

인증과 권한

김영욱 (YoungWook Kim)
Hello AI
youngwook@outlook.com

인증과 권한

인증(Authentication)

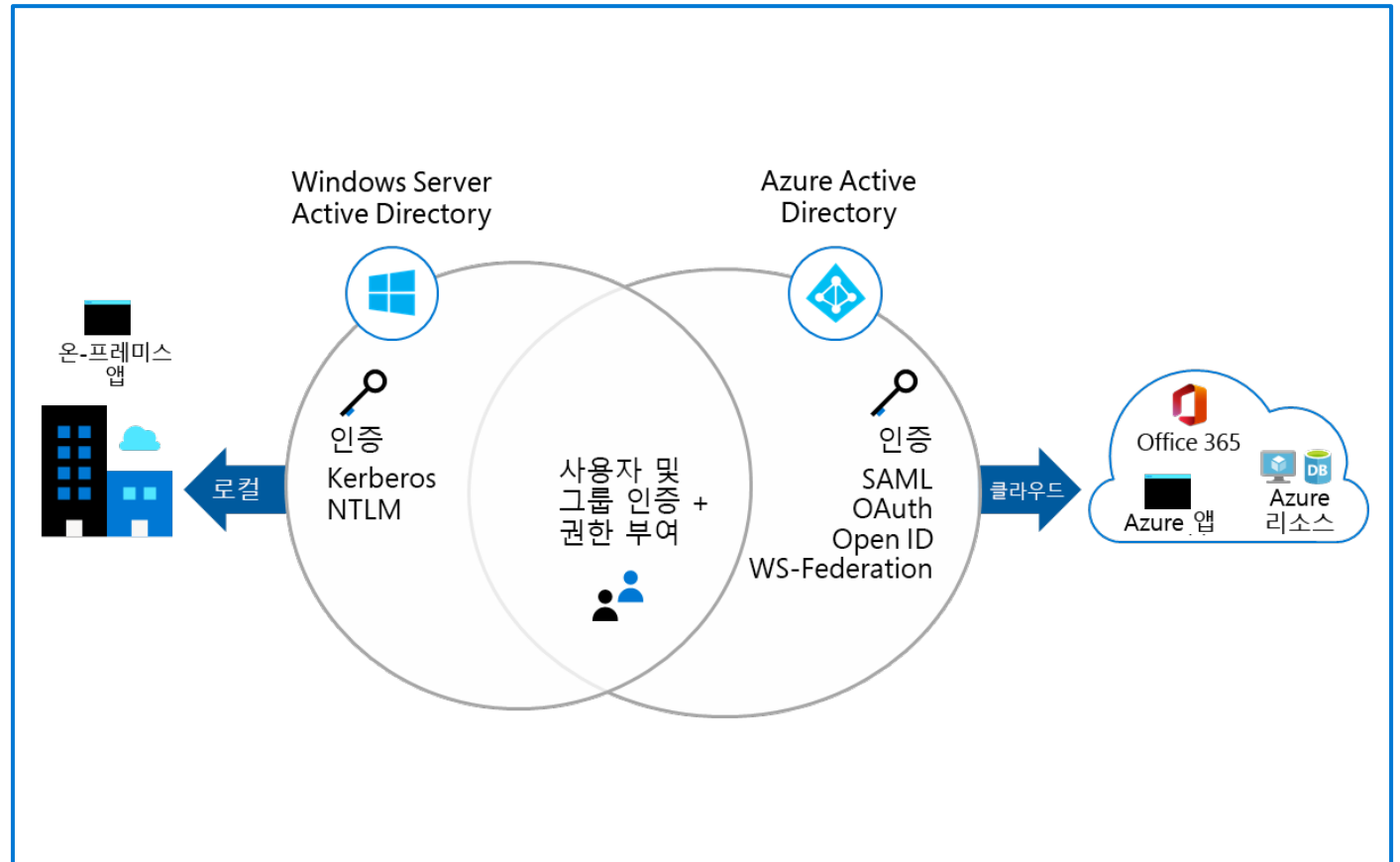
- User 또는 Service 계정 식별
- 정상적인 요청으로 액세스 자격 증명 획득
- 액세스 제어 규칙을 만들기 위한 기초

권한(Authorization)

- 인증된 User 또는 Service의 액세스 수준 정의
- 액세스 할 수 있는 리소스와 함께 수행할 수 있는 작업을 정의

Azure AD(Azure Active Directory)

