1.1. 사용자 계정 관리 [시작]

취약점 설명

AWS에서는 계정마다 권한을 부여하거나, 권한들의 집합인 **Role** 을 부여할 수 있습니다.

* **Role**을 통해 사용자 권한을 관리하는 방식을 **RBAC (Role Based Access Control)** 라고 합니다.

AWS에는 수 많은 서비스 **(200**개 이상 **)**가 존재하기 때문에 권한 관리는 굉장히 중요합니다.

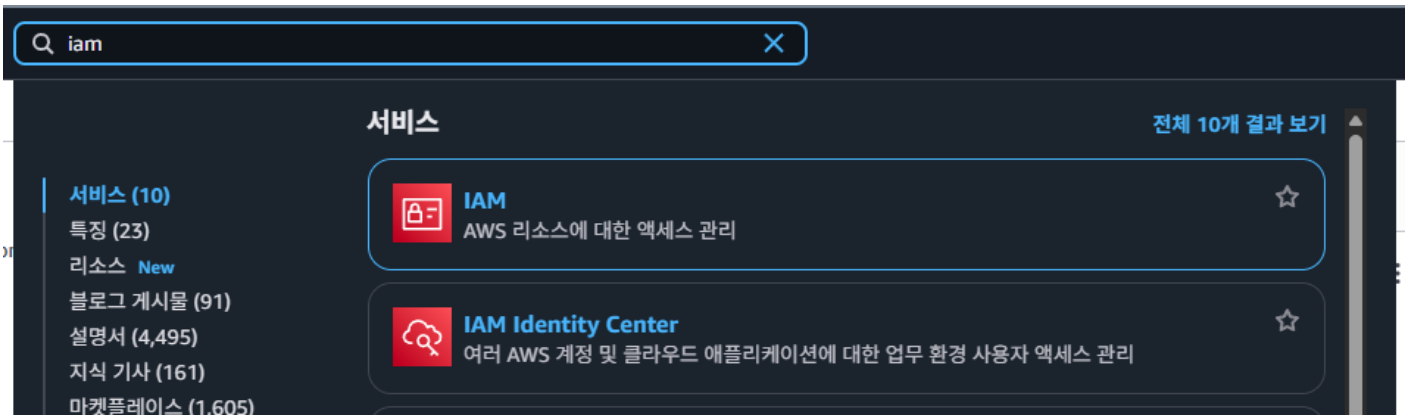
AWS에서는 한 파트에 대한 모든 권한을 관리하는 **Full Access** 권한이 존재함으로 필요에 따라 권한이 부여되어 있는지 확인합니다.

딴소리

진단을 인터뷰로 하는 경우도 있지만 그냥 **Read-Only** 계정 하나 파서 직접 진단하라 그러는 곳도 있습니다.

진단 방법

01. IAM 서비스 진입



IAM
AWS 리소스에 대한 액세스 관리

IAM Identity Center
여러 AWS 계정 및 클라우드 애플리케이션에 대한 업무 환경 사용자 액세스 관리

02. 사용자 정보 확인

- 원래같으면 여러 계정들이 있겠죠?

- 담당자분께 각 사용자들의 대한 권한 관리를 하고 계신지 여쭤보면 됩니다.
- 모든 보안 진단이 그렇듯 계정 별로 필요한 최소한의 계정을 부여하는 것이 중요합니다.

사용자 (0) 정보

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

☐	사용자 이름	경로	그룹	마지막 활동	MFA	암호 수명	콘솔 마지막 로그인
	표시할 리소스 없음						

양호 취약 기준

진단 기준	양호기준 : 관리자 권한을 보유한 다수 계정이 존재하지 않고 불필요한 계정이 존재하지 않을 경우 취약기준 : 관리자 권한을 보유한 다수 계정이 존재하거나 불필요한 계정이 존재할 경우

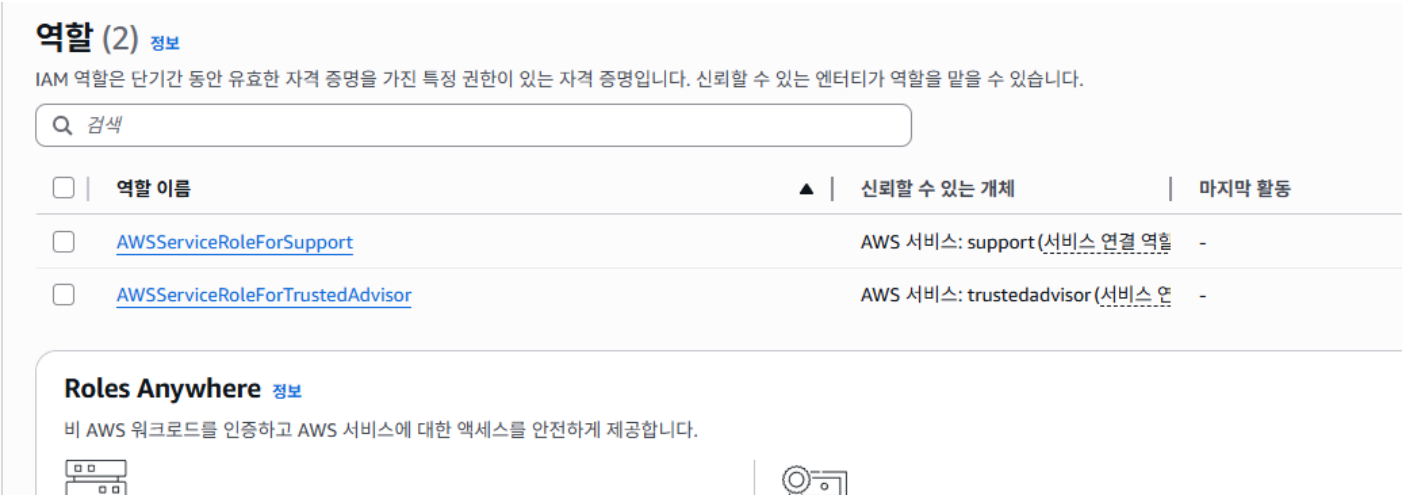
질문 : 사용자의 역할에 따라 권한 관리를 진행하고 계시나요?

