

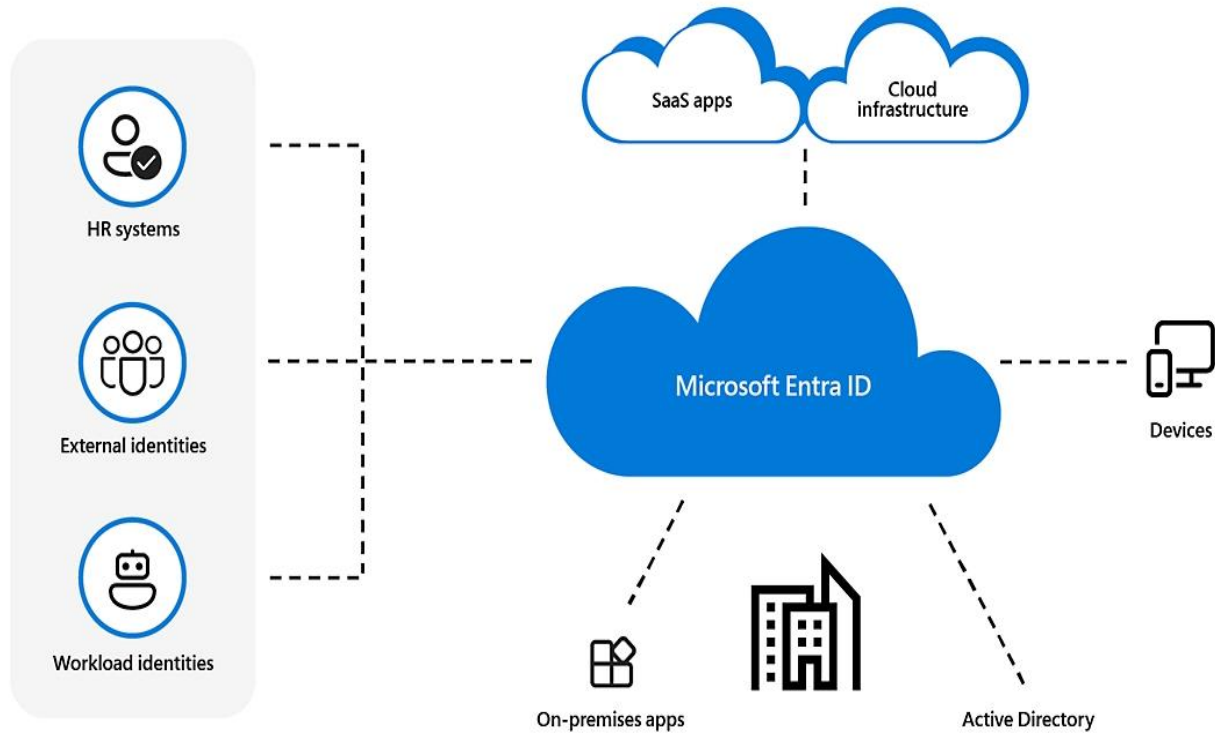


## 4장 Azure 사용자와 그룹, 액세스 관리

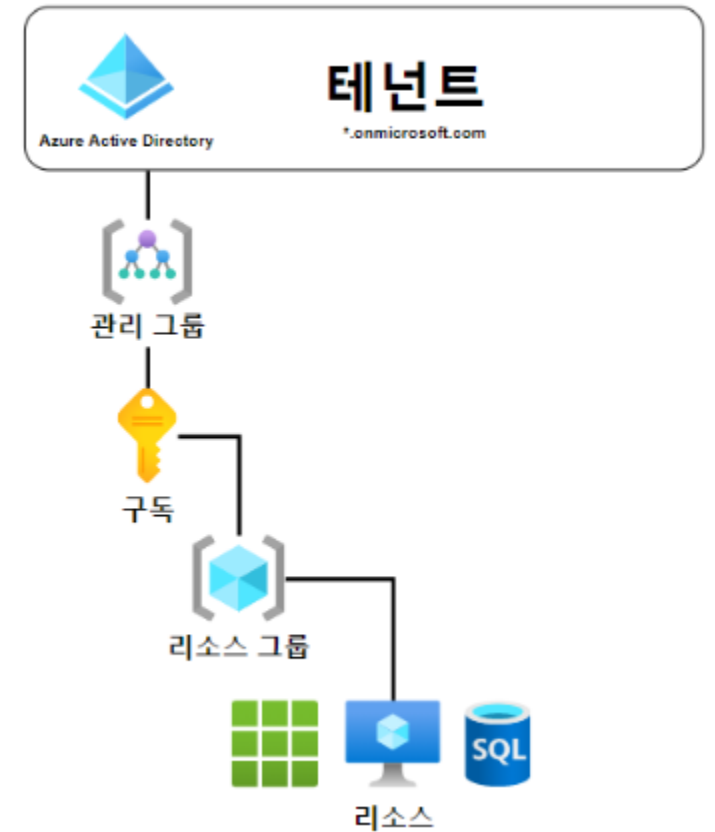
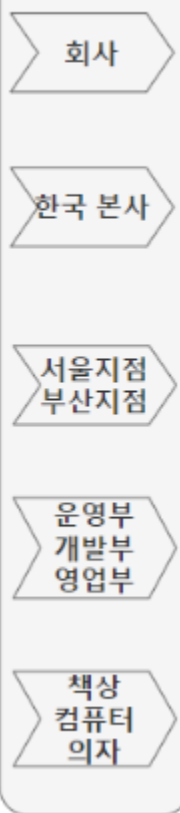


## 4장 개요

팀원들과 협업 하는 환경에서 사용자와 그룹 관리, 그리고 역할에 따른 액세스 제어의 핵심인 **Microsoft Entra ID**와 **구독**



### [예시]





## 1. Microsoft Entra ID와 구독

- Microsoft Entra ID는 팀의 구성원이 로그인 하고 권한에 따라 리소스를 액세스할 수 있게 해주는 Microsoft Azure의 ID와 액세스 관리 서비스입니다.
- 구독은 여러분이 만든 리소스가 존재하는 논리적인 공간이면서 리소스의 사용 비용을 지불하는 주체
- 보안주체 : 사용자와 그룹, 디바이스, 애플리케이션



## 1. Microsoft Entra ID

- 태넌트(tenant) – 사전적인 의미는 세입자나 임차인을 뜻하지만, 공간을 사용하는 사용자/그룹 등을 대표하는 용어
- Microsoft Entra ID 테넌트는 하나 이상의 구독과 연결 가능
- Microsoft Entra ID는 사용자와 그룹, 디바이스, 애플리케이션 보안 주체의 관리, 인증 및 권한 관리를 제공하며 Azure에서 만든 리소스나 외부 애플리케이션과 서비스에 대한 액세스 제어를 제공합니다.



# 1. Microsoft Entra ID

Microsoft Azure

연암공과대학교산학협력단 | 개요

개요

미리 보기 기능

문제 진단 및 해결

관리

사용자

그룹

External Identities

역할 및 관리자

관리 단위

위임된 관리자 파트너

엔터프라이즈 애플리케이션

디바이스

앱 등록

Identity Governance

애플리케이션 프록시

사용자 지정 보안 특성

라이선스

테넌트 간 동기화

Microsoft Entra Connect

사용자 지정 도메인 이름

모바일(MDM 및 WIP)

암호 재설정

회사 브랜딩

사용자 설정

검색 기록

기본

microsoft entra

구독

태그

리소스 그룹

최근 서비스

Microsoft Entra ID

구독

태그

리소스 그룹

내 리소스

리소스 가드

최근 리소스

test

helloazure

공용 IP 주소

리소스 그룹

모든 구독을 검색하는 중입니다.

피드백 제공

알림

활동 로그의 더 많은 이벤트 →

모두 해제

태그를 할당했습니다.

태그 2개가 리소스 1개에 할당되었습니다.

42분 전

배포 성공

리소스 그룹 'helloazure'에 대한 'PublicIPaddress-ARM' 배포에 성공했습니다.

