

AZ-104. Challenge Lab 04

## **LAB 05. 가상 네트워크 서비스 엔드포인트 구성**

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

**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.

저작권에 관련된 법률을 준수하는 것은 고객의 역할이며, 이 문서를 마이크로소프트의 사전 동의 없이 어떤 형태(전자 문서, 물리적인 형태 막론하고) 어떠한 목적으로 재 생산, 저장 및 다시 전달하는 것은 허용되지 않습니다.

마이크로소프트는 이 문서에 들어있는 특허권, 상표, 저작권, 지적 재산권을 가집니다. 문서를 통해 명시적으로 허가된 경우가 아니면, 어떠한 경우에도 특허권, 상표, 저작권 및 지적 재산권은 다른 사용자에게 허용되지 않습니다.

© 2023 Microsoft Corporation All right reserved.

Microsoft®는 미합중국 및 여러 나라에 등록된 상표입니다.

이 문서에 기재된 실제 회사 이름 및 제품 이름은 각 소유자의 상표일 수 있습니다.

## 문서 작성 연혁

날짜	버전	작성자	변경 내용
2023.08.27	1.0.0	우진환	LAB 05 내용 작성

## 목차

<b>도전 과제</b> .....	<b>5</b>
STEP 01. AZURE KEY VAULT에 비밀 만들기.....	5
STEP 02. BACKEND 서브넷에 대한 아웃바운드 보안 규칙 구성 .....	5
STEP 03. 가상 네트워크 서비스 엔드포인트 구성.....	5
STEP 04. 서비스 엔드포인트에 액세스 확인 .....	6
<b>TASK 01. AZURE KEY VAULT에 비밀 만들기</b> .....	<b>7</b>
<b>TASK 02. BACKEND 서브넷에 대한 아웃바운드 보안 규칙 구성</b> .....	<b>8</b>
<b>TASK 03. 가상 네트워크 서비스 엔드포인트 구성</b> .....	<b>10</b>
<b>TASK 04. 서비스 엔드포인트에 액세스 확인</b> .....	<b>12</b>

## 도전 과제

이 실습에서는 애플리케이션 백 엔드 티어에서 Azure Key Vault의 서비스 엔드포인트에 대한 액세스를 구성합니다.

- Key Vault에 비밀을 만든 다음 가상 네트워크의 **backend** 서브넷에 대한 아웃바운드 보안 규칙을 만듭니다.
- Key Vault 비밀에 대한 액세스를 제공하도록 가상 네트워크 서비스 엔드포인트를 구성합니다.
- 서비스 엔드포인트에 액세스할 수 있는지 확인합니다.

### STEP 01. Azure Key Vault에 비밀 만들기

1. `mykeyvault<xxxxxxxx>` Key Vault에 다음 속성을 사용하여 새 비밀을 만듭니다.

속성	값
이름	challenge-secret
비밀 값	mykvstring

2. [Cloud Shell]의 Bash 세션을 다음 설정을 구성합니다.

속성	값
Cloud Shell 지역	미국 동부
리소스 그룹	RG1
스토리지 계정	기존에 만들어져 있는 스토리지 계정을 사용
파일 공유	cloud-shell-share

3. `az keyvault secret show` 명령을 사용하여 비밀 값을 확인합니다.

### STEP 02. backend 서브넷에 대한 아웃바운드 보안 규칙 구성

1. **VNET** 가상 네트워크의 **backend** 서브넷에 **Microsoft.KeyVault**에 대한 서비스 엔드포인트가 설정되어 있는지 확인합니다.
2. **webapp-nsg** 네트워크 보안 그룹에서 다음과 같은 아웃바운드 보안 규칙을 설정합니다.

