 권한 관리 List (예시)**   |  |  |  |  | | --- | --- | --- | --- | | 역할 | **계정 관리**  (그룹 및 계정명) | **AWS 관리형 정책** | **취약**  **유/무** | | AWS Root 관리자 | Ex) S3\_Admin  (admin\_accout) | Ex) S3\_Admin  (CustomS3FullAccess) | N/A | | Infra 운영/관리자 및 담당자 |  |  | N/A | | Application 운영/관리자 및 담당자 |  |  | N/A | | 개발 관리자 및 담당자 |  |  | N/A | | 재무 / 비용 관리자 및 담당자 |  |  | N/A | | | |
| **진단 기준** | **양호 기준**  S3 서비스 IAM 사용 권한이 각각 서비스 역할에 맞게 설정되어 있을 경우  **취약 기준**  S3 서비스 IAM 사용 권한이 각각 서비스 역할에 맞게 설정되어 있지 않을 경우 | | |
| **점검 내용** | **가. S3 관리자/운영자 권한 설정**  1) S3 서비스 IAM 사용 권한이 역할에 맞게 설정되어 있는지 확인 | | |
| **조치 내용 설명** | 시스템 운영 시 관리적 측면에서 역할에 맞게 IAM 관리형 정책 권한 List를 생성하여 권한 관리를 해야 한다. | | |

**4) Access Key 정책 관리**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 계정관리 | **중요도** | **중** |
| **점검 날짜** | 2022년 6월 7일 | **결과** | **양호** |
| **점검 대상** | AWS Identity and Access Management (IAM) | | |
| **항목명** | Access Key 정책 관리 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | Access Key는 AWS의 CLI 도구나 API를 사용할 때 필요한 인증수단으로 생성 사용자에 대한 결제 정보를 포함한 모든 AWS 서비스의 전체 리소스에 대한 권한을 갖고 있으므로 유출 시 심각한 피해가 발생할 가능성이 높기에 AWS Root Account에 대한 Access Key 삭제를 권장합니다.  **※ Access Key 관리 주기**  Key 수명(60일 이내), 비밀번호 수명(60일 이내), 마지막 활동(30일 이내) | | |
| **진단 기준** | **양호 기준**  AWS Root 및 IAM 사용자 계정에 Access Key가 존재하지 않을 경우  **취약 기준**  AWS Root 및 IAM 사용자 계정에 Access Key가 존재할 경우 | | |
| **점검 내용** | **가. AWS IAM User Access Key 확인**  1) Access Key 확인  - Access Key가 존재하지 않음 | | |

**5) Admin Console 관리자 정책 관리**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 계정관리 | **중요도** | **중** |
| **점검 날짜** | 2022년 6월 7일 | **결과** | **양호** |
| **점검 대상** | AWS Identity and Access Management (IAM) | | |
| **항목명** | Admin Console 관리자 정책 관리 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | AWS Cloud 사용을 위해 처음 발급한 계정은 IAM 사용자 계정과 달리 모든 서비스에 접근할 수 있는 최고 관리자 계정입니다. Cloud 서비스 특성 상 인터넷 연결이 가능한 망에서 계정정보를 입력하여 WEB Console에 접근하게 됩니다. 이는 최고 권한을 보유하고 있는 관리자 계정이 아닌 권한이 조정된 IAM 사용자 계정을 기본으로 사용해야 보다 안전한 접근이 이뤄질 수 있습니다. | | |
| **진단 기준** | **양호 기준**  AWS 회원가입 시 처음 발급한 Admin 계정을 서비스 용도로 사용하지 않을 경우  **취약 기준**  AWS 회원가입 시 처음 발급한 Admin 계정을 서비스 용도로 사용할 경우 | | |
| **점검 내용** | **가. Admin 계정 외 서비스 용도 IAM 계정 확인**  1) IAM 사용자 확인  - 서비스 용도인 IAM 계정 (sk101-00X 계정) 확인    2) IAM 사용자 권한 확인  - ‘AdministratorAccess’ 정책을 부여하여 IAM계정으로 서비스 제공 | | |

**6) IAM 사용자 및 그룹 정책 관리**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 계정관리 | **중요도** | **중** |
| **점검 날짜** | 2022년 6월 7일 | **결과** | **양호** |
| **점검 대상** | AWS Identity and Access Management (IAM) | | |
| **항목명** | IAM 사용자 및 그룹 정책 관리 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | AWS IAM(Identity and Access Management)은 AWS 리소스에 대한 접근 및 사용권한을 부여하여 관리하는 자격 증명 기반 정책 서비스로 무분별한 IAM 계정 생성 및 유추하기 쉬운 계정명(test, user, adm, abcd 등) 사용 시 보안상 위험을 발생시킬 수 있으므로 계정 생성 시 사용자 식별 및 유추하기가 쉽지 않은 계정명을 사용해야 합니다. | | |
| **진단 기준** | **양호 기준**  IAM 그룹에 포함된 사용자 계정 중 불필요한 계정이 존재하지 않을 경우  **취약 기준**  IAM 그룹에 포함된 사용자 계정 중 불필요한 계정이 존재할 경우 | | |
| **점검 내용** | 가. 그룹에 따라 불필요한 계정 확인  1) 사용자 그룹(skhealth\_IT)에 불필요한 계정 확인  - 그룹의 사용자에 그룹의 실질적인 사용자인 계정(sk101-005)만 존재 | | |