리소스로 이동

대시보드에 고정

49분 전

기본 정보

이름

연암공과대학교

테넌트 ID

7d06fe6f-ff85-4

주 도메인

styc.ac.kr

라이선스

Microsoft Entra

경고

Microsoft Entra Connect v1 사용 중지

2023년 10월~2024년 3월 사이에 Microsoft Entra Connect(이전의 AAD Connect)의 모든 버전 1.x 빌드 작동이 곧 중지됩니다. 클라우드 동기화 또는 Microsoft Entra Connect v2.x로 이동해야 합니다.

자세히 알아보기

이제 Azure AD가 Microsoft Entra ID입니다.

Microsoft Entra ID는 Azure Active Directory의 새 이름입니다. 사용자가 취해야 할 조치는 없습니다.

자세히 알아보기

예정된 MFA 서버 사용 중단

서비스 영향을 방지하려면 2024년 9월까지 MFA 서버에서 Microsoft Entra 다단계 인증으로 마이그레이션하세요.

자세히 알아보기

전역 관리자

6

Microsoft는 전역 관리자를 5명 미만으로 권장합니다.

권한 있는 역할 할당 보기

내 피드



# 1. Microsoft Entra ID

Microsoft Azure

리소스, 서비스 및 문서 검색(G+I)

대시보드 > 연암공과대학교산학협력단

연암공과대학교산학협력단 | 속성

Microsoft Entra ID

위임된 관리자 파트너

엔터프라이즈 애플리케이션

디바이스

앱 등록

Identity Governance

애플리케이션 프록시

사용자 지정 보안 특성

라이선스

테넌트 간 동기화

Microsoft Entra Connect

사용자 지정 도메인 이름

모바일(MDM 및 WIP)

암호 재설정

회사 브랜딩

사용자 설정

속성

보안

모니터링

로그인 로그

감사 로그

프로비저닝 로그

상태(미리 보기)

Log Analytics

진단 설정

통합 문서

<<

>>

이름

국가 또는 지역

데이터 위치

알림 언어

테넌트 ID

기술 담당자

전역 개인 정보 보호 연락처

개인정보처리방침 URL

Azure 리소스에 대한 액세스 관리

은새 조(22371025@st.yc.ac.kr)은(는) 이 테넌트의 모든 Azure 구독과 관리 그룹에 대한 액세스를 관리할 수 있습니다.  
[자세히 알아보기](#)

☐ 아니요

보안 기본값

보안 기본값은 Microsoft에서 권장하는 기본 ID 보안 메커니즘입니다. 이러한 권장 사항을 사용하도록 설정하면 조직에 자동으로 적용됩니다. 일반적인 ID 관련 공격으로부터 관리자와 사용자를 더 잘 보호합니다.  
[자세히 알아보기](#)

⚠ 조직이 보안 기본값으로 보호되지 않습니다.  
[보안 기본값 관리](#)

저장

취소



# 1. Microsoft Entra ID

[대시보드](#) > [연암공과대학교산학협력단](#) | [개요](#) >



## 테넌트 관리 ...

[+ 만들기](#) [↺ 새로 고침](#) [☰ 열](#) | [↔ 전환](#) [🗑 삭제](#) [⊖ 테넌트 나가기](#) [✓ 기본 테넌트 만들기](#) [① 추가 정보](#) | [🗣 피드백이 있나요?](#)

현재 테넌트: 연암공과대학교산학협력단

[+ 필터 추가](#)

1/1개 결과 표시

<input type="checkbox"/> 조직 이름	↑↓ 도메인 이름	↑↓ 테넌트 유형	↑↓ 조직 ID	↑↓ 즐겨찾기	↑↓
<input type="checkbox"/>  연암공과대학교산학협력단 (기본값)	st.yc.ac.kr	Microsoft Entra ID	7d06fe6f-ff85-48d3-a9ee-c40fcfcc7f72		

[대시보드](#) > [연암공과대학교산학협력단](#) | [개요](#) > [테넌트 관리](#) >

## 테넌트 만들기 ...

Microsoft Entra ID

[\\* 기본](#) [\\* 구성](#) 검토 + 만들기

디렉터리 세부 정보

새 디렉터리 구성

조직 이름 * ①	<input type="text" value="Avengers"/>	✓
초기 도메인 이름 * ①	<input type="text" value="avengersjes"/>	✓
	avengersjes.onmicrosoft.com	
위치 ①	<input type="text" value="한국"/>	▼

✓ 지리적 위치 - 아시아 태평양

위에서 선택한 위치에 따라 Microsoft Entra ID가 Core Store 데이터만 저장할 지리적 위치가 결정됩니다. Microsoft가 귀하의 Microsoft Entra ID 데이터를 저장하거나 처리할 위치를 결정하려면 [Microsoft Entra ID 데이터 상주](#)를 참조하세요.



