한국 마이크로소프트

Microsoft Technical Trainer

Enterprise Skills Initiative

AZ-104. LAB02A

구독 및 RBAC 관리

이 문서는 Microsoft Technical Trainer팀에서 ESI 교육 참석자분들에게 제공해 드리는 문서입니다.

Microsoft Technical Trainer

Microsoft

요약

이 내용들은 표시된 날짜에 Microsoft에서 검토된 내용을 바탕으로 하고 있습니다. 따라서, 표기된 날짜 이후에 시장의 요구사항에 따라 달라질 수 있습니다. 이 문서는 고객에 대한 표기된 날짜 이후에 변화가 없다는 것을 보증하지 않습니다.

이 문서는 정보 제공을 목적으로 하며 어떠한 보증을 하지는 않습니다.

문서 작성 연혁

날짜	버전	작성자	변경 내용
2021.11.17	1.0.0	우진환	LAB02A 작성
2022.10.02	1.1.0	우진환	Azure 포털 변경 사항 적용
2023.02.10	1.2.0	우진환	Cloudslice 변경 사항 적용
2023.05.30	1.3.0	우진환	Cloudslice 변경 사항 적용

목차

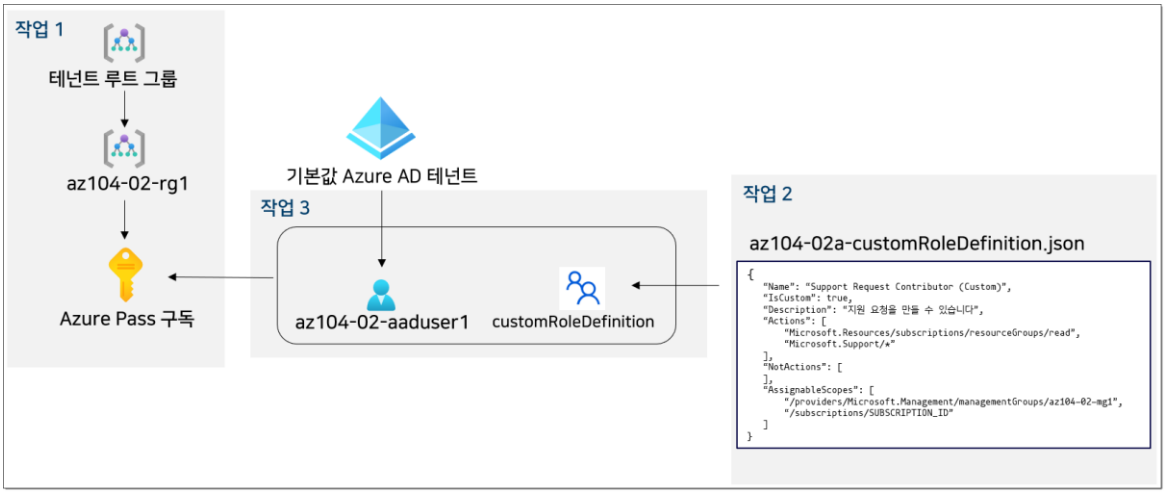
이 실습에서는 Azure Active Directory(Azure AD) 사용자를 만들고, 사용자 지정 Azure RBAC(역할 기반 액세스 제어) 역할을 만들고, 해당 역할을 Azure AD 사용자에게 할당하기 위한 사용 권한이 필요합니다.

실습 시나리오

Contoso에서 Azure 리소스 관리를 개선하기 위해 다음 기능을 구현하는 업무를 맡았습니다.

- Contoso의 Azure 구독에 관리 그룹을 사용합니다.
- 지원 요청을 제출할 수 있는 사용자 권한을 부여합니다. 이 사용자의 권한은 지원 요청 티켓을 만들고 리소스 그룹을 보는 것으로 한정됩니다.