## **데이터관리**

**1) 인스턴스 암호화 설정**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 데이터관리 | **중요도** | **중** |
| **점검 날짜** | 2022년 6월 8일 | **결과** | **양호** |
| **점검 대상** | Amazon EC2 | | |
| **항목명** | 인스턴스 암호화 설정 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | EBS는 EC2 인스턴스 생성 및 이용 시 사용되는 블록 형태의 스토리지 볼륨이며 파일시스템 생성 및 블록 디바이스 사용 등을 할 수 있습니다. 또한 EBS는 AES-256 알고리즘을 사용하여 볼륨 암호화를 지원하며 데이터 및 애플리케이션에 대한 다양한 정보를 안전하게 저장할 수 있게 해줍니다. | | |
| **진단 기준** | **양호 기준**  EC2 인스턴스 스토리지 내 블록 디바이스 암호화가 활성화되어 있을 경우  **취약 기준**  EC2 인스턴스 스토리지 내 블록 디바이스 암호화가 비활성화되어 있을 경우 | | |
| **점검 내용** | **가. EC2 스토리지 암호화 확인**  1) 인스턴스 스토리지 암호화 확인 | | |

**2) RDS 암호화 설정**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 데이터관리 | **중요도** | **중** |
| **점검 날짜** | 2022년 6월 8일 | **결과** | **양호** |
| **점검 대상** | Amazon RDS | | |
| **항목명** | RDS 암호화 설정 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | RDS는 데이터 보호를 위해 DB 인스턴스에서 암호화 옵션 기능을 제공하며 암호화 시 AES-256 암호화 알고리즘을 이용하여 DB 인스턴스의 모든 로그, 백업 및 스냅샷 암호화가 가능합니다. | | |
| **진단 기준** | **양호 기준**  RDS 스토리지 암호화가 활성화되어 있을 경우  **취약 기준**  RDS 스토리지 암호화가 비활성화되어 있을 경우 | | |
| **점검 내용** | **가. RDS 암호화 확인**  1) RDS 확인    2) RDS 스토리지 암호화 확인 | | |

**3) S3 암호화 설정**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 데이터관리 | **중요도** | **중** |
| **점검 날짜** | 2022년 6월 8일 | **결과** | **양호** |
| **점검 대상** | Amazon S3 | | |
| **항목명** | S3 암호화 설정 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | 버킷 기본 암호화 설정은 S3 버킷에 저장되는 모든 객체를 암호화되도록 하는 설정이며 Amazon S3 관리형 키(SSE-S3) 또는 AWS KMS 관리형 키(SSE-KMS)로 서버 측 암호화를 사용하여 객체를 암호화합니다.  **※ S3 버킷 신규 생성 시 기본 암호화 (SSE-S3, SSE-KMS)를 설정할 수 있으며, 버킷에 기본 암호화가 적용된 상태에서 객체가 저장될 경우 하위 객체까지 자동으로 암호화 설정이 가능함** | | |
| **진단 기준** | **양호 기준**  Amazon S3 키(SSE-S3)로 서버 측 암호화 사용 또는 SSE-KMS로 서버 측 암호화가  설정되어 있을 경우  **취약 기준**  Amazon S3 키(SSE-S3)로 서버 측 암호화 사용 또는 SSE-KMS 로 서버 측 암호화가  설정되어 있지 않을 경우 | | |
| **점검 내용** | **가. S3 암호화 확인**  1) S3 서버측 암호화 확인 | | |

## **가상 리소스 관리**

**1) 보안그룹 인/아웃바운드 ANY 설정 관리**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 가상 리소스 관리 | **중요도** | **중** |
| **점검 날짜** | 2022년 6월 8일 | **결과** | **양호** |
| **점검 대상** | Amazon EC2 | | |
| **항목명** | 보안그룹 인/아웃 바운드 ANY 설정 관리 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | VPC에서의 Security Group은 EC2 인스턴스에 대한 인/아웃 바운드 트래픽을 제어하는 가상 방화벽 역할을 합니다. VPC에서 EC2 인스턴스를 시작할 때 최대 5개의 Security Group에 인스턴스를 할당할 수 있습니다. Security Group은 서브넷 수준이 아니라 인스턴스 수준에서 작동하므로 VPC에 있는 서브넷의 각 인스턴스를 서로 다른 Security Group 세트에 할당할 수 있습니다.  보안그룹은 인/아웃 바운드의 규칙 편집을 통해 특정 소스(출발지)에서의 통신이 가능하도록 유형(네트워크 프로토콜) 및 단일/범위 Port를 설정할 수 있습니다. | | |
| **진단 기준** | **양호 기준**  : EC2 인스턴스에 대한 인/아웃 바운드의 Port가 Any로 허용되어 있지 않을 경우  **취약 기준**  : EC2 인스턴스에 대한 인/아웃 바운드의 Port가 Any로 허용되어 있을 경우 | | |
| **점검 내용** | **가. 보안그룹 인/아웃 바운드 확인**  1) 인스턴스 보안그룹 인/아웃 바운드 규칙의 포트 범위 확인  - 포트 범위 Any가 아닌 22번 확인 | | |

