한국 마이크로소프트

Microsoft Technical Trainer

Enterprise Skills Initiative

AZ-104. Challenge Lab 02

LAB 01. RBAC 및 사용자 지정 역할

Microsoft Partner Program – Technical Advisory Service

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
2023.08.23	1.0.0	우진환	LAB 01 내용 작성

목차

도전 과제

이 실습에서는 역할 기반 액세스 제어(RBAC)를 사용하여 계정 보안을 구성한 다음 사용자 지정 역할을 디자인합니다.

STEP 01. 빌트-인 역할 할당 및 권한 확인

1. `Dev1-<XXXXXXXX>` 계정이 `corp-datalod<XXXXXXXX>` 리소스 그룹의 특정 리소스를 관리할 수 있도록 권한을 할당합니다. 이 사용자는 스토리지 계정, 가상 머신, 네트워크만 관리할 수 있어야 합니다.
2. `Dev1-<XXXXXXXX>` 계정으로 Azure 포털에 로그인한 후 `corp-datalod<XXXXXXXX>` 리소스 그룹에 `sa<XXXXXXXX>` 스토리지 계정을 기본 설정으로 만듭니다.

STEP 02. 개발자 계정으로 가상 머신 만들기

1. "`Dev1-<XXXXXXXX>`" 계정으로 Azure 포털에 로그인합니다.
2. `corp-datalod<XXXXXXXX>` 리소스 그룹에 다음 속성을 사용하여 가상 머신을 만듭니다.

속성	값
리소스 그룹	corp-datalod<XXXXXXXX>
가상 머신 이름	VM1
이미지	Windows Server 2019 Datacenter - Gen2
크기	Standard_B2s - 2 vcpu, 4 GiB 메모리
사용자 이름	testUser
암호	Pa55w.rd1234
공용 인바운드 포트	RDP

STEP 03. 사용자 지정 역할 디자인

1. "`Virtual Machine Operator<xxxxxxxx>`" 이름의 사용자 지정 역할을 만들고 가상 머신 정보 보기, 가상 머신 시작 및 중지 작업을 수행할 수 있도록 역할을 정의합니다.

TASK 01. 빌트-인 역할 할당 및 권한 확인

1. Azure 포털의 검색창에서 "리소스 그룹"을 검색한 후 클릭합니다. [리소스 그룹] 블레이드에서 corp-datalod<XXXXXXXX> 리소스 그룹을 클릭합니다.

2. [corp-datalod<XXXXXXXX> 리소스 그룹] 블레이드의 [액세스 제어(IAM)]으로 이동한 후 메뉴에서 [추가 - 역할 할당 추가]를 클릭합니다.

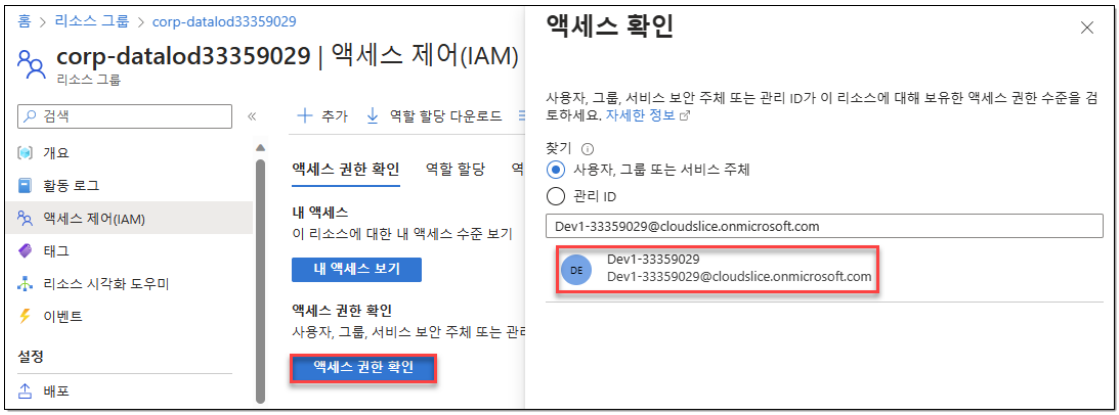
3. [역할 할당 추가] 블레이드의 [역할] 탭에서 "Storage 계정 참가자" 역할을 검색한 후 선택하고 [다음]을 클릭합니다.