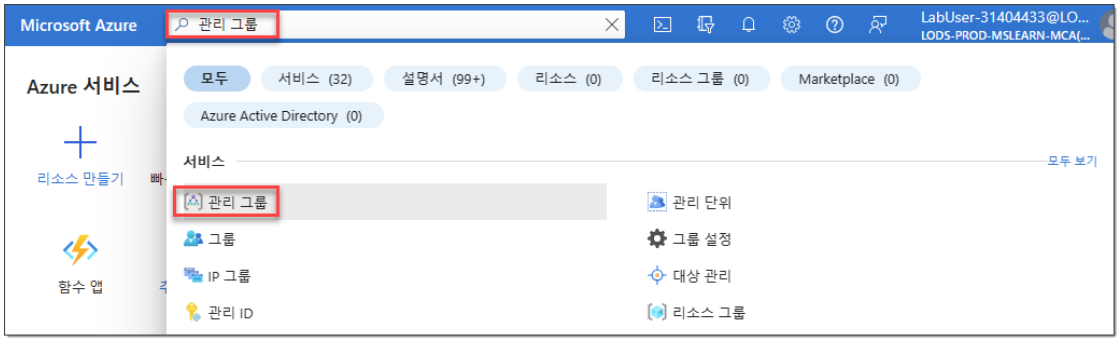
아키텍처 다이어그램



TASK 01. 관리 그룹 구현

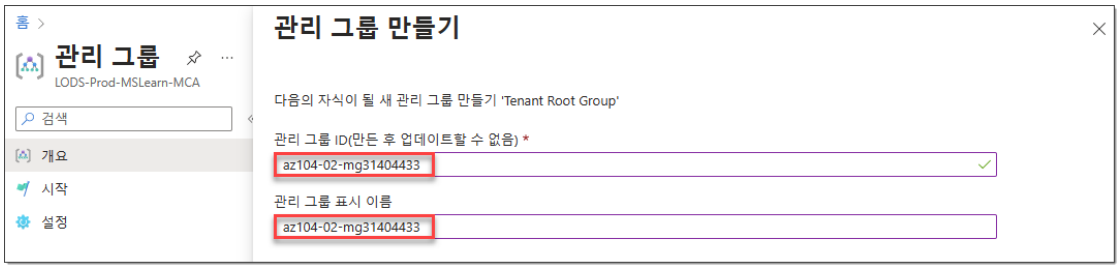
이 작업에서는 관리 그룹을 만들고 구성합니다.

1. Azure 포털의 검색창에서 "관리 그룹"을 검색하고 검색된 [관리 그룹]을 클릭합니다.

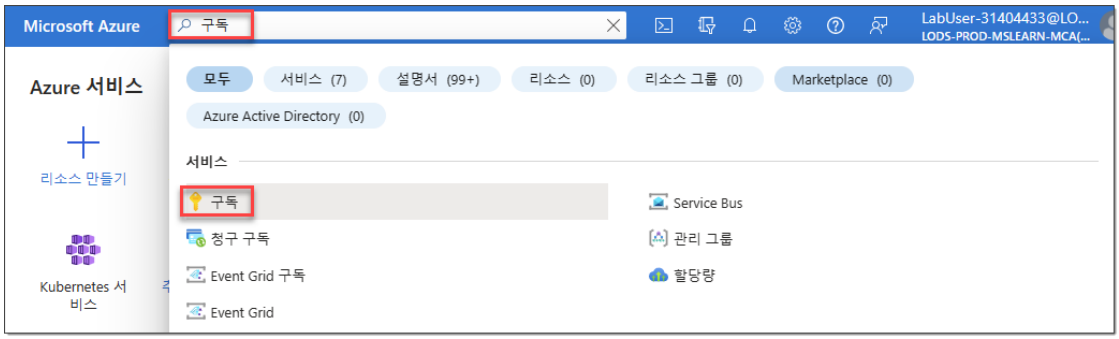


2. [관리 그룹] 블레이드의 [개요]에서 [만들기]를 클릭합니다.

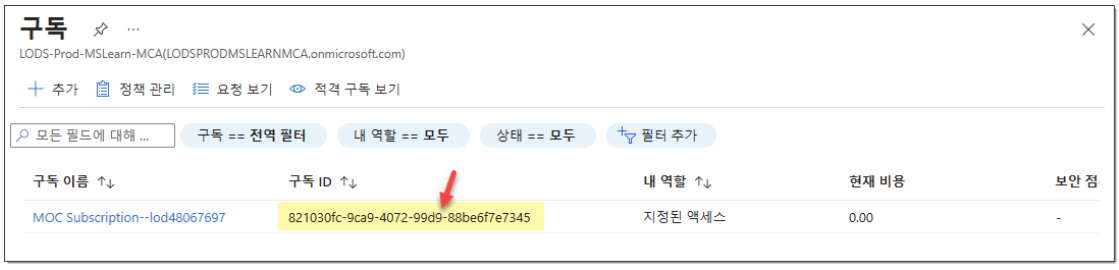
3. [관리 그룹 만들기] 창에서 관리 그룹 ID와 관리 그룹 표시 이름에 모두 "`az104-02-mg<xxxxxxxxx>`"으로 입력한 후 [Submit]을 클릭합니다. `<xxxxxxxxx>`는 로그인 계정에 포함되어 있는 8자리 숫자입니다.



4. Cloudslice 실습에서는 새로 만든 관리 그룹에 구독을 추가할 수 없습니다. 프로덕션 환경에서는 위와 같은 방법으로 만든 관리 그룹에 구독을 추가하여 관리할 수 있습니다.
5. Azure 포털의 검색창에서 "구독"을 검색한 후 클릭합니다.



