

보안 점검 보고서

사업명	의류 쇼핑몰 마케팅 전략을 위한 데이터 인프라 구축
주관사	Find Customers
담당자	김민경

2024. 06. 25.

목차

1. 개요	3
보안 점검 체크리스트	3
위험도 구분	3
2. 점검 결과	4
2.1. 계정	4
IAM 사용자 계정 관리	4
IAM 사용자 계정 식별	5
2.2. 권한	5
인스턴스 서비스 정책 관리	5
S3 버킷 접근 권한 관리	7
2.3. 운영	8
S3 암호화 설정	8
2.4. 보안그룹	9
인/아웃바운드 설정	9

보안 점검 보고서

1. 개요

점검 체크리스트는 보안 점검을 수행합니다.

모든 항목들에 대해 취약점으로 인해 발생한 피해에 대하여 위험도 산정을 통해 상, 중, 하 3 단계로 분류하였습니다.

보안 점검 체크리스트

영역	항목명	중요도
계정	IAM 사용자 계정 관리	상
	IAM 사용자 계정 식별	중
권한	인스턴스 서비스 정책 관리	상
	S3 버킷 접근 권한 관리	상
운영	S3 암호화 설정	중
보안 그룹	S3 암호화 설정	상

위험도 구분

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


2. 점검 결과

2.1. 계정

IAM 사용자 계정 관리

영역	계정																																																																	
항목명	사용자 계정 관리																																																																	
항목 설명	불필요한 계정 지속적으로 IAM 사용자 계정을 확인하여 불필요한 계정이 생성되지 않았는지 확인해야 합니다. 불필요한 계정의 종류는 다음과 같습니다. <ul style="list-style-type: none">• 비임직원 계정• 테스트 계정• 미사용 계정 – 퇴직 및 휴직자 또는 6 개월이상 미접속 계정																																																																	
점검 방법	불필요한 계정 존재 여부 확인 <div><div>IAM > 사용자</div><div><div>사용자 (4) 정보</div><div>IAM 사용자는 계정에서 AWS와 상호 작용하는 데 사용되는 장기 자격 증명을 가진 자격 증명입니다.</div><div><div>검색</div></div><table><thead><tr><th><input type="checkbox"/></th><th>사용자 이름</th><th>▲</th><th>경로</th><th>▼</th><th>그룹</th><th>▼</th><th>마지막 활동</th><th>▼</th><th>MFA</th><th>▼</th><th>암호 수명</th><th>▼</th></tr></thead><tbody><tr><td><input type="checkbox"/></td><td>kgh-admin</td><td></td><td>/</td><td></td><td>1</td><td></td><td>🟢 8시간 전</td><td></td><td>가상</td><td></td><td>🟢 50일</td><td></td></tr><tr><td><input type="checkbox"/></td><td>kmk-admin</td><td></td><td>/</td><td></td><td>1</td><td></td><td>🟢 3시간 전</td><td></td><td>가상</td><td></td><td>🟢 49일</td><td></td></tr><tr><td><input type="checkbox"/></td><td>lhs-admin</td><td></td><td>/</td><td></td><td>1</td><td></td><td>🟢 1시간 전</td><td></td><td>가상</td><td></td><td>🟢 47일</td><td></td></tr><tr><td><input type="checkbox"/></td><td>njw-admin</td><td></td><td>/</td><td></td><td>1</td><td></td><td>🟢 6시간 전</td><td></td><td>-</td><td></td><td>🟢 50일</td><td></td></tr></tbody></table></div></div>	<input type="checkbox"/>	사용자 이름	▲	경로	▼	그룹	▼	마지막 활동	▼	MFA	▼	암호 수명	▼	<input type="checkbox"/>	kgh-admin		/		1		🟢 8시간 전		가상		🟢 50일		<input type="checkbox"/>	kmk-admin		/		1		🟢 3시간 전		가상		🟢 49일		<input type="checkbox"/>	lhs-admin		/		1		🟢 1시간 전		가상		🟢 47일		<input type="checkbox"/>	njw-admin		/		1		🟢 6시간 전		-		🟢 50일	
<input type="checkbox"/>	사용자 이름	▲	경로	▼	그룹	▼	마지막 활동	▼	MFA	▼	암호 수명	▼																																																						
<input type="checkbox"/>	kgh-admin		/		1		🟢 8시간 전		가상		🟢 50일																																																							
<input type="checkbox"/>	kmk-admin		/		1		🟢 3시간 전		가상		🟢 49일																																																							
<input type="checkbox"/>	lhs-admin		/		1		🟢 1시간 전		가상		🟢 47일																																																							
<input type="checkbox"/>	njw-admin		/		1		🟢 6시간 전		-		🟢 50일																																																							
진단 기준	양호 기준 <ul style="list-style-type: none">- 불필요한 계정이 존재하지 않은 경우 취약 기준 <ul style="list-style-type: none">- 불필요한 계정이 존재할 경우- MFA 를 사용하지 않은 계정이 존재하는 경우 심각 기준 <ul style="list-style-type: none">- Console Admin 계정에 MFA 를 사용하지 않은 경우																																																																	
결과	양호																																																																	
비고																																																																		