4. [구성원] 탭에서 "구성원 선택" 링크를 클릭합니다. [구성원 선택] 창에서 "Dev1-<XXXXXXXX>" 계정을 검색한 후 추가하고 [선택]을 클릭합니다. [구성원] 탭에서 [검토 + 할당]을 클릭합니다. [검토 + 할당] 탭에서 [검토 + 할당]을 클릭합니다.

5. 동일한 방법으로 다음과 같은 역할을 추가합니다.

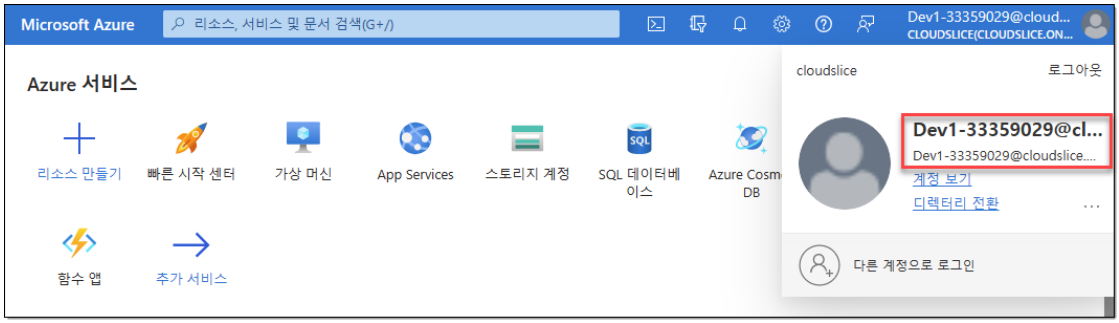
추가할 역할	추가할 구성원
가상 머신 참가자	`Dev1-<XXXXXXXXX>`
네트워크 참가자	`Dev1-<XXXXXXXXX>`

6. `[corp-datalod<XXXXXXXXX>` 리소스 그룹] 블레이드의 [액세스 제어(IAM)]으로 이동한 후 [액세스 권한 확인] 탭에서 [액세스 권한 확인]을 클릭합니다. [액세스 확인] 창에서 "`Dev1-<XXXXXXXXX>`" 계정을 검색한 후 선택합니다.



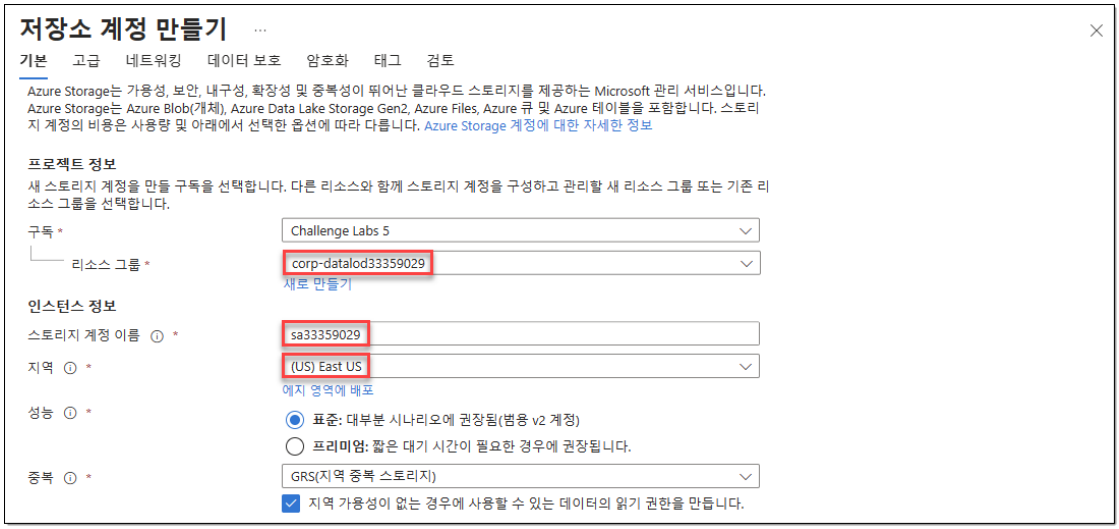
7. [현재 역할 할당] 탭에서 아래와 같이 "`Storage 계정 참가자`", "`가상 머신 참가자`", "`네트워크 참가자`" 역할이 할당된 것을 확인합니다.