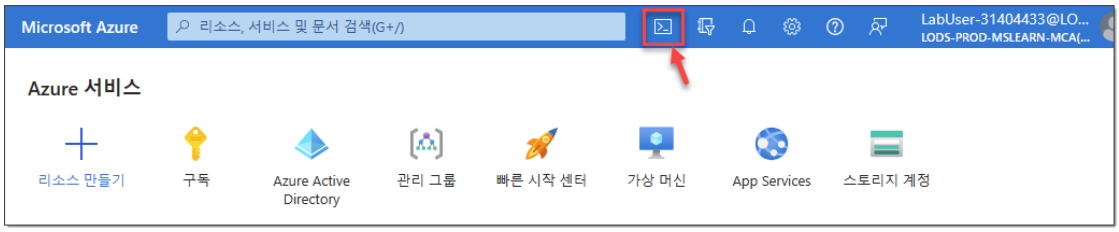
6. [구독] 블레이드에서 표시되는 자신의 "구독 ID"를 메모장에 복사합니다.



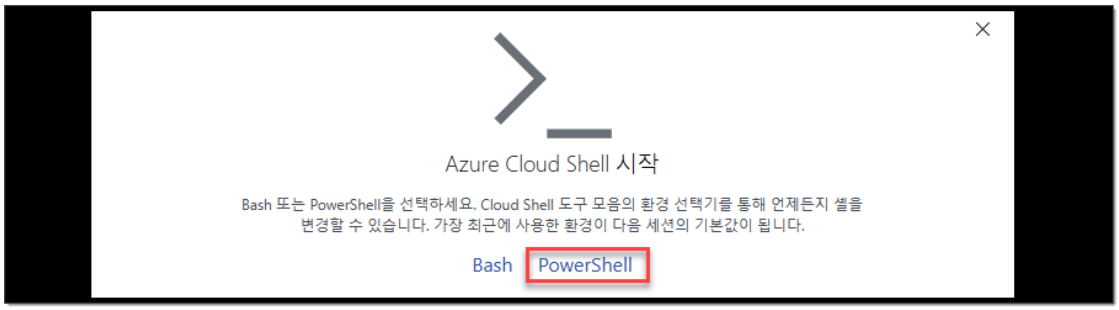
TASK 02. 사용자 지정 RBAC 역할 만들기

이 작업에서는 사용자 지정 RBAC 역할 정의를 만듭니다.

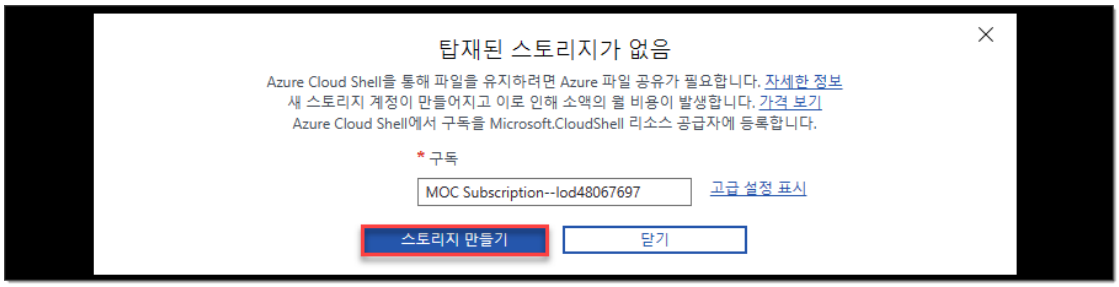
1. Azure 포털의 우측 상단 메뉴에서 [Cloud Shell] 아이콘을 클릭합니다.



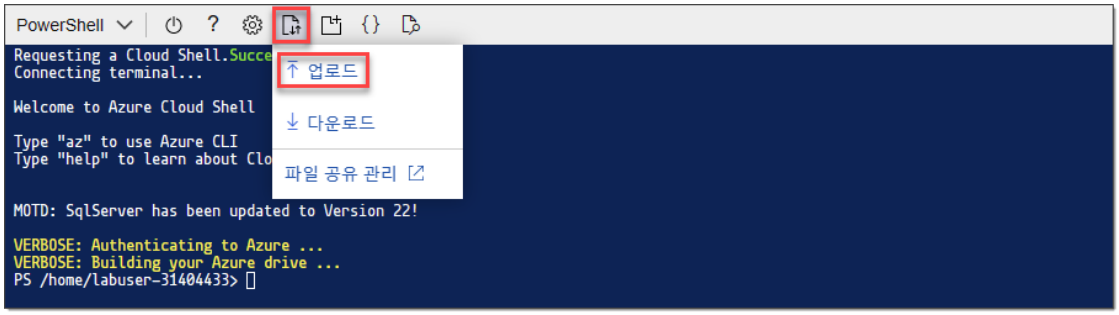
2. [Azure Cloud Shell 시작] 창에서 "`PowerShell`"을 클릭합니다.



