

AZ-104. Challenge Lab 08

## **LAB 05. BitLocker와 Key Vault를 사용하여 디스크 암호화**

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
2023.08.30	1.0.0	우진환	LAB 05 내용 작성

## 목차

<b>도전 과제</b> .....	<b>5</b>
STEP 01. 가상 머신 만들기 .....	5
STEP 02. 가상 머신에 새 데이터 디스크 추가.....	5
STEP 03. AZURE DISK ENCRYPTION 활성화.....	5
<b>TASK 01. 가상 머신 만들기</b> .....	<b>7</b>
<b>TASK 02. AZURE 가상 머신에 새 데이터 디스크 추가</b> .....	<b>9</b>
<b>TASK 03. AZURE DISK ENCRYPTION 활성화</b> .....	<b>12</b>

## 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

- 다음 속성을 사용하여 새 가상 머신을 만듭니다.

속성	값
리소스 그룹	corp-datalod<XXXXXXXXXX>
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

- 가상 머신에 다음 속성으로 새 데이터 디스크를 추가합니다.

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

- 가상 머신에 RDP로 로그인한 후 서버 관리자를 사용하여 새로 추가한 데이터 디스크를 "DataFiles" 이름의 볼륨 레이블로 초기화합니다.

### STEP 03. Azure Disk Encryption 활성화

- 다음 속성을 사용하여 Key Vault를 만듭니다.

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

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

속성	값
리소스 그룹	corp-datalod<XXXXXXXXXX>
스토리지 계정	cs<XXXXXXXXXX>
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.



### 가상 머신 만들기

기본 사항 디스크 네트워킹 관리 모니터링 고급 태그 검토 + 만들기

Linux 또는 Windows를 실행하는 가상 머신을 만듭니다. Azure Marketplace에서 이미지를 선택하거나 고유한 사용자 지정 이미지를 사용합니다. [기본] 탭을 완료하고 [검토 + 만들기]하여 기본 매개 변수로 가상 머신을 프로비전하거나, 전체 사용자 지정에 대해 각 탭을 검토합니다. [자세한 정보](#)

**프로젝트 정보**  
 배포된 리소스와 비용을 관리할 구독을 선택합니다. 폴더 같은 리소스 그룹을 사용하여 모든 리소스를 정리 및 관리합니다.

구독 \*

리소스 그룹 \*   
[새로 만들기](#)

**인스턴스 정보**

가상 머신 이름 \*

지역 \*

가용성 옵션

보안 유형   
[보안 기능 구성](#)

이미지 \*   
[모든 이미지 보기](#) | [VM 설정 구성](#)

VM 아키텍처 ☐ Arm64 ☒ x64  
 Arm64는 선택한 이미지에서 지원되지 않습니다.

Azure Spot 할인으로 실행 ☐

크기 \*   
[모든 크기 보기](#)  
 선택한 범위에 대한 정책 할당을 기준으로 한 항목 가용성입니다.  
 policyAssignment1156 ([정책 세부 정보](#))

**관리자 계정**

사용자 이름 \*

암호 \*

암호 확인 \*

**인바운드 포트 규칙**  
 공용 인터넷에서 액세스할 수 있는 가상 머신 네트워크 포트를 선택하세요. [네트워킹] 탭에서 더 제한되거나 세분화된 네트워크 액세스를 지정할 수 있습니다.

공용 인바운드 포트 \* ☐ 없음 ☒ 선택한 포트 허용

인바운드 포트 선택 \*   
 인터넷의 모든 트래픽이 기본적으로 차단됩니다. [VM] > [네트워킹] 페이지에서 인바운드 포트 규칙을 변경할 수 있습니다.

**라이선싱**  
 Azure 하이브리드 혜택을 사용하여 이미 소유한 라이선스로 최대 49%를 절약하세요. [자세한 정보](#)

기존 Windows Server 라이선스를 사용하 시겠습니까? ☐

[Azure 하이브리드 혜택 준수 검토](#)

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

### 가상 머신 만들기

기본 사항 디스크 네트워킹 관리 모니터링 고급 태그 검토 + 만들기

Azure VM에 하나의 운영 체제 디스크와 단기 저장을 위한 임시 디스크가 있습니다. 추가 데이터 디스크를 연결할 수 있습니다. VM의 크기에 따라 사용 가능한 스토리지 유형 및 허용된 데이터 디스크 수가 결정됩니다. [자세한 정보](#)