8. Azure 포털에 "Dev1-<XXXXXXXX>" 계정으로 로그인합니다.



9. Azure 포털의 검색창에서 "스토리지 계정"을 검색한 후 클릭합니다. [스토리지 계정] 블레이드의 메뉴에서 [만들기]를 클릭합니다.

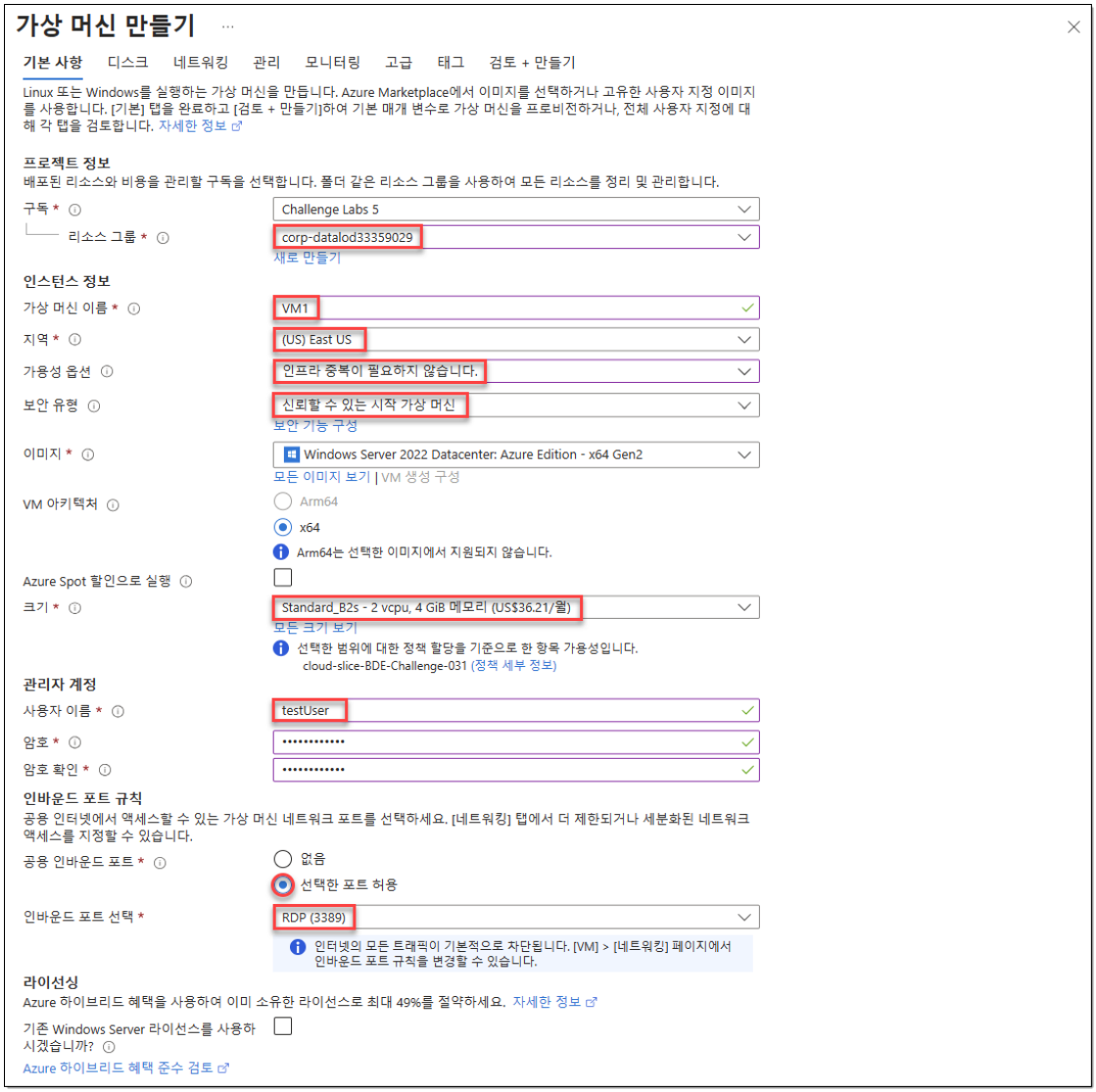
10. [저장소 계정 만들기] 블레이드의 [기본] 탭에서 아래와 같이 구성한 후 [검토]를 클릭합니다. [검토] 탭에서 [만들기]를 클릭합니다.
    - [프로젝트 정보 - 리소스 그룹]: corp-datalod<XXXXXXXX>
    - [인스턴스 정보 - 스토리지 계정 이름]: sa<XXXXXXXX>
    - [인스턴스 정보 - 지역]: (US) East US
    - 다른 설정은 기본값을 유지합니다.