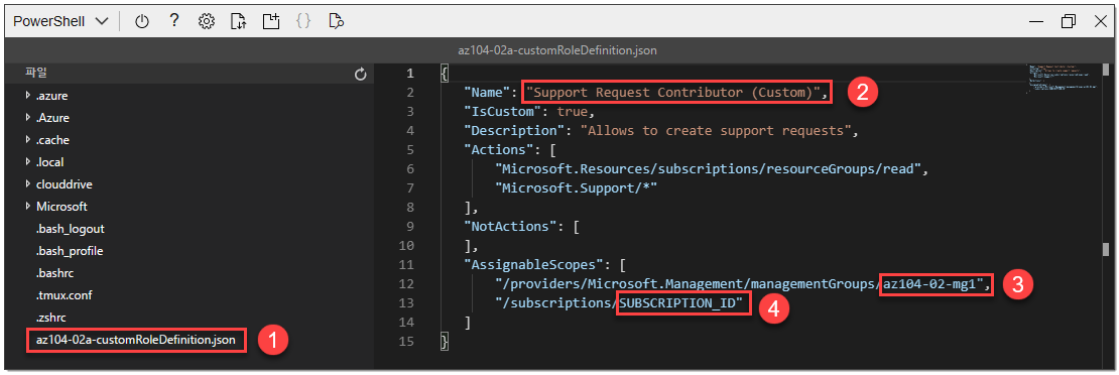
3. [탑재된 스토리지가 없음] 창에서 자신의 구독을 선택하고 [스토리지 만들기]를 클릭합니다.



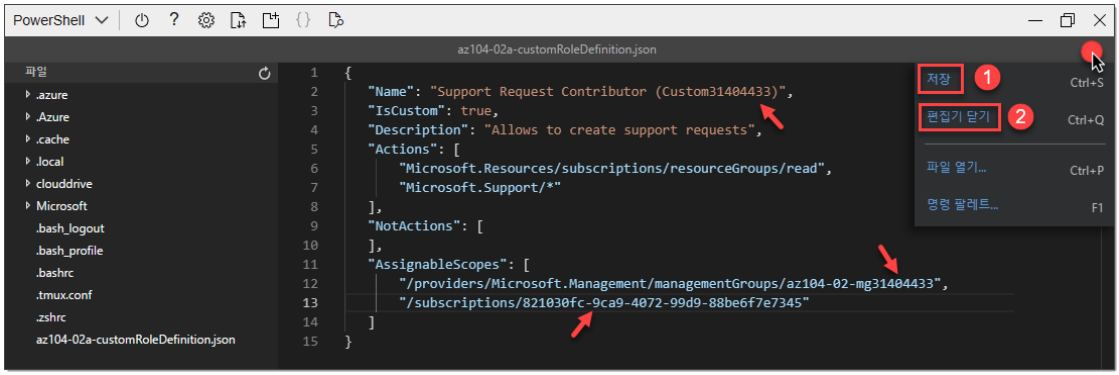
4. Cloud Shell이 시작되면 [파일 업로드/다운로드 - 업로드]를 클릭합니다. "`Labs\02\az104-02a-customRoleDefinition.json`" 파일을 선택하여 Cloud Shell의 홈 디렉터리로 업로드합니다.



5. [Cloud Shell]의 메뉴에서 [편집기 열기]를 클릭합니다. 편집기에서 업로드한 "`az104-02a-customRoleDefinition.json`" 파일을 선택합니다. 코드 편집창에서 아래와 같은 내용을 변경합니다.
   - "`Support Request Contributor (Custom)`"을 "`Support Request Contributor (Custom<xxxxxxxx>)`"으로 변경합니다. `<xxxxxxxx>`은 자신의 로그인 계정 뒤의 8자리 숫자를 입력합니다.
   - "`/providers/Microsoft.Management/managementGroups/az104-02-mg1`"을 관리 그룹 이름을 앞서 만들었던 관리 그룹 이름인 "`az104-02-mg<xxxxxxxx>`"으로 변경합니다.
   - `SUBSCRIPTION_ID` 값을 앞서 복사했던 구독 ID 값으로 대체합니다.

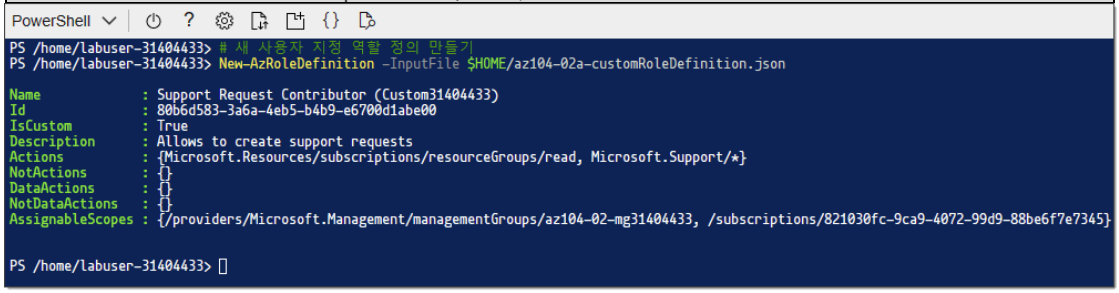


6. 편집기 우측 상단의 빈 공간을 클릭하고 [저장]을 클릭하여 편집한 내용을 저장합니다. 그런 다음 [편집기 닫기]를 클릭하여 편집기를 닫습니다.