IAM 사용자 계정 식별

영역	계정
항목명	IAM 사용자 계정 식별
항목 설명	태그 설정을 통해 IAM 사용자를 구별할 수 있습니다. 또한 추후에 동일한 태그를 가진 리소스를 한 번에 삭제하는 기능 또한 이용하실 수도 있습니다.
점검 방법	<p>IAM 사용자별 태그 확인</p> <ul style="list-style-type: none"> IAM > 사용자 > 해당 사용자 클릭 > 태그 탭 
진단 기준	<p>양호 기준</p> <ul style="list-style-type: none"> IAM 사용자 태그가 설정되어 있을 경우 <p>취약 기준</p> <ul style="list-style-type: none"> IAM 사용자 태그가 설정되어 있지 않을 경우
결과	취약
비고	

2.2. 권한

인스턴스 서비스 정책 관리

영역	권한		
항목명	인스턴스 서비스 정책 관리		
항목 설명	AWS 인스턴스 서비스(EC2, RDS, S3 등)의 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.		
	인스턴스 서비스 별 관리형 정책		
	S3	AmazonS3FullAccess	모든 버킷에 대한 전체 액세스 권한
	AmazonS3OutpostsFull	Outposts의 Amazon S3에 대한 전체 액세스 권한	

		Access	세스 권한
		AmazonS3ReadOnlyAccess	모든 버킷에 대한 읽기 전용 액세스 권한
	RDS	AmazonRDSFullAccess	RDS 리소스에 대한 전체 접근 권한 부여
		AmazonRDSReadOnlyAccess	RDS 리소스에 대한 읽기 전용 접근 권한 부여

1. 인스턴스에 사용될 인스턴스 그룹을 생성

[IAM](#) > 사용자 그룹

사용자 그룹 (1) 정보 🔄 삭제 그룹 생성

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

🔍 검색

<input type="checkbox"/>	그룹 이름	▲	사용자	▼	권한	▼	생성 시간	▼
<input type="checkbox"/>	KDT_MSP_Class1		4		✓ 정의됨		1개월 전	