TASK 02. 개발자 계정으로 가상 머신 만들기

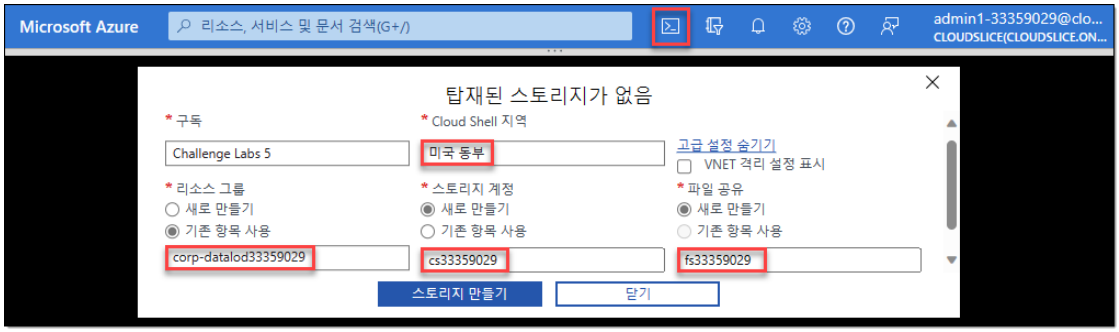
1. Azure 포털에 "`Dev1-<XXXXXXXX>`" 계정으로 로그인합니다.
2. Azure 포털에서 [리소스 만들기]를 클릭한 후 "`Windows Server`"를 검색합니다. [Windows Server] 블레이드에서 "`Windows Server 2022 Datacenter: Azure Edition`" 플랜을 선택하고 [만들기]를 클릭합니다.

3. [가상 머신 만들기] 블레이드의 [기본 사항] 탭에서 아래와 같이 구성한 후 [검토 + 만들기]를 클릭합니다. [검토 + 만들기] 탭에서 [만들기]를 클릭합니다.
   - [프로젝트 정보 - 리소스 그룹]: `corp-datalod<XXXXXXXX>`
   - [인스턴스 정보 - 가상 머신 이름]: VM1
   - [인스턴스 정보 - 지역]: (US) East US
   - [인스턴스 정보 - 가용성 옵션]: 인프라 중복이 필요하지 않습니다.
   - [인스턴스 정보 - 보안 유형]: 신뢰할 수 있는 시작 가상 머신
   - [인스턴스 정보 - 크기]: Standard_B2s
   - [관리자 계정 - 사용자 이름]: testUser
   - [관리자 계정 - 암호]: Pa55w.rd1234
   - [인바운드 포트 규칙 - 공용 인바운드 포트]: 선택한 포트 허용
   - [인바운드 포트 규칙 - 인바운드 포트 선택]: RDP (3389)



TASK 03. 사용자 지정 역할 디자인

1. Azure 포털에 "`admin1-<xxxxxxxx>`" 계정으로 로그인합니다.
2. Azure 포털의 우측 상단에서 [Cloud Shell] 아이콘을 클릭하고 "`PowerShell`"을 클릭합니다. [탑재된 스토리지가 없음] 창에서 "`고급 설정 표시`"를 클릭합니다. [탑재된 스토리지가 없음] 페이지에서 아래와 같이 구성한 후 [스토리지 만들기]를 클릭합니다.
   - Cloud Shell 지역: 미국 동부
   - 리소스 그룹: `corp-datalod<xxxxxxxx>`
   - 스토리지 계정: `cs<xxxxxxxx>`
   - 파일 공유: `fs<xxxxxxxx>`