7. 다음 명령을 실행하여 사용자 지정 역할 정의를 생성합니다.

```
# 새 사용자 지정 역할 정의 만들기
New-AzRoleDefinition -InputFile $HOME/az104-02a-customRoleDefinition.json
```

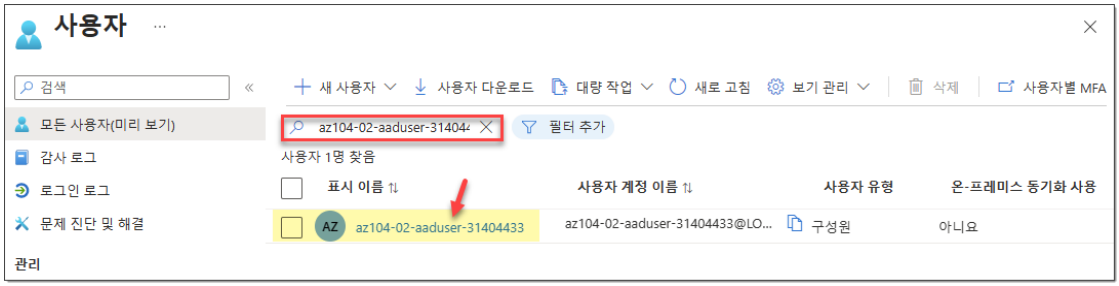


8. Cloud Shell 창을 닫습니다.

TASK 03. RBAC 역할 할당

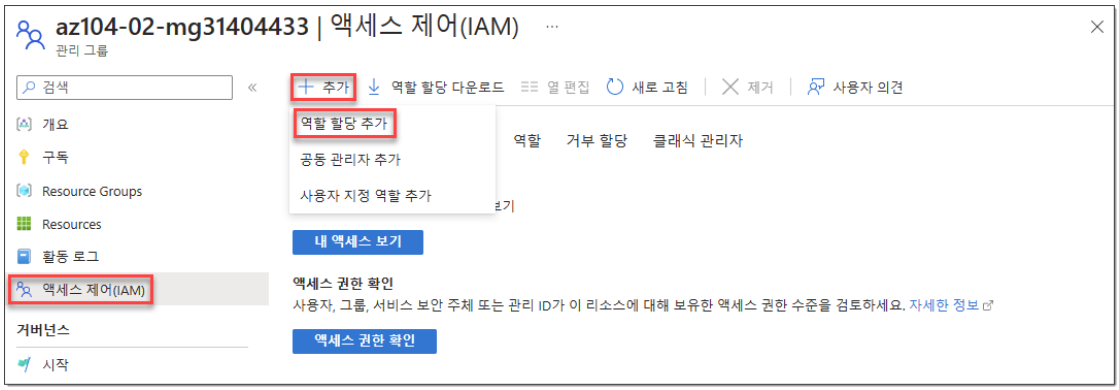
이 작업에서는 Azure AD 사용자를 만들고 이전 작업에서 만들었던 RBAC 역할을 사용자에게 할당하고 사용자가 RBAC 역할 정의에 지정된 작업을 수행할 수 있는지 확인합니다.

1. Azure 포털에서 [Azure Active Directory] 블레이드의 [관리 - 사용자]로 이동합니다. [사용자] 블레이드에서 "`az104-02-aaduser-<xxxxxxxxx>`" 사용자를 검색합니다. Cloudslice 실습 환경에서는 사용자 계정을 기본 테넌트에 만들 수 없기 때문에 이미 만들어져 있는 사용자 계정을 이 작업에서 사용합니다.



2. [관리 그룹] 블레이드로 이동한 후 `az104-02-mg<xxxxxxxxx>` 관리 그룹을 클릭합니다.