**2) 보안그룹 인/아웃 바운드 불필요 정책 관리**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 가상 리소스 관리 | **중요도** | **중** |
| **점검 날짜** | 2022년 6월 8일 | **결과** | **양호**  **(조치)** |
| **점검 대상** | Amazon EC2 | | |
| **항목명** | 보안그룹 인/아웃 바운드 불필요 정책 관리 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | VPC에서의 Security Group은 EC2 인스턴스에 대한 인/아웃 바운드 트래픽을 제어하는 가상 방화벽 역할을 합니다. VPC에서 EC2 인스턴스를 시작할 때 최대 5개의 Security Group에 인스턴스를 할당할 수 있습니다. Security Group은 서브넷 수준이 아니라 인스턴스 수준에서 작동하므로 VPC에 있는 서브넷의 각 인스턴스를 서로 다른 Security Group 세트에 할당할 수 있습니다.  보안그룹은 인/아웃 바운드의 규칙 편집을 통해 특정 소스(출발지)에서의 통신이 가능하도록 유형(네트워크 프로토콜) 및 단일/범위 정책을 설정할 수 있습니다. | | |
| **진단 기준** | **양호 기준**  EC2 인스턴스에 대한 인/아웃 바운드 소스와 목적지의 불필요한 정책이 허용되어 있지 않을 경우  **취약 기준**  EC2 인스턴스에 대한 인/아웃 바운드 소스와 목적지의 불필요한 정책이 허용되어 있을 경우 | | |
| **점검 내용** | **가. 보안그룹 인/아웃 바운드 소스 정책 확인**  1) 보안그룹 인바운드 규칙 내 소스 확인  - 불필요한 정책이 허용되어 있음    2) 보안그룹 아웃바운드 규칙 내 대상 확인  - 불필요한 정책이 허용되어 있음 | | |
| **조치 내용** | **가. 보안그룹 인/아웃 바운드 소스 정책 변경**  1) 관리자IP로 인바운드 규칙 편집    2) 관리자IP로 아웃바운드 규칙 편집 | | |
| **조치 내용 설명** | 생성한 인스턴스 인/아웃 바운드 규칙의 소스/대상이 0.0.0.0/0으로 설정되어 있어 불필요한 접근이 허용되어 있다. 이처럼 불필요한 정책이 허용되어 있어 취약하다.  이를 방지하기 위하여 소스/대상을 관리자IP로 설정하여 불필요한 접근이 불가능하도록 한다. | | |

**3) ACL 네트워크 인/아웃 바운드 트래픽 정책 관리**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 가상 리소스 관리 | **중요도** | **상** |
| **점검 날짜** | 2022년 6월 8일 | **결과** | **양호** |
| **점검 대상** | Amazon VPC | | |
| **항목명** | ACL 네트워크 인/아웃 바운드 트래픽 정책 관리 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | ACL(Access Control List)은 1개 이상의 서브넷 내부와 외부의 트래픽을 제어하기 위한 방화벽 역할을 하는 VPC의 선택적 보안 계층입니다. 보안 그룹과 비슷한 규칙으로 네트워크 ACL을 설정하여 VPC에 보안 계층을 더 추가할 수 있습니다. ACL은 VPC 서브넷 계층에서 동작하며 VPC 서브넷과는 1:1로 대응합니다. 정책의 방식은 허용(Allow) 및 거부(deny) 정책(WhiteList or BlackList) 기능으로 Stateless 방식으로 사용이 됩니다. VPC에 있는 각 서브넷을 네트워크 ACL과 연결하여 사용할 수 있으며, 서브넷을 네트워크 ACL에 명시적으로 연결하지 않을 경우, 서브넷은 기본 네트워크 ACL에 자동적으로 연결합니다. (단, 하나의 네트워크 ACL은 다수의 서브넷과 연결할 수 있지만 하나의 서브넷은 하나의 ACL에만 연결할 수 있음)  (\*) 기본 네트워크 ACL 규칙 기본 네트워크 ACL은 연결된 서브넷을 드나드는 트래픽 흐름을 모두 허용하도록 구성되어 있습니다. 각 네트워크 ACL에는 규칙 번호가 별표로 되어 있는 규칙도 포함되어 있습니다. 이 규칙은 패킷이 번호가 매겨진 다른 어떤 규칙과도 일치하지 않을 경우에는 거부되도록 되어 있습니다. 이 규칙을 수정하거나 제거할 수 없습니다.   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | **Inbound** | | | | | | | **규칙#** | **유형** | **프로토콜** | **포트** | **소스** | **허용/거부** | | **100** | **모든 IPv4 트래픽** | **모두** | **모두** | **0.0.0.0/0** | **허용** | | **\*** | **모든 IPv4 트래픽** | **모두** | **모두** | **0.0.0.0/0** | **거부** |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | **Outbound** | | | | | | | **규칙#** | **유형** | **프로토콜** | **포트** | **소스** | **허용/거부** | | **100** | **모든 IPv4 트래픽** | **모두** | **모두** | **0.0.0.0/0** | **허용** | | **\*** | **모든 IPv4 트래픽** | **모두** | **모두** | **0.0.0.0/0** | **거부** | | | |
| **진단 기준** | **양호 기준**  인/아웃 바운드에 대한 모든 트래픽이 허용되어 있지 않을 경우  **취약 기준**  인/아웃 바운드에 대한 모든 트래픽이 허용되어 있을 경우 | | |
| **점검 내용** | **가. 네트워크 ACL 정책 확인**  1) 네트워크 ACL 인바운드 규칙 확인  - 네트워크 ACL 인바운드 규칙에 모든 트래픽이 허용되어 있지 않음    2) 네트워크 ACL 아웃바운드 규칙 확인  - 네트워크 ACL 아웃바운드 규칙에 모든 트래픽이 허용되어 있지 않음 | | |