# 1. Microsoft Entra ID

홈 > Avengers | 개요 >

## 테넌트 관리 ...

+ 만들기   ↺ 새로 고침   ≡ 열 |   ⇄ 전환   🗑 삭제   ➖ 테넌트 나가기   ✓ 기본 테넌트 만들기   ⓘ 추가 정보 |   👤 피드백이 있나요?

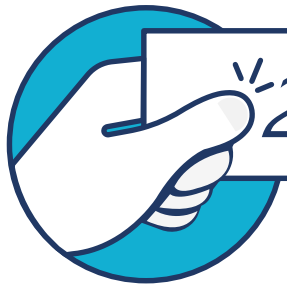
현재 테넌트: Avengers

  + 필터 추가

2/2개 결과 표시

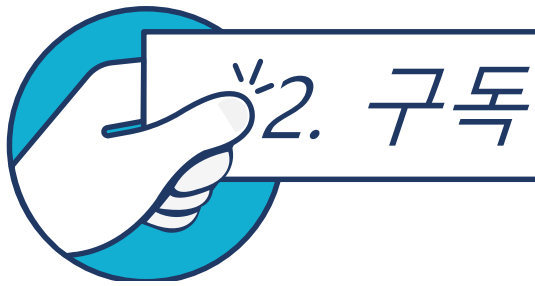
<input type="checkbox"/> 조직 이름	↑↓ 도메인 이름	↑↓ 테넌트 유형	↑↓ 조직 ID	↑↓ 즐겨찾기	↑↓
<input type="checkbox"/>  Avengers (기본값)	avengersjes.onmicrosoft.com	Microsoft Entra ID	77d2064b-2864-4e80-bb8e-69151b5eaf97	☆	
<input type="checkbox"/>  연암공과대학교산학협력단	styc.ac.kr	Microsoft Entra ID	7d06fe6f-ff85-48d3-a9ee-c40fcfcc7f72	☆	





## 2. 구독

- Azure 구독은 계정과 연결된 클라우드 리소스의 논리적인 관리 단위이며 비용을 청구하는 단위입니다.
- Azure 구독은 반드시 Microsoft Entra ID 테넌트에 1대1로 연결되어야 한다.



대시보드 >

## Azure for Students ...

구독 취소 | 이름 바꾸기 | 디렉터리 변경 | 피드백

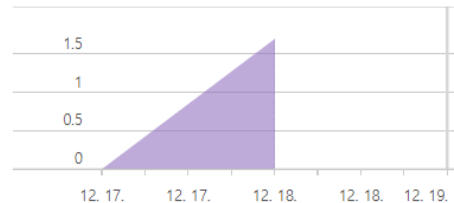
### 기본 정보

구독 ID : 6f3c9a43-87df-4f23-8687-40a455d9b69b  
디렉터리 : 연암공과대학교산학협력단 (st.yc.ac.kr)  
상태 : 활성  
부모 관리 그룹 : ---

구독 이름 : [Azure for Students](#)  
내 역할 : 소유자  
계획 : Azure 플랜  
보안 점수 : [사용할 수 없음](#)

클립보로 복사

### 지출 비율 및 예측



현재 비용  
₩1.69

세부 정보 보기

### 리소스별 비용



세부 정보 보기

### 리소스 수를 기준으로 한 상위 제품



### Azure Defender 검사

### 사용량별 인기 무료 서비스

한도 내에서 사용됨 1/2 0  
제한 초과 0

서비스 사용량

Azure Cosmos DB, Free Data Stored 0 / 25 (1 GB/Month)

Azure Cosmos DB, Free 100 RU/s 0 / 2976 (1/Hour)

Storage, Files, LRS Data Stored 0 / 100 (1 GB/Month)

