한국 마이크로소프트

Microsoft Technical Trainer

Enterprise Skills Initiative

AZ-104. Challenge Lab 08

LAB 05. BitLocker와 Key Vault를 사용하여 디스크 암호화

Microsoft

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.

문서 작성 연혁

날짜	버전	작성자	변경 내용
2023.08.30	1.0.0	우진환	LAB 05 내용 작성

목차

도전 과제 **5**

STEP 01. 가상 머신 만들기 5
STEP 02. 가상 머신에 새 데이터 디스크 추가 5
STEP 03. AZURE DISK ENCRYPTION 활성화 5

TASK 01. 가상 머신 만들기 **7**

TASK 02. AZURE 가상 머신에 새 데이터 디스크 추가 **9**

TASK 03. AZURE DISK ENCRYPTION 활성화 **12**

도전 과제

이 실습에서는 Azure 가상 머신에 Azure Disk Encryption을 사용하도록 설정합니다.

- 가상 머신을 만듭니다.
- 가상 머신에 데이터 디스크를 추가합니다.
- Azure Disk Encryption을 사용하도록 설정합니다.

STEP 01. 가상 머신 만들기

1. 다음 속성을 사용하여 새 가상 머신을 만듭니다.

속성	값
리소스 그룹	corp-datalod<XXXXXXXX>
가상 머신 이름	webVM1
이미지	Windows Server 2019 Datacenter – Gen2
크기	Standard_B2ms
사용자 이름	azureAdmin
암호	Pa55w.rd1234
공용 인바운드 포트	선택한 포트 허용
인바운드 포트 선택	RDP (3389)
OS 디스크 유형	표준 HDD
부트 진단	사용 안 함

STEP 02. 가상 머신에 새 데이터 디스크 추가

1. 가상 머신에 다음 속성으로 새 데이터 디스크를 추가합니다.

디스크 이름	스토리지 유형	크기(GiB)	암호화
DataFiles	표준 HDD	128	플랫폼 관리형 키

2. 가상 머신에 RDP로 로그온한 후 서버 관리자를 사용하여 새로 추가한 데이터 디스크를 "`DataFiles`" 이름의 볼륨 레이블로 초기화합니다.

STEP 03. Azure Disk Encryption 활성화

1. 다음 속성을 사용하여 Key Vault를 만듭니다.

속성	값
리소스 그룹	corp-datalod<XXXXXXXX>
주요 자격 증명 모음 이름	KV<XXXXXXXXX>
가격 책정 계층	표준
볼륨 암호화를 위한 Azure Disk Encryption	선택

2. 다음과 같은 정보를 사용하여 Cloud Shell을 만들고 PowerShell 세션을 엽니다.