- 다중 테넌트 클라우드 기반 디렉터리 및 ID 관리
- 클라우드 애플리케이션 및 리소스용 Single Sign-On 액세스 기능 제공
- 전역 범위에서 원활하게 앱 개발
- 전체 ID 관리 기능 제공:
 - 셀프 서비스 암호 및 그룹 관리
 - 권한 있는 계정 관리
 - 역할 기반 액세스 제어
 - 앱 사용량 모니터링
 - 보안 모니터링
 - 디바이스 등록
 - 경고
 - MFA(Multi-Factor Authentication)



Azure AD 개념

개념	설명
ID	인증할 수 있는 개체
계정	연결된 데이터가 있는 ID
Azure AD 계정	Azure AD 또는 기타 Microsoft 클라우드 서비스를 통해 만든 ID
Azure AD 테넌트/디렉터리	<p>테넌트는 조직에서 Microsoft 클라우드 서비스 구독에 가입할 때 자동으로 만들어지는 Azure AD의 신뢰할 수 있는 전용 인스턴스입니다.</p> <ul style="list-style-type: none">• Azure AD의 추가 인스턴스를 만들 수 있습니다.• Azure AD는 ID 서비스를 제공하는 기본 제품입니다.• <i>테넌트</i>라는 용어는 단일 조직을 나타내는 Azure AD의 단일 인스턴스를 의미합니다.• 테넌트와 디렉터리는 종종 서로 교환해서 사용되는 용어입니다.
Azure 구독	Azure Cloud Services 비용을 지불하는 데 사용됩니다.

Azure Active Directory 버전

기능	무료	Microsoft 365 앱	Premium P1	Premium P2
디렉터리 개체	개체 500,000개	개체 제한 없음	개체 제한 없음	개체 제한 없음
Single Sign-On	무제한	무제한	무제한	무제한
핵심 ID 및 액세스	X	X	X	X
B2B Collaboration	X	X	X	X
O365에 대한 ID 및 액세스		X	X	X
프리미엄 기능			X	X
하이브리드 ID			X	X
고급 그룹 액세스			X	X
조건부 액세스			X	X
ID 보호				X
ID 거버넌스				X

기본 디렉터리

- 모든 계정은 기본적으로 기본 디렉터리로 로그인 된다.
- 별도로 도메인을 등록하지 않으면 onmicrosoft.com이라는 하위 도메인과 Azure에 가입할 때 사용한 메일 별칭 그리고 최상위 도메인으로 조합된 이름을 사용한다.