**4) 라우팅 테이블 정책 관리**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 가상 리소스 관리 | **중요도** | **중** |
| **점검 날짜** | 2022년 6월 8일 | **결과** | **취약** |
| **점검 대상** | Amazon VPC | | |
| **항목명** | 라우팅 테이블 정책 관리 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | 라우팅 테이블에는 네트워크 트래픽을 전달할 위치 결정 시 사용되는 규칙입니다. VPC의 각 서브넷을 라우팅 테이블에 연결해야 하며, 테이블에서는 서브넷에 대한 라우트를 제어하게 됩니다. 서브넷을 한 번에 하나의 라우팅 테이블에만 연결할 수 있지만 여러 서브넷을 동일한 라우팅 테이블에 연결하는 것은 가능합니다. VPC를 신규 생성하게 될 경우 기본 라우팅 테이블이 자동으로 생성됩니다. Amazon VPC 콘솔의 [라우팅 테이블] 페이지의 [Main] 열에서 [Yes]를 찾아 VPC에 대한 기본 라우팅 테이블을 볼 수 있습니다. 기본 라우팅 테이블은 다른 라우팅 테이블과 명시적으로 연결되지 않은 모든 서브넷에 대한 라우트를 제어합니다. 기본 라우팅 테이블에서 라우트를 추가 및 제거하고 수정할 수 있습니다. | | |
| **진단 기준** | **양호 기준**  목적지가 ANY 미설정 및 서비스 타겟별로 설정 또는 활성화되어 있을 경우  **취약 기준**  목적지가 ANY로 설정되어 있을 경우 | | |
| **점검 내용** | **가. 라우팅 테이블 확인**  1) 라우팅 테이블 대상 확인 | | |
| **조치 내용** | 외부 인터넷으로 연결하기 위한 인터넷 게이트웨이를 사용하기 때문에 대상을 ANY로 설정하여야 한다. 따라서 현재 조치를 취할 수 없는 취약점으로 판단된다. | | |

**5) NAT 게이트웨이 연결 관리**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 가상 리소스 관리 | **중요도** | **중** |
| **점검 날짜** | 2022년 6월 8일 | **결과** | **양호** |
| **점검 대상** | Amazon VPC | | |
| **항목명** | NAT 게이트웨이 연결 관리 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | NAT 게이트웨이는 NAT 디바이스를 사용하여 프라이빗 서브넷의 인스턴스를 인터넷(예: 소프트웨어 업데이트용) 또는 기타 AWS 서비스에 연결하는 한편, 인터넷에서 해당 인스턴스와의 연결을 시작하지 못하도록 할 수 있습니다. NAT 디바이스는 프라이빗 서브넷의 인스턴스에서 인터넷 또는 기타 AWS 서비스로 트래픽을 전달한 다음 인스턴스에 응답을 다시 보냅니다. 트래픽이 인터넷으로 이동하면 소스 IPv4 주소가 NAT 디바이스의 주소로 대체되고, 이와 마찬가지로 응답 트래픽이 해당 인스턴스로 이동하면 NAT 디바이스에서 주소를 해당 인스턴스의 프라이빗 IPv4 주소로 다시 변환합니다. | | |
| **진단 기준** | **양호 기준**  NAT 게이트웨이가 설정되어 있지 않거나 실 사용중인 Private 서브넷 인스턴스가 연결되어 있을 경우  **취약 기준**  NAT 게이트웨이를 사용할 경우 사용하지 않는 Private 서브넷 인스턴스가 연결되어 있을 경우 | | |
| **점검 내용** | **가. NAT 게이트웨이 설정 확인**  1) NAT 게이트웨이 사용 안함 | | |