**VM 디스크 암호화**  
 Azure Disk Storage 암호화는 클라우드에 유지할 때 기본적으로 미사용 Azure 관리 디스크(OS 및 데이터 디스크)에 저장된 데이터를 자동으로 암호화합니다.

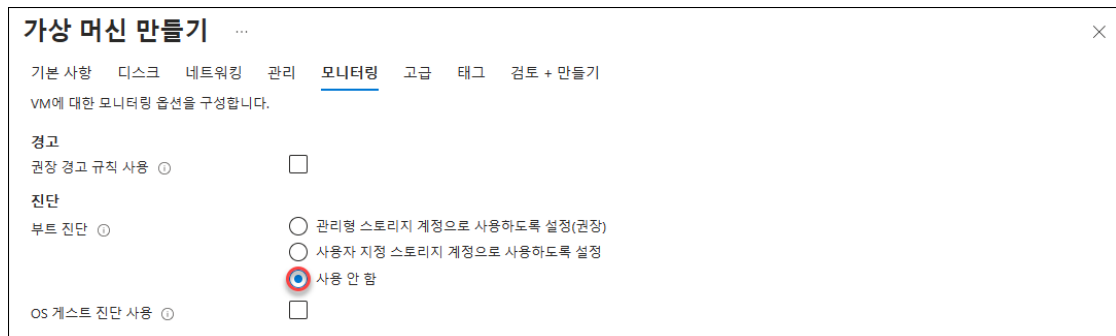
호스트에서 암호화 ☐  
 선택한 구독에 대해 호스트 암호화가 등록되지 않았습니다.  
[이 기능 사용에 대해 자세히 알아보기](#)

**OS 디스크**

OS 디스크 유형 \*   
 선택한 VM 크기는 프리미엄 디스크를 지원하지 않습니다. IOPS가 높은 워크로드의 경우 프리미엄 SSD를 사용하는 것이 좋습니다. 프리미엄 SSD 디스크를 사용하는 가상 머신은 99.9%의 연결 SLA를 제공합니다.

VM으로 삭제 ☒

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.



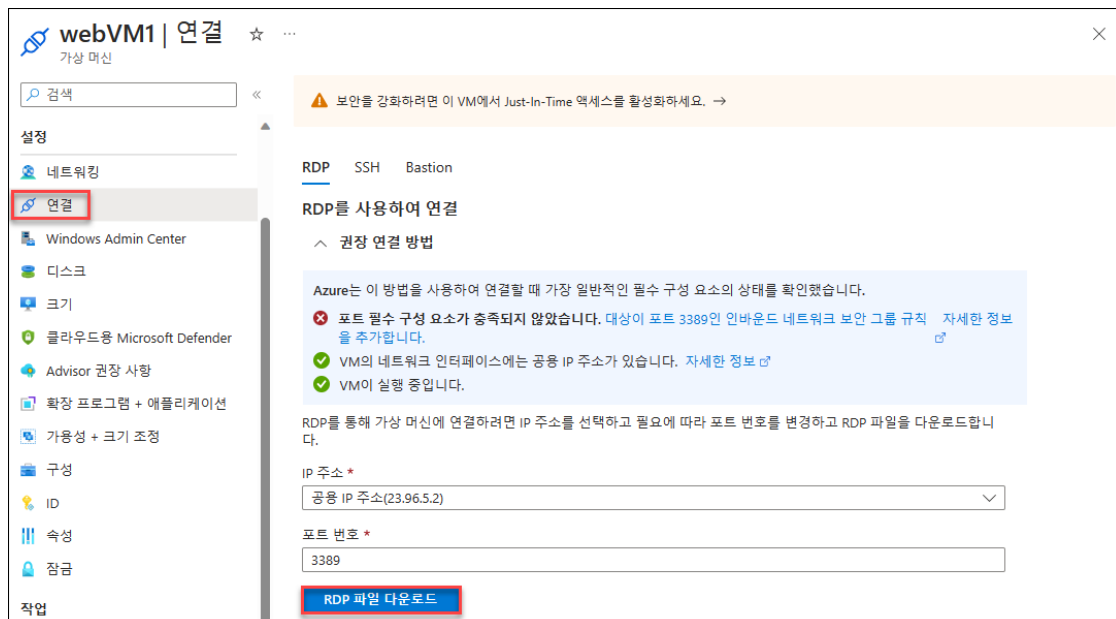
## TASK 02. Azure 가상 머신에 새 데이터 디스크 추가

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.