ex) youngwook@outlook.com

youngwookoutlook.onmicrosoft.com

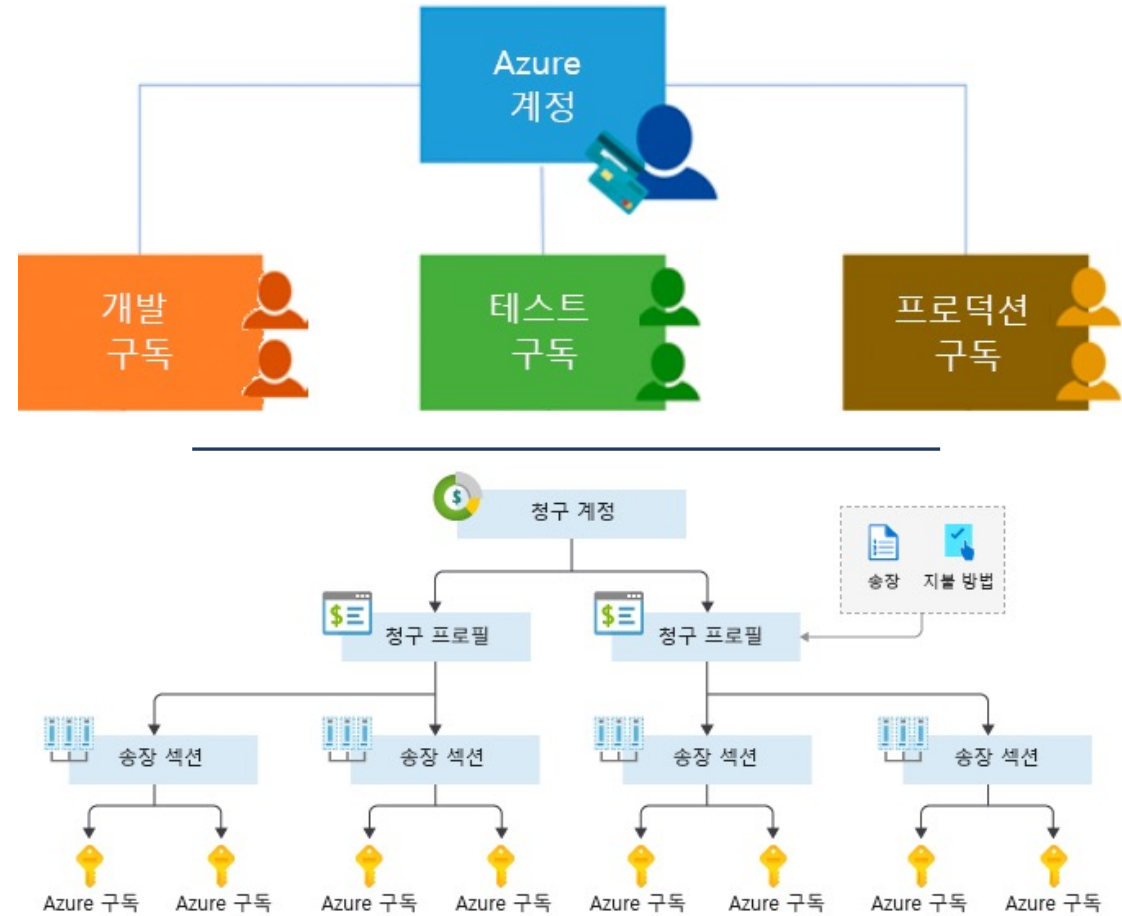
기본 디렉터리외 추가 디렉터리

- 개발이나 테스트를 위한 Azure AD의 필요
- 시스템에 따라 인증을 분리하고자 하는 경우 필요
- 필요하다면 추가 디렉터리를 추가할 수도 삭제 할 수도 있다.