2. IAM 관리자/운영자 권한 사용자 추가

[IAM](#) > 사용자

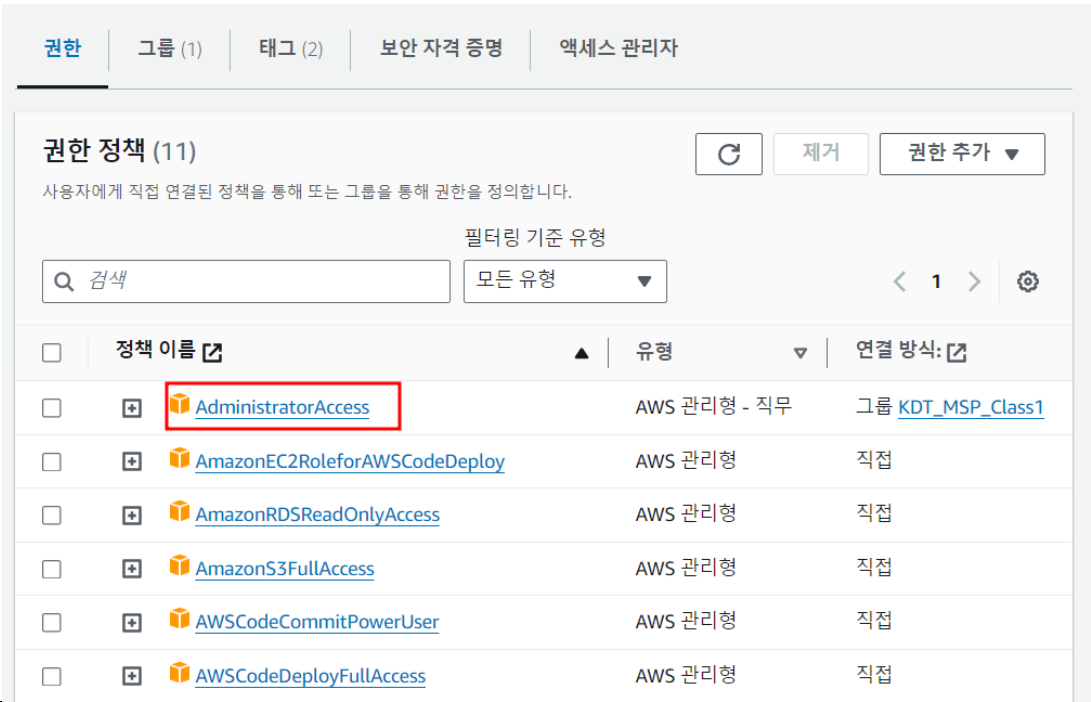
사용자 (4) 정보

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

🔍 검색


<input type="checkbox"/>	사용자 이름	▲	경로	▼	그룹	▼	마지막 활동	▼
<input type="checkbox"/>	kgh-admin		/		1		✓ 8시간 전	
<input type="checkbox"/>	kmk-admin		/		1		✓ 3시간 전	
<input type="checkbox"/>	lhs-admin		/		1		✓ 53분 전	
<input type="checkbox"/>	njw-admin		/		1		✓ 5시간 전	

점검
방법

	<h3>3. 추가된 권한 확인</h3> 
진단 기준	<p>양호 기준</p> <ul style="list-style-type: none"> - 사용 서비스에 필요한 권한만 연결된 경우 <p>취약 기준</p> <ul style="list-style-type: none"> - 사용 서비스 외 불필요한 권한이 추가된 경우
결과	취약
비고	

S3 버킷 접근 권한 권리

영역	권한
항목명	S3 버킷 접근 권한 관리
항목 설명	<p>S3 버킷의 경우, 생성된 리소스(버킷)의 소유자는 기본적으로 해당 리소스에 접근할 수 있습니다. 다른 사용자에게 액세스 권한을 부여하려면 별도로 액세스 정책(버킷 및 객체 수준)을 설정해야 합니다. 또한 퍼블릭 액세스 차단 설정이 되어 있지 않으면 외부에서 버킷 및 객체가 노출될 수 있으므로, 안전한 접근을 위해 적절한 설정을 해야 합니다.</p> <p>퍼블릭 액세스 차단 관리</p> <ul style="list-style-type: none"> - 퍼블릭 액세스 허용: 외부 사용자가 액세스하여 중요한 데이터 및 정보를

	확인할 수 있기 때문에 퍼블릭 액세스는 권장하지 않습니다.
점검 방법	<p>퍼블릭 액세스 차단 여부 확인</p> <ul style="list-style-type: none"> • S3 > 버킷 > 확인하려는 버킷 선택 > 권한 탭 > 퍼블릭 액세스 차단(버킷 설정) 확인 - 다음과 같이 모든 퍼블릭 액세스 차단이 활성화되어 있어야 함. <div> <p>퍼블릭 액세스 차단(버킷 설정) 편집</p> <p>퍼블릭 액세스는 ACL(엑세스 제어 목록), 버킷 정책, 액세스 지정 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 액세스 지점에만 적용됩니다. AWS에서는 [모든 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 설정을 사용자 지정할 수 있습니다. 자세히 알아보기</p> <div> <p>모든 퍼블릭 액세스 차단</p> <p> 활성화</p> <p>▶ 이 버킷의 개별 퍼블릭 액세스 차단 설정</p> </div> </div>
진단 기준	<p>양호 기준</p> <ul style="list-style-type: none"> - 모든 퍼블릭 액세스 차단이 활성화된 경우 <p>취약 기준</p> <ul style="list-style-type: none"> - 모든 퍼블릭 액세스 차단이 비활성화된 경우
결과	양호
비고	