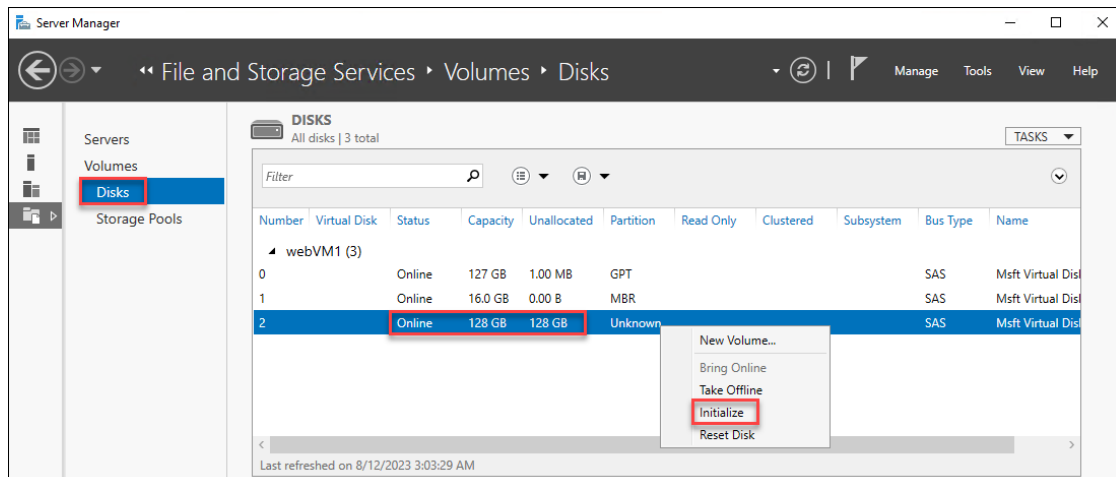
디스크 이름	스토리지 유형	크기(GiB)	암호화
DataFiles	표준 HDD	128	플랫폼 관리형 키



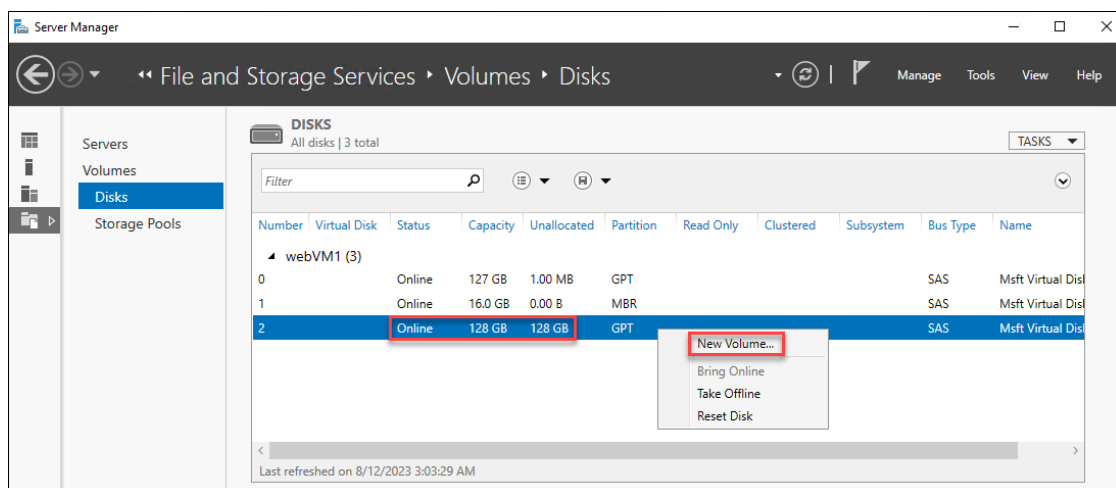
2. [webVM1 가상 머신] 블레이드의 [설정 - 연결]로 이동한 후 [RDP 파일 다운로드]를 클릭합니다.  
다운로드한 RDP 파일을 실행한 후 사용자 이름(azureAdmin)과 암호(Pa55w.rd1234)를 사용하여 로그인합니다.