실습 – 새로운 테넌트(디렉터리)의 추가

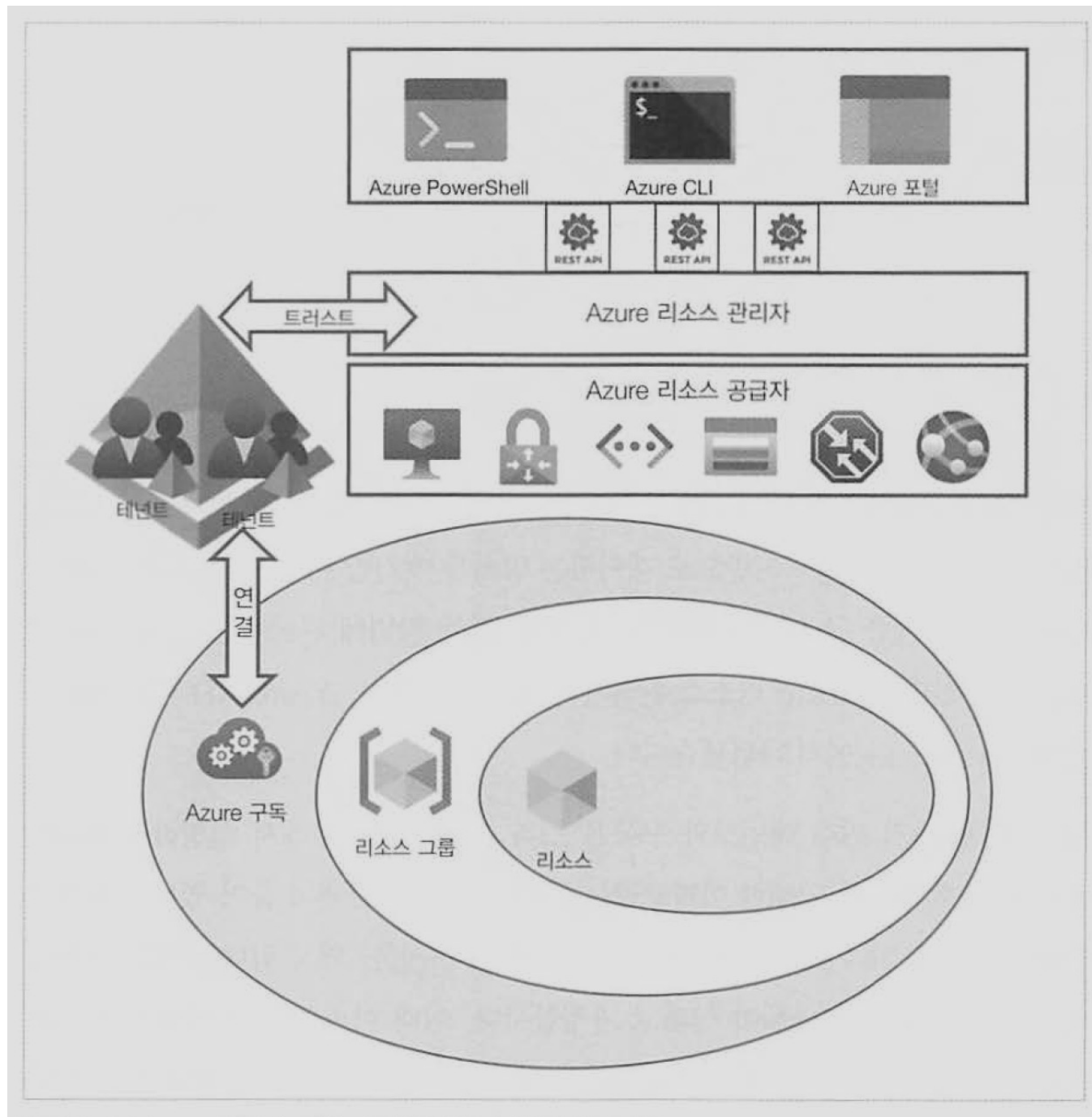
구독

- Azure 구독은 Azure 계정에 대한 액세스를 인증하고 이러한 액세스에 필요한 권한을 부여합니다.
- **청구 경계:** 각 구독에 해당하는 개별 청구 보고서와 청구서를 생성합니다.
- **액세스 제어 경계:** 사용자가 특정 구독으로 프로비전할 수 있는 리소스 액세스를 관리/제어할 수 있습니다.



실습 - 구독을 다른 테넌트로 변경하기

구독



사용자 계정

 사용자 | 모든 사용자(미리 보기) ...

(주)클라우드메이트 - Azure Active Directory

«

+ 새 사용자

+ 새 게스트 사용자

대량 작업

↺ 새로 고침

🔑 암호 재설정

🔗 Multi-Factor Authentication

🗑 사용자 삭제

☰ 열

...

모든 사용자(미리 보기)

삭제된 사용자(미리 보기)

🔑 암호 재설정

⚙ 사용자 설정

🔧 문제 진단 및 해결

활동

🔄 로그인

📄 감사 로그

🌿 대량 작업 결과

🔍 사용자 검색

+ 필터 추가

126명의 사용자를 찾았습니다.

	이름	↑↓	사용자 계정 이름 ↑↓	사용자 유형	디렉터리가 동기...	ID 발급자	회사 이름	만들기 유형
<input type="checkbox"/>	 123 456		test111_cloudmate.s...	게스트	아니요	cloudmatekorea.onmic		초대
<input type="checkbox"/>	 2clean8		2clean8_naver.com#...	게스트	아니요	cloudmatekorea.onmic		초대
<input type="checkbox"/>	 AAD DC Admin		aaddcadmin@cloud...	구성원	아니요	cloudmatekorea.onmic		
<input type="checkbox"/>	 Admin		admin@cloudmt.co.kr	구성원	아니요	cloudmatekorea.onmic		

- 모든 사용자는 계정을 소유하여야 합니다.
- 직접 생성 또는 Azure AD 계정을 게스트로 초대할 수 있습니다.
- Windows AD와 통합이 가능합니다.

사용자 계정


- 클라우드 ID: 클라우드 상에서만 존재하는 아이디로 테넌트에 추가된다.
- 게스트 사용자: 외부의 다른 클라우드 공급자에게 제공된 경우로 구글이나 페이스북 그리고 마이크로소프트에서 제공한 아이디
- 하이브리드 ID: Windows Server의 ADDS(Active Directory Domain Services)와 Azure AD를 동기화 시켜 생성한 사용자 계정

사용자 계정

성	이름	직함	역할	초기 암호
Rogers	Steve	Captain America	전역 관리자	(자동 생성)
Stark	Tony	Iron Man	사용자	(자동 생성)
Parker	Peter	Spider Man	사용자	(자동 생성)

실습 – 사용자 추가

그룹 관리

 그룹 | 모든 그룹 ...
(주)클라우드메이트 - Azure Active Directory

모든 그룹

삭제된 그룹

문제 진단 및 해결

설정

일반

만료

Naming policy

활동

+ 새 그룹

↓ 그룹 다운로드

🗑 삭제

🔄 새로 고침

|

☰ 열

|

🔍 미리 보기 기능

|

💡 피드백이 있나요?