Storage, Premium Page Blob, P6 Disks 0 / 2.2 (1/Month)

Storage, Standard HDD

## 디렉터리 변경

×

디렉터를 변경해도 구독에 대한 청구 소유권은 변경되지 않습니다. 청구 소유권이 다른 사용자에게 양도될 때까지 원래 디렉터를 삭제할 수 없습니다. [자세히](#)

공급업체  
연암공과대학교산학협력단 (st.yc.ac.kr)

보조 사이트

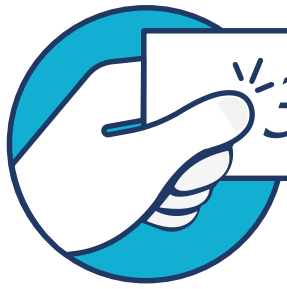
디렉터리 선택

디렉터를 변경하면 일부 리소스가 전송되지 않는다는 점, 예를 들어 모든 Azure 역할 기반 액세스 제어 할당이 삭제되고(영향을 받는 사용자 참조) 시스템/사용자가 할당한 관리 ID가 무효화되고 대상 디렉터리에 전송되지 않음을 이해합니다. [자세히](#)



변경

취소



### 3. 사용자와 그룹

- Microsoft Entra ID 테넌트에 사용자 계정을 등록하여 액세스 제어 가능 하지만 사용자 계정만으로 권한을 제어하기 보다는 사용자 그룹을 사용할 권한관리를 구현해야 한다.
- 사용자 계정 = Microsoft Entra ID 테넌트에서 만든 사용자 개체
- 처음 가입시 관리자 계정으로 생성됨



### 3. 사용자와 그룹

대시보드 > 연암공과대학교산학협력단 | 사용자 >



사용자

연암공과대학교산학협력단 - Microsoft Entra ID



검색



새 사용자



사용자 다운로드



대량 작업



새로 고침



보기 관리



삭제



사용자별 MFA



피드백이 있나요?



모든 사용자



감사 로그



로그인 로그



문제 진단 및 해결

관리



삭제된 사용자



암호 재설정



사용자 설정



대량 작업 결과

문제 해결 및 지원



새 지원 요청



Azure Active Directory는 이제 Microsoft Entra ID입니다.

조은



필터 추가

사용자 1명 찾음



표시 이름 ↑

사용자 계정 이름 ↑

사용자 유형

온-프레미스 동...

ID

회사 이름

만들기 유형



조은 조은새

22371025@st.yc.ac.kr

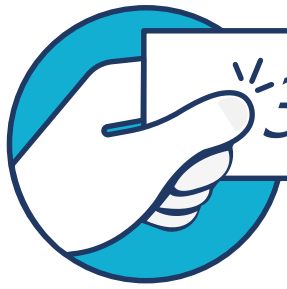


구성원

아니요

ycstu.onmicrosoft.com

테넌트를 만들면서 자동으로 추가된 Azure 계정



### 3. 사용자와 그룹


- Azure에서는 3가지 유형의 사용자 계정을 등록할 수 있다.
  - 클라우드 ID : Microsoft Entra ID 상에서만 존재하는 계정
  - 게스트 사용자 : 사용자가 계정이 Azure 외부의 신뢰할 수 있는 다른 ID 공급자나 다른 Microsoft Entra ID 테넌트에서 제공된 경우 ex) 구글, 페이스북
  - 하이브리드 ID : 기업 내의 ID 공급자인 Windows 서버 ADDS 등과 Microsoft Entra ID를 동기화시켜 생성한 사용자 계정





### 3. 사용자와 그룹


홈 > Avengers | 사용자 >

 사용자 ...  
Avengers - Microsoft Entra ID


 모든 사용자


 감사 로그


 로그인 로그


 문제 진단 및 해결

관리


 삭제된 사용자

 암호 재설정


 사용자 설정

 대량 작업 결과

문제 해결 및 지원

 새 지원 요청

 새 사용자  사용자 다운로드  대량 작업  새로 고침  보기 관리  삭제  사용자별 MFA  피드백이 있나요?