**6) 인터넷 게이트웨이 연결 관리**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 가상 리소스 관리 | **중요도** | **하** |
| **점검 날짜** | 2022년 6월 8일 | **결과** | **양호** |
| **점검 대상** | Amazon VPC | | |
| **항목명** | 인터넷 게이트웨이 연결 관리 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | 인터넷 게이트웨이는 수평 확장되고 가용성이 높은 중복 VPC 구성 요소로, VPC의 인스턴스와 인터넷 간에 통신이 가능할 수 있게 해주는 기능이며 네트워크 트래픽 가용성 위험이나 대역폭 제약조건이 별도로 발생하진 않습니다. 인터넷 게이트웨이에는 인터넷 Route 가능 트래픽에 대한 VPC 라우팅 테이블에 대상을 제공하고, 퍼블릭 IPv4 주소가 할당된 인스턴스에 대해 NAT(네트워크 주소 변환)를 수행하는 두 가지 목적이 있으며, IPv4, IPv6 트래픽을 모두 지원합니다.  (\*) 기본 VPC와 기본이 아닌 VPC에 대한 인터넷 액세스   |  |  |  | | --- | --- | --- | | **구분** | **기존 VPC** | **기본이 아닌 VPC** | | 인터넷 게이트웨이 | 예 | VPC 마법사의 첫 번째 또는 두 번째 옵션을 사용하여 VPC를 생성한 경우. 그렇지 않은 경우, 인터넷 게이트웨이를 수동으로 생성하여 연결해야 합니다. | | IPv4 트래픽을 위한 인터넷 게이트웨이로 가는 경로가 있는 라우팅 테이블(0.0.0.0/0) | 예 | VPC 마법사의 첫 번째 또는 두 번째 옵션을 사용하여 VPC를 생성한 경우. 그렇지 않은 경우, 라우팅 테이블을 수동으로 생성하여 경로를 추가해야 합니다. | | IPv6 트래픽을 위한 인터넷 게이트웨이로 가는 경로가 있는 라우팅 테이블(::/0) | 아니요 | VPC 마법사의 첫 번째 또는 두 번째 옵션을 사용하여 VPC를 생성한 경우, 그리고 IPv6 CIDR 블록을 VPC와 연결하기 위해 옵션을 지정한 경우. 그렇지 않은 경우, 라우팅 테이블을 수동으로 생성하여 경로를 추가해야 합니다. | | 서브넷에서 시작된 인스턴스에 자동 할당된 퍼블릭 IPv4 주소 | 예 (기본 서브넷) | 아니요(기본이 아닌 서브넷) | | 서브넷에서 시작된 인스턴스에 자동 할당된 IPv6 주소 | 예 (기본 서브넷) | 아니요(기본이 아닌 서브넷) | | | |
| **진단 기준** | **양호 기준**  다수의 인터넷 게이트웨이 관리 시 연결된 VPC내 인스턴스가 존재할 경우  **취약 기준**  다수의 인터넷 게이트웨이 관리 시 연결된 VPC내 인스턴스가 존재하지 않을 경우 | | |
| **점검 내용** | 하나의 인터넷 게이트웨이만 사용하여 SK헬스의 점검 대상에 해당하지 않는다. | | |

**7) S3 버킷 접근 관리**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 가상 리소스 관리 | **중요도** | **중** |
| **점검 날짜** | 2022년 6월 8일 | **결과** | **양호** |
| **점검 대상** | Amazon S3 | | |
| **항목명** | S3 버킷 접근 관리 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | S3는 AWS 인터넷 클라우드 스토리지 서비스로 언제 어디서나 원하는 양의 데이터를 저장하고 검색할 수 있는 서비스이며, 데이터 저장/관리를 하기 위해 S3 서비스 내 버킷 사용이 필요하며 버킷 설정 시 접근 보안에 대해 다음과 같은 설정 / 관리 / 정책 등을 고려해야 합니다.  **1) 버킷 권한 부여**  -Public S3: 외부 사용의 관한 연결 통로를 제공하는 것이기 때문에 설정을 제한해야 합니다.  -Private S3: 접근 가능한 IAM 계정에 대한 권한이 설정되어 있어야 합니다.  **※ AWS Root Account로의 접근은 지양하며 가급적 IAM 계정을 통한 S3 접근을 권장함** | | |
| **진단 기준** | **양호 기준**  "Everyone" 그룹에 권한이 모두 미설정일 경우  **취약 기준**  "Everyone" 그룹에 " 객체 목록 생성", "객체 쓰기", "버킷 읽기 권한", "버킷 쓰기 권한"이 부여되어 있을 경우 | | |
| **점검 내용** | **가. S3 버킷 그룹 권한 확인**  1) S3 버킷 확인    2) S3 버킷 권한 확인 | | |