속성	값
리소스 그룹	corp-datalod<XXXXXXXX>
스토리지 계정	cs<XXXXXXXX>
파일 공유	cloudshell

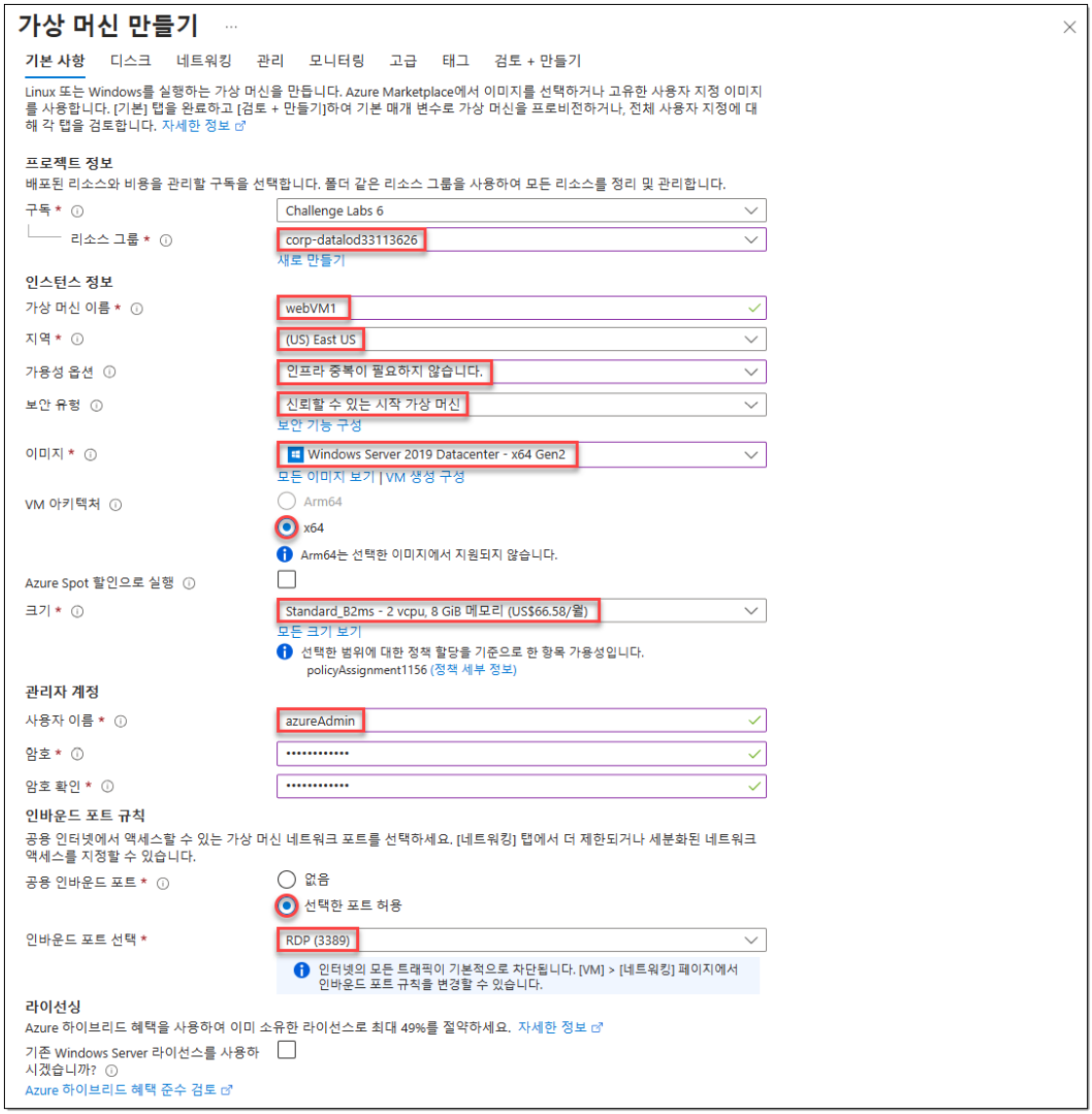
3. Cloud Shell에서 `Get-AzKeyVault` 명령을 사용하여 새로 만든 Key Vault를 확인합니다.
4. Cloud Shell에서 `Set-AzVMDiskEncryptionExtension` 명령을 사용하여 `webVM1`에 대한 Azure Disk Encryption을 활성화합니다.
5. Cloud Shell에서 `Get-AzVmDiskEncryptionStatus` 명령을 사용하여 디스크 암호화 상태를 확인합니다.
6. Azure 포털에서 `webVM1` 가상 머신의 데이터 디스크가 "`PMK 및 ADE를 사용하는 SSE`"로 표시되는지 확인합니다.

TASK 01. 가상 머신 만들기

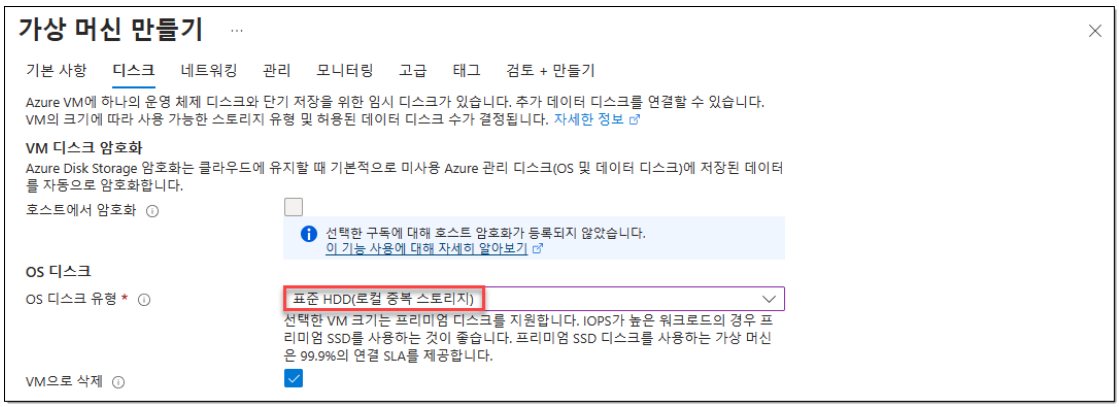
Azure 디스크 스토리지의 SSE (Server-side Encryption)는 기본적으로 사용하도록 설정되어 있으며 PMK (Platform-managed Key)를 사용하여 스토리지 서버 수준에서 디스크를 암호화합니다. 암호화 키는 플랫폼에서 자동으로 관리되며 Azure에서 키를 보호하고 정기적으로 교체합니다. CMK (Customer-managed Key)로 Server-side Encryption을 사용하여 규정 준수를 위해 암호화 키를 수동으로 관리할 수 있습니다. ADE (Azure Disk Encryption)는 운영 체제 수준에서 BitLocker (Windows) 또는 DM-Crypt (Linux)와 같은 기술을 사용하여 암호화를 적용합니다. ADE (Azure Disk Encryption)와 Server-side Encryption를 결합하여 미사용 데이터(at-rest)에 대한 높은 보안 요구 사항을 구성할 수 있습니다.