 [Azure Active Directory는 이제 Microsoft Entra ID입니다.](#)

 필터 추가

사용자 1명 찾음

<input type="checkbox"/>	표시 이름 ↑	사용자 계정 이름 ↑↓	사용자 유형	온-프레미스 동...	ID	회사 이름	만들기 유형
<input type="checkbox"/>	은조 은새 조	22371025_st.yc.ac.kr#EXT...	 구성원	아니요	ExternalAzureAD		



### 3. 사용자와 그룹

홈 > Avengers | 사용자 > 사용자 >

## 새 사용자 만들기 ...

조직에서 새 내부 사용자 만들기

기초    속성    할당    검토 + 만들기

최대 20개의 그룹 또는 역할 할당을 구성합니다. 최대 1개의 관리 단위에만 사용자를 추가할 수 있습니다.




+ 관리 단위 추가    + 그룹 추가    + 역할 추가

표시할 할당이 없습니다.

## 디렉터리 역할

**i** 사용자 지정 역할을 사용자에게 할당하려면 조직에 Microsoft Entra ID Premium P1 또는 P2가 필요합니다.

이 사용자에게 할당하려는 관리자 역할을 선택하세요. [자세한 정보](#)

역할	↑↓	설명
<input checked="" type="checkbox"/>  전역 관리자		Microsoft Entra ID를 사용하는 Microsoft Entra ID 및 Microsoft 서비스의 모든 측면을 관리할 수 있습니다.
<input type="checkbox"/>  전역 보안 액세스 관리자		퍼블릭 및 프라이빗 엔드포인트에 대한 액세스 관리를 포함해 Microsoft Entra 인터넷 액세스 및 Microsoft Entra 개인 액세스의 모든 측면을 만들고 관리합니다.
<input type="checkbox"/>  전역 읽기 권한자		전역 관리자가 할 수 있는 모든 내용을 읽을 수 있지만 업데이트할 수는 없습니다.

검토 + 만들기

< 이전

다음: 검토 + 만들기 >

선택




### 3. 사용자와 그룹


홈 > Avengers | 사용자 >


 사용자 ...  
Avengers - Microsoft Entra ID




검색 < + 새 사용자 v ↓ 사용자 다운로드 대량 작업 v 새로 고침 보기 관리 v 삭제 사용자별 MFA 피드백이 있나요?

 모든 사용자


 [Azure Active Directory는 이제 Microsoft Entra ID입니다.](#)

 감사 로그

검색 필터 추가


 로그인 로그


3명의 사용자를 찾았습니다.


 문제 진단 및 해결


<input type="checkbox"/>	표시 이름 ↑	사용자 계정 이름 ↕	사용자 유형	온-프레미스 동...	ID	회사 이름	만들기 유형
<input type="checkbox"/>	 goodbird	gjsl1945_naver.com#EXT#...	 게스트	아니요	avengersjes.onmicrosoft.com		초대
<input type="checkbox"/>	 Steve Rogers	CaptinAmerica@avengers...	 구성원	아니요	avengersjes.onmicrosoft.com		
<input type="checkbox"/>	 은조 은새 조	22371025_st.yc.ac.kr#EXT#...	 구성원	아니요	ExternalAzureAD		

관리


 삭제된 사용자

 암호 재설정

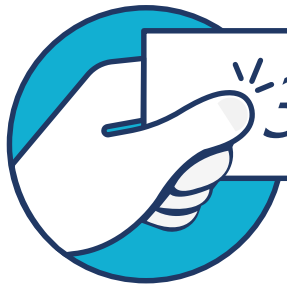
 사용자 설정

 대량 작업 결과

문제 해결 및 지원

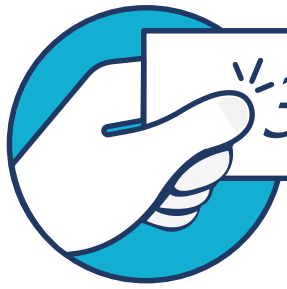
 새 지원 요청





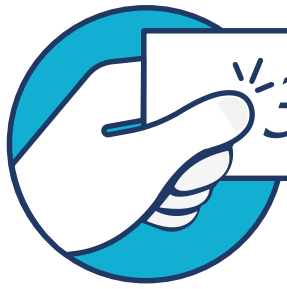
### 3. 사용자와 그룹

- 사용자가 많아지면 사용자 단위로 권한을 관리하는 것은 어렵다.
- 그룹을 통해 리소스에 권한을 할당하고 그룹 멤버십을 관리해 사용자에게 권한을 부여하거나 제거하는 방식이 바람직하다.