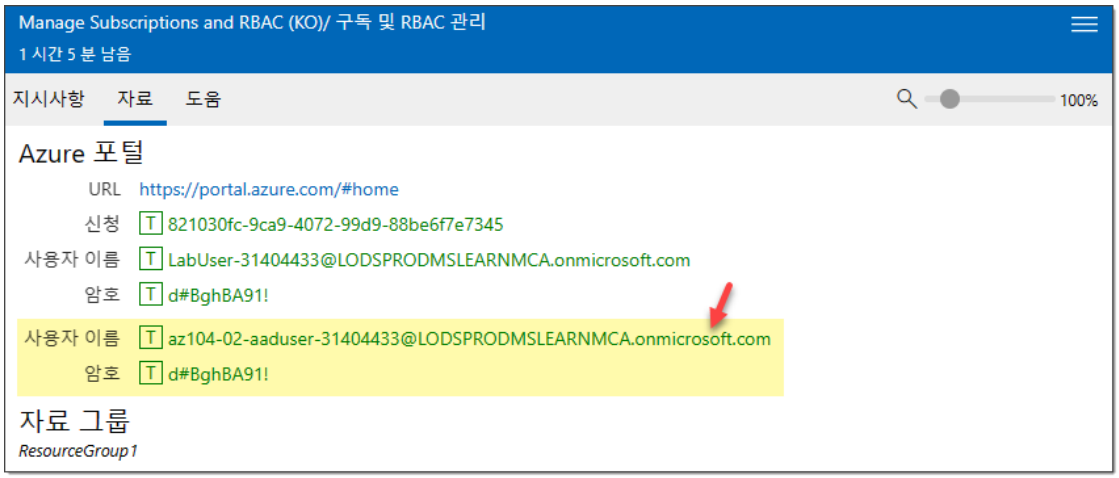
3. [`az104-02-mg<xxxxxxxxx>` 관리 그룹] 블레이드의 [액세스 제어(IAM)]으로 이동한 후 [추가 - 역할 할당 추가]를 클릭합니다.



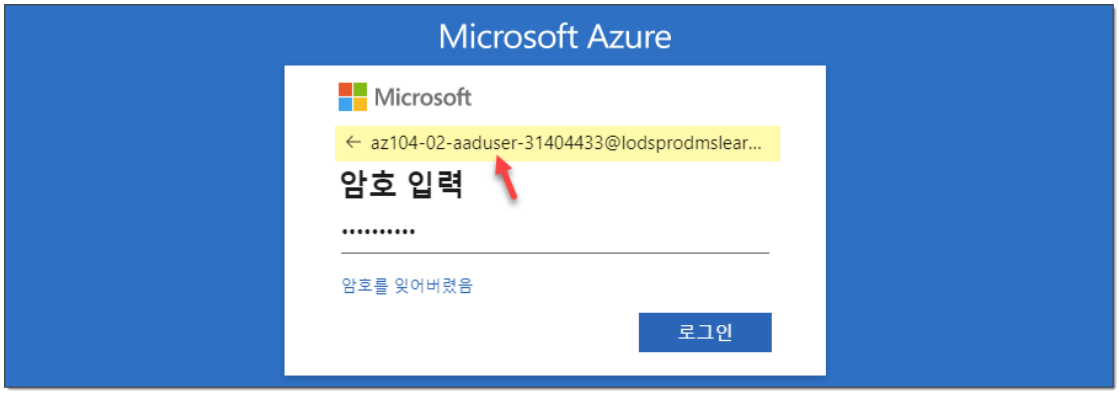
4. [역할 할당 추가] 블레이드의 [역할] 탭에서 "`Support Request Contributor (Custom<xxxxxxxxx>)`" 역할을 검색하여 선택하고 [다음]을 클릭합니다. 이 사용자 지정 역할은 Cloud Shell을 통해 만든 역할입니다.

5. [구성원] 탭에서 "구성원 선택" 링크를 클릭합니다. [구성원 선택] 창에서 앞서 만들었던 `az104-02-aaduser-<xxxxxxxxx>` 계정을 선택하고 [선택]을 클릭합니다. [구성원] 탭에서 [검토 + 할당]을 클릭합니다. [검토 + 할당] 탭에서 [검토 + 할당]을 클릭합니다.

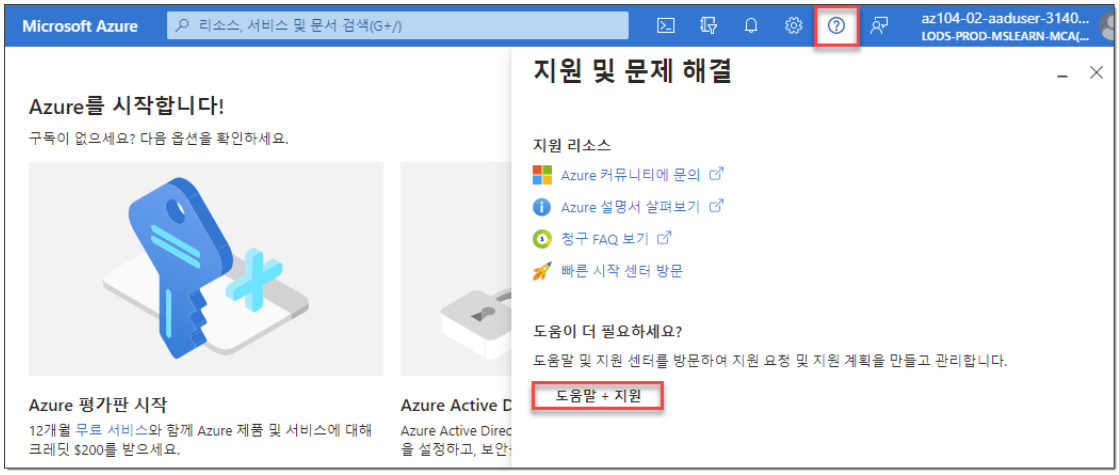
6. Cloudslice 실습 환경의 [자료] 탭에서 `az104-02-aaduser-<xxxxxxxxx>` 계정의 사용자 이름과 암호를 메모장에 복사합니다.