답변

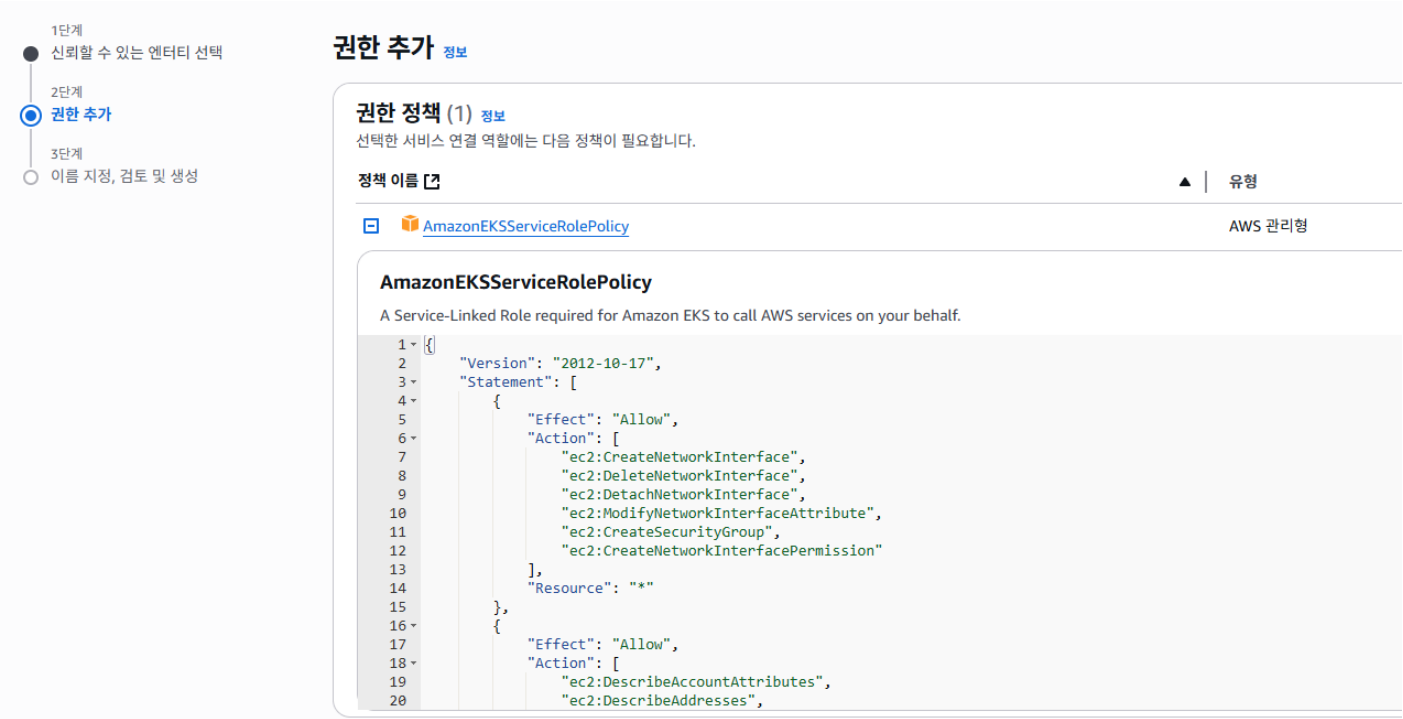
- 각 부서에 맞게 최소 권한을 부여하여 관리하고 있습니다. -> 양호
- 관리하긴 하는데 몇몇 불필요한 **FullAccess** 권한이 보이네요 -> 취약
- 따로 권한 관리는 안하고있습니다. -> 취약

참고

1. **(Role)** .



, Json .



2. SSO .

Revision #5
Created 2025-09-11 11:57:22 UTC by minwoo
Updated 2025-09-19 22:05:41 UTC by minwoo