1.10 AWS 계정 패스워드 정책 관리

취약점 설명

패스워드를 생성할 때는 복잡도를 충족하도록 설정해야 한다 .

일반적으로 **3**종류 이상의 조합 **(**대 소문자 **,** 숫자 특수문자 **)** 및 **8**자리 이상의 패스워드를 기준으로 한다 .

또는 **2**종류 이상의 조합 **+ 10**자리 이상의 패스워드도 가능 .

AWS에서는 계정의 패스워드를 설정할때 복잡도를 충족하도록 강제하는 정책이 기본적으로 적용되는데 **,**

해당 설정을 개인 설정으로 변경하여 취약하게 사용할 경우 보안적으로 위험할 수 있다 .

딴소리

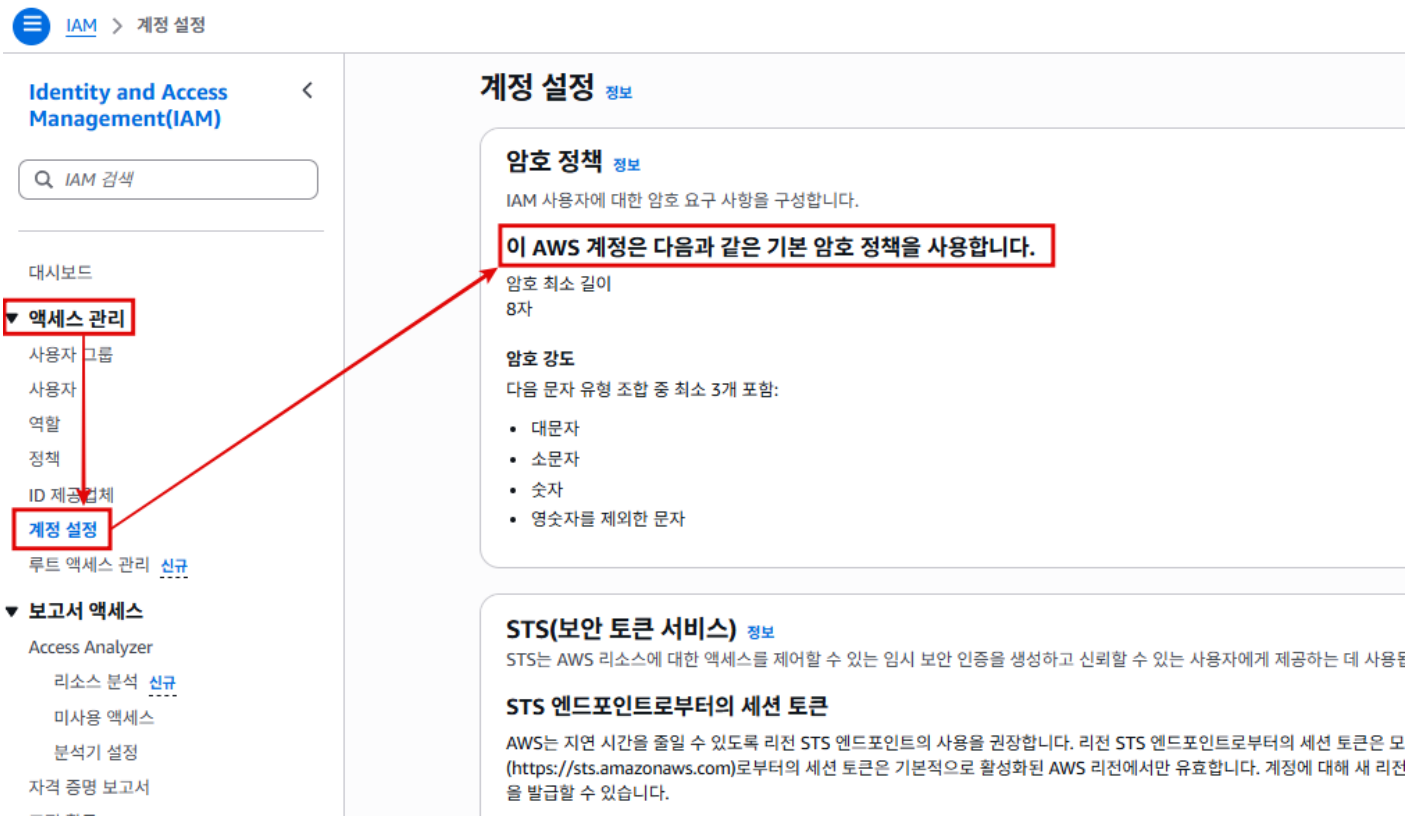
SK AWS 진단 가이드에선 패스워드 만료 및 이전 패스워드 사용 제한을 설정하도록 권고하고 있는데 **,**

해당 사항은 **AWS** 기본 정책에 적용되어 있지 않기 때문에 계정 설정에서 개인 설정을 통해 해당 정책을 설정해주어야 한다 .