7. InPrivate 브라우저를 열고 Azure 포털에 연결한 후 위에서 확인한 사용자 계정으로 로그인합니다.

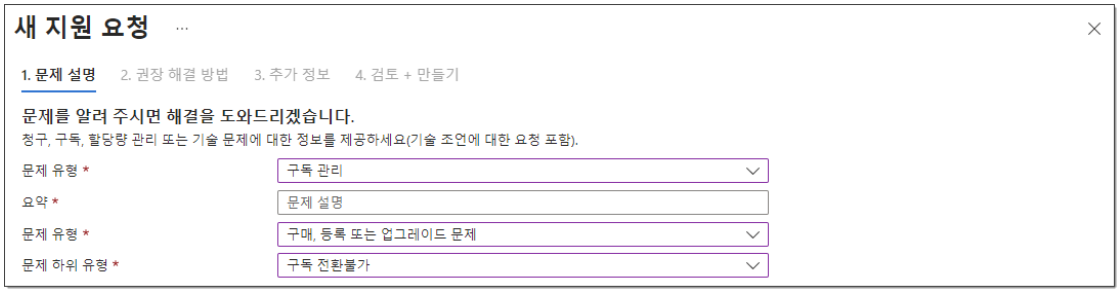


8. Azure 포털의 네비게이션 메뉴에서 다음 내용을 검토합니다.
   - [리소스 그룹]으로 이동하여 아무런 리소스 그룹도 표시되지 않는 것을 확인합니다. 이 사용자가 권한을 가지는 관리 그룹의 구독에는 리소스 그룹이 없기 때문에 아무런 리소스 그룹도 표시되지 않습니다.
   - [모든 리소스]로 이동하여 아무런 리소스도 볼 수 없는 것을 확인합니다.
9. Azure 포털의 우측 상단에서 [도움말] 아이콘을 클릭한 후 [도움말 + 지원]을 클릭합니다.



10. [도움말 + 지원] 블레이드의 메뉴에서 [지원 요청 만들기]를 클릭합니다.

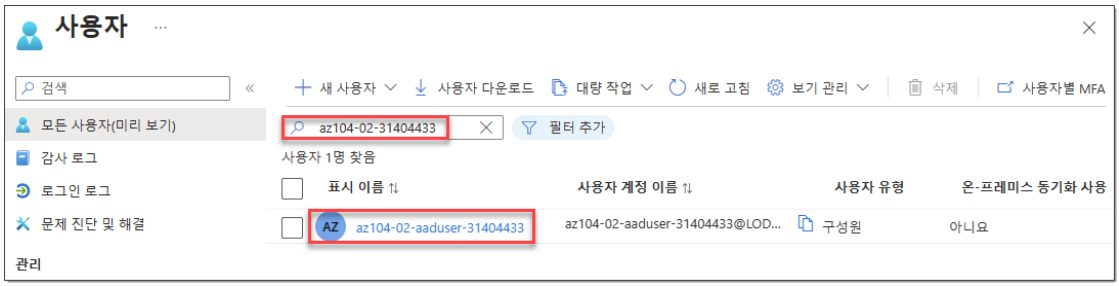
11. [새 지원 요청] 블레이드의 [1. 문제 설명] 탭에서 사용할 수 있는 메뉴를 확인합니다. "구독"에서 사용 중인 구독을 선택할 수 있으면 사용 중인 계정이 구독 전용 지원 요청을 만드는데 필요한 권한이 있음을 의미합니다. 지원 요청을 만들 수 있는지 확인한 후 실제 지원 요청은 생성하지 않습니다.