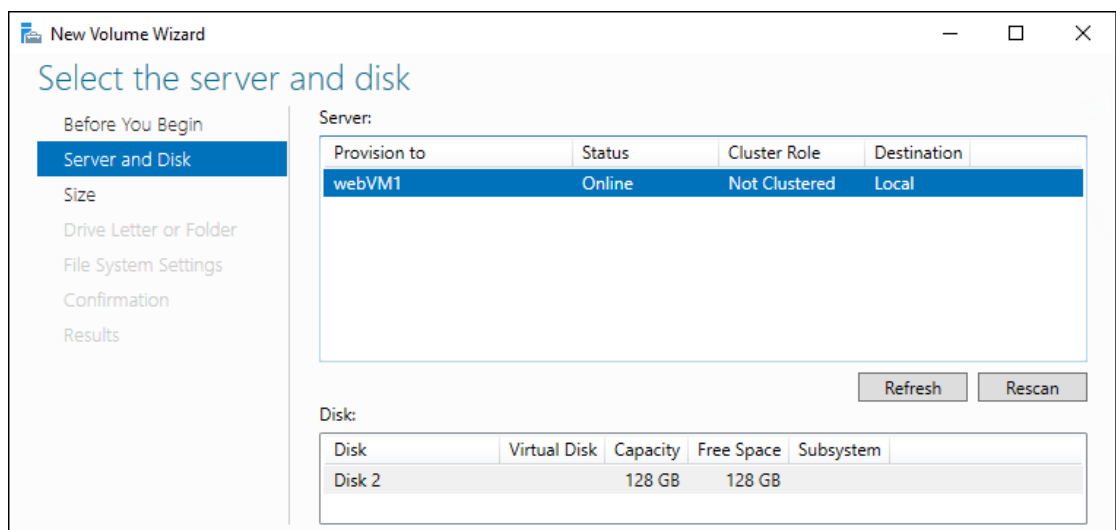
3. webVM1 가상 머신의 [Server Manager]에서 [File and Storage Services - Volumes - Disks]로 이동합니다. 새로 추가한 데이터 디스크를 마우스 우 클릭한 후 [Initialize]를 클릭합니다.



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.

**Key Vault 만들기** ...

기본 액세스 구성 네트워킹 태그 검토 + 만들기

Azure Key Vault는 키, 비밀 및 인증서를 관리하는 데 사용되는 클라우드 서비스입니다. Key Vault를 사용하면 개발자가 코드에 보안 정보를 저장할 필요가 없습니다. Key Vault는 애플리케이션 비밀의 스토리지를 중앙 집중화하여 비밀이 유출될 가능성을 크게 줄입니다. 또한 Key Vault를 사용하면 HSM(하드웨어 보안 모듈) 지원 키와 비밀을 안전하게 저장할 수 있습니다. 사용되는 HSM은 FIPS(Federal Information Processing Standards) 140-2 수준 2 유효성이 검사되었습니다. 그리고 Key Vault는 비밀에 대한 모든 액세스 및 사용량 시도 로그를 제공하므로 규정 준수를 위해 전체 감사 내역을 확인할 수 있습니다.

**프로젝트 정보**  
배포된 리소스와 비용을 관리할 구독을 선택합니다. 폴더 같은 리소스 그룹을 사용하여 모든 리소스를 정리 및 관리합니다.

구독 \* Challenge Labs 6

리소스 그룹 \* corp-datalod33113626  
[새로 만들기](#)

**인스턴스 정보**

주요 자격 증명 모음 이름 \* KV33113626 ✓

지역 \* East US

가격 책정 계층 \* 표준

**복구 옵션**  
이 키 자격 증명 모음에서 일시 삭제 방식이 자동으로 사용하도록 설정됩니다. 이 기능을 사용하면 보존 기간 동안 키 자격 증명 모음과 비밀을 복구하거나 영구히 삭제할 수 있습니다. 이 보호는 키 자격 증명 모음과 키 자격 증명 모음에 저장된 비밀에 적용됩니다.  
필수 보존 기간을 적용하고 보존 기간이 경과하기 전에 키 자격 증명 모음 또는 비밀을 영구적으로 삭제하는 것을 방지하려면 제거 보호를 켜 수 있습니다. 제거 보호를 사용하도록 설정하면 사용자 또는 Microsoft에서 비밀을 제거할 수 없습니다.