속성	값
소스	Service Tag
원본 서비스 태그	VirtualNetwork
대상 주소	Service Tag
대상 서비스 태그	AzureKeyVault
대상 포트 범위	*
우선 순위	100
이름	AllowKeyVault

### STEP 03. 가상 네트워크 서비스 엔드포인트 구성

1. **VNET** 가상 네트워크의 **backend** 서브넷만 Key Vault에 액세스할 수 있도록 네트워킹 규칙을 추가합니다.
2. [Cloud Shell]에서 Key Vault 비밀을 확인하고 네트워킹 규칙으로 인해 작업이 실패하는 것을 확인합니다.

**STEP 04. 서비스 엔드포인트에 액세스 확인**

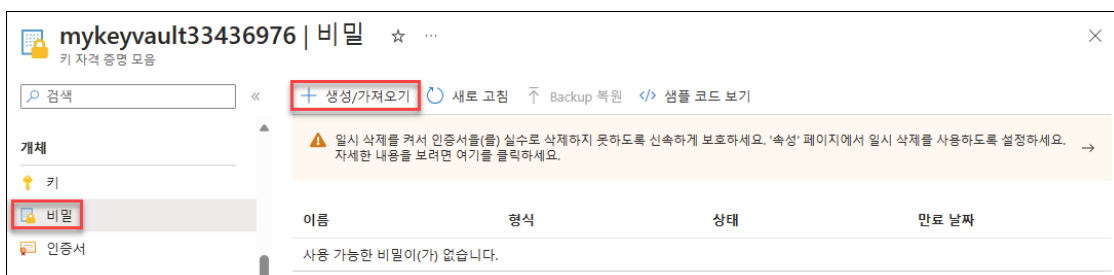
1. [Cloud Shell]의 Bash 세션에서 `az vm list-ip-addresses` 명령을 사용하여 VM2 가상 머신의 공용 IP를 확인합니다.
2. [Cloud Shell]에서 VM2 가상 머신에 SSH 세션을 연결합니다.
3. VM2 가상 머신에 Azure CLI 도구를 설치합니다.
4. VM2 가상 머신에서 Azure CLI를 사용하여 Azure 포털에 로그인합니다.
5. VM2 가상 머신에서 Azure CLI를 사용하여 Key Vault의 비밀을 볼 수 있는지 확인합니다.

## TASK 01. Azure Key Vault에 비밀 만들기

1. Azure 포털의 검색창에서 "키 자격 증명 모음"을 검색한 후 클릭합니다. [키 자격 증명 모음] 블레이드에서 `mykeyvault<xxxxxxxx>` 키 자격 증명 모음을 클릭합니다.



2. `mykeyvault<xxxxxxxx>` 키 자격 증명 모음 블레이드의 [개체 - 비밀]로 이동한 후 메뉴에서 [생성/가져오기]를 클릭합니다.

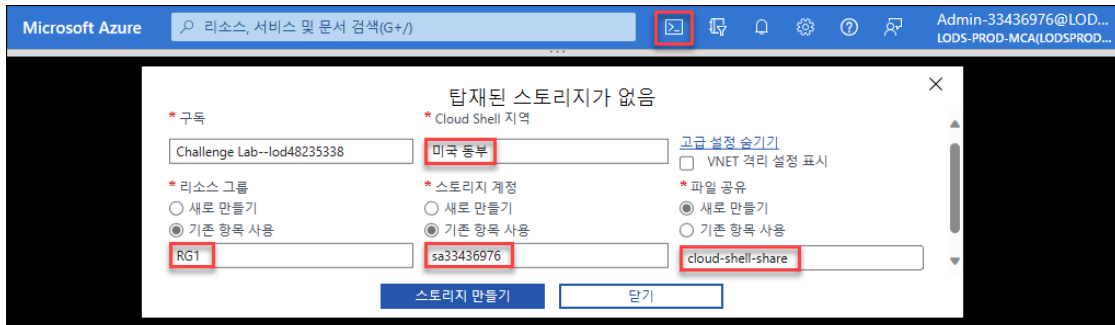


3. [비밀 만들기] 블레이드에서 아래와 같이 구성한 후 [만들기]를 클릭합니다.
  - 업로드 옵션: 수동
  - 이름: challenge-secret
  - 비밀 값: mykvstring



4. Azure 포털에서 [Cloud Shell]을 클릭한 후 "Bash"를 선택합니다. [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: "기존 항목 사용"을 선택한 후 "RG1"을 선택합니다.
  - 스토리지 계정: "기존 항목 사용"을 선택한 후 "sa<xxxxxxxx>" 계정을 선택합니다.
  - 파일 공유: "새로 만들기"를 선택한 후 "cloud-shell-share"를 입력합니다.