**8) RDS 리소스 액세스 권한 관리**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 가상 리소스 관리 | **중요도** | **중** |
| **점검 날짜** | 2022년 6월 8일 | **결과** | **양호** |
| **점검 대상** | AWS Identity and Access Management (IAM) | | |
| **항목명** | RDS 리소스 액세스 권한 관리 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | Amazon RDS에서의 기본 리소스는 DB 인스턴스입니다. Amazon RDS 기본 리소스와 함께 사용할 수 있는 다른 리소스 (예:DB 스냅샷, 파라미터 그룹, 이벤트 구독 등)를 지원하며 이러한 리소스를 가리켜 하위 리소스라고 합니다. 하기 표에 나와 있는 것처럼 이러한 리소스와 하위 리소스에는 고유한 Amazon 리소스 이름(ARN)이 연결되어 있습니다.  **※ RDS 리소스 유형 및 ARN 형식 표**   |  |  | | --- | --- | | 리소스 유형 | **ARN 형식** | | DB 클러스터 | arn:aws:rds:region:account-id:cluster:db-cluster-name | | DB 클러스터 파라미터 그룹 | arn:aws:rds:region:account-id:cluster-pg:cluster-parametergroup-name | | DB 클러스터 스냅샷 | arn:aws:rds:region:account-id:cluster-snapshot:clustersnapshot-name | | DB 인스턴스 | arn:aws:rds:region:account-id:db:db-instance-name | | DB 옵션 그룹 | arn:aws:rds:region:account-id:og:option-group-name | | DB 파라미터 그룹 | arn:aws:rds:region:account-id:pg:parameter-group-name | | DB 스냅샷 | arn:aws:rds:region:account-id:snapshot:snapshot-name | | DB 보안 그룹 | arn:aws:rds:region:account-id:secgrp:security-group-name | | DB 서브넷 그룹 | arn:aws:rds:region:account-id:subgrp:서브넷-group-name | | 이벤트 구독 | arn:aws:rds:region:account-id:es:subscription-name | | 읽기 전용 복제본 | arn:aws:rds:region:account-id:db:db-instance-name | | 예약 DB 인스턴스 | arn:aws:rds:region:account-id:ri:reserved-db-instance-name |   RDS 정책을 "계정 내 사용자 또는 그룹에 권한 정책 연결" 및 "역할에 권한 정책 연결(교차 계정 권한 부여)" 같이 IAM 자격 증명에 연결할 수 있습니다.  - 계정 내 사용자 또는 그룹에 권한 정책 연결: 계정 관리자는 특정 사용자에 연결된 권한 정책을 사용하여 해당 사용자에게 Amazon RDS 리소스 생성 권한을 부여할 수 있습니다.  - **역할에 권한 정책 연결(교차 계정 권한 부여)**: 자격 증명 기반 권한 정책을 IAM 역할에 연결하여 교차 계정 권한을 부여할 수 있습니다. 예를 들어, 계정 A의 관리자는 다음과 같이 다른 AWS 계정(예: 계정 B) 또는 AWS 서비스에 교차 계정 권한을 부여할 역할을 생성할 수 있습니다.  : 계정 A 관리자는 IAM 역할을 생성하고 계정 A의 리소스에 대한 권한을 부여하는 역할에 권한 정책을 연결  : 계정 A 관리자는 계정 B 역할을 대신할 보안 주체로 신뢰 정책을 연결  : 계정 B 관리자는 계정 B의 사용자에게 역할을 수임할 권한을 위임할 수 있습니다. 이럴 경우 계정 B의 사용자가 계정 A에서 리소스를 생성하거나 액세스 할 수 있게 됩니다. | | |
| **진단 기준** | **양호 기준**  root 계정 관리자가 다수 사용자에게 RDS 리소스 생성 권한을 설정하지 않았을 경우  **취약 기준**  root 계정 관리자가 다수 사용자에게 RDS 리소스 생성 권한을 설정했을 경우 | | |
| **점검 내용** | **가. RDS 리소스 권한 관리**  1) IAM 사용자 계정 확인  - ‘sk101-005’를 RDS 리소스 관리자로 지정    2) 부여된 권한 확인  - ‘sk101-005’ 사용자에게 ‘AmazonRDSFullAccess’ 권한 부여 | | |

**9) RDS API 작업 권한 관리**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 가상 리소스 관리 | **중요도** | **중** |
| **점검 날짜** | 2022년 6월 8일 | **결과** | **양호** |
| **점검 대상** | AWS Identity and Access Management (IAM) | | |
| **항목명** | RDS API 작업 권한 관리 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | Amazon RDS는 관리자 콘솔 외 API를 통해 리소스 접근 및 사용이 가능하기에 역할에 맞게 권한을 부여하여 비인가 된 사용자가 API를 통해 RDS 관련 작업을 할 수 없도록 해야 합니다.  ※ 예) 역할에 따른 권한 부여 AWS Root Account, 관리자(Infra, DBMS): AmazonRDSFullAccess DBMS 개발 및 운영자: AmazonRDSDataFullAccess DBMS 감사 및 비용담당자: AmazonRDSReadOnlyAccess  또한, CLI/API를 통해 RDS 리소스 접근 및 작업 시 사용되는 Access Key에 대해 주기적(3개월)으로 관리하여 보안상 문제가 발생되지 않도록 해야 합니다.  ※ Access Key 수명(60일 이내), 비밀번호 수명(60일 이내), 마지막 활동(30일 이내)  **※ RDS IAM Default 정책 표**   |  |  |  | | --- | --- | --- | | **구분** | **AWS 관리형 정책** | **정책 설명** | | **RDS** | AmazonRDSDataFullAccess | RDS 데이터 API, 자격 증명을 위한 비밀 저장소 API, DB 콘솔 쿼리 관리 API를 통한 AWS 계정의 Aurora Serverless 클러스터에서 SQL 문 실행 권한 | | AmazonRDSFullAccess | Management Console을 통해 Amazon RDS에 대한 전체 액세스 권한 제공 | | AmazonRDSReadOnlyAccess | Management Console을 통해 Amazon RDS에 대한 읽기 전용 액세스 권한 제공 | | AWSApplicationAutoscaling RDSClusterPolicy | Application Auto Scaling에 대한 권한을 부여하여 RDS 및 CloudWatch에 액세스하는 정책 | | AmazonRDSBetaServiceRolePolicy | Application Auto Scaling에 대한 권한을 부여하여 RDS 및 CloudWatch에 액세스하는 정책 | | AmazonRDSDirectoryServiceAccess | RDS가 사용자를 대신하여 AWS 리소스를 관리함 | | AmazonRDSEnhancedMonitoringRole | RDS가 도메인에 가입 한 SQL Server DB 인스턴스에 대해 고객 대신 Directory Service Managed AD에 액세스하도록 허용함 | | AmazonRDSPreviewServiceRolePolicy | CloudWatch for RDS Enhanced Monitoring에 대한 액세스 제공 | | AmazonRDSServiceRolePolicy | RDS가 사용자를 대신하여 AWS 리소스를 관리함 | | AWSQuickSightDescribeRDS | QuickSight에서 RDS 리소스를 설명하도록 | | RDSCloudHsmAuthorizationRole | RDS 서비스 역할의 기본 정책 | | | |
| **진단 기준** | **양호 기준**  IAM 일반 사용자 권한에 RDS API 기능을 사용할 수 있는 권한이 부여되어 있지 않은 경우  **취약 기준**  IAM 일반 사용자 권한에 RDS API 기능을 사용할 수 있는 권한이 부여되어 있을 경우 | | |
| **점검 내용** | **가. IAM 사용자 계정 별 권한 확인 및 설정**  1) 사용자의 권한 확인 및 권한 추가/삭제 | | |