일시 삭제 ① 사용

삭제된 자격 증명 모음 보존 일 수 \* 90

제거 보호 ① ☒ 보호 제거 사용 안 함(키 자격 증명 모음 및 개체를 보존 기간 동안 제거할 수 있음)  
☐ 보호 제거 사용(삭제된 자격 증명 모음 및 자격 증명 모음 개체에 필수 보존 기간 적용)

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

**Key Vault 만들기** ...

기본 액세스 구성 네트워킹 태그 검토 + 만들기

이 키 자격 증명 모음에 대한 데이터 평면 액세스 구성  
데이터 평면에서 키 자격 증명 모음에 액세스하려면 모든 호출자(사용자 또는 애플리케이션)에 적절한 인증 및 권한 부여가 있어야 합니다. 인증은 호출자의 ID를 설정합니다. 권한 부여는 호출자가 실행할 수 있는 작업을 결정합니다. [자세히 알아보기](#)

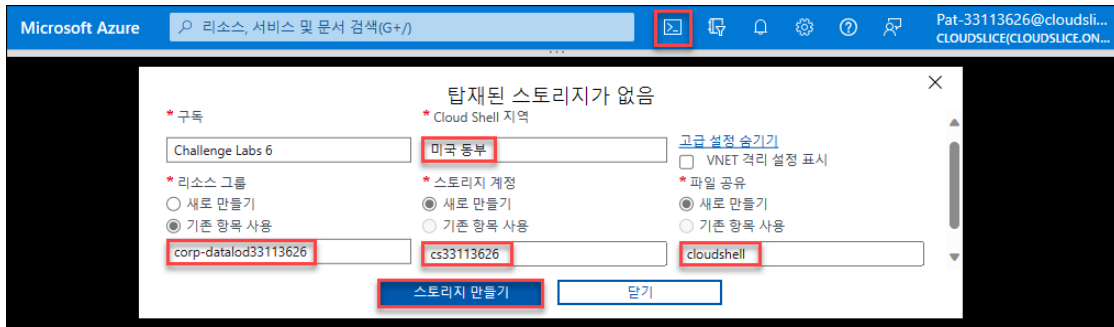
**권한 모델**  
다음을 사용하여 데이터 평면 액세스 권한 부여 [Azure RBAC or Key Vault 액세스 정책](#)

☒ Azure 역할 기반 액세스 제어(권장) ①  
☐ 자격 증명 모음 액세스 정책 ①

**리소스 액세스**

☐ 배포를 위한 Azure Virtual Machines ①  
☐ 템플릿 배포를 위한 Azure Resource Manager ①  
☒ 볼륨 암호화를 위한 Azure Disk Encryption ①

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>

PowerShell
PS /home/pat-33113626> # Key Vault 확인
PS /home/pat-33113626> $KeyVault = Get-AzKeyVault -VaultName KV33113626 -ResourceGroupName corp-datalod33113626
PS /home/pat-33113626>
```

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

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

PowerShell
PS /home/pat-33113626> # Key Vault의 키로 디스크 암호화
PS /home/pat-33113626> Set-AzVMDisksEncryptionExtension -ResourceGroupName corp-datalod33113626 -VMName webVM1 -DiskEncryptionKeyVaultUrl $KeyVault.VaultUri -DiskEncryptionKeyVaultId $KeyVault.ResourceId

Enable AzureDiskEncryption on the VM. This cmdlet prepares the VM and enables encryption which may reboot the machine and takes 10-15 minutes to finish. Please save your work before confirming. Do you want to continue?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

RequestId IsSuccess StatusCode ReasonPhrase
-----
True OK OK

PS /home/pat-33113626>
```

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>

PowerShell
PS /home/pat-33113626> # 디스크 암호화 상태 확인
PS /home/pat-33113626> Get-AzVmDiskEncryptionStatus -VMName webVM1 -ResourceGroupName corp-datalod33113626

OsVolumeEncrypted : Encrypted
DataVolumesEncrypted : Encrypted
OsVolumeEncryptionSettings : Microsoft.Azure.Management.Compute.Models.DiskEncryptionSettings
ProgressMessage : [2.4.0.2]

PS /home/pat-33113626>
```

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