5. [Cloud Shell]의 Bash 세션에서 다음 명령을 실행하여 앞서 만들었던 Key Vault의 비밀에 액세스할 수 있는지 확인합니다.

```
# Key Vault의 비밀 확인
az keyvault secret show --vault-name mykeyvault<xxxxxxxx> \
--name challenge-secret

Bash
admin-33436976 [ ~ ]$ # Key Vault의 비밀 확인
admin-33436976 [ ~ ]$ az keyvault secret show --vault-name mykeyvault33436976 --name challenge-secret
{
  "attributes": {
    "created": "2023-08-27T08:28:05+00:00",
    "enabled": true,
    "expires": null,
    "notBefore": null,
    "recoverableDays": 0,
    "recoveryLevel": "Purgeable",
    "updated": "2023-08-27T08:28:05+00:00"
  },
  "contentType": null,
  "id": "https://mykeyvault33436976.vault.azure.net/secrets/challenge-secret/d35de5d42beb49e180253c051c9dc117",
  "kid": null,
  "managed": null,
  "name": "challenge-secret",
  "tags": {},
  "value": "mykvstring"
}
```

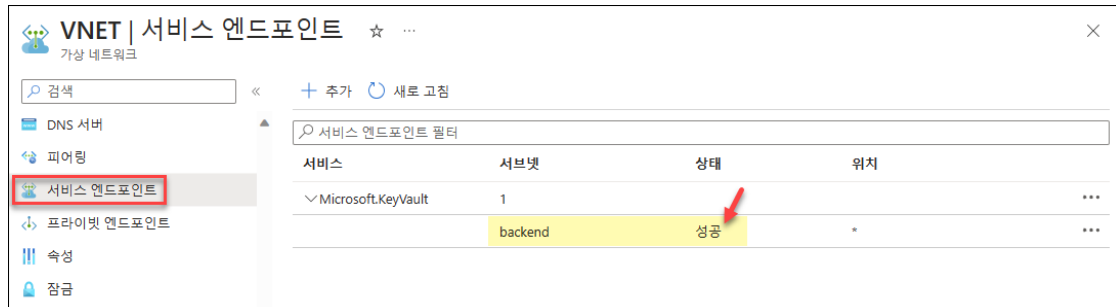
## TASK 02. backend 서버넷에 대한 아웃바운드 보안 규칙 구성

서비스 엔드포인트 액세스를 확인하려면 먼저 가상 네트워크 서비스 엔드포인트를 구성해야 합니다. 이전 작업에서 Key Vault 비밀을 만들었으므로 backend 서버넷에 대한 아웃바운드 보안 규칙을 만들어야 합니다. 먼저 Microsoft.KeyVault 서비스 엔드포인트가 활성화되어 있는지 확인한 다음 아웃바운드 보안 규칙을 만듭니다.