2.3. 운영

S3 암호화 설정

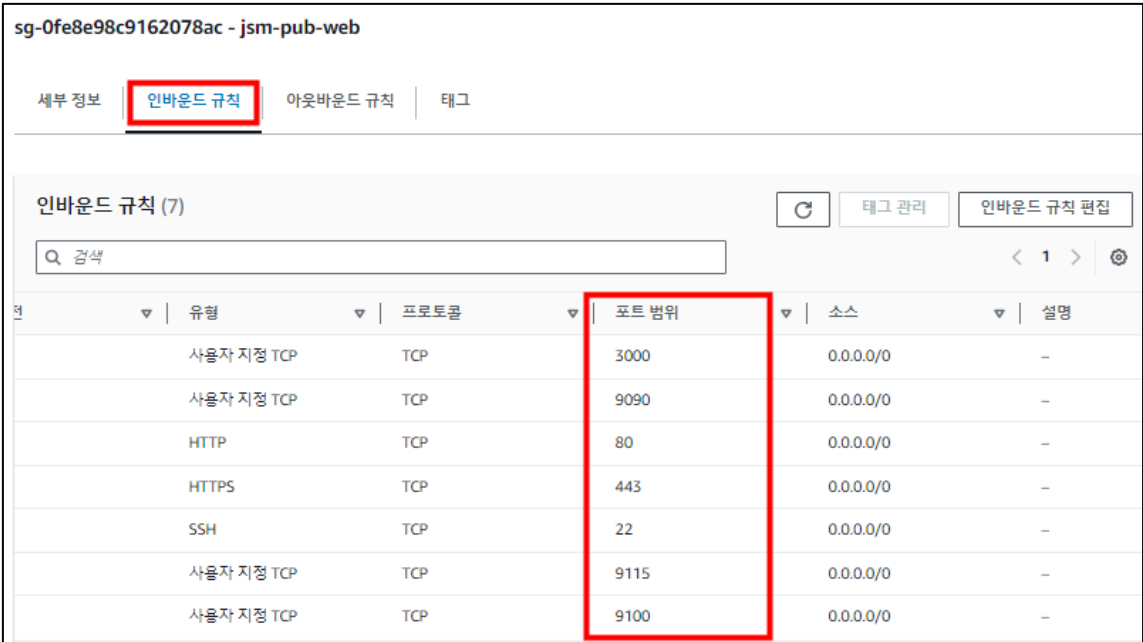
영역	운영				
항목명	S3 암호화 설정				
항목 설명	<p>S3는 보안을 위해 데이터 저장 및 전송 시 암호화할 수 있는 방식을 제공한다. 암호화를 하는 주체에 따라 서버측 암호화와 클라이언트 측 암호화로 분리된다.</p> <p>서버 측 암호화</p> <table> <tr> <td>SSE-S3</td><td>AWS 회사 자체에서 관리되는 keys를 이용해 암호화</td></tr> <tr> <td>SSE-KMS</td><td>KMS(아마존 키 매니저 서비스 - AWS의 암호를 관리</td></tr> </table>	SSE-S3	AWS 회사 자체에서 관리되는 keys를 이용해 암호화	SSE-KMS	KMS(아마존 키 매니저 서비스 - AWS의 암호를 관리
SSE-S3	AWS 회사 자체에서 관리되는 keys를 이용해 암호화				
SSE-KMS	KMS(아마존 키 매니저 서비스 - AWS의 암호를 관리				

		해주는 서비스)를 이용해 암호화
	SSE-C	사용자에 의해 직접 정의된 keys를 이용해 암호화
	클라이언트 측 암호화 데이터를 업로드하기 전에 암호화를 진행한 후에 전송하는 방식이다. 데이터 인출 시에도 클라이언트 측에서 복호화 작업을 거쳐야 한다.	
점검 방법	<ul style="list-style-type: none"> S3 버킷 암호화 설정 확인 - S3 > 버킷 > 해당 버킷 선택 > 속성 탭 > 기본 암호화 <div> <div>기본 암호화 정보</div> <div> <div> <div>암호화 유형 정보</div> <div>AWS Key Management Service 키를 사용한 서버 측 암호화(SSE-KMS)</div> </div> <div> <div>암호화 키 ARN</div> <div>arn:aws:kms:ap-northeast-1:381492154999:key/429214e0-6b20-4c6a-b4ed-60912c9a5150</div> </div> <div> <div>버킷 키</div> <div>KMS 암호화가 이 버킷의 새 객체를 암호화하는 데 사용되는 경우 버킷 키는 AWS KMS에 대한 호출을 줄여 암호화 비용을 줄입니다. 자세히 알아보기</div> </div> </div> <div> <div>활성화됨</div> </div> </div>	
진단 기준	양호 기준 <ul style="list-style-type: none"> S3 버킷의 기본 암호화가 설정되어 있을 경우 취약 기준 <ul style="list-style-type: none"> S3 버킷의 기본 암호화가 설정되어 있지 않을 경우 	
결과	양호	
비고		

2.4. 보안그룹

인/아웃바운드 설정

영역	보안그룹
항목명	보안 그룹 인/아웃 바운드 관리
항목 설명	보안 그룹의 규칙은 보안 그룹과 연결된 리소스에 도달하도록 허용된 인바운드 트래픽을 제어합니다. 인스턴스에서 나갈 수 있는 아웃바운드 트래픽을 제어합니다.