1. Azure 포털의 검색창에서 "가상 머신"을 검색한 후 클릭합니다. [가상 머신] 블레이드의 메뉴에서 [만들기 - Azure 가상 머신]을 클릭합니다.

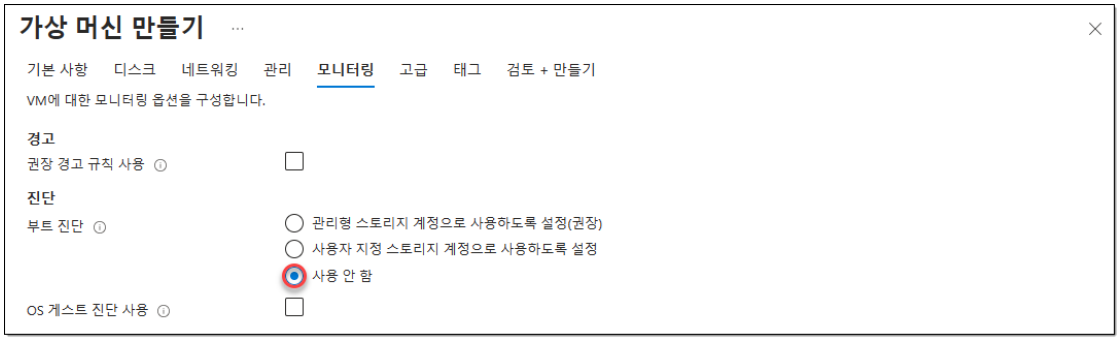
2. [가상 머신 만들기] 블레이드의 [기본 사항] 탭에서 아래와 같이 구성한 후 [다음]을 클릭합니다.
   - [프로젝트 정보 - 리소스 그룹]: `corp-datalod<XXXXXXXX>`
   - [인스턴스 정보 - 가상 머신 이름]: webVM1
   - [인스턴스 정보 - 지역]: (US) East US
   - [인스턴스 정보 - 가용성 옵션]: 인프라 중복이 필요하지 않습니다.
   - [인스턴스 정보 - 보안 유형]: 신뢰할 수 있는 시작 가상 머신
   - [인스턴스 정보 - 이미지]: Windows Server 2019 Datacenter - x64 Gen2
   - [인스턴스 정보 - VM 아키텍처]: x64
   - [인스턴스 정보 - Azure Spot 할인으로 실행]: 선택하지 않습니다.
   - [인스턴스 정보 - 크기]: Standard_B2ms
   - [관리자 계정 - 사용자 이름]: azureAdmin
   - [관리자 계정 - 암호]: Pa55w.rd1234
   - [인바운드 포트 규칙 - 공용 인바운드 포트]: 선택한 포트 허용
   - [인바운드 포트 규칙 - 인바운드 포트 선택]: RDP (3389)
   - [라이선싱 - 기존 Windows Server 라이선스를 사용하시겠습니까?]: 선택하지 않습니다.



3. [디스크] 탭에서 OS 디스크 유형을 "표준 HDD(로컬 중복 스토리지)"로 선택한 후 [모니터링] 탭을 클릭합니다.



4. [모니터링] 탭에서 부트 진단을 "사용 안 함"으로 설정한 후 [검토 + 만들기]를 클릭합니다. [검토 + 만들기] 탭에서 [만들기]를 클릭합니다.