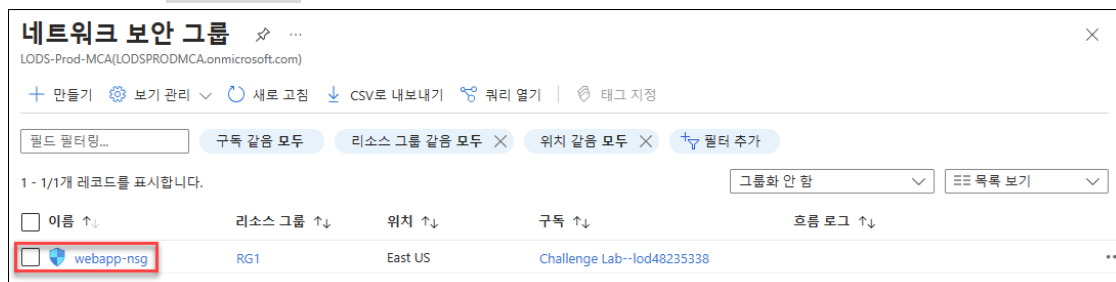
1. Azure 포털의 검색창에서 "가상 네트워크"를 검색한 후 클릭합니다. [가상 네트워크] 블레이드에서 VNET 가상 네트워크를 클릭합니다.



2. [VNET 가상 네트워크] 블레이드의 [설정 - 서비스 엔드포인트]로 이동합니다. 아래와 같이 backend 서버넷에 서비스 엔드포인트의 상태가 "성공" 상태로 표시되는지 확인합니다.



3. Azure 포털의 검색창에서 "네트워크 보안 그룹"을 검색한 후 클릭합니다. [네트워크 보안 그룹] 블레이드에서 **webapp-nsg** 네트워크 보안 그룹을 클릭합니다.



4. [webapp-nsg 네트워크 보안 그룹] 블레이드의 [설정 - 아웃바운드 보안 규칙]으로 이동한 후 메뉴에서 [추가]를 클릭합니다.



5. [아웃바운드 보안 규칙 추가] 창에서 아래와 같이 구성한 후 [추가]를 클릭합니다.

- 소스: Service Tag
- 원본 서비스 태그: VirtualNetwork
- 원본 포트 범위: \*
- 대상 주소: Service Tag
- 대상 서비스 태그: AzureKeyVault
- 서비스: Custom
- 대상 포트 범위: \*
- 프로토콜: Any
- 작업: 허용
- 우선 순위: 100
- 이름: AllowKeyVault

**아웃바운드 보안 규칙 추가**  
webapp-nsg

소스 ①  
Service Tag

원본 서비스 태그 \* ①  
VirtualNetwork

원본 포트 범위 \* ①  
\*

대상 주소 ①  
Service Tag

대상 서비스 태그 ①  
AzureKeyVault

서비스 ①  
Custom

대상 포트 범위 \* ①  
\*

프로토콜  
☒ Any  
☐ TCP  
☐ UDP  
☐ ICMP

작업  
☒ 허용  
☐ 거부

우선 순위 \* ①  
100

이름 \*  
AllowKeyVault

설명

### TASK 03. 가상 네트워크 서비스 엔드포인트 구성

**backend** 서버넷에 대한 아웃바운드 보안 규칙이 생성되었으므로 이제 가상 네트워크 서비스 엔드포인트를 구성해야 합니다. 먼저 가상 네트워크 서비스 엔드포인트를 구성한 다음 [Cloud Shell]을 사용하여 Key Vault의 비밀 값을 확인합니다.

1. Azure 포털의 검색창에서 "키 자격 증명 모음"을 검색한 후 클릭합니다. [키 자격 증명 모음] 블레이드에서 **mykeyvault<xxxxxxxx>** 키 자격 증명 모음을 클릭합니다.

**키 자격 증명 모음** ...

LODS-Prod-MCA(LODSPRODMCA.onmicrosoft.com)