3. [Cloud Shell]의 PowerShell 세션에서 다음 명령을 실행하여 가상 머신과 관련된 작업을 확인합니다.

```
# 가상 머신과 관련된 작업 확인
Get-AzProviderOperation "Microsoft.Compute/virtualmachines/*" `
  | FT Operation, Description -AutoSize
```

```
PS /home/admin1-33359029> # 가상 머신과 관련된 작업 확인
PS /home/admin1-33359029> Get-AzProviderOperation "Microsoft.Compute/virtualmachines/*" | FT Operation, Description -AutoSize

Operation                                                  Description
---------                                                  -----------
Microsoft.Compute/virtualMachines/read                     Get the properties of a virtual machine
Microsoft.Compute/virtualMachines/write                    Creates a new virtual machine or updates an existing virtual mac…
Microsoft.Compute/virtualMachines/delete                   Deletes the virtual machine
Microsoft.Compute/virtualMachines/start/action             Starts the virtual machine
Microsoft.Compute/virtualMachines/powerOff/action          Powers off the virtual machine. Note that the virtual machine wi…
Microsoft.Compute/virtualMachines/reapply/action           Reapplies a virtual machine's current model
Microsoft.Compute/virtualMachines/redeploy/action          Redeploys virtual machine
Microsoft.Compute/virtualMachines/restart/action           Restarts the virtual machine
Microsoft.Compute/virtualMachines/retrieveBootDiagnosticsData/action Retrieves boot diagnostic logs blob URIs
```

4. [Cloud Shell]의 PowerShell 세션에서 다음 명령을 실행하여 "가상 머신 참가자(Virtual Machine Contributor)" 빌트-인 역할 정의에 할당되어 있는 작업을 확인한 후 설정 내용을 JSON 파일로 내보냅니다.

```
# 빌트-인 역할 정의에 구성된 내용을 JSON 파일로 내보내기
Get-AzRoleDefinition -Name "Virtual Machine Contributor" `
  | ConvertTo-Json `
  | Out-File $home\clouddrive\VMOperatorRole.json
```

```
PS /home/admin1-33359029> # 빌트-인 역할 정의에 구성된 내용을 JSON 파일로 내보내기
PS /home/admin1-33359029> Get-AzRoleDefinition -Name "Virtual Machine Contributor" `
>>   | ConvertTo-Json `
>>   | Out-File $home\clouddrive\VMOperatorRole.json
PS /home/admin1-33359029>
```

5. [Cloud Shell]의 PowerShell 세션에서 다음 명령을 실행하여 사용자 정의 역할을 할당할 리소스 그룹의 ResourceId를 확인합니다. 표시되는 ResourceId를 메모장에 복사합니다.

```
# 리소스 그룹의 ID 확인
Get-AzResourceGroup
```

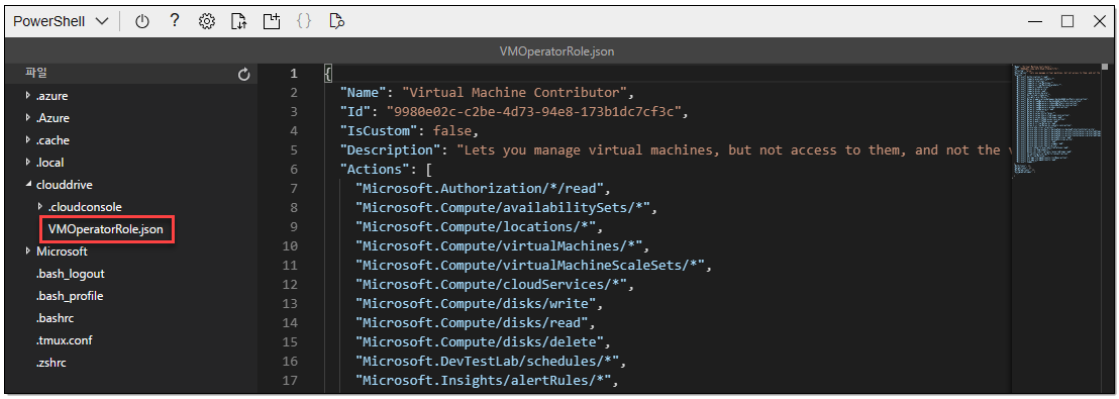
```
PS /home/admin1-33359029> # 리소스 그룹의 ID 확인
PS /home/admin1-33359029> Get-AzResourceGroup

ResourceGroupName : corp-datalod33359029
Location          : eastus
ProvisioningState : Succeeded
Tags              :
                    Name          Value
                    ============  ================
                    PoolOrgId     444
                    TS            133372685946832495
                    SeriesId      16131
                    LODManaged    lod
                    LabProfile    136819
                    ProfileOrgId  1340
                    LabInstance   33359029

ResourceId        : /subscriptions/970fa9a7-1df2-4b06-b4ec-a075587ddf86/resourceGroups/corp-datalod33359029
```