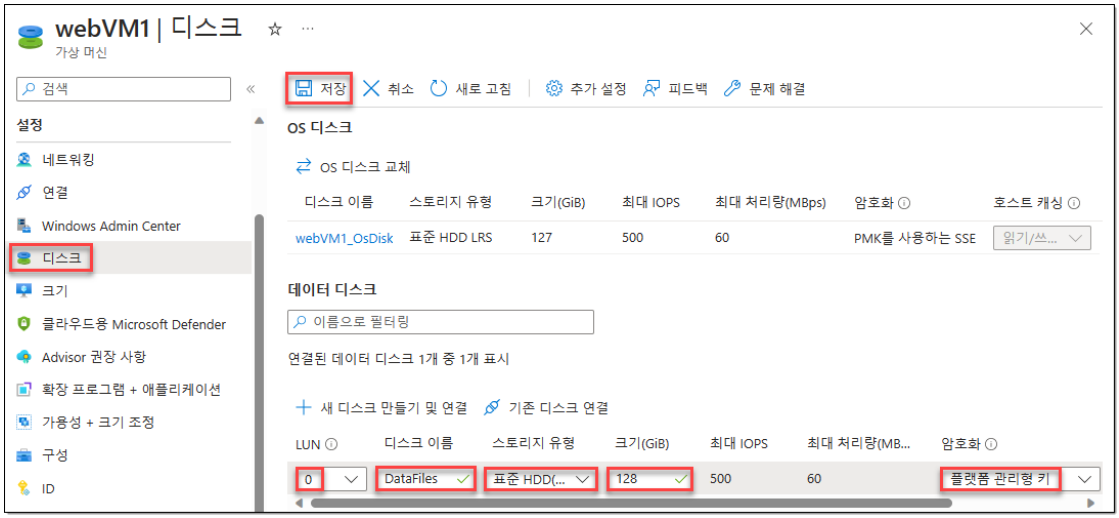


5. 새로 만든 [webVM1 가상 머신] 블레이드의 [설정 - 디스크]로 이동합니다. OS 디스크가 PMK를 사용하는 SSE로 암호화된 것을 확인할 수 있습니다. 또한 데이터 디스크는 하나도 추가되어 있지 않은 것을 확인할 수 있습니다.

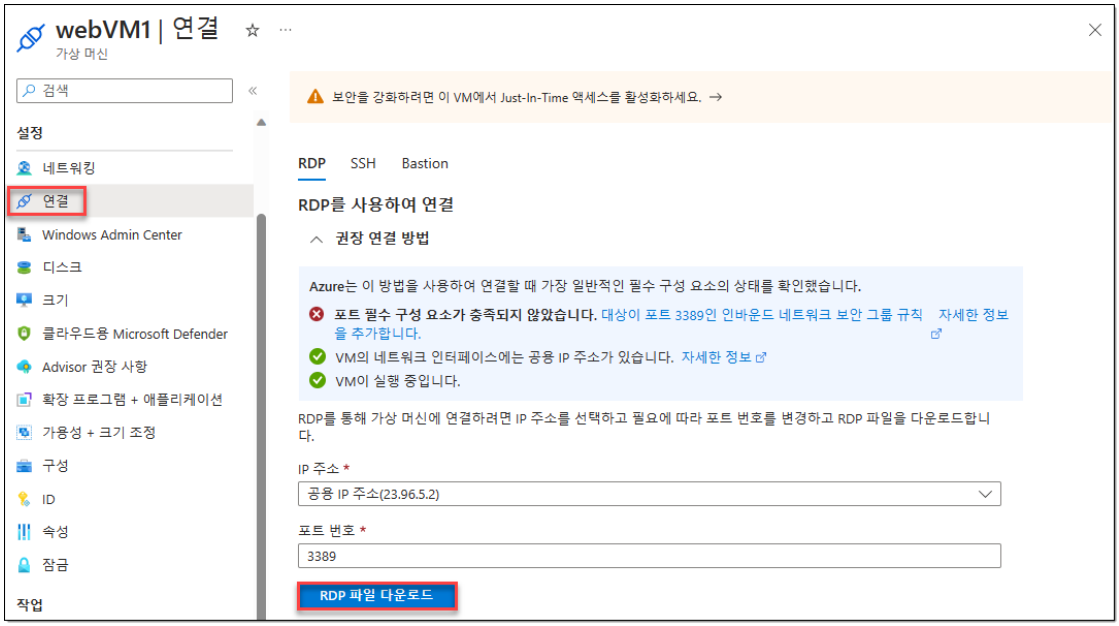
TASK 02. Azure 가상 머신에 새 데이터 디스크 추가

1. [webVM1 가상 머신] 블레이드의 [설정 - 디스크]로 이동합니다. "데이터 디스크" 영역에서 [새 디스크 만들기 및 연결]을 클릭합니다. 디스크 추가에서 다음과 같이 구성한 후 [저장]을 클릭합니다.

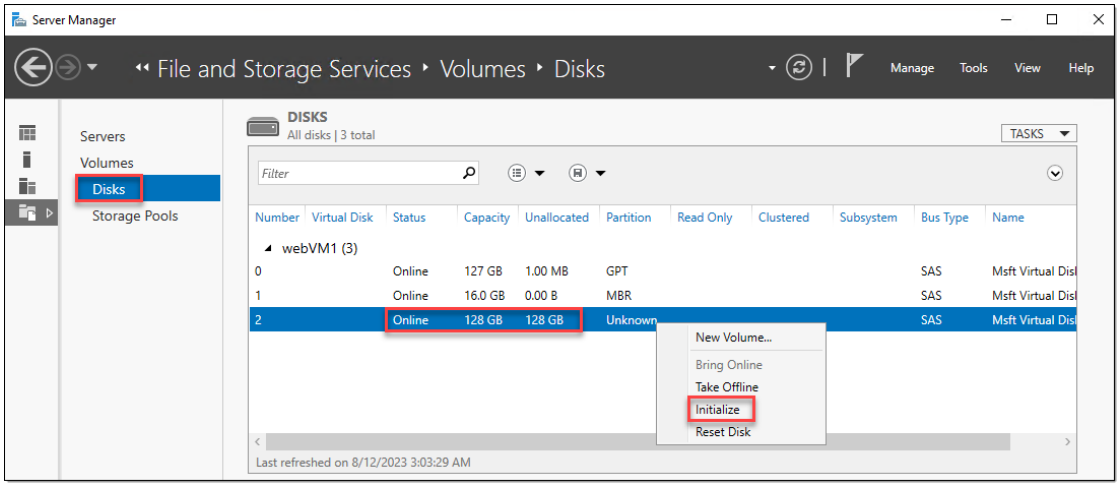
디스크 이름	스토리지 유형	크기(GiB)	암호화
DataFiles	표준 HDD	128	플랫폼 관리형 키