**10) RDS 서브넷 가용 영역 관리**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 가상 리소스 관리 | **중요도** | **중** |
| **점검 날짜** | 2022년 6월 8일 | **결과** | **양호** |
| **점검 대상** | Amazon RDS | | |
| **항목명** | RDS API 작업 권한 관리 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | 서브넷이란 하나의 IP 네트워크 주소를 지역적으로 나누어 이 하나의 네트워크 IP 주소가 실제로 여러 개의 서로 연결된 지역 네트워크로 사용할 수 있도록 하는 방법으로 EC2 인스턴스와 RDS 상호 통신 시 필요하나 불필요한 서브넷이 포함되어 있을 경우 보안성 위험을 발생시킬 수 있으므로 불필요한 서브넷의 유무를 관리해야 합니다. | | |
| **진단 기준** | **양호 기준**  가상 인스턴스와 RDS 연결 간의 서브넷이 설정되어 있을 경우  **취약 기준**  가상 인스턴스와 RDS 연결 간의 불필요한 서브넷이 설정되어 있을 경우 | | |
| **점검 내용** | **가. 서브넷 그룹에 연결된 서브넷 확인**  1) 연결된 서브넷 확인  10.0.2.0/24 | | |

## **감사/추적 관리**

**1) AWS 사용자 계정 로깅 설정**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 감사/추적 관리 | **중요도** | **하** |
| **점검 날짜** | 2022년 6월 8일 | **결과** | **양호**  **(조치)** |
| **점검 대상** | AWS CloudTrail | | |
| **항목명** | AWS 사용자 계정 로깅 설정 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | AWS CloudTrail 은 계정의 거버넌스, 규정 준수, 운영 및 위험 감사를 활성화하도록 도와주는 서비스로서 사용자, 역할 또는 AWS 서비스가 수행하는 작업들의 이벤트가 기록됩니다. 또한 CloudTrail 은 생성 시 AWS 계정에서 활성화됩니다. 활동이 AWS 계정에서 이루어지면 해당 활동이 CloudTrail 이벤트에 기록됩니다. | | |
| **진단 기준** | **양호 기준**  AD 감사 로그를 별도로 보관(물리적/논리적)하는 정책이 존재하고 있을 경우  **취약 기준**  AD 감사 로그를 별도로 보관(물리적/논리적)하는 정책이 존재하고 있지 않을 경우 | | |
| **점검 내용** | **가. CloudTrail 확인**  1. CloudTrail 확인 | | |
| **조치**  **내용** | **가. CloudTrail 및 CloudWatch 관리 이벤트 설정**  1) CloudTrail 추적 생성    2) CloudWatch Logs 로그 그룹 생성  - 신규 로그 그룹 생성    3) 관리 이벤트 확인    4) S3 확인  - 감사 로그 S3에서 별도로 저장되는 지 확인 | | |
| **조치 내용 설명** | 감사 로그를 별도로 보관하는 정책이 존재하지 않아 기준을 충족시키지 못하였다. 따라서 생성한 로그 그룹을 별도의 S3 버킷과 연결하여 로그 데이터 보관을 가능하도록 하였다. | | |