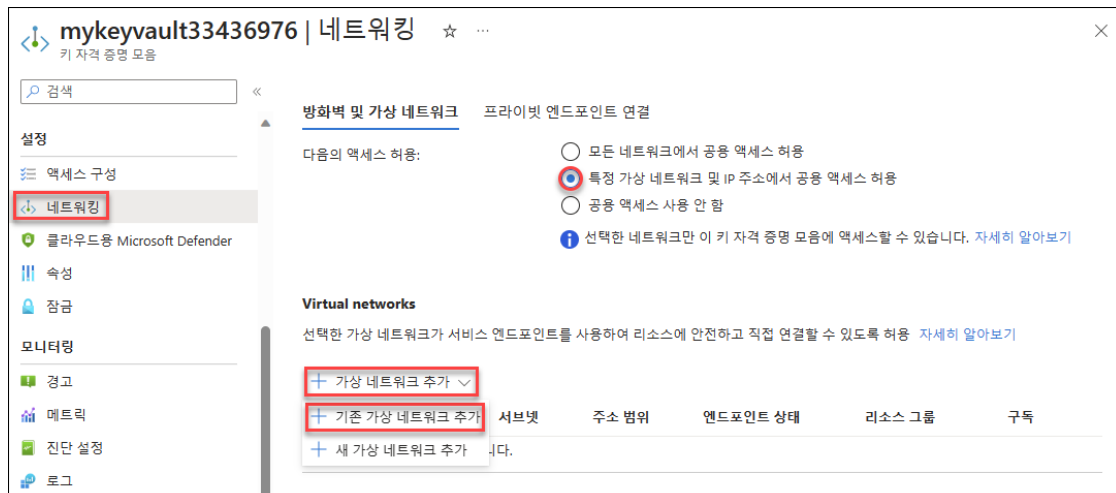
+ 만들기 | 삭제된 자격 증명 모음 관리 | 보기 관리 | 새로 고침 | CSV로 내보내기 | 쿼리 열기 | 태그 지정

필드 필터링... | 구독 있음 모두 | 리소스 그룹 있음 모두 X | 위치 있음 모두 X | 필터 추가

1 - 1/1개 레코드를 표시합니다. | 그룹화 안 함 | 프리 목록 보기

이름 ↑↓	형식 ↑↓	리소스 그룹 ↑↓	위치 ↑↓	구독 ↑↓	태그
<input checked="" type="checkbox"/> mykeyvault33436976	키 자격 증명 모음	RG1	East US	Challenge Lab--lod48235338	**

2. **mykeyvault<xxxxxxxx>** 키 자격 증명 모음 블레이드의 [설정 - 네트워킹]으로 이동합니다. [방화벽 및 가상 네트워크] 탭에서 아래와 같이 구성합니다.
  - 다음의 액세스 허용: 특정 가상 네트워크 및 IP 주소에서 공용 액세스 허용
  - "Virtual networks" 영역에서 [가상 네트워크 추가 - 기존 가상 네트워크 추가]를 클릭합니다.