🔑 이 페이지에는 평가에 사용할 수 있는 미리 보기가 포함되어 있습니다. 미리 보기 보기 →

🔍 그룹 검색

+ 필터 추가

	이름	개체 ID	그룹 유형	구성원 자격 유형	메일	원본
<input type="checkbox"/>	<div>20</div> 2020군장병온라...	3f02cab2-a103-4cf9-97...	Microsoft 365	할당됨	2020@cloudmt.co.kr	클라우드
<input type="checkbox"/>	<div>AD</div> AAD DC Admini...	bb3c633a-a30b-4809-8...	보안	할당됨		클라우드
<input type="checkbox"/>	<div>AD</div> AdminAgents	03f43778-1deb-4b5c-8...	보안	할당됨		클라우드
<input type="checkbox"/>	<div>AM</div> Asset Managem...	4072376f-74ca-41c2-8...	Microsoft 365	할당됨	AssetManagement@cl...	클라우드

- 사용자 계정을 그룹으로 묶어 관리할 수 있습니다.
- Microsoft 365 그룹과 보안 그룹으로 나뉩니다.
- 구성원 유형은 할당됨, 동적 사용자, 동적 디바이스로 구분됩니다.

Azure AD 권한 관리







- Azure AD를 관리할 수 있는 권한입니다.
- 사용자 계정에 Azure AD를 조작할 수 있는 권한을 부여합니다.
- 이 권한으로 Azure 리소스를 조작할 수 없습니다.
- 계정 생성, 비밀번호 초기화 등을 구성할 수 있습니다.

관리 역할

관리 역할은 Azure AD 및 기타 Microsoft 서비스에 대한 액세스 권한을 부여하는 데 사용할 수 있습니다. [자세한 정보](#)