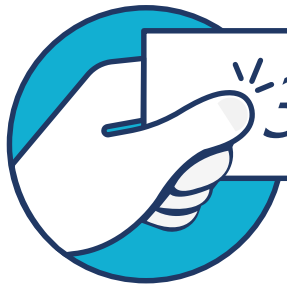
### 3. 사용자와 그룹

- 보안그룹
  - 그룹으로 멤버십을 구성하면 Azure의 구독이나 리소스 그룹, 개별 리소스의 액세스를 관리할 수 있다.
- Microsoft 365
  - Exchange의 공유 사서함과 일정, 파일 공유, SharePoint 사이트 등에 대한 액세스 권한을 부여한다.



### 3. 사용자와 그룹

- 사용자를 그룹에 추가해 멤버십을 할당하는 방식에는 정적 방식과 동적 방식이 있다. (프리티어는 정적만가능)
- 동적 사용자 : 동적 규칙을 기반으로 규칙 요구사항을 만족하면 멤버십을 부여하고 만족하지 않으면 멤버십 제거
- 동적 디바이스 : 디바이스의 특성 값에 따라 시스템이 동적 그룹 규칙을 기반으로 디바이스 등록/삭제



### 3. 사용자와 그룹

- 그룹에 직접 사용자 계정을 추가하는 3가지 방법
- 할당됨
  - 그룹을 만들때 [p148]처럼 구성원 섹션에서 멤버추가
  - 그룹을 만든 다음 그룹 계정 정보에서 사용자 추가하기
  - 사용자 계정 정보에서 그룹 선택하기



### 3. 사용자와 그룹

홈 > Avengers | 그룹 > 그룹 | 모든 그룹 >

## 새 그룹 ...

피드백이 있나요?

그룹 유형 \* ①

보안

그룹 이름 \* ①

SHEILD

그룹 설명 ①

국제평화

구성원 자격 유형 ①

할당됨

소유자

소유자가 선택되지 않음

구성원

선택한 멤버가 없음

## 구성원 추가

① 검색하는 내용이 보이지 않으면 필터를 변경하거나 추가해 보세요.

검색 ①



24 results found

모두 사용자 그룹 디바이스 엔터프라이즈 애플리케이션

	이름	유형	사용자 주체 이름
<input checked="" type="checkbox"/>	은새 조	사용자	22371025@st.yc.ac.kr
<input type="checkbox"/>	goodbird	사용자	gjsl1945@naver.com
<input type="checkbox"/>	Steve Rogers	사용자	CaptinAmerica@avengersjes.onmicrosoft.com

선택함(1개)

다시 설정



은새 조  
22371025@st.yc.ac.kr




만들기

선택



## 3. 사용자와 그룹

홈 > 그룹 | 모든 그룹 > SHEILD

 **SHEILD** | 소유자 ...  
그룹

개요

문제 진단 및 해결

관리

속성

구성원

**소유자**

역할 및 관리자

관리 단위

그룹 구성원 자격

애플리케이션

라이선스

Azure 역할 할당

활동

Privileged Identity Management

액세스 검토

감사 로그

대량 작업 결과

+ 소유자 추가 >

이름으로 검색

이름

소유자를 찾을 수 없음

### 소유자 추가

검색하는 내용이 보이지 않으면 필터를 변경하거나 추가해 보세요.