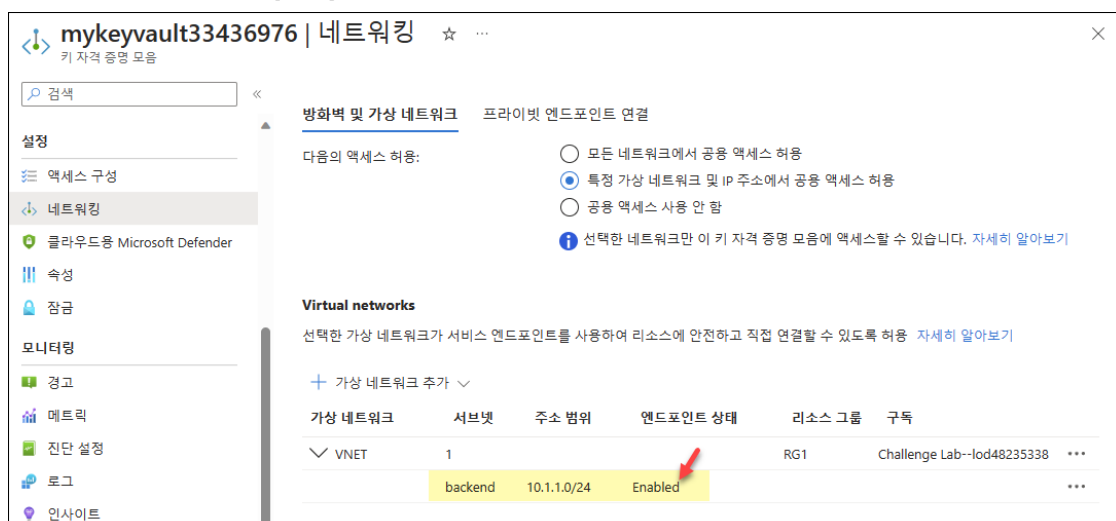


3. [네트워크 추가] 창에서 아래와 같이 선택한 후 [추가]를 클릭합니다.

- 가상 네트워크: VNET
- 서브넷: backend

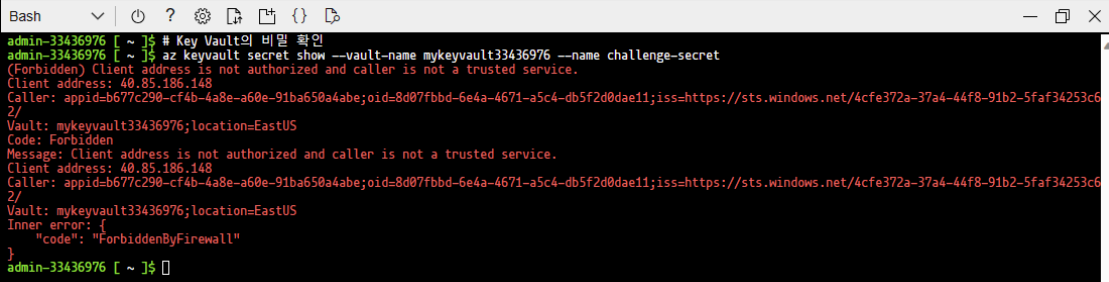


4. [mykeyvault<xxxxxxx> | 네트워킹] 블레이드에서 VNET 가상 네트워크의 backend 서브넷이 추가된 것을 확인한 후 [적용]을 클릭합니다.



5. [Cloud Shell]의 Bash 세션에서 다음 명령을 실행하여 [Cloud Shell]을 실행하는 가상 머신에서 Key Vault의 비밀에 액세스할 수 없는 것을 확인합니다.

```
# Key Vault의 비밀 확인
az keyvault secret show --vault-name mykeyvault<xxxxxxxx> \
--name challenge-secret
```



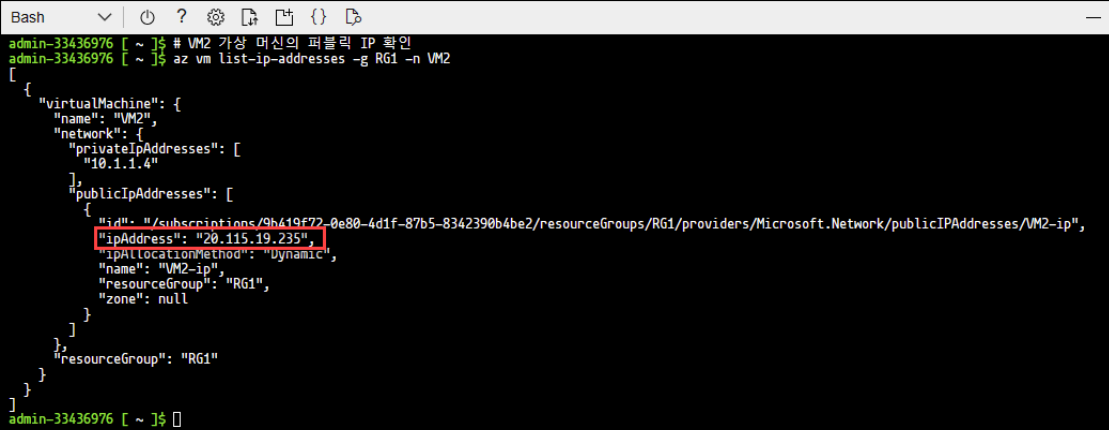
```
Bash
admin-33436976 [ ~ ]$ # Key Vault의 비밀 확인
admin-33436976 [ ~ ]$ az keyvault secret show --vault-name mykeyvault33436976 --name challenge-secret
(Forbidden) Client address is not authorized and caller is not a trusted service.
Client address: 40.85.186.148
Caller: appid=b677c290-cf4b-4a8e-a60e-91ba650a4abe;oid=8d07fbbd-6e4a-4671-a5c4-db5f2d0dae11;iss=https://sts.windows.net/4cfe372a-37a4-44f8-91b2-5faf34253c62/
Vault: mykeyvault33436976;location=EastUS
Code: Forbidden
Message: Client address is not authorized and caller is not a trusted service.
Client address: 40.85.186.148
Caller: appid=b677c290-cf4b-4a8e-a60e-91ba650a4abe;oid=8d07fbbd-6e4a-4671-a5c4-db5f2d0dae11;iss=https://sts.windows.net/4cfe372a-37a4-44f8-91b2-5faf34253c62/
Vault: mykeyvault33436976;location=EastUS
Inner error: {
  "code": "ForbiddenByFirewall"
}
admin-33436976 [ ~ ]$
```