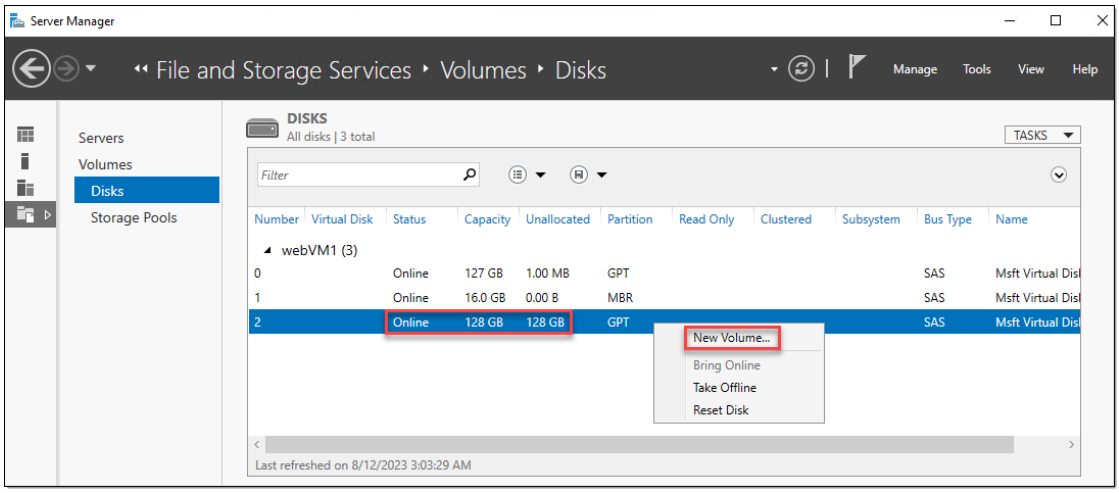
2. [webVM1 가상 머신] 블레이드의 [설정 - 연결]로 이동한 후 [RDP 파일 다운로드]를 클릭합니다. 다운로드한 RDP 파일을 실행한 후 사용자 이름(azureAdmin)과 암호(Pa55w.rd1234)를 사용하여 로그온합니다.



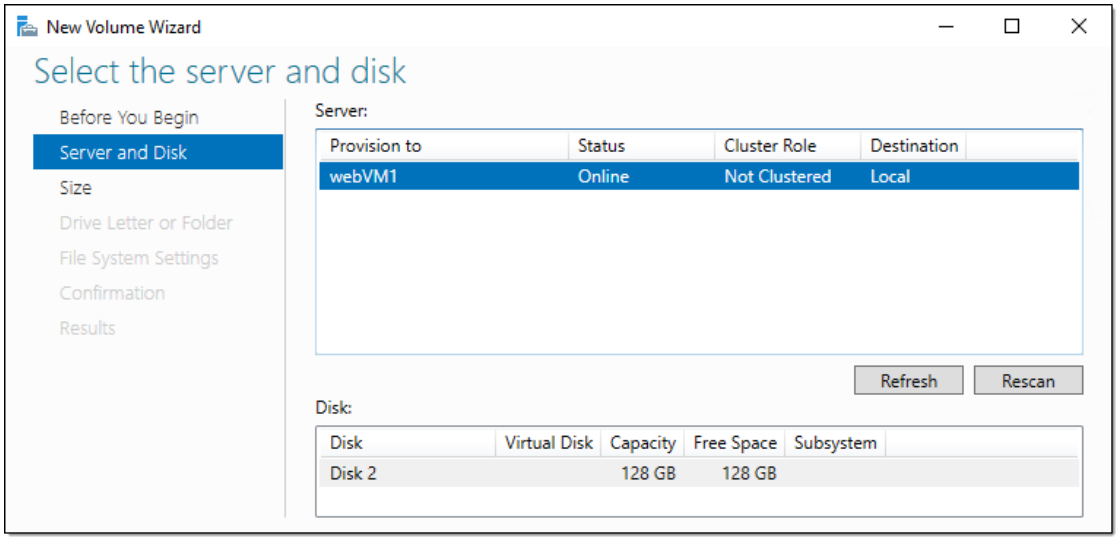
3. webVM1 가상 머신의 [Server Manager]에서 [File and Storage Services - Volumes - Disks]로 이동합니다. 새로 추가한 데이터 디스크를 마우스 우 클릭한 후 [Initialize]를 클릭합니다.