진단 방법

01. [IAM] -> [액세스 관리 **] -> [**계정 설정 **] ->** 암호 정책을 올바르게 설정하여 사용하고 있는지 확인

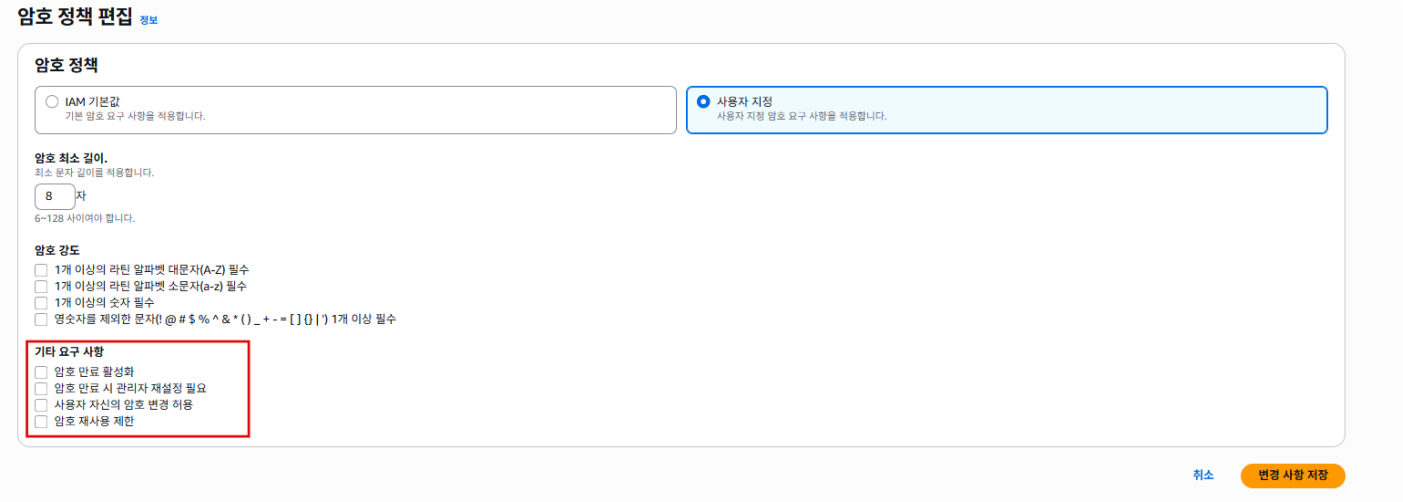
*** AWS** 기본암호 정책은 패스워드 만료 **,** 이전패스워드 사용 금지 정책이 존재하지 않으므로 취약


IAM > 계정 설정
Identity and Access Management(IAM)
IAM 검색
대시보드
액세스 관리
사용자 그룹
사용자
역할
정책
ID 제공업체
계정 설정
루트 액세스 관리 신규
보고서 액세스
Access Analyzer
리소스 분석 신규
미사용 액세스
분석기 설정
자격 증명 보고서
계정 설정 정보
암호 정책 정보
IAM 사용자에 대한 암호 요구 사항을 구성합니다.
이 AWS 계정은 다음과 같은 기본 암호 정책을 사용합니다.
암호 최소 길이
8자
암호 강도
다음 문자 유형 조합 중 최소 3개 포함:
대문자
소문자
숫자
영숫자를 제외한 문자
STS(보안 토큰 서비스) 정보
STS는 AWS 리소스에 대한 액세스를 제어할 수 있는 임시 보안 인증을 생성하고 신뢰할 수 있는 사용자에게 제공하는 데 사용
STS 엔드포인트로부터의 세션 토큰
AWS는 지연 시간을 줄일 수 있도록 리전 STS 엔드포인트의 사용을 권장합니다. 리전 STS 엔드포인트로부터의 세션 토큰은 모
(https://sts.amazonaws.com)로부터의 세션 토큰은 기본적으로 활성화된 AWS 리전에서만 유효합니다. 계정에 대해 새 리전
을 발급할 수 있습니다.

02. □□ □□ □□□ □□ □□ □□□ □□


계정 설정 정보
암호 정책 정보
편집
IAM 사용자에 대한 암호 요구 사항을 구성합니다.
이 AWS 계정은 다음과 같은 기본 암호 정책을 사용합니다.
암호 최소 길이
8자
암호 강도
다음 문자 유형 조합 중 최소 3개 포함:
대문자
소문자
숫자
영숫자를 제외한 문자
기타 요구 사항
비밀번호가 만료되지 않음
AWS 계정 이름 또는 이메일 주소와 동일할 수 없음
STS(보안 토큰 서비스) 정보
STS는 AWS 리소스에 대한 액세스를 제어할 수 있는 임시 보안 인증을 생성하고 신뢰할
STS 엔드포인트로부터의 세션 토큰
AWS는 지연 시간을 줄일 수 있도록 리전 STS 엔드포인트의 사용을 권장합니다. 리전 STS 엔드포인트를 사용할 경우 봊포인트
(https://sts.amazonaws.com)로부터의 세션 토큰은 기본적으로 활성화된 AWS 리전에서 활성화하려는 경우 리전 STS 엔드포인트로부터의 세션 토큰을 사용하AWS에서 유효한 세션 토큰
을 발급할 수 있습니다.

03. □□□ □□□□ □□□□ □□ □□□□□ □□□□ □□ □□ □□□ □□□□ □□□ □ □□ .



진단 기준	**양호기준** : Admin Console 및 IAM 계정의 패스워드 복잡성 기준 준수 및 암호 만료/재사용 제한을 설정하고 있을 경우 **취약기준** : Admin Console 및 IAM 계정의 패스워드 복잡성 기준 준수 및 암호 만료/재사용 제한을 설정하고 있지 않을 경우
비고	

Revision #1
Created 2025-09-19 22:35:05 UTC by minwoo
Updated 2025-09-19 23:22:55 UTC by minwoo