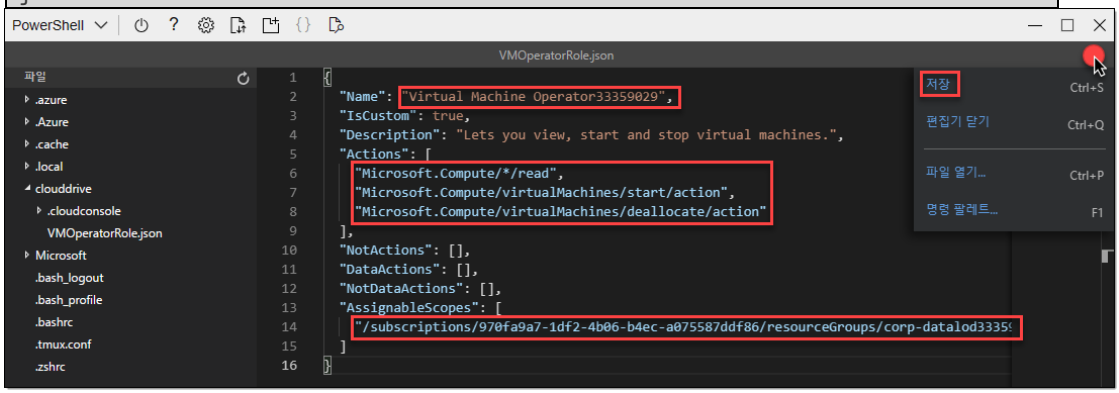
6. [Cloud Shell]에서 [편집기 열기] 아이콘을 클릭합니다. "clouddrive\VMOperatorRole.json" 파일을

엽니다.



7. "VMOperatorRole.json" 파일 편집 창에서 다음과 같은 JSON 역할 정의 파일을 설정합니다. 역할 정의를 구성한 후 [저장]을 클릭합니다.

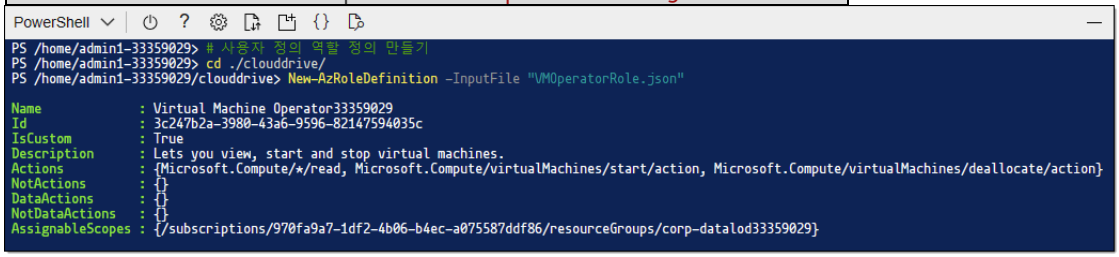
```
{
  "Name": "Virtual Machine Operator<xxxxxxxx>",
  "IsCustom": true,
  "Description": "Lets you view, start and stop virtual machines.",
  "Actions": [
    "Microsoft.Compute/*/read",
    "Microsoft.Compute/virtualMachines/start/action",
    "Microsoft.Compute/virtualMachines/deallocate/action"
  ],
  "NotActions": [],
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
    "your_resource_group_id"
  ]
}
```



8. [Cloud Shell]의 PowerShell 세션에서 다음 명령을 실행하여 새 사용자 지정 역할 정의를 만듭니다.

```
# 사용자 정의 역할 정의 만들기
cd ./clouddrive/

New-AzRoleDefinition -InputFile "VMOperatorRole.json"
```



9. [corp-datalod<xxxxxxxx> 리소스 그룹] 블레이드의 [액세스 제어(IAM)]으로 이동한 후 메뉴에서 [추가 - 역할 할당 추가]를 클릭합니다.

10. [역할 할당 추가] 블레이드의 [역할] 탭에서 "Virtual Machine Operator" 역할을 검색한 후 PowerShell로 만든 사용자 지정 역할이 표시되는지 확인합니다.