**2) 가상 인스턴스 로깅 설정**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 감사/추적 관리 | **중요도** | **하** |
| **점검 날짜** | 2022년 6월 8일 | **결과** | **양호**  **(조치)** |
| **점검 대상** | Amazon EC2 | | |
| **항목명** | 가상 인스턴스 로깅 설정 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | Amazon CloudWatch Logs는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스, AWS CloudTrail, Route 53 및 기타 소스에서 로그 파일을 모니터링, 저장 및 액세스할 수 있습니다. 또한, 가상 인스턴스에 agent를 설치하여 로그 그룹에 등록된 로그 스트림을 통해 관련 로그를 확인할 수 있습니다. | | |
| **진단 기준** | **양호 기준**  가상 인스턴스 로그를 별도로 보관(물리적/논리적)하는 정책이 존재하고 있을 경우  **취약 기준**  가상 인스턴스 로그를 별도로 보관(물리적/논리적)하는 정책이 존재하고 있지 않을 경우 | | |
| **점검 및**  **조치 내용** | **가. 로그 그룹 및 로그 스트림 내 EC2 로깅 확인 방법**  1) EC2 내 CloudWatch 에이전트 설치    2) S3와 연결된 로그 그룹에서 로그 확인 | | |
| **조치 내용 설명** | 가상 인스턴스 로그를 별도로 보관하는 정책이 존재하지 않아 기준을 충족시키지 못하였다. 따라서 생성한 EC2의 인스턴스 내에서 CloudWatch Agent를 설치하여 로그 확인을 가능하도록 하였다. | | |

**3) RDS 로깅 설정**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 감사/추적 관리 | **중요도** | **하** |
| **점검 날짜** | 2022년 6월 8일 | **결과** | **양호**  **(조치)** |
| **점검 대상** | Amazon RDS | | |
| **항목명** | RDS 로깅 설정 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | Amazon CloudWatch Logs는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스, AWS CloudTrail, Route 53 및 기타 소스에서 로그 파일을 모니터링, 저장 및 액세스할 수 있습니다. 또한, 데이터베이스 옵션(로그 내보내기)을 수정하여 로그 그룹에 등록된 로그 스트림을 통해 RDS 로그를 확인할 수 있습니다. | | |
| **진단 기준** | **양호 기준**  RDS 로그를 별도로 보관(물리적/논리적)하는 정책이 존재하고 있을 경우  **취약 기준**  RDS 로그를 별도로 보관(물리적/논리적)하는 정책이 존재하고 있지 않을 경우 | | |
| **점검 내용** | **가. 데이터베이스 활동 스트림 확인**  1) RDS 내 데이터베이스 스트림 확인  - 데이터베이스 활동 스트림이 비활성화 확인 | | |
| **조치 내용** | **가. 로그 그룹 및 로그 스트림 내 RDS 로깅 확인 방법**  1) RDS 내 데이터베이스 수정  - 감사 로그, 에러 로그, 일반 로그, 느린 쿼리 로그 내보내기 확인    2) RDS 내 데이터베이스 수정 확인    3) 로그 그룹 확인    4) 로그 스트림 확인    5) RDS 로깅 확인 | | |
| **조치 내용 설명** | 생성된 RDS의 데이터베이스 스트림이 비활성화 되어 있어 진단 기준을 충족시키지 못하였다. 따라서 생성된 RDS의 데이터베이스 스트림을 활성화함으로써 로그를 별도로 보관하는 정책을 설정하였다. | | |

**4) S3 버킷 로깅 설정**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 감사/추적 관리 | **중요도** | **하** |
| **점검 날짜** | 2022년 6월 8일 | **결과** | **양호**  **(조치)** |
| **점검 대상** | Amazon S3 | | |
| **항목명** | S3 버킷 로깅 설정 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | AWS CloudTrail 은 계정의 거버넌스, 규정 준수, 운영 및 위험 감사를 활성화하도록 도와주는 서비스로서 사용자, 역할 또는 AWS 서비스가 수행하는 작업들의 이벤트가 기록됩니다. 또한 버킷의 옵션(서버 액세스 로깅) 활성화를 통해 API 호출 및 관련 이벤트를 추적할 수 있습니다. | | |
| **진단 기준** | **양호 기준**  S3 버킷 로그를 별도로 보관(물리적/논리적)하는 정책이 존재하고 있을 경우  **취약 기준**  S3 버킷 로그를 별도로 보관(물리적/논리적)하는 정책이 존재하고 있지 않을 경우 | | |
| **점검 내용** | **가. CloudTrail 서버 액세스 로그 설정**  1) CloudTrail 추적 확인    2) CloudTrail 추적 로그 위치 확인    3) S3 버킷 확인 | | |
| **조치 내용** | **가. S3 서버 액세스 로그 활성화**  1) 서버 액세스 로깅 비활성화 확인    2) 서버 액세스 로깅 편집    3) 서버 액세스 로깅 활성화 확인 | | |
| **조치 내용 설명** | 서버 액세스 로깅이 비활성화되어 있어 진단 기준을 충족시키지 못하였다. 따라서 생성된 S3의 서버 액세스 로깅을 활성화함으로써 로그를 별도로 보관하는 정책을 설정하였다. | | |

# **참조**

* SK쉴더스, “2021 클라우드 보안가이드 – AWS”
* 과학기술정보통신부 KISA, ‘주요정보통신기반시설 기술적 취약점 분석·평가 방법 상세가이드라인(2017.12)’
* 과학기술정보통신부 KISA, ‘클라우드 취약점 점검 가이드(2020.12)’