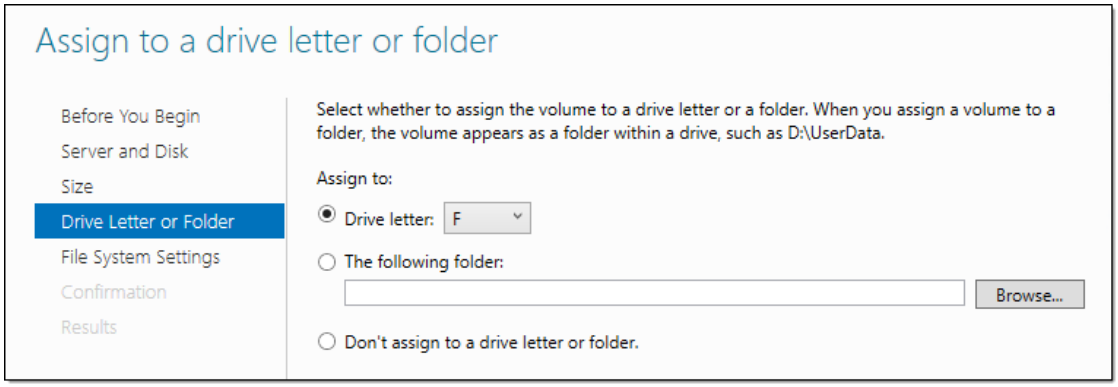
4. 초기화된 디스크를 마우스 우 클릭한 후 [New Volume...]을 클릭합니다.



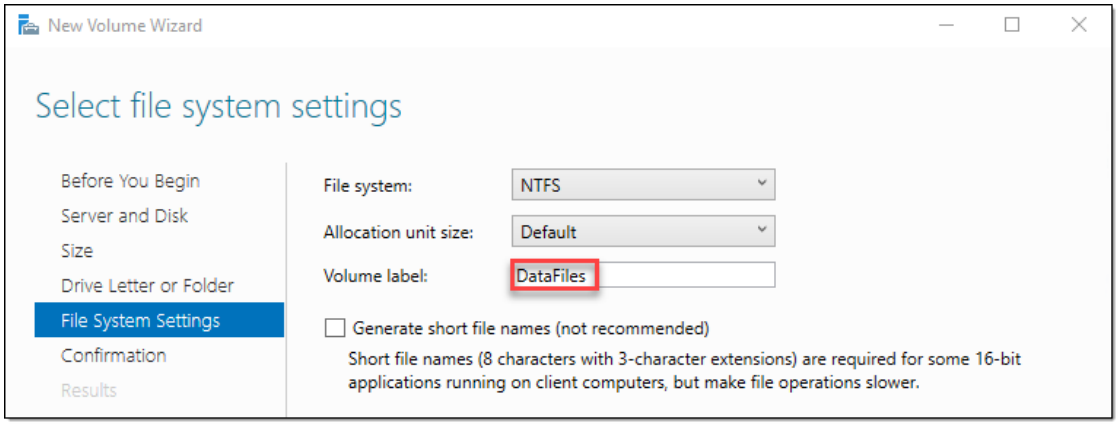
5. [New Volume Wizard] 창의 [Before you begin] 페이지에서 [Next]를 클릭합니다. [Select the server and disk] 페이지에서 [Next]를 클릭합니다.



6. [Specify the size of the volume] 페이지에서 128GB 크기를 선택하고 [Next]를 클릭합니다. [Assign to a driver letter or folder] 페이지에서 F 드라이브를 선택하고 [Next]를 클릭합니다.



7. [Select file system settings] 페이지에서 다른 설정은 기본값으로 유지하고 볼륨 레이블은 "`DataFiles`"를 입력한 후 [Next]를 클릭합니다. [Confirm selections] 페이지에서 [Create]를 클릭합니다.