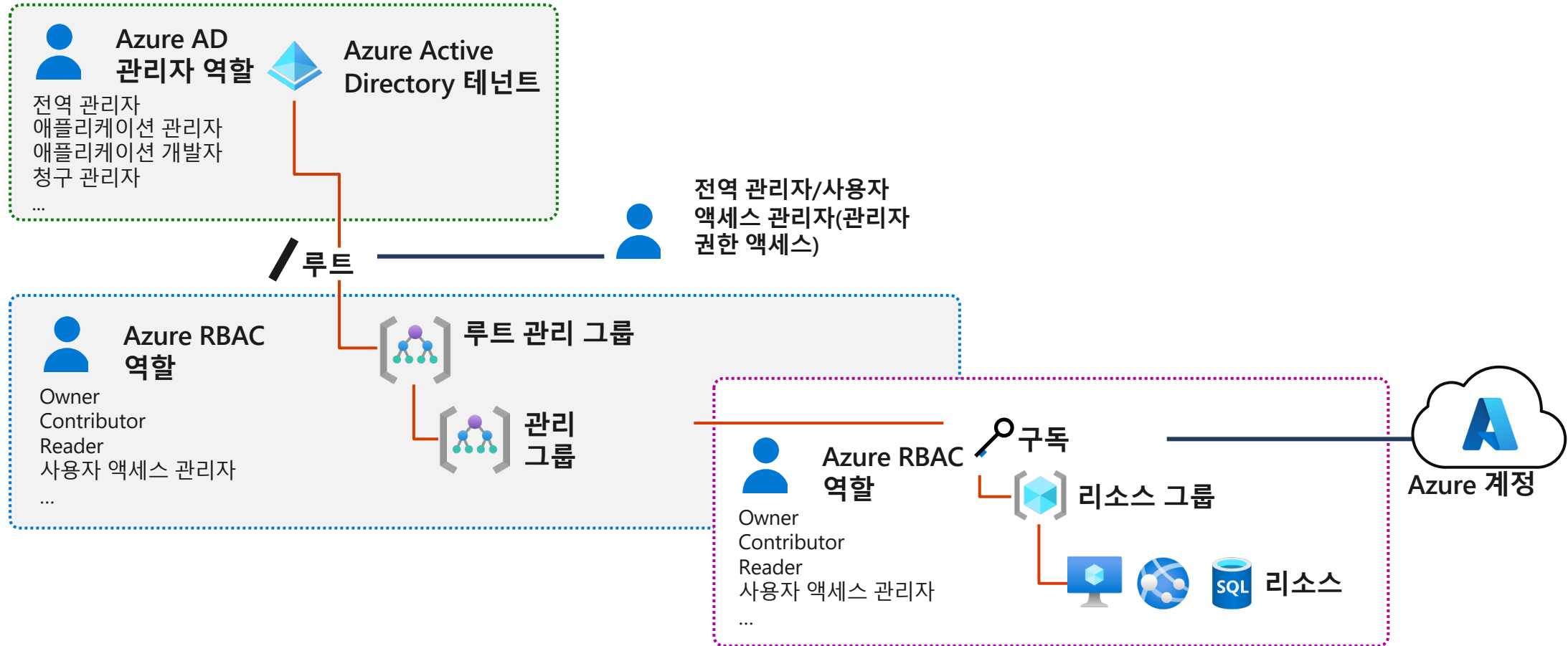
+

필터 추가

역할	↑↓	설명	유형	↑↓
<input type="checkbox"/>  검색 관리자		Microsoft Search 설정의 모든 측면을 만들고 관리...	기본 제공	...
<input type="checkbox"/>  검색 편집기		책갈피, 질문 및 답변, 위치, 평면도와 같은 편집 ...	기본 제공	...
<input type="checkbox"/>  게스트 초대자		'멤버가 게스트를 초대할 수 있음' 설정에 관계없...	기본 제공	...
<input type="checkbox"/>  고객 LockBox 액세스 승인		고객 조직 데이터에 액세스하려는 Microsoft 지원...	기본 제공	...
<input type="checkbox"/>  고급 플랫폼 관리자		Microsoft Dynamics 365, PowerApps 및 Microsoft...	기본 제공	...
<input type="checkbox"/>  공격 시뮬레이션 관리자		공격 시뮬레이션 캠페인의 모든 측면을 만들고 관...	기본 제공	...
<input type="checkbox"/>  공격 페이로드 작성자		 관리자가 나중에 시작할 수 있는 공격 페이로드를...	기본 제공	...
<input type="checkbox"/>  권한 있는 역할 관리자		Azure AD의 역할 할당 및 Privileged Identity Man...	기본 제공	...
<input type="checkbox"/>  권한 있는 인증 관리자		사용자(관리자 또는 비관리자)의 인증 메서드 정...	기본 제공	...
<input type="checkbox"/>  그룹 관리자		명명 및 만료 정책과 같은 그룹 및 그룹 설정의 모...	기본 제공	...
<input type="checkbox"/>  기술 지원팀 관리자		비관리자 및 기술 지원팀 관리자의 암호를 다시 ...	기본 제공	...
<input type="checkbox"/>  네트워크 관리자		 네트워크 위치를 관리하고 Microsoft 365 Softwar...	기본 제공	...
<input type="checkbox"/>  대금 청구 관리자		결제 정보 업데이트와 같은 일반 결제 관련 작업...	기본 제공	...
<input type="checkbox"/>  데스크톱 분석 관리자		데스크톱 관리 도구 및 서비스에 액세스하고 관리...	기본 제공	...
<input type="checkbox"/>  도메인 이름 관리자		 클라우드 및 온-프레미스에서 도메인 이름을 관리...	기본 제공	...
<input type="checkbox"/>  디렉터리 쓰기 권한자		기본 디렉터리 정보를 읽고 쓸 수 있습니다. 애플...	기본 제공	...
<input type="checkbox"/>  디렉터리 읽기 권한자		기본 디렉터리 정보를 읽을 수 있습니다. 일반적...	기본 제공	...

실습 - 그룹

Azure 권한 구성



역할 기반 액세스 제어(RBAC)

- RBAC(Role Based Access Control)
- 액세스 할 수 있는 영역과 Azure 리소스, 리소스 그룹 단위로 액세스 제어가 가능하다.
- 사전에 정의된 RBAC의 역할을 제공한다.

역할 기반 액세스 제어(RBAC)

- 소유자: 모든 권한을 가지고 있으며 다른 사용자 계정에 액세스 권한을 할당할 수도 있다.
- 기여자: 할당된 사용 권한 내에서 완전히 관리 가능하지만 다른 사용자 계정에 액세스 권한을 할당 할 수 없다.
- 독자: 모든 Azure 리소스를 확인 할 수 있는 권한만 있다.

실습 – RBAC