	<p>보안 그룹의 규칙을 추가하거나 제거할 수 있습니다(인바운드 또는 아웃바운드 액세스 권한 부여 또는 취소라고도 함). 규칙은 인바운드 트래픽(수신)이나 아웃바운드 트래픽(송신)에 적용됩니다. 특정 소스 또는 대상에 대한 액세스 권한을 부여할 수 있습니다.</p>																																																
점검 방법	<p>보안 그룹 인/아웃바운드 확인</p> <ul style="list-style-type: none"> • EC2 > 인스턴스 > 확인하려는 인스턴스 선택 > 보안 탭 <ul style="list-style-type: none"> - 인바운드 규칙이 특정 소스에서 특정 포트로 접근할 때만 접속 허용을 할 수 있도록 설정할 수 있습니다. - 보안 그룹을 처음 만들 때 인바운드 규칙이 없는 상태임. 따라서 추후에 추가해야함. <p>1) 선택된 보안 그룹 인바운드 규칙 내 포트 확인</p>  <table border="1"> <thead> <tr> <th>순</th> <th>유형</th> <th>프로토콜</th> <th>포트 범위</th> <th>소스</th> <th>설명</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>사용자 지정 TCP</td> <td>TCP</td> <td>3000</td> <td>0.0.0.0/0</td> <td>-</td> </tr> <tr> <td>2</td> <td>사용자 지정 TCP</td> <td>TCP</td> <td>9090</td> <td>0.0.0.0/0</td> <td>-</td> </tr> <tr> <td>3</td> <td>HTTP</td> <td>TCP</td> <td>80</td> <td>0.0.0.0/0</td> <td>-</td> </tr> <tr> <td>4</td> <td>HTTPS</td> <td>TCP</td> <td>443</td> <td>0.0.0.0/0</td> <td>-</td> </tr> <tr> <td>5</td> <td>SSH</td> <td>TCP</td> <td>22</td> <td>0.0.0.0/0</td> <td>-</td> </tr> <tr> <td>6</td> <td>사용자 지정 TCP</td> <td>TCP</td> <td>9115</td> <td>0.0.0.0/0</td> <td>-</td> </tr> <tr> <td>7</td> <td>사용자 지정 TCP</td> <td>TCP</td> <td>9100</td> <td>0.0.0.0/0</td> <td>-</td> </tr> </tbody> </table>	순	유형	프로토콜	포트 범위	소스	설명	1	사용자 지정 TCP	TCP	3000	0.0.0.0/0	-	2	사용자 지정 TCP	TCP	9090	0.0.0.0/0	-	3	HTTP	TCP	80	0.0.0.0/0	-	4	HTTPS	TCP	443	0.0.0.0/0	-	5	SSH	TCP	22	0.0.0.0/0	-	6	사용자 지정 TCP	TCP	9115	0.0.0.0/0	-	7	사용자 지정 TCP	TCP	9100	0.0.0.0/0	-
	순	유형	프로토콜	포트 범위	소스	설명																																											
1	사용자 지정 TCP	TCP	3000	0.0.0.0/0	-																																												
2	사용자 지정 TCP	TCP	9090	0.0.0.0/0	-																																												
3	HTTP	TCP	80	0.0.0.0/0	-																																												
4	HTTPS	TCP	443	0.0.0.0/0	-																																												
5	SSH	TCP	22	0.0.0.0/0	-																																												
6	사용자 지정 TCP	TCP	9115	0.0.0.0/0	-																																												
7	사용자 지정 TCP	TCP	9100	0.0.0.0/0	-																																												
진단 기준	<p>양호기준 : 보안 그룹 내 인/아웃바운드의 포트가 Any로 허용되어 있지 않을 경우</p> <p>취약기준 : 보안 그룹 내 인/아웃바운드의 포트가 Any로 허용되어 있을 경우</p>																																																
결과	양호																																																
비고																																																	