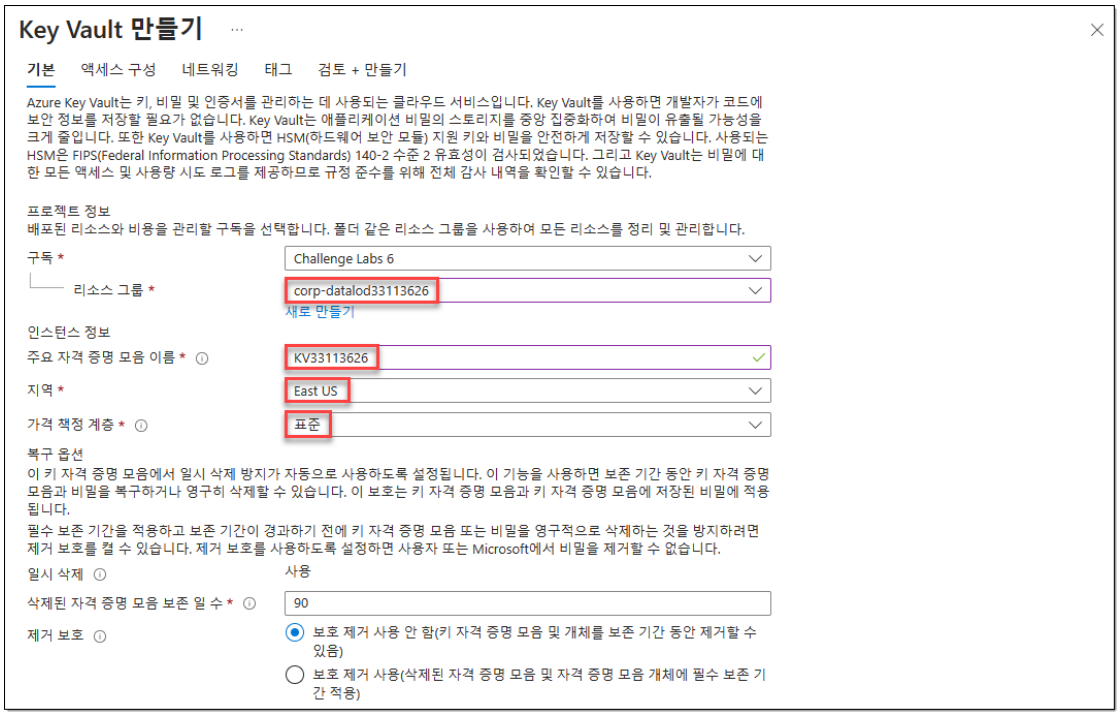


TASK 03. Azure Disk Encryption 활성화

1. Azure 포털의 검색창에서 "`키 자격 증명 모음`"을 검색한 후 클릭합니다. [키 자격 증명 모음] 블레이드에서 [만들기]를 클릭합니다.

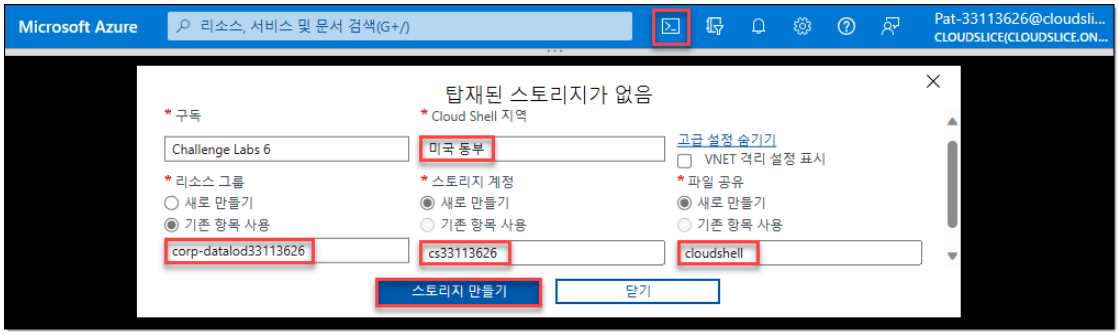
2. [Key Vault 만들기] 블레이드의 [기본] 탭에서 아래와 같이 구성한 후 [다음]을 클릭합니다.
   - [프로젝트 정보 - 리소스 그룹]: `corp-datalod<XXXXXXXX>`
   - [인스턴스 정보 - 주요 자격 증명 모음 이름]: "`KV<XXXXXXXX>`" 이름을 입력합니다.
   - [인스턴스 정보 - 지역]: East US
   - [인스턴스 정보 - 가격 책정 계층]: 표준

- 다른 옵션은 기본 설정을 사용합니다.



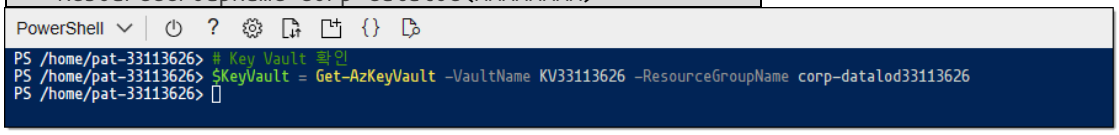
3. [액세스 구성] 탭에서 "볼륨 암호화를 위한 Azure Disk Encryption" 옵션을 체크하고 [검토 + 만들기]를 클릭합니다. [검토 + 만들기] 탭에서 [만들기]를 클릭합니다.