#### TASK 04. 서비스 엔드포인트에 액세스 확인

이제 가상 네트워크 서비스 엔드포인트를 구성했으므로 서비스 엔드포인트에 액세스할 수 있는지 확인해야 합니다. 먼저 Linux 가상 머신에 연결한 다음 Linux 가상 머신에서 Azure CLI를 설치합니다. 마지막으로 Azure CLI에 로그인한 다음 Key Vault 비밀 값을 확인합니다. 실습 환경에서는 Cloud Shell에서 SSH 연결에 문제가 있기 때문에 자신의 컴퓨터에 있는 터미널에서 SSH 연결을 확인합니다.

1. [Cloud Shell]의 Bash 세션에서 다음 명령을 실행하여 VM2 가상 머신(backend 서버넷에 있음)의 공용 IP 주소를 확인합니다. 표시되는 공용 IP 주소를 메모장에 기록합니다.

```
# VM2 가상 머신의 퍼블릭 IP 확인
az vm list-ip-addresses -g RG1 -n VM2
```



```
Bash
admin-33436976 [ ~ ]$ # VM2 가상 머신의 퍼블릭 IP 확인
admin-33436976 [ ~ ]$ az vm list-ip-addresses -g RG1 -n VM2
[
  {
    "virtualMachine": {
      "name": "VM2",
      "network": {
        "privateIpAddresses": [
          {
            "ipAddress": "10.1.1.4"
          }
        ],
        "publicIpAddresses": [
          {
            "id": "/subscriptions/9b419f72-0e80-4d1f-87b5-8342390b4be2/resourceGroups/RG1/providers/Microsoft.Network/publicIPAddresses/VM2-ip",
            "ipAddress": "20.115.19.235",
            "ipAllocationMethod": "Dynamic",
            "name": "VM2-ip",
            "resourceGroup": "RG1",
            "zone": null
          }
        ]
      }
    },
    "resourceGroup": "RG1"
  }
]
admin-33436976 [ ~ ]$
```

2. 자신의 컴퓨터에서 [터미널]을 열고 다음 명령을 실행하여 VM2 가상 머신에 SSH 세션으로 연결합니다. 암호는 "AzurePassw0rd!"를 사용합니다.

```
# VM2 가상 머신에 SSH 세션 연결
ssh azureadmin@<VM2 Public IP>
```

```

azureadmin@VM2: ~
PS C:\Users\JinHwan> # VM2 가상 머신에 SSH 세션 연결
PS C:\Users\JinHwan> ssh azureadmin@20.115.19.235
The authenticity of host '20.115.19.235 (20.115.19.235)' can't be established.
ED25519 key fingerprint is SHA256:WaCiBIfprCBUlyip6SB03bpFXEbTEFx9z7QF2P9h2Fg.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '20.115.19.235' (ED25519) to the list of known hosts.
azureadmin@20.115.19.235's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-1109-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