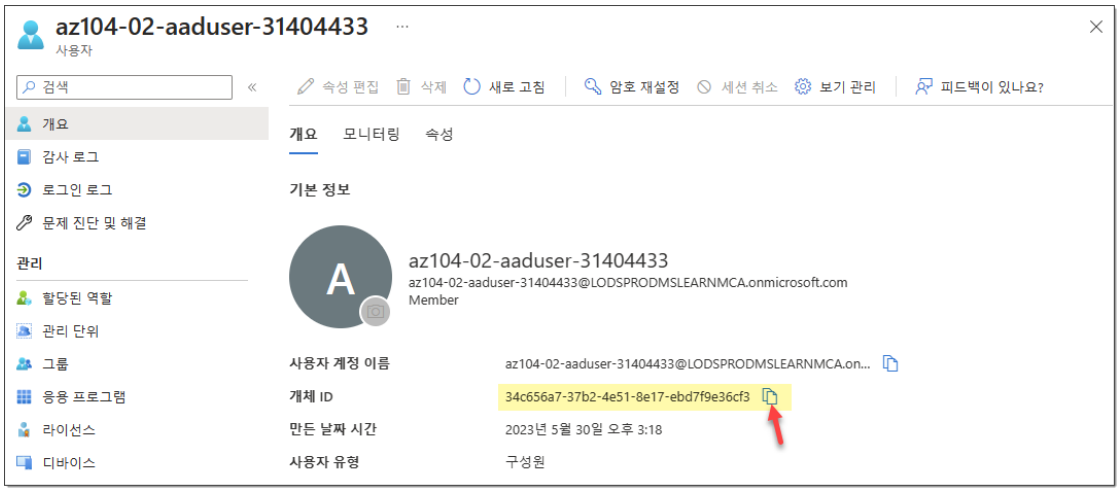
12. InPrivate 브라우저를 닫습니다.

TASK 04. 리소스 정리

1. Azure 포털에 `LabUser-<xxxxxxxxx>` 계정으로 다시 로그인합니다.
2. Azure 포털에서 [Azure Active Directory] 블레이드의 [관리 - 사용자]로 이동합니다. [사용자] 블레이드에서 "`az104-02-aaduser-<xxxxxxxxx>`" 계정을 검색한 후 클릭합니다.



3. [`az104-02-aaduser-<xxxxxxxxx>` 사용자] 블레이드의 [개요]에서 개체 ID 값을 메모장에 복사합니다.



4. [Cloud Shell]을 열고 다음 명령을 실행하여 위에서 확인한 사용자를 사용자 지정 역할 정의의 할당에서 제거합니다.
   - `Custom<xxxxxxxxx>` 값은 이전 작업에서 만들었던 사용자 지정 역할 이름으로 입력합니다.
   - `'[object_ID]'`는 위에서 확인한 사용자의 개체 ID를 입력합니다.

```
# 사용자 계정을 역할 할당 정의에서 제거
$scope = (Get-AzRoleDefinition -Name 'Support Request Contributor
(Custom<xxxxxxxxx>)').AssignableScopes `
```

```
  | Where-Object {$_ -like '*managementgroup*'}

Remove-AzRoleAssignment -ObjectId '[object_ID]' `
  -RoleDefinitionName 'Support Request Contributor (Custom<xxxxxxxx>)' `
  -Scope $scope
```

```
PS /home/labuser-31404433> # 사용자 계정을 역할 할당 정의에서 제거
PS /home/labuser-31404433> $scope = (Get-AzRoleDefinition -Name 'Support Request Contributor (Custom31404433)').AssignableScopes `
>> | Where-Object {$_ -like '*managementgroup*'}
PS /home/labuser-31404433>
PS /home/labuser-31404433> Remove-AzRoleAssignment -ObjectId '34c656a7-37b2-4e51-8e17-ebd7f9e36cf3' `
>>   -RoleDefinitionName 'Support Request Contributor (Custom31404433)' -Scope $scope
Succesfully removed role assignment for AD object '34c656a7-37b2-4e51-8e17-ebd7f9e36cf3' on scope '/providers/Microsoft.Management/managementG
2-mg31404433' with role definition 'Support Request Contributor (Custom31404433)'
PS /home/labuser-31404433>
```

5. [Cloud Shell]에서 다음 명령을 실행하여 사용자 지정 역할 정의를 삭제합니다. `<xxxxxxxx>`는 이전 단계에서 확인한 값과 동일한 값을 입력합니다.

```
# 사용자 지정 역할 정의 삭제
Remove-AzRoleDefinition -Name 'Support Request Contributor (Custom<xxxxxxxx>)' `
  -Force
```

```
PS /home/labuser-31404433> # 사용자 지정 역할 정의 삭제
PS /home/labuser-31404433> Remove-AzRoleDefinition -Name 'Support Request Contributor (Custom31404433)' -Force
PS /home/labuser-31404433>
```

6. [관리 그룹] 블레이드로 이동한 후 이전 작업에서 만들었던 `az104-02-mg<xxxxxxxx>` 관리 그룹을 선택합니다. [... - 삭제]를 클릭하여 관리 그룹을 삭제합니다. [그룹 삭제] 창에서 [예]를 클릭합니다.