4. Azure 포털의 우측 상단에서 [Cloud Shell] 아이콘을 클릭한 후 "PowerShell"을 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>" 이름을 입력합니다.
   - 파일 공유: cloudshell



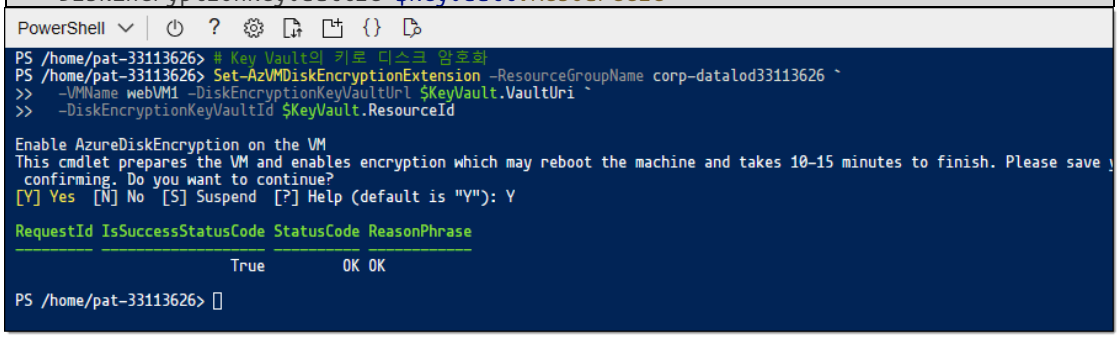
5. [Cloud Shell]의 PowerShell 세션에서 다음 명령을 실행하여 배포한 Key Vault를 변수로 저장합니다.

```
# Key Vault 확인
$KeyVault = Get-AzKeyVault -VaultName KV<XXXXXXXX> `
  -ResourceGroupName corp-datalod<XXXXXXXX>
```



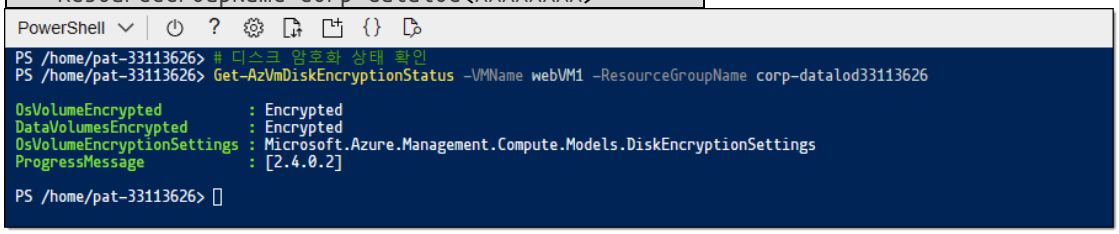
6. [Cloud Shell]의 PowerShell 세션에서 다음 명령을 실행하여 KeyVault의 키로 디스크 암호화를 진행합니다.

```
# Key Vault의 키로 디스크 암호화
Set-AzVMDiskEncryptionExtension -ResourceGroupName corp-datalod<XXXXXXXX> `
  -VMName webVM1 -DiskEncryptionKeyVaultUrl $KeyVault.VaultUri `
  -DiskEncryptionKeyVaultId $KeyVault.ResourceId
```



7. [Cloud Shell]의 PowerShell 세션에서 다음 명령을 실행하여 디스크 암호화 상태를 확인합니다.

```
# 디스크 암호화 상태 확인
Get-AzVmDiskEncryptionStatus -VMName webVM1 `
  -ResourceGroupName corp-datalod<XXXXXXXX>
```



8. [`webVM1` 가상 머신] 블레이드의 [설정 - 디스크]로 이동합니다. OS 디스크와 데이터 디스크의 암호화가 모두 "`PMK 및 ADE를 사용하는 SSE`"로 구성된 것을 확인합니다.


webVM1 | 디스크
가상 머신
검색
설정
네트워킹
연결
Windows Admin Center
디스크
크기
클라우드용 Microsoft Defender
Advisor 권장 사항
확장 프로그램 + 애플리케이션
가용성 + 크기 조정
구성
ID
저장
취소
새로 고침
추가 설정
피드백
문제 해결
OS 디스크
OS 디스크 교체
디스크 이름
스토리지 ...
크기(...
최대 IO...
최대 처리...
암호화
호스트 캐싱
webVM1_OsDisk_1
표준 HDD LRS
127
500
60
PMK 및 ADE를 사용하는 SSE
읽기/...
데이터 디스크
이름으로 필터링
연결된 데이터 디스크 1개 중 1개 표시
새 디스크 만들기 및 연결
기존 디스크 연결
LUN
디스크 ...
스토리지 ...
크기(G...
최대 I...
최...
암호화
호스트 캐싱
0
DataFiles
표준 HDD L...
128
500
60
PMK 및 ADE를 사용하는 SSE
없음