```

3. [터미널] 창의 SSH 세션에서 다음 명령을 실행하여 Azure CLI 도구를 설치합니다.

```
# Azure CLI 도구 설치
```

```
curl -sL https://aka.ms/InstallAzureCLIDeb | sudo bash
```

```

azureadmin@VM2: ~
azureadmin@VM2:~$ # Azure CLI 도구 설치
azureadmin@VM2:~$ curl -sL https://aka.ms/InstallAzureCLIDeb | sudo bash
Hit:1 http://azure.archive.ubuntu.com/ubuntu bionic InRelease
Get:2 http://azure.archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Get:3 http://azure.archive.ubuntu.com/ubuntu bionic-backports InRelease [83.3 kB]
Get:4 http://azure.archive.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Get:5 http://azure.archive.ubuntu.com/ubuntu bionic/universe amd64 Packages [8570 kB]
Get:6 http://azure.archive.ubuntu.com/ubuntu bionic/universe Translation-en [4941 kB]
Get:7 http://azure.archive.ubuntu.com/ubuntu bionic/multiverse amd64 Packages [151 kB]
Get:8 http://azure.archive.ubuntu.com/ubuntu bionic/multiverse Translation-en [108 kB]
Get:9 http://azure.archive.ubuntu.com/ubuntu bionic-updates/main amd64 Packages [3045 kB]
Get:10 http://azure.archive.ubuntu.com/ubuntu bionic-updates/main Translation-en [553 kB]

```

4. [터미널]의 SSH 세션에서 다음 명령을 실행하여 Azure 포털에 로그인합니다.

```
# Azure 포털에 로그인
```

```
az login
```

```

azureadmin@VM2: ~
azureadmin@VM2:~$ # Azure 포털에 로그인
azureadmin@VM2:~$ az login
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code E6EVNTHWB to authenticate.
[
  {
    "cloudName": "AzureCloud",
    "homeTenantId": "4cfe372a-37a4-44f8-91b2-5faf34253c62",
    "id": "9b419f72-0e80-4d1f-87b5-8342390b4be2",
    "isDefault": true,
    "managedByTenants": [],
    "name": "Challenge Lab--lod48235338",
    "state": "Enabled",
    "tenantId": "4cfe372a-37a4-44f8-91b2-5faf34253c62",
    "user": {
      "name": "Admin-33436976@L0DSPR0DMCA.onmicrosoft.com",
      "type": "user"
    }
  }
]
azureadmin@VM2:~$

```

5. [터미널]의 SSH 세션에서 다음 명령을 실행하여 VM2 가상 머신에서 Key Vault의 비밀에 액세스할 수 있는지 확인합니다.

```
# Key Vault의 비밀 확인
```

```
az keyvault secret show --vault-name mykeyvault<xxxxxxxx> \
--name challenge-secret
```

```
azureadmin@VM2: ~  
azureadmin@VM2:~$ # Key Vault의 비밀 확인  
azureadmin@VM2:~$ az keyvault secret show --vault-name mykeyvault33436976 --name challenge-secret  
{  
  "attributes": {  
    "created": "2023-08-27T08:28:05+00:00",  
    "enabled": true,  
    "expires": null,  
    "notBefore": null,  
    "recoverableDays": 0,  
    "recoveryLevel": "Purgeable",  
    "updated": "2023-08-27T08:28:05+00:00"  
  },  
  "contentType": null,  
  "id": "https://mykeyvault33436976.vault.azure.net/secrets/challenge-secret/d35de5d42beb49e180253c051c9dc117",  
  "kid": null,  
  "managed": null,  
  "name": "challenge-secret",  
  "tags": {},  
  "value": "mykvstring"  
}
```