검색



3 results found

**모두** 사용자

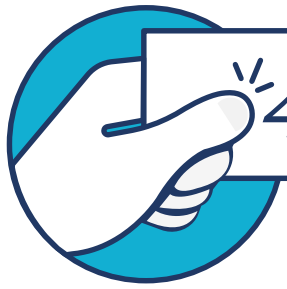
	이름	유형	세부 정보
<input type="checkbox"/>	 은새 조	사용자	22371025@st.yc.ac.kr
<input type="checkbox"/>	 goodbird	사용자	gjsl1945@naver.com
<input type="checkbox"/>	 Steve Rogers	사용자	CaptinAmerica@avengersjes.onmicrosoft.com

선택

소유자(0)

[다시 설정](#)

소유자가 선택되지 않음



## 4. 역할 기반 액세스 제어(RBAC)

- 기업에서 클라우드를 사용할 경우 조직 구성원이 각자의 역할에 따라 클라우드의 리소스를 액세스해야 하는 기능이 반드시 필요
- RBAC를 사용하면 사용자가 액세스할 수 있는 영역과 Azure 리소스, 이 리소스로 할 수 있는 작업을 지정할 수 있다.



## 4. 역할 기반 액세스 제어(RBAC)

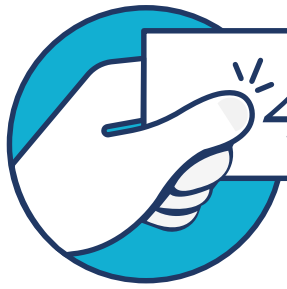
- Microsoft Entra ID와 Azure RBAC의 차이
- Microsoft Entra ID 역할은 사용자나 그룹, 도메인과 같은 테넌트 관리의 사용 권한 제어에 사용
- Azure RBAC는 관리 그룹과 구독, 구독에서 만드는 Azure 리소스 관리의 사용 권한을 제어한다.





## 4. 역할 기반 액세스 제어(RBAC)

- Azure RBAC 기본 역할
  - 모든 리소스에 사용할 수 있는 역할
  - 특정 Azure 리소스 유형만 관리할 수 있는 역할
  - 사용자 액세스만 관리할 수 있는 역할
- 모든 Azure 리소스 유형을 관리할 수 있는 역할은 소유자, 기여자, 독자입니다.



## 4. 역할 기반 액세스 제어(RBAC)

- **소유자** : 할당된 사용 권한 제어 범위 내에서 모든 Azure 리소스를 완전히 관리할 수 있는 권한을 가지며 다른 사용자 계정에 액세스 권한을 할당할 수도 있다.
- **기여자** : 모든 리소스 관리는 가능하지만 다른 사용자 계정에 액세스 권한 할당 불가능
- **독자** : 할당된 사용 권한 제어 범위 내에서 모든 Azure 리소스의 정보만 확인할 수 있으며 변경할 수는 없다.



## 4. 역할 기반 액세스 제어(RBAC)

Azure for Students | 액세스 제어(IAM) ☆ ...

구독

검색

<<

+ 추가 ↓ 역할 할당 다운로드 ≡ 열 편집 ↺ 새로 고침 ✕ 제거 👤 사용자 의견

개요

활동 로그

액세스 제어(IAM)

태그

문제 진단 및 해결

보안

이벤트

비용 관리

비용 분석

비용 경고

예산

관리자 권장 사항

청구

청구 프로필 청구서

설정

프로그래밍 방식 배포

청구 속성

리소스 그룹

리소스

미리 보기 기능

사용량 및 할당량

정책

관리 인증서

액세스 권한 확인 역할 할당 역할 거부 할당 클래식 관리자

내 액세스

이 리소스에 대한 내 액세스 수준 보기

내 액세스 보기

액세스 권한 확인

사용자, 그룹, 서비스 보안 주체 또는 관리 ID가 이 리소스에 대해 보유한 액세스 권한 수준을 검토하세요. [자세한 정보](#)

액세스 권한 확인

이 리소스에 액세스 권한 부여

역할을 할당하여 리소스에 대한 액세스 권한을 부여합니다.

[자세한 정보](#)

역할 할당 추가

이 리소스에 대한 액세스 권한 보기

이 리소스와 기타 리소스에 대한 액세스 권한을 부여하는 역할 할당을 봅니다.

[자세한 정보](#)

보기

거부 할당 보기

이 범위에서 특정 작업에 대한 액세스가 거부된 역할 할당을 봅니다.

[자세한 정보](#)

보기

사용자 지정 역할 만들기

조직의 특정 요구 사항을 충족하는 고유한 권한 세트를 사용하여 Azure 리소스에 대한 사용자 지정 역할을 만듭니다.

[자세한 정